Humanistische Union

Das Recht auf Anonymität im digitalen Raum

in: vorgänge Nr. 225/226 (1/2/2019), S. 43 - 56

Wenn um das Recht auf Anonymität gestritten wird, geht es meist um digitale Kontexte. Michael Kuhn zeigt im folgenden Beitrag, dass der mit Anonymität verbundene Schutz keineswegs neu ist. Auch der grundrechtliche Schutz in der analogen Welt enthalte Vorkehrungen gegen die Identifizierung der/des Einzelnen, etwa bei Versammlungen oder politischen Meinungsäußerungen - ohne dass bisher ein Konzept der Anonymität explizit formuliert oder ihre Bedeutung für den grundrechtlichen Datenschutz voll erkannt wurde. Beim Anspruch auf Anonymität geht es nach Kuhn jedoch weniger um eine ja/nein-Entscheidung, sondern um unterschiedliche Intensitätsgrade ihrer Ausprägung, die dem jeweiligen grundrechtlichen Gefahrenpotenzial entsprechen. Vor diesem Hintergrund beschreibt der Beitrag die Bedeutung und die zu erwartende künftige Entwicklung der Anonymität im digitalen Raum. Nach Kuhns Einschätzung wird das Austarieren von Anonymität und Identifizierbarkeit entscheidend dafür sein, um die grundrechtlichen Werte in den digitalen Raum übertragen zu können.

Kaum ein Begriff steht für die Debatte um die Chancen und Risiken des digitalen Raums[1] so sehr wie Anonymität - Namenlosigkeit oder Nicht-Identifizierbarkeit. Er ist zum "ambivalenten Schlüsselbegriff unserer Zeit"[2] geworden.

Bereits im Ansatz scheinen sich dabei zwei konträre Sichtweisen gegenüberzustehen. Für die einen ist Anonymität eine Eigenart des digitalen Raums, die in der physischen Welt so nicht existiert. Sie wird verantwortlich gemacht für die Gefahr rechtsfreier Räume und eine Verrohung der Kommunikation, für die die Bezeichnung "Hasskommentar" verwendet wird. Für andere ist Anonymität dagegen ein in der physischen Welt alltägliches Phänomen, das im digitalen Raum bedroht ist. Mehr noch, Anonymität wird als Grundrecht und zentraler Baustein des liberalen Verfassungsstaates angesehen.[3]

Dieses unterschiedliche Verständnis weist darauf hin, dass es sich bei Anonymität um mehr als um ein Schlagwort handelt. Die Fragen nach dem Umgang mit Anonymität im digitalen Raum erweisen sich vielmehr als die Zuspitzung der grundlegenden rechtlichen und sozialen Herausforderung, wie ein in der physischen Welt gewachsenes Verständnis von Freiheit in den digitalen Raum transformiert werden kann. Ist der digitale Raum ein Raum, in dem aufgrund seiner Andersartigkeit gefestigte Grundannahmen nicht mehr gelten können?

Das soll in vier Schritten diskutiert werden. Im ersten Teil "Das Recht auf Anonymität in der physischen Welt" wird argumentiert, dass ein Recht auf Anonymität im Sinne eines ausreichenden Maßes an Anonymität als eine zentrale Komponente des grundrechtlichen Datenschutzes angesehen werden kann - auch wenn, zumindest im deutschen Rechtskreis, kein Recht auf Anonymität als eigenständige dogmatische Kategorie entwickelt wurde. Im zweiten Teil "Bedingungen für Anonymität im digitalen Raum" wird skizziert, warum es erforderlich ist, einen Grundkonsens über ein ausreichendes Maß an Anonymität für den digitalen Raum neu zu entwickeln. Im dritten Teil "Das Recht auf Anonymität im digitalen Raum" soll schlaglichtartig gezeigt werden, dass dies bisher nicht in ausreichendem Maß gelungen ist und es sollen die Gründe hierfür gesucht werden. Im abschließenden vierten Teil "Zukunft der Anonymität im digitalen Raum" soll dargelegt werden, dass sich die Relevanz der gesamtgesellschaftlichen Aufgabe, einen solchen Grundkonsens zu entwickeln, zukünftig weiter erhöhen wird.

Das Recht auf Anonymität in der physischen Welt

Die politische und rechtliche Debatte um die Bedeutung von Anonymität als Recht ist erst mit der Entstehung und massenhaften Nutzung des digitalen Raums als Ort der Persönlichkeitsentfaltung in den Vordergrund gerückt und hat daher auch erst in den letzten gut zehn Jahren in der höchstrichterlichen Rechtsprechung Beachtung gefunden.[4] Dabei hat sich aber - zumindest in der bisherigen deutschen und europäischen Rechtsprechung - kein Grundrecht auf Anonymität als eigenständige dogmatische Kategorie herausgebildet. Zudem wird Anonymität im einfachen Recht nur vereinzelt explizit geschützt. Prominentestes Beispiel ist § 13 Absatz 6 Satz 1 TMG. Danach hat ein Anbieter von Telemediendiensten ihre Nutzung und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist.

Es würde aber zu kurz greifen, aus dieser oberflächlichen Betrachtung den Schluss zu ziehen, dass sich die Frage nach einem Recht auf Anonymität nur im digitalen Raum stellen würde oder sie gar generell nebensächlich wäre. Vielmehr kann man ein Recht auf Anonymität als zentrale Komponente des grundrechtlichen Datenschutzes ansehen.

In diese Richtung lässt sich bereits der Anknüpfungspunkt des Datenschutzes deuten – die Verarbeitung *personenbezogener* Daten. Das sind gemäß Artikel 4 Nr. 1 DSGVO alle Informationen, die sich auf eine *identifizierte* oder *identifizierbare* natürliche Person beziehen.[5] Die (mögliche) Identifizierung - d.h. Deanonymisierung - einer Person ist damit der Auslöser für das datenschutzrechtliche Regelungsregime. Sein Gegenstand kann damit auch und gerade als die Frage formuliert werden, gegenüber wem und unter welchen Bedingungen Anonymität gewährt, aufgehoben oder (wieder)hergestellt wird.

Bereits im Volkszählungsurteil, in dem das Bundesverfassungsgericht das Datenschutz-Grundrecht auf informelle Selbstbestimmung vor dem Hintergrund der Bedingungen moderner Datenverarbeitung entwickelt hat, finden sich weitere Hinweise auf die rechtliche Bedeutung von Anonymität für die Einzelnen und die Gesellschaft. Darin heißt es:

"Individuelle Selbstbestimmung setzt […] voraus, daß dem Einzelnen Entscheidungsfreiheit über vorzunehmende oder zu unterlassende Handlungen einschließlich der Möglichkeit gegeben ist, sich auch entsprechend dieser Entscheidung tatsächlich zu verhalten. […] Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Wer damit rechnet, daß etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und daß ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten. Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist."[6]

Betrachtet man diese Aussage vor der Folie eines Rechts auf Anonymität, lassen sich daraus zwei Schlussfolgerungen ziehen. Erstens ist es ein zentrales Anliegen des Rechts auf informationelle Selbstbestimmung, dass Menschen ihre Meinung kundtun dürfen, ohne dafür ihre Identität gegenüber dem Staat offenlegen zu müssen. Anders gewendet: es gibt ein legitimes Interesse, gegenüber dem Staat anonym zu bleiben, und dies selbst dann wenn man sich im öffentlichen Raum äußert. Zweitens wird der/die sich Äußernde darin geschützt, "Risiken" vermeiden zu wollen, die mit der Meinungskundgabe verbunden sind. Ansonsten entsteht - nach später entwickelter Terminologie - ein Einschüchterungs- oder

Abschreckungseffekt durch das Gefühl ständiger Beobachtung. Dieser betrifft nicht nur den einzelnen Menschen, sondern gefährdet mit Blick auf die Bedeutung freier Kommunikation auch das demokratische Gemeinwesen.

Allerdings wird Anonymität vom Bundesverfassungsgericht nicht direkt als individuelles Recht genannt. Ein Hinweis auf eine Erklärung warum das nicht geschehen ist, könnte darin liegen, dass das Gericht als Beispiel die unbeobachtete Teilnahme an einer Versammlung und nicht etwa ganz allgemein die unbeobachtete Meinungskundgabe wählte. So wurde in den USA die Ableitung eines expliziten Rechts auf Anonymität aus der Redefreiheit durch einen Fall angestoßen, der Meinungskundgabe in Form von anonymen Flugblättern betraf.[7] Im Gegensatz zu Flugblättern kann aber auf einer Versammlung von Vornherein keine *absolute Anonymität* hergestellt werden. Gesehen und erkannt werden können die Teilnehmenden an einer Versammlung im Regelfall grundsätzlich jederzeit. Die Möglichkeit, diese einer Identitätsfeststellung zu unterziehen, ist zudem durch das Vermummungsverbot der Versammlungsgesetze abgesichert. Die Anonymität, die als Grundbedingung eines freiheitlichen öffentlichen Raums vorausgesetzt wird, ist damit zunächst ein *alltägliches Maß an faktischer, relativer Anonymität*. Dieses *Maß an Anonymität* begrifflich als Anonymität zu fassen, mag vielleicht nicht naheliegend erscheinen, da der Begriff der Namenlosigkeit einen absoluten Schutz vor Identifizierung impliziert. Der Wirklichkeit entspricht es aber eher davon auszugehen, dass es stets nur abgestufte Grade von Anonymität geben kann. Das gilt sowohl bezüglich der Frage, gegenüber wem Anonymität besteht, als auch unter welchen rechtlichen Bedingungen oder mit wie viel technischem Aufwand diese Anonymität aufgedeckt werden kann. Unter dieser Prämisse ist ein Recht auf Anonymität auch grundsätzlich der Abwägung mit anderen Rechtsgütern zugänglich. Es erlangt erst durch eine solche Abwägbarkeit eine größere Bedeutungstiefe.

In späteren Entscheidungen hat das Gericht weiter herausgearbeitet, dass die Voraussetzungen einer jederzeitigen Identifizierbarkeit im öffentlichen Raum nicht geschaffen werden dürfen. Das gilt nicht nur für eine vorherige Registrierung, sondern auch und gerade für den Einsatz technischer Überwachung.[8] Jüngst hat das Gericht seine Rechtsprechung mit Blick auf die automatisierten Kennzeichenkontrollen noch verschärft. Dabei hat es festgestellt, dass diese auch dann in das Recht auf informationelle Selbstbestimmung eingreifen, wenn das Ergebnis zu einem "Nichttreffer" führt und die Daten sogleich gelöscht werden. Dazu hat es ausgeführt:

"Zur Freiheitlichkeit des Gemeinwesens gehört es, dass sich die Bürgerinnen und Bürger grundsätzlich fortbewegen können, ohne dabei beliebig staatlich registriert zu werden, hinsichtlich ihrer Rechtschaffenheit Rechenschaft ablegen zu müssen und dem Gefühl eines ständigen Überwachtwerdens ausgesetzt zu sein (…). Jederzeit an jeder Stelle unbemerkt registriert und darauf überprüft werden zu können, ob man auf irgendeiner Fahndungsliste steht oder sonst in einem Datenbestand erfasst ist, wäre damit unvereinbar."[9]

Vor diesem Hintergrund greift die mit Blick auf den digitalen Raum gelegentlich vertretenen Auffassung, nur die passiv-konsumtive Nutzung des Internets könne von einem Recht auf Anonymität gedeckt sein[10), zu kurz. Es ist gerade auch die freie Bewegung und Entfaltung im öffentlichen Raum, die nicht Gegenstand ständiger Beobachtung sein darf. Auch wenn grundsätzlich ein starkes Interesse an Identifizierung ein größeres Maß an Überwachung bedingen kann, so darf dieses Überwachungsinteresse nie zur ständigen Beobachtung führen. In Konsequenz heißt das auch, dass das Recht zwar einerseits eine effektive Gefahrenabwehr und Rechtsverfolgung durch die Möglichkeiten der Identifizierung gebietet, andererseits aber auch eine Identifizierung um jeden Preis verbietet. Anders gewendet: Ein *Maß an Anonymität* im öffentlichen Raum muss immer gewährleistet sein.

Bedingungen für Anonymität im digitalen Raum

Diese Grundsätze eines Rechts auf Anonymität gewinnen besondere Bedeutung im digitalen Raum. Auch

dort kann es abgestufte Grade von Anonymität geben, die Rahmenbedingungen dafür sind aber andere als in der physischen Welt. Zwar ist im digitalen Raum einerseits die Kommunikation unter Nutzung von Pseudonymen alltäglich, anderseits ist Anonymität dort trotzdem keine faktische Selbstverständlichkeit. Jede Bewegung hinterlässt dort Datenspuren, die durch den technischen Fortschritt immer einfacher in noch größeren Mengen erfasst, gespeichert und ausgewertet werden können. Durch technische Maßnahmen können diese Spuren verringert oder verschleiert, aber nie ganz umgangen werden. Damit besteht im Grundsatz ein Umfeld der *technischen Identifizierbarkeit*.

Da das Internet privatrechtlich organisiert ist, fallen diese Spuren zunächst vor allem[11] bei den privaten Intermediären an, die den Zugang zum digitalen Raum und den dort angebotenen Diensten bereitstellen. Bei den Internetzugangsprovidern sind das Bestands- und Verkehrsdaten, bei genutzten Diensten Bestands- und Nutzungsdaten, die auch auf technischen Nachverfolgungsmechanismen ("*tracking*") basieren können.

Die privaten Intermediäre ermöglichen also die Bewegung im digitalen Raum, haben aber dadurch auch einen potentiell weitreichenden Einblick in diese Bewegungen. Nur wenige Intermediäre haben dabei das Ziel bzw. das Geschäftsmodell, diese Spuren zu minimieren. Insbesondere die Geschäftsmodelle der massenhaft genutzten Dienste wie Facebook oder Google beruhen vielmehr auch darauf, möglichst viele Daten zu einer Person zu sammeln, um wirtschaftlich verwertbare Aussagen zu deren Interessen treffen zu können. Staatliche Stellen können sich wiederum auf diese Daten zu Zwecken der Strafverfolgung oder Gefahrenabwehr Zugriffsmöglichkeiten schaffen.

Aber auch für Dritte ist Verhalten im Internet grundsätzlich identifizierbar. Das gilt auch, wenn keine Pflicht besteht, Klarnamen zu verwenden. Das zeigt sich besonders deutlich an den Internetprotokoll-Adressen (IP-Adressen). Das sind Nummern, anhand derer die Netzwerkanschlüsse der beteiligten Kommunikationspartner_innen identifiziert werden, um die Datenpakete bei der Übertagung zwischen diesen Beteiligten adressieren zu können. Bereits aus diesem Grund bietet jede Internetkommunikation grundsätzlich einen Anhaltspunkt für die Identifizierung des beteiligten Netzwerkanschlusses und damit der diesen Anschluss nutzenden Person.[12] Im Bereich der privaten Nutzung werden diese Adressen bisher häufig bei jeder neuen Verbindung mit dem Internet neu zugeteilt (dynamische IP-Adressen). Die Zuordnung einer IP-Adresse zu einem Anschluss ist damit grundsätzlich nur so lange möglich, wie der Internetzugangsprovider speichert, welchem Anschluss er zu einer bestimmten Zeit eine bestimmte IP-Adresse zugewiesen hat. Diese Art der Vergabe war allerdings dem beschränkten Adressraum nach dem Standard IPv4 geschuldet. Der neuere Standard IPv6 bietet einen so großen Adressraum, dass theoretisch jedem netzwerkfähigen Gerät zukünftig dauerhaft eine weltweit eindeutige IP-Adresse zugewiesen werden könnte.[13]

Das Recht auf Anonymität im digitalen Raum

Unter diesen knapp skizzierten Bedingungen der technischen Identifizierbarkeit im digitalen Raum kann die Grundannahme alltäglicher faktischer Anonymität in der physischen Welt dort nicht unverändert fortgelten. Daher muss für den digitalen Raum ein Grundkonsens von einem ausreichenden Maß an Anonymität neu entwickelt werden. Dabei kommt der Frage nach einem Recht auf Anonymität eine besondere Bedeutung zu, wenn es um das Austarieren von Anonymität und Identifizierbarkeit geht. Der in den Grundrechten zum Ausdruck kommende gesellschaftlichen Grundkonsens muss dabei der Maßstab für die konkret zu entscheidenden Fragen sein.

Anhand zweier kurzer Schlaglichter soll hier deutlich gemacht werden, dass eine Grundvorstellung von einem notwendigen Maß an Anonymität bisher nicht in ausreichenden Umfang entwickelt werden konnte. Dabei sollen Beispiele aus zwei unterschiedlichen Problemkreisen gewählt werden. Zum einen die Deanonymisierung direkt auf Betreiben Dritter zur zivilrechtlichen Rechtsverfolgung - zum anderen die

Deanonymisierung auf Betreiben des Staates zu Strafverfolgung und Gefahrenabwehr.

Ein Beispiel aus dem ersten Problemkreis, der Deanonymisierung auf Betreiben Dritter, ist die Rechtsprechung des Bundesgerichtshofs zu Online-Bewertungsportalen. In diesem Rahmen hat sich der BGH explizit mit dem Schutz anonymer Meinungsäußerung beschäftigt. Dabei hat er ausgeführt, dass anonyme Bewertungen nicht nur der Meinungsfreiheit unterfallen, sondern auch keinen geringeren Schutz erfahren dürfen als nicht-anonyme Bewertungen. Ohne Anonymität bestünde nämlich die Gefahr, dass Menschen gerade im sensiblen Bereich der medizinischen Versorgung von einer Bewertung absehen könnten.[14] Um unter den beschriebenen Bedingungen der technischen Identifizierbarkeit eine Abwägung der schutzwürdigen Interessen der bewerteten Person mit der Anonymität der bewertenden Personen zu ermöglichen, hat der BGH dem Intermediär, also dem Bewertungsportal, eine zentrale Rolle zugewiesen. Wird etwa das Bestehen eines Behandlungskontaktes von der bewerteten Person bestritten, müsse sich das Portal an die bewertende Person wenden, um das Bestehen eines Behandlungskontakts zu überprüfen und dazu ggf. Nachweise anfordern.[15] 2014 hat der BGH noch entschieden, dass aufgrund fehlender Rechtsgrundlage - selbst bei persönlichkeitsrechtsverletzenden Bewertungen - kein direkter zivilrechtlicher Auskunftsanspruch der bewerteten Person über die Identität der bewertenden Person bestehen könne. Über eine solche Möglichkeit müsse der Gesetzgeber entscheiden.[16] Möglich war damit nur ein Unterlassungsanspruch gegenüber dem Bewertungsportal oder eine Strafanzeige gegen die bewertende Person.

Im Ergebnis lässt sich diese Argumentation als Drittwirkung des oben skizzierten Rechts auf Anonymität deuten, in deren Rahmen die Bedeutung und der Schutz von anonymer Kommunikation im digitalen Raum in bemerkenswerter Weise akzentuiert wurde. Allerdings hat der Gesetzgeber - in Reaktion auf diese Rechtsprechung - mit der Einführung des Netzwerkdurchsetzungsgesetzes einen zivilrechtlichen Auskunftsanspruch gegenüber Anbietern von Telemediendiensten geschaffen.[17] Gemäß § 14 Absatz 3 und 4 sowie § 15 Absatz 5 Satz 4 TMG kann nunmehr ein Diensteanbieter allgemein - also nicht nur soziale Netzwerke - verpflichtet werden, über Bestands- und Nutzungsdaten Auskunft an Dritte zu erteilen, um die Identität von nutzenden Personen offenzulegen. Notwendig ist die (behauptete) Verletzung absolut geschützter Rechte aufgrund rechtswidriger Inhalte, die von § 1 Absatz 3 des NetzDG erfasst werden. Mit dem Begriff der absolut geschützten Rechte verweist das Gesetz im Ergebnis auf § 823 Absatz 1 BGB und damit grundsätzlich auch auf eine mögliche Verletzung der kommerziellen Reputation des eingerichteten und ausgeübten Gewerbebetriebes.[18]

Zwar wurden im Gesetzgebungsverfahren noch die Beschränkung auf die durch das NetzDG erfassten Tatbestände und ein Richtervorbehalt eingeführt.[19] Dennoch bleibt der Eindruck, dass die vom BGH herausgearbeiteten Maßstäbe zu Bedeutung und Absicherung anonymer Meinungskundgabe nur unterkomplex diskutiert wurden. Das wird umso deutlicher, wenn man berücksichtigt, dass gleichzeitig einerseits die bereits erwähnte Verpflichtung eines Dienstanbieters besteht, die anonyme Nutzung zu ermöglichen (§ 13 Absatz 6 TMG)[20] und anderseits grundsätzlich keine rechtliche Verpflichtung für Diensteanbieter existiert, überhaupt Nutzerdaten zu erfassen.[21] Der Auskunftsanspruch richten sich damit auf Daten, die etwa für technische Kontrollzwecke gespeichert werden dürfen, aber eigentlich gelöscht werden müssen, sobald dieser Zweck erfüllt ist.[22]Eine Speicherpflicht entsteht - solange keine Vorratsdatenspeicherung Anwendung findet - erst mit der Anordnung einer Telekommunikationsüberwachung.[23] Zudem ist an dem gerichtlichen Auskunftsverfahren nur der Diensteanbieter beteiligt. Die eigentlich betroffenen Nutzer der Dienste, um deren Anonymität es geht, dürfen lediglich vom Diensteanbieter über die Einleitung des Verfahrens unterrichtet werden, § 14 Absatz 5 TMG.

Zu dem zweiten Problemkreis, der Deanonymisierung auf Betreiben des Staates, gehören die Urteile des Bundesverfassungsgerichts zur Vorratsdatenspeicherung und zur Bestandsdatenauskunft. Auch hier zeigt sich, dass die Rechtsprechung für die Gewichtung anonymer Kommunikation vor allem auf den Gesetzgeber verweist. Von diesem fordert das Gericht zwar eine klare Entscheidung über die Voraussetzungen der Aufhebung von Anonymität, macht aber ihm darüber hinaus dafür nur spärliche materielle Vorgaben. Während das Gericht für eine anlasslose Vorratsdatenspeicherung von Telekommunikationsverkehrsdaten

noch besondere Voraussetzungen fordert, entschärft es diese für die "bloße" Deanonymisierung von IP-Adressen - die es als "Aufhebung der Anonymität im Internet"[24] bezeichnet - deutlich. Für diesen Fall verlangt das Gericht lediglich eine ausdrückliche gesetzliche Regelung, die zumindest auf die Verfolgung "besonders gewichtiger Ordnungswidrigkeiten" gerichtet sein müsse.[25] Schließlich sei die für eine Deanonymisierung notwendige Datenspeicherung weniger umfangreich und habe daher ein erheblich weniger belastendes Gewicht - im Übrigen dürfe in einem Rechtsstaat auch das Internet keinen rechtsfreien Raum bilden. Die Qualifikation der Verfolgung "besonders gewichtiger Ordnungswidrigkeiten" zeigt zwar, dass auch das Bundesverfassungsgericht im Grundsatz die Bedeutung von Anonymität im digitalen Raum anerkennt. Mit ihrem geringen materiellen Gehalt wirkt sie dabei aber als wenig mehr als ein bloßes Feigenblatt.

Dieser Eindruck verfestigt sich mit Blick auf die Rechtsprechung des Bundesverfassungsgerichts zur Bestandsdatenauskunft. Wie bereits angesprochen fallen auch ohne Vorratsdatenspeicherung Daten wie IP-Adressen bzw. deren Zuordnung zu Internetanschlüssen bei den privaten Intermediären an und können aufgrund von Auskunftsansprüchen abgefragt werden - grundsätzlich unabhängig von der Frage, ob sie dort zu anderen Zwecken - ggf. nur vorübergehend - gespeichert werden durften. Dazu wurden die Instrumente der Bestandsdatenauskunft gegenüber Telekommunikationsdienstleistern - wie Internetzugangsprovidern - gemäß § 113 TKG und gegenüber Anbietern von Telemediendiensten gemäß § 14 Absatz 2 TMG geschaffen. In seinem Urteil zur Bestandsdatendatenauskunft hat das Gericht zwei Aussagen zur Anonymität getroffen, die hier relevant sind. Zum einen hat es für die Möglichkeit der Identifizierung von dynamischen IP-Adressen eine normenklare gesetzgeberische Entscheidung gefordert, ob und unter welchen Voraussetzungen eine solche Identifizierung vorgenommen werden könne - sie erlaube nämlich in weitem Umfang eine Deanonymisierung von Kommunikationsvorgängen im Internet.[26] Zum anderen hat es darauf hingewiesen, dass sich die Bewertung ändern könne, wenn auch Privaten regelmäßig statische IP-Adressen zugeteilt würden, da dadurch zumindest in weitem Umfang die Identität von Internetnutzern ermittelt und Kommunikationsvorgänge im Netz nicht nur für eine begrenzte Zeit, sondern auch dauerhaft deanonymisiert werden könnten. Den Gesetzgeber treffe insoweit eine Beobachtungs- und gegebenenfalls Nachbesserungspflicht.[27] Der Gesetzgeber hat auf dieses Urteil mittlerweile lediglich mit der Klarstellung reagiert, dass auch dynamische IP-Adressen mit dem Mittel der Bestandsdatenauskunft deanonymisiert werden können, vgl. § 113 Absatz 1 Satz 3 TKG. Eine Reaktion auf den potentiellen Einfluss statischer IP-Adressen - etwa durch eine rechtliche Verpflichtung der Vergabe dynamischer IP-Adressen - ist dagegen nicht erfolgt.

Diese beiden Schlaglichter zeigen, dass die Bedeutung anonymer Kommunikation zwar in der deutschen Rechtsprechung grundsätzlich gewürdigt wird, eine Grundvorstellung über ein ausreichendes Maß an Anonymität aber nur in Ansätzen entwickelt wurde. Insbesondere fällt auf, dass die Anonymität im Internet nicht so stark gewichtet wird wie die oben beschriebene faktische Anonymität in der physischen Welt. Vielmehr wird häufig auf den Gesetzgeber verwiesen, dem über eine klare Regelung der Voraussetzungen für eine Deanonymisierung hinaus aber kaum materielle Vorgaben gemacht werden. Der Gesetzgeber sieht darin regelmäßig eher Aufträge, Überwachungs- und Auskunftslücken zu schließen, als differenziert das notwendige Maß an Anonymität im digitalen Raum zu bewerten.

Diese unterschiedliche Wertung ist umso bemerkenswerter, als für Überwachung im digitalen Raum und in der physischen Welt die gleichen dogmatischen Grundüberlegungen gelten, die an die oben angesprochene Rechtsfigur des Abschreckungseffekts auf die Grundrechtsausübung anknüpfen. Als dogmatisches Werkzeug scheint diese aber starken Limitationen ausgesetzt zu sein. Der Abschreckungseffekt ist zwar eine plausible Überlegung, mit der die Eröffnung des Schutzbereichs von Grundrechten wie der Meinungsfreiheit, der informationellen Selbstbestimmung und der Telekommunikationsfreiheit begründet werden kann. Auf Abwägungsebene lassen sich damit aber nur die äußeren Grenzen scharf zeichnen: auf der einen Seite die ständige Überwachung und Identifizierbarkeit, auf der anderen Seite unbedingte Anonymität, die den Schutz von Rechten Dritter und Interessen der Allgemeinheit ausschließt. Diese beiden Extreme sind aber bereits aus faktischen Gründen wenig relvant. Zur Herausarbeitung eines notwendigen *Maßes an Anonymität* auf Abwägungsebene in alltäglichen Einzelfällen hat der Abschreckungseffekt aber keine befriedigende Operationalisierung erfahren. Das kann etwa am Beispiel der Rechtsprechung des

Bundesverfassungsgerichts zur Vorratsdatenspeicherung verdeutlicht werden. Dort wird zwar ein schwerwiegender Eingriff angenommen, weil die Vorratsdatenspeicherung ein "Gefühl des ständigen Überwachtwerdens" und eine "diffuse Bedrohlichkeit" hervorrufen könne.[28] Warum dann aber etwa eine Speicherdauer von sechs Monaten die Obergrenze des rechtfertigbaren nicht überschreiten soll,[29] wäre mit Blick auf ein geringeres Maß an Einschüchterung zumindest erläuterungsbedürftig gewesen. Das gilt erst recht für die Annahme, die "bloße" Aufdeckung von Anonymität anhand der Identifizierung von IP-Adressen unter Zuhilfenahme von Vorratsdaten sei weniger streng zu bewerten.[30)

Im Gegenteil liegt es eher nahe, dass - wie bei einer Bewegung im öffentlichen Raum - ein für die Freiheitsausübung erforderliches Maß an Anonymität nur gegeben sein kann, wenn Überwachung in einer Weise begrenzt wird, dass sie tatsächlich nicht oder nicht ständig bzw. nicht überall stattfindet. Und das gilt selbst und gerade dann, wenn es nur um Deanonymisierung von Verhalten geht. In diese Richtung weisen auch die Urteile des Europäischen Gerichtshofs zur Vorratsdatenspeicherung[31], in denen sich keine Einschränkung des Verbots der anlasslosen Überwachung findet, wenn es um die "bloße" Deanonymisierung von Bewegung im digitalen Raum geht. Auch der Europäische Gerichtshof für Menschenrechte tendiert zu einer stärkeren Gewichtung von Anonymität in diesem Sinne. Er hat kürzlich mit Verweis auf die Bedeutung von Anonymität entschieden, dass auch für die Identifizierung eines/einer Nutzer_in anhand einer dynamischen IP-Adresse ein Richtervorbehalt vorzusehen sei[32], was das Bundesverfassungsgericht ohne weitere Begründung noch ausdrücklich verneint hatte.[33] Besonders verkürzt wirkt im Vergleich zu den für die physische Welt geltenden Grundsätzen die apodiktische Aussage des Bundesverfassungsgerichts, dass es in einem Rechtsstaat keine rechtsfreien Räume geben dürfe. Schließlich wäre vor dem Hintergrund der Rechtsstaatlichkeit die jederzeitige Identifizierbarkeit von Verhalten grundsätzlich - wie dargelegt - ebenfalls zu problematisieren. Zudem zeigt gerade das Beispiel der Vorratsdatenspeicherung, dass intensive Überwachungsinstrumente mit der Notwendigkeit der Abwehr schwerster Gefahren wie Terrorismus begründet werden können, bei dieser Gelegenheit, quasi nebenbei, aber auch der "bloßen" Aufdeckung von Anonymität dienen dürfen.

Eine unterschiedliche Wertung von Anonymität und Überwachung in der physischen Welt und im digitalen Raum kann unterschiedliche Ursachen haben. So mag aufgrund der beschriebenen Grundbedingung der technischen Identifizierbarkeit die Überwachung im digitalen Raum weniger eingriffsintensiv wirken. Schließlich kann sie auf den notwendigerweise anfallenden Datenspuren aufbauen und Verhalten muss nicht erst aufwendig erstmals technisch erfasst werden. Möglicherweise erscheint der digitale Raum auch im Vergleich zur physischen Welt (noch) als für die aktive Persönlichkeitsentfaltung von untergeordneter Bedeutung. Nicht zuletzt mag auch hinderlich sein, dass für die physische Welt bisher kein explizites Recht auf Anonymität entwickelt wurde, das als Folie zur Bewertung von Überwachung im digitalen Raum dienen könnte. Die für beide Räume gültige Rechtsfigur des Abschreckungseffektes scheint im Ergebnis zu beliebig zu sein, um eine differenzierte Transformation der für die physische Welt entwickelten Maßstäbe leisten zu können. Ob man dieser Beliebigkeit nur mit der Forderung nach dogmatischer Schärfung, Strukturierung und empirischer Unterfütterung der Abschreckungsfigur begegnen kann[34], ohne die Frage nach der spezifischen rechtlichen und gesellschaftlichen Bedeutung von Anonymität zu stellen, erscheint sehr fraglich.

Die bisherige Rechtsentwicklung bietet aber genügend Ansätze, ein Maß an Anonymität im digitalen Raum zu sichern und abwägbar zu halten. Dazu könnte etwa der Verzicht auf anlasslose Vorratsdatenspeicherung und der Ausschluss dauerhafter Deanonymisierungsmöglichkeiten gehören – zugunsten von anlassbezogener Überwachung in Einzelfällen von gewissem Gewicht. Ebenso kann die Einschränkung von Auskunftsrechten zur privaten Rechteverfolgung angedacht werden, etwa durch Beschränkung auf strafrechtlich relevante Fälle. Schließlich könnte die Beteiligung von Nutzer_innen an dem Verfahren ihrer Deanonymisierung erwogen werden, gerade wenn in diesem Verfahren dafür komplexe Wertungen von Aussagen im Lichte der Meinungsfreiheit nötig werden.

Dabei ist auch der Gesetzgeber gefordert. Leider zeigt gerade die Politik nur wenig Ansätze, eine Diskussion über ein ausreichendes Maß an Anonymität zu führen. Das gilt sowohl für Umfang der zur Deanonymisierung notwendigen Überwachung, als auch für die Begrenzung der Zwecke einer Deanonymisierung. Das zeigt z.B. der Katalog des § 1 Absatz 3 NetzDG, der – wie dargelegt – auch für die

Deanonymisierung von Meinungsäußerungen im Internet auf Betreiben privater Dritter Anwendung findet. Dieser wenig nachvollziehbare Katalog reicht von einfacher Beleidigung bis zur Bildung terroristischer Vereinigungen und ist damit "letztlich ein Spiegel der völlig durcheinandergeratenen Debatten unserer Zeit"[35], die durch völlig unbestimmte Anglizismen wie "*hate speech*" und "*fake news*" noch verschärft werden. In diesem Kontext ist auch für den Umgang mit Anonymität nur schwer eine differenzierte Debatte möglich.

Zukunft der Anonymität im digitalen Raum

Trotz dieser Schwierigkeiten wird sich die Relevanz der Aufgabe, eine Grundvorstellung von einem notwendigen Maß an Anonymität im digitalen Raum zu entwickeln, durch die zunehmenden technischen Möglichkeiten der Überwachung weiter erhöhen. Denn mit zunehmender Überwachung steigen auch die bisher vielleicht eher abstrakt wirkenden Überwachungskosten für den/die Einzelnen, aber auch für die Gesellschaft. Wollte man etwa die Anonymität im digitalen Raum tatsächlich aufheben, müsste man nicht nur eine ständige Überwachung etablieren, sondern auch Techniken zur Verschlüsselung und Anonymisierung der Kommunikation effektiv umgehen oder regulieren und sanktionieren. Dafür müsste aber massiv in das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme eingegriffen und Möglichkeiten des informellen Selbstschutzes beschränkt werden.[36]

Dabei zeigt gerade das weltweite Internet, dass Anonymität im digitalen Raum weder eine technische noch eine rechtliche Selbstverständlichkeit ist. Für autokratische Systeme sind die schwierigen Abwägungsfragen zwischen Anonymität und Identifizierbarkeit wesentlich einfacher zu treffen. Nordkorea gewährt zum Beispiel nur wenigen tausend ausgesuchten Personen Zugang zum weltweiten Internet.[37] Das verdeutlicht, wie verletzlich der digitale Raum selbst gegen rein nationale Regulierung sein kann. Der Fall China zeigt, dass dazu noch nicht einmal die völlige Abschottung vom Internet notwendig ist. Dort wird in großem Umfang versucht, ausländische Internetinhalte zu zensieren und Anonymisierungstechniken zu unterbinden. Das dazu entwickelte Projekt "Goldener Schild" wird in Anlehnung an die chinesische Mauer auch "*Great Firewall of China*" genannt. Im Rahmen der Einführung seines "Sozialkreditsystems" plant China zudem die technischen Möglichkeiten für eine Überwachung zu nutzen, in der auch in der realen Welt durch weiträumige Videoüberwachung keine Anonymität mehr gewährleistet ist.

Der Blick auf diese Beispiele verdeutlicht, dass der freie Fluss von Informationen, insbesondere von Meinungen und gerade auch von anonymen Meinungen nicht etwas ist, dass Demokratien gefährdet, sondern etwas, dass sie auszeichnet. Die Meinungsfreiheit ist - in den Worten des BVerfG - ein für die Demokratie schlechthin konstitutives Recht. Sie schützt nicht nur die Mehrheitsmeinung oder das wohl abgewogene Argument, sondern gerade auch Ansichten, die manche vielleicht bereits als "*hate speech*" oder "*fake news*" bezeichnen würden, bis an die Schwelle der Strafbarkeit heran. Es bleibt abzuwarten, inwieweit die mit dem NetzDG eingeführten Auskunftsansprüche gegenüber Dienstanbietern von den Gerichten gehandhabt werden. Die in diesem Rahmen zu treffenden Entscheidungen bieten jedenfalls auch das Potential herauszukristallisieren, dass das Recht kein Mittel dafür ist, für einen sachlich ausgewogenen und irritationsfreien Diskurs im digitalen Raum zu sorgen. Der Umgang mit den negativen Folgen von Anonymität ist daher gerade mit Blick auf die Umgangsformen eine gesamtgesellschaftliche Aufgabe und keine Frage, die sich mit der Beseitigung "rechtsfreier Räume" durch Überwachung erledigt.

Zudem ist zweifelhaft, ob sich selbst mit einer Aufhebung der Anonymität im Internet überhaupt alle damit assoziierten Probleme lösen ließen. Viele Probleme - wie Beleidigungen im Internet - könnten vielmehr eine Folge der veränderten, unpersönlichen Kommunikation im digitalen Raum sein und nicht bloß an der Anonymität der Äußerungen festgemacht werden. Das zeigt das Beispiel Südkorea. Dort wurde 2007 beschlossen, dass Bürgerinnen und Bürger Kommentare auf Internetseiten nur abgeben dürfen, wenn sie sich zuvor mit ihrem Namen und ihrer Einwohneridentifikationsnummer registriert haben. Nach einer

Untersuchung des Forschers Daegon Cho wurden zwar kurzfristig weniger Schimpfwörter verwendet, langfristig war der Effekt aber geringer, zudem wurden kreativere Formen der Beleidigung gewählt.[38] Nachdem wiederholt die zur Registrierung verwendeten Daten in großem Umfang von Hackern entwendet und verkauft wurden,[39] hat das südkoreanische Verfassungsgericht das Gesetz schließlich für verfassungswidrig erklärt. Dabei hat es auf seine geringe Wirksamkeit und die Benachteiligung inländischer Internetseiten gegenüber ausländischen abgestellt.[40]

So bleibt zu konstatieren, dass dem Recht bei der Frage nach dem Umgang mit Anonymität im digitalen Raum zwar eine bedeutende Rolle zukommt, es dabei aber nur ein Teil einer gesamtgesellschaftlichen Aufgabe einer Neukalibrierung von Alltäglichkeit im digitalen Raum sein kann. Dazu gehört - wie auch in der physischen Welt - nicht zuletzt die Frage nach einem notwendigen Maß an alltäglicher Anonymität in einer freien Gesellschaft.

MICHAEL KUHN *Jahrgang 1981, studierte Rechtswissenschaften an den Universitäten in Passau, Cardiff und der Humboldt-Universität in Berlin. Zu seinen Schwerpunkten gehören Europarecht, Staats- und Verwaltungsrecht sowie Datenschutz- und Internetrecht. Er ist beim Bundeszentralamt für Steuern angestellt und promoviert zum Recht auf Anonymität im Internet.*

Anmerkungen:

1 Der Begriff "digitaler Raum" steht hier zunächst für das Internet und die damit verbundenen informationstechnischen Systeme in ihrer gegenwärtigen Form, auf die sich die zitierte Rechtsentwicklung und Rechtsprechung maßgeblich bezieht. Der Begriff soll verdeutlichen, dass es sich dabei um mehr als ein Kommunikationsmittel handelt, sondern in zunehmenden Maße um einen Raum menschlicher Persönlichkeitsentfaltung, in den sich diese mehr und mehr verlagert. In diesem Sinn soll der Begriff auch als Platzhalter dienen für zukünftige Entwicklungen. Auch ohne diese Entwicklungen genau absehen zu können, ist davon auszugehen, dass sich die Bedeutung vernetzter informationstechnischer Systeme sowohl für das private wie öffentliche Leben und damit auch für die Ausübung von grundrechtlich garantierten Freiheiten weiter erhöhen wird.

2 *Kersten, Jens* 2017: Anonymität in der liberalen Demokratie, in: JuS 2017, S. 193 (193).

3 Vgl. *Kersten, Jens* 2017: Anonymität in der liberalen Demokratie, in: JuS 2017, S. 193 (194).

4 Vgl. Teil "Das Recht auf Anonymität im digitalen Raum"

5 Anonyme Daten sind damit nicht geschützt, vgl. Erwägungsgrund 26 der DSGVO - dies aber gerade deshalb, weil sie die Anonymität der Person nicht gefährden.

6 BVerfG, Urteil vom 15.12.1983, BVerfGE 65, 1 - Volkszählung, S. 42 f.

7 Vgl. US Supreme Court, McIntyre v. Ohio Elections Commission, 514 U.S. 334 (1995); vgl. auch Froomkin, A. Michael 2008: Anonymity and the Law in the United States, in: Kerr u.a. (Hrsg.), Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society.

8 Vgl. BVerfG, Beschluss vom 23.02.2007 - 1 BvR 2368/06 - Städtische Videoüberwachung; BVerfG, Urteil vom 20.11.2007, BVerfGE 120, 378 - Automatisierte Kennzeichenerfassung I.

9 BVerfG, Beschluss vom 18.12.2018 - 1 BvR 142/15 - Automatisierte Kennzeichenerfassung II, Rn. 51 -

bverfg.de.

10 In diesem Sinne etwa *Kutscha, Martin/Thomé, Sarah* 2013: Grundrechtsschutz im Internet, S. 50 m.w.N.

11 Zumindest, wenn man von den durch die Snowden-Leaks bekannt gewordenen Möglichkeiten der Massenüberwachung des Internetverkehrs durch Geheimdienste absieht.

12 Aus diesem Grund hat auch der EuGH zu Recht klargestellt, dass es sich bei IP-Adressen um personenbezogene Daten handelt, soweit grundsätzlich die (rechtliche) Möglichkeit besteht, die Zuordnung einer IP-Adresse zu einer Person vorzunehmen, vgl. EuGH, Urteil vom 19.10.2016 - C-582/14 - Breyer.

13 Vgl. dazu *Wegener, Christoph / Heidrich, Joerg* 2011: Neuer Standard - Neue Herausforderungen: IPv6 und Datenschutz, in: CR 2011, S.479.

14 Vgl. BGH, Urteil vom 20.02.2018 - VI ZR 30/17- Ärztebewertung III, Urteil vom 23.06.2009 - VI ZR 196/08 - spickmich.de.

15 Vgl. BGH, Urteil vom 01.03.2016 - VI ZR 34/15.

16 Vgl. BGH, Urteil vom 01.07.2014 - VI ZR 345/13 = BGHZ 201, 380 - Ärztebewertung II.

17 Art. 2 des Gesetzes vom 1.9.2017, BGBl. I 3352.

18 Vgl. *Spindler, Gerald* 2017: Der Regierungsentwurf zum Netzwerkdurchsetzungsgesetz - europarechtswidrig?, in: ZUM 2017, 473 (486).

19 Vgl. *Schmitz, Peter* in *Spindler, Gerald/Schmitz, Peter,* Telemediengesetz, 2. Aufl. 2018, § 14, Rn. 53.

20 Siehe dazu *Spindler, Gerald* 2017: Der Regierungsentwurf zum Netzwerkdurchsetzungsgesetz - europarechtswidrig?, in: ZUM 2017, 473 (484 f.)

21 Vgl. *Pille, Jens-Ullrich* 2018, Der Grundsatz der Eigenverantwortlichkeit im Internet, in: NJW 2018, 3545 (4546).

22 Siehe dazu mit Blick auf Webseitenbetreiber: BGH, Urteil vom 16.05.2017 - VI ZR 135/13, für Internetzugangsprovider: BGH, Urteil vom 03.07.2014 - III ZR 391/13.

23 Vgl. dazu BVerfG, Beschluss vom 20.12.2018 - 2 BvR 2377/16 - posteo.

24BVerfG, Urteil vom 02.03.2010 - 1 BvR 256/08 - Vorratsdatenspeicherung, Rn. 262 - bverfg.de.

25Vgl. ebd., Rn. 226.

26Vgl. BVerfG, Beschluss vom 24.01.2012 - 1 BvR 1299/05 - Bestandsdatenauskunft, Rn. 174 - bverfg.de.

27Vgl. ebd., Rn. 161.

28 Vgl. BVerfG, Urteil vom 02.03.2010 - 1 BvR 256/08 - Vorratsdatenspeicherung, 241 f. - bverfg.de.

29 Vgl. ebd., Rn. 254 ff, 288 ff.

30 Vgl. ebd., Rn. 257.

31 Vgl. EuGH, Urteil vom 08.04.2015 - C-293/12 und C-594/12 - Vorratsdatenspeicherung; EuGH, Urteil vom 21. 12.2016 - C-203/15; C-698/15 - Tele2 Sverige AB.

32 Vgl. EGMR, Urteil vom 24.04.2018, 62357/14 - Benedik v. Slovenien.

33 Vgl. BVerfG, Urteil vom 02.03.2010 - 1 BvR 256/08 - Vorratsdatenspeicherung, Rn. 261 - bverfg.de.

34 Zu diesen Forderungen vgl. *Staben, Julian* 2016: Der Abschreckungseffekt auf die Grundrechtsausübung, S. 75 ff.

35 *Richter, Philipp* 2017: Das NetzDG - Wunderwaffe gegen "Hate Speech" und "Fake News" oder ein neues Zