Für einen Opferschutz ohne Massenüberwachung

Eine Erwiderung auf Joachim Herrmann

Erik Tuchtfeld

08.10.2024 doi: 10.59704/99adae7eb0e2aecd

Die Vorratsdatenspeicherung erlebt einen neuen Höhenflug: Der Bundesrat hat auf Initiative (des schwarz/rot regierten) Hessens den Bundestag aufgefordert, eine einmonatige Speicherung von IP-Adressen einzuführen, Nordrhein-Westfalen, Schleswig-Holstein und Baden-Württemberg (die schwarz/grünen Koalitionen der Bundesrepublik) unterstützen eine ähnliche Initiative und auch hier auf dem Verfassungsblog fordert der bayrische (CSU-)Innenminister Joachim Herrmann „Mehr Opferschutz durch Vorratsdatenspeicherung“. In der aktuellen Blütezeit der Sicherheitspakete lässt sich nun also auch eine „ganz große Koalition“ für eine Speicherpflicht von IP-Adressen beobachten.

Herrmann argumentiert, in der Sache stellvertretend für die Koalition der Speicherwilligen, dass die veränderte Sicherheitslage in Deutschland und Europa Verfassungsgerichte dazu zwinge, die Verhältnismäßigkeitsmaßstäbe vergangener Entscheidungen neu zu überdenken und insbesondere die Einführung der Vorratsdatenspeicherung zu ermöglichen. Er zeichnet dabei ein dystopisches Bild der Lage in Deutschland, die von Hass und Gewalt geprägt sei. Was er und seine politischen Mitstreiter:innen dabei übersehen: Die digitalen Ermittlungsmöglichkeiten der Strafverfolgungsbehörden waren noch nie besser, die digitalen Datentöpfe, die ausgewertet werden können, nie größer.

Die unendliche Geschichte der Vorratsdatenspeicherung

Seit rund 20 Jahren ist die Vorratsdatenspeicherung zur Bekämpfung von Straftaten mit Internetbezug ein politischer und juristischer Dauerbrenner. Das Bundesverfassungsgericht und der Europäische Gerichtshof (EuGH) haben inzwischen in (mindestens) acht verschiedenen Urteilen Stellung bezogen zur Zulässigkeit und Ausgestaltung einer präventiven Speicherpflicht von Metadaten (wie Rufnummern und Zeitpunkte von Telefonaten, den Anschlussinhaber hinter einer IP-Adresse und Standortdaten der Mobilfunktelefone, siehe Art. 5 der Vorratsdatenspeicherungsrichtlinie von 2006). Wenig überzeugend ist der Vorwurf Herrmanns, dass „Vorratsdatenspeicherung“ eine „irreführende Begriffsbildung“ eines bestimmten „politischen Lagers“ darstelle. Die 2014 vom EuGH aufgehobene europäische Richtlinie trug den Titel „Richtlinie [...] über die Vorratsspeicherung von Daten [...]“, der Vorwurf kann sich folglich im Grunde nur selbstkritisch an die damalige (konservative) Mehrheit in Rat und Parlament richten, die die Richtlinie mit diesem Namen beschlossen hat.

Seit nunmehr fast zwei Dekaden ist die Vorratsdatenspeicherung Teil intensiver politischer und rechtswissenschaftlicher Auseinandersetzungen. In Deutschland wurde sie 2007 eingeführt, unmittelbar durch eine einstweilige Anordnung des Bundesverfassungsgerichts eingeschränkt, 2010 für verfassungswidrig erklärt, 2015 erneut – in abgewandelter Form – vom Bundestag beschlossen, 2017 vom OVG Münster für unionsrechtswidrig und deshalb nicht anwendbar erklärt, eine Einschätzung die der EuGH schließlich 2022 bestätigte. Der Koalitionsvertrag der Ampel-Regierung sieht vor, dass Regelungen zur Vorratsdatenspeicherung so ausgestaltet werden, dass sie „rechtssicher anlassbezogen und durch richterlichen Beschluss gespeichert werden können“. Während Justizminister Buschmann diese Vereinbarung als Auftrag zur Umsetzung des Quick Freeze-Konzepts versteht (bei dem Metadaten nur anlassbezogen nach einer Straftat „eingefroren“ werden), fordert Innenministerin Faeser – unbeeindruckt vom Koalitionsvertrag

und nun im Einklang mit der Opposition und dem Bundesrat – die Einführung einer anlasslosen IP-Vorratsdatenspeicherung. Die knapp 20 Jahre alte Geschichte der Vorratsdatenspeicherung in Deutschland ist durchaus verwirrend und von vielen Einigungen, Aufkündigungen von Einigungen, Urteilen und zivilgesellschaftlichen Protesten geprägt.

Die Sache mit der Anonymität im Internet

Die Vorratsdatenspeicherung ist also umkämpft wie kaum ein anderes Instrument der deutschen Innenpolitik. Die aktuellen Forderungen beschränken sich auf die Einführung einer IP-Vorratsdatenspeicherung. Hierbei geht es – anders als bspw. bei der Speicherung von Standortdaten und Zeitpunkten sowie Teilnehmenden von Telefonaten – nicht um die Möglichkeit der nachträglichen Erforschung des Lebens eines *bekannten* Tatverdächtigen, sondern um die Identifikation eines *unbekannten* Tatverdächtigen, konkret um den jeweiligen Anschlussinhaber. Es ist also primär ein Werkzeug der Deanonymisierung, nicht der umfassenden Profilbildung. Dementsprechend hat das Bundesverfassungsgericht bereits in seiner Entscheidung aus 2010 (Rn. 254-263) sowie der EuGH seit 2020 (Rn. 152-159) betont, dass die Anforderungen an IP-Vorratsdatenspeicherung geringer sind als an die Speicherung anderer Metadaten.

Es bleibt jedoch dabei, wie Kritiker:innen immer wieder an verschiedenen Stellen betonen, dass die anlasslose Vorratsdatenspeicherung Bürger:innen unter Generalverdacht stellt. Anonymität wird als Gefahr verstanden, deren primäre Funktion die eines Deckmantels für die Begehung von Straftaten ist. Folglich werden auch Bürger:innen zunächst einmal als mögliche Täter:innen gesehen, die Grundrechtseingriffe hinnehmen müssen, um zu dem Zeitpunkt, in dem sich der Verdacht realisiert und eine Straftat begangen wird, identifizierbar zu sein. Die Möglichkeit der Identifizierung ist kein Nebenprodukt anderer Datenverarbeitungen – wie bei der Speicherung von IP-Adressen zu Abrechnungszwecken oder zur Störungsbekämpfung –, sondern alleiniges Ziel des staatlichen Speicherbefehls. Übersehen wird dabei, dass Anonymität – im virtuellen wie im physischen Raum – eine Voraussetzung von Freiheit ist. Schon das bloße Vorhandensein von Überwachung erhöht den Konformitätsdruck und führt zu *chilling effects* für die Ausübung von grundrechtlich geschützten Freiheiten, also unter anderem dazu, dass Bürger:innen von (vermeintlich) kontroversen Äußerungen abgeschreckt werden.

Die Kontextabhängigkeit grundrechtlicher Urteile

Herrmann hat recht, wenn er die Kontextabhängigkeit der rechtlichen Bewertung von Grundrechtseingriffen betont. So ist es beispielsweise denkbar, dass neue technologische Entwicklungen oder Erkenntnisse über alternative Ermittlungsverfahren dazu führen, dass mildere, gleich geeignete Mittel zur Erreichung eines legitimen Ziels vorliegen, sodass ein vorher zulässiger Grundrechtseingriff nun nicht mehr erforderlich ist. In seiner Entscheidung zur Vorratsdatenspeicherung aus 2010 hat das Bundesverfassungsgericht außerdem deutlich gemacht, dass die Verhältnismäßigkeit einer einzelnen Überwachungsmaßnahme immer im Kontext des Gesamtumfangs staatlicher Überwachung bewertet werden muss („Überwachungsgesamtrechnung“):

> *[…] die Speicherung der Telekommunikationsverkehrsdaten [darf] nicht als Schritt hin zu einer Gesetzgebung verstanden werden, die auf eine möglichst flächendeckende vorsorgliche Speicherung aller für die Strafverfolgung oder Gefahrenprävention nützlichen Daten zielte. Eine solche Gesetzgebung wäre, unabhängig von der Gestaltung der Verwendungsregelungen, von vornherein mit der Verfassung unvereinbar. Die verfassungsrechtliche Unbedenklichkeit einer vorsorglich anlasslosen Speicherung der Telekommunikationsverkehrsdaten setzt vielmehr voraus, dass diese eine Ausnahme bleibt. Sie darf auch nicht im Zusammenspiel mit anderen vorhandenen Dateien zur Rekonstruierbarkeit praktisch aller Aktivitäten der Bürger führen.*

Um den grundrechtlichen Schutz gegenüber der „Rekonstruierbarkeit praktisch aller Aktivitäten der Bürger“ im heutigen

„Überwachungskapitalismus“ (*Zuboff*) zu effektivieren, bedarf es einer umfassenden Betrachtung aller Datensammlungen, die staatlichen Organen zur Verfügung stehen. Zwar beklagen Strafverfolgungsbehörden, dass die zunehmende Nutzung von Verschlüsselungstechnologien die Überwachung von Kommunikation erschwert (oft bezeichnet als „going dark“). Tatsächlich ist es aber so, dass in der Geschichte der Menschheit Individuen noch nie so viele persönliche Daten produziert haben wie heute. Dass diese Datensammlungen, die bei privaten Unternehmen liegen, von Strafverfolgungsbehörden zweckentfremdet werden, lässt sich in den USA intensiv beobachten. Dort haben sich Strafverfolgungsbehörden beispielsweise von Google Informationen darüber geben lassen, welche Nutzenden bestimmte Suchwörter verwendet oder sich an bestimmten Orten aufgehalten haben. Ein prägnantes Beispiel für diese Zweckentfremdung auch sensibelster Daten ist die begründete Befürchtung, dass zur Verfolgung illegaler Abtreibungen zukünftig auf die Daten von Menstruationsapps zugegriffen wird.

Nun sind all das Kontexte und gesellschaftliche Rahmenbedingungen, die Herrmann zu übersehen scheint. Er betont stattdessen nachdrücklich die Gefährdung „der Sicherheit im Innern in einer Dimension, die man sich einige Jahre zuvor noch kaum vorstellen konnte“ und arbeitet sich an der „aus den 1970er Jahren überkommene[n] Vorstellung“ ab, „dass Überwachungsmaßnahmen zwangsläufig zu weniger Freiheit führen“. An dieser Stelle sei deshalb der Hinweis gestattet, dass das Leben in Deutschland insgesamt – trotz teilweise problematischer Entwicklungen der letzten Jahre – so sicher ist wie selten zuvor. Es gibt in der Langzeitbetrachtung weniger Tötungsdelikte, weniger Gewalt, mehr Rechte für Frauen und Minderheiten und weniger Terrorismus als früher. Es kann also zumindest kein Weniger an Sicherheit in den letzten Jahrzehnten sein, das dazu führt, dass die Vorstellung einer Gesellschaft frei von Überwachung nach Herrmann als „überkommen“ zu qualifizieren ist.

Die IP-Vorratsdatenspeicherung als Allheilmittel

Dazu passend skizziert Herrmann das Bild eines Internets, in dem „unzählige Gefahren“ lauern, in dem „hemmungslos schwere Straftaten begangen werden“ und „[u]ngehemmter Hass und Hetze [um sich greifen]“. Das ist für das Internet so (un-)zutreffend wie für den physischen Raum: Wo Menschen zusammenkommen, gibt es Austausch von Wissen und Erfahrungen, Kreativität und Inspiration, Freundschaft und Solidarität. Es werden aber auch – wie in jedem sozialen Kontext – Normverstöße, auch schwerste Straftaten, begangen (zum komplexen Forschungsstand der Auswirkungen sozialer Plattformen für die Demokratie siehe hier). Diese gilt es – auch aufgrund der Schutzpflicht des Staates für seine Bürger:innen – zu einem ausreichenden Grad präventiv zu verhindern und andernfalls zu sanktionieren. Das von Herrmann aufgebauten Panorama der Internetkriminalität vom Austausch von Abbildungen von Kindesmissbrauch bis zu Ransomware-Angriffen erweckt allerdings den Eindruck, dass zwischen dem Zustand durch Anonymität hervorgerufener ausufernder Gewalt und Rechtslosigkeit auf der einen und einem guten Leben in absoluter Sicherheit auf der anderen Seite nur die IP-Vorratsdatenspeicherung stünde.

Das überspannt die Erwartungen an die IP-Vorratsdatenspeicherung deutlich. Zunächst ist es bereits jetzt der Fall, dass in der Praxis alle deutschen Telekommunikationsanbieter IP-Adressen nach Auskunft des Bundeskriminalamts (BKA) freiwillig für sieben Tage[1] zu Abrechnungszwecken speichern. Auch die oben genannte Bundesratsinitiative erkennt dies explizit an (S. 4, E.2). Diese sieben Tage genügen bereits, um in gut drei Viertel aller Verfahren eine Identifikation der Verdächtigen zu ermöglichen.

Es gibt jedoch viele Gründe, warum IP-Adressen oft nicht den erhofften Erfolg bringen: Ist der ermittelte Anschlussinhaber beispielsweise der Betreiber eines öffentlichen WLAN-Hotspots, wie es sie in Cafés, der Bahn und vielen anderen öffentlichen Orten gibt, führt die Ermittlung ins Leere. Selbst bei der gemein-

[1] Die verlinkte Grafik ist etwas missverständlich. Freenet ist ein reiner Reseller, verwendet also die Netze der anderen Telekommunikationsanbieter, bei denen die Speicherung entsprechend erfolgt.

samen Nutzung eines Anschlusses in einer Wohngemeinschaft oder Familie ist die Feststellung des Tatverdächtigen mit erheblichen weiteren Ermittlungen verbunden. IP-Adressen lassen sich darüber hinaus technisch ohne weiteres verschleiern, beispielsweise durch die Nutzung eines *Virtual Private Networks* (VPNs) oder eines Proxys. Insbesondere im Bereich der Schwerstkriminalität nutzen Kriminelle zudem oft das sogenannte „*Darknet*“ (es sei an dieser Stelle aber darauf hingewiesen, dass die Nutzung des *Darknets* elementar für Menschenrechtsaktivist:innen in autoritären Regimen ist). Damit wird ein Teil des Internets bezeichnet, der nicht über herkömmliche Browser, sondern über das Tor Netzwerk mit dem Tor Browser zugänglich ist. Dieses Netzwerk besteht aus mehreren Schichten (Tor ist eine Abkürzung für „The Onion Routing“), die verschlüsselte und anonyme Kommunikation sicherstellen. Anders als Herrmann behauptet bieten IP-Adressen hier regelmäßig gerade *nicht* „den einzigen Anhaltspunkt für Ermittlungsmaßnahmen der Sicherheitsbehörden“, sondern sind unbrauchbar, weil sie stets verschleiert sind.

Vielversprechender – und der staatlichen Schutzverpflichtung angemessen – ist es stattdessen, zielgerichtete Lösungen für einzelne Kriminalitätsphänomene zu entwickeln. Ein zentraler Ermittlungsansatz ist hierbei das Nutzerkonto, welches die Kontaktaufnahme zu späteren Opfern ermöglicht und somit eine Voraussetzung für die Begehung der Straftaten ist. Ein solches Konto kann eine Vielzahl von Hinweisen bieten, die durch Open Source Intelligence (OSINT)– bzw. Social Media Intelligence (SOCMINT)-Ermittlungen ausgewertet werden können. Das erkennt auch der EuGH an (Rn. 120-121), betont allerdings die besondere Eingriffsintensität, die solche umfassenden Ermittlungen für den Betroffenen haben, da weitere Informationen über ihr Privatleben ermittelt werden. Nicht zu berücksichtigen scheint er hierbei jedoch, dass diese Grundrechtseingriffe sich auf einen spezifischen Tatverdächtigen beschränken und damit deutlich weniger Streuwirkung entfalten als die massenhafte Speicherung der Daten aller Bürger:innen.

Nutzerkonten als Ermittlungsansatz bei schwerer Kriminalität

Darüber hinaus werden die Konten oft wiederholt verwendet, sodass eine präventive Speicherung von IP-Adressen nicht notwendig ist, um sie zu Ermittlungszwecken zu nutzen. Stattdessen würde es ausreichen, die IP-Adresse des Nutzerkontos bei der nächsten Nutzung des Kontos nach Feststellung eines Tatverdachts auszuleiten und dann unmittelbar aufzulösen, um den Anschlussinhaber zu ermitteln.

Diese Ansätze sind selbst bei schwerer Kriminalität, wie der Verbreitung von Abbildungen von Kindesmissbrauch, erfolgversprechend. Denn eine Vielzahl dieser Fälle werden nur aufgrund von Meldungen der US-amerikanischen Organisation NCMEC bekannt, die mit sozialen Plattformen und Cloud-Diensten kooperiert, die systematisch die bei ihnen hochgeladenen – öffentlichen oder privaten – Inhalte auf Abbildungen von Kindesmissbrauch durchsuchen. Zwar wird von Seiten der Strafverfolgungsbehörden betont, dass in diesen Fällen die „IP-Adresse der beste Ermittlungsansatz [sei], um die Täter zu identifizieren, in manchen sogar der einzige“. Es handelt sich jedoch in all diesen Konstellationen um Tatverdächtige, die ein Nutzerkonto auf dem jeweiligen Dienst angelegt haben. Die wiederkehrende Verwendung des Kontos führt dazu, dass das jeweilige Unternehmen immer wieder – bei jeder einzelnen Interaktion – Kenntnis von der aktuellen IP-Adresse des Nutzers erhält. Somit kann in diesen Fällen nach richterlicher Überprüfung die tagesaktuelle IP-Adresse an die Strafverfolgungsbehörden weitergegeben werden, die dann in Echtzeit von den Telekommunikationsanbietern aufgelöst werden kann. Für die Speicherung der IP-Adressen von Personen ohne jeden Tatbezug gibt es dagegen keine Notwendigkeit.

Gleiches gilt auch für Fälle des *Groomings*, in denen Erwachsene sich Kindern und Jugendlichen mit sexueller Absicht nähern. Diese Annäherung erfolgt regelmäßig über soziale Plattformen, die attraktiv für Kinder und Jugendliche sind. Erforderlich ist also ein regelmäßig genutztes Nutzerkonto für die Täter, um Kontakt mit den Minderjährigen aufnehmen und

halten zu können. Das Ziel der Täter, eine Vertrauensbasis mit den Minderjährigen aufzubauen und ggf. sogar ein Abhängigkeitsverhältnis zu schaffen, ist nur durch wiederkehrende Nutzung des Kontos möglich.

Die Angemessenheit von Grundrechtseingriffen

Herrmann hat Recht, soweit er betont, dass es originäre Aufgabe der Politik sei, kollidierende Grundrechte miteinander in Ausgleich zu bringen. Hierfür schlagen unterschiedliche Parteien und Regierungsmehrheiten unterschiedliche Lösungen vor, die im demokratischen Wettbewerb miteinander stehen. Der Rahmen dieses demokratischen Wettbewerbs wird von der Verfassung vorgegeben. Es gibt kein von Herrmann behauptetes „Primat der Politik" über das Recht, sondern vielmehr eine Bindung der Gesetzgebung „an die verfassungsmäßige Ordnung" und die Grundrechte „als unmittelbar geltendes Recht" (Art. 1 Abs. 3; 20 Abs. 3 GG). Diese Begrenzung öffentlicher Gewalt durch das Recht zeichnet den Rechtsstaat aus. Es ist gefährlich, zu suggerieren, dass das gerichtliche Verbot einer bestimmten Überwachungsmaßnahme einer Erhebung der Judikative zur „Supergesetzgebung" gleichkomme, in der es nur noch Raum für „eine verhältnismäßige Lösung" gäbe. Die Bewertung von eigenen politischen Vorhaben als grundrechtswidrig mag schmerzhaft sein, sollte allerdings eher zur selbstkritischen Reflektion des eigenen politischen Programms als zur Gerichtsschelte anregen. Denn es bleiben viele verhältnismäßige Lösungen möglich – nur eben nicht die eine, grundrechtswidrige Maßnahme.

Fraglich ist, ob bzw. wie die IP-Vorratsdatenspeicherung in den vom EuGH vorgegeben Rahmen des politischen Handlungsspielraums passt. Der EuGH hat in *La Quadrature du Net II* zwar festgestellt, dass die Speicherung von IP-Adresse „keinen schweren Eingriff" darstellt. Die apodiktische Feststellung des Urteils, dass ohne IP-Vorratsdatenspeicherung „eine echte Gefahr der systemischen Straflosigkeit" bestünde (Rn. 119), verkennt meines Erachtens jedoch zum einen, wie umfangreich die Ermittlungsmöglichkeiten der Strafverfolgungsbehörden mit ihren Zugriffen auf private Datensammlungen bereits jetzt sind. Die Einschätzung, dass die Speicherung zusätzlicher Daten dem Grundrechtsschutz zugutekommt, ist in der Sache wenig überzeugend (so aber Rn. 120-121). Darüber hinaus bietet – wie oben gezeigt – in der Struktur des heutigen Internets die weitverbreitete Verwendung von Nutzerkonten bei der Begehung von Straftaten Möglichkeiten, Tatverdächtige auch ohne eine präventive Speicherung über ihre IP-Adresse zu identifizieren.

Zum anderen wäre es ein Fehler, das Urteil als Blankoscheck für IP-Vorratsdatenspeicherungen zu deuten. Die vom EuGH postulierte geringe Eingriffstiefe gilt nur, wenn „eine wirksame strikte Trennung der verschiedenen Kategorien auf Vorrat gespeicherter Daten [gewährleistet wird], so dass die Kombination von Daten verschiedener Kategorien effektiv ausgeschlossen ist" (Rn. 103). Diese hohen technischen Anforderungen an die Speicherung, insbesondere die Trennung verschiedener Datenkategorien zur Vermeidung von Nutzerprofilen, haben dazu geführt, dass Branchenverbände davon ausgehen, dass sie faktisch keine Daten mehr speichern dürfen und die bestehende freiwillige Speicherung von IP-Adressen einstellen müssen. Es ist derzeit noch unklar, wie sich diese Anforderungen in der Praxis umsetzen lassen. Die Einführung einer IP-Vorratsdatenspeicherung ist deshalb nach wie vor mit hohen rechtlichen Unsicherheiten verbunden. Sicher scheint nach dem 30. April nur zu sein, dass die Vorratsdatenspeicherung Gerichte in ganz Europa weiterhin beschäftigen wird.

Eine Zeitenwende für die Innenpolitik

Die Menschen in Deutschland haben einen Anspruch auf staatlichen Schutz. Die Innenpolitik der vergangenen Jahrzehnte segelte oft am Rande der Verfassungswidrigkeit – und ging nicht selten auch darüber hinaus. Eine solche Politik macht das Land nicht sicherer. Sie führt vielmehr zu ungerechtfertigten Grundrechtseingriffen, Rechts- und Planungsunsicherheit. Viel Zeit und Energie geht in Gesetzgebungsprozessen verloren, deren Produkt von Höchstgerichten Jahre später für nichtig erklärt wird. Den Opfern von Gewalt ist damit nicht geholfen.

Die Innenpolitik bedarf einer Zeitenwende, in der Sicherheitsbehörden gemeinsam mit Betroffenen und

Zivilgesellschaft in offenen Prozessen zielgerichtete Maßnahmen für die Strafverfolgung und den Opferschutz entwickeln, ohne Massenüberwachung aus- und Rechtsschutz abzubauen. Erst vor kurzem hat Höffler hier auf dem Blog anschaulich ausgeführt, warum die beste Innenpolitik eine Gesellschaftspolitik ist, die die strukturellen Ursachen für Ausgrenzung und Gewalt behandelt und so das Land für alle sicherer macht.

Unsere Demokratie – da stimme ich mit Joachim Herrmann überein – ist in Gefahr. Längst sicher geglaubte Freiheiten, die in den letzten Jahrzehnten erkämpft wurden, werden wieder infrage gestellt. Der wachsende Rechtsextremismus in diesem Land gefährdet das demokratische Miteinander. Deshalb ist es wichtig, dass unsere demokratischen und rechtsstaatlichen Institutionen gestärkt werden. Dazu gehört im besonderen Maße die Gewaltenteilung und der effektive Rechtsschutz. Es gilt, sich von den Gegnern der Freiheit nicht einschüchtern zu lassen, sondern ihnen mehr Offenheit und mehr Demokratie entgegenzusetzen.

AUTOR*IN

Erik Tuchtfeld

Erik Tuchtfeld ist wissenschaftlicher Mitarbeiter am Max-Planck-Institut für ausländisches öffentliches Recht und Völkerrecht und leitet dort die humanet3-Gruppe. Er ist Associate Editor beim Verfassungsblog.

EMPFOHLENE ZITATION

Tuchtfeld, Erik: Für einen Opferschutz ohne Massenüberwachung: Eine Erwiderung auf Joachim Herrmann, Verfassungsblog, 08.10.2024, doi: 10.59704/99adae7eb0e2aecd.

Lizensiert unter CC BY-SA 4.0.

Langzeitarchiviert bei IntRechtDok unter: doi.org/10.17176/20241009-010053-0.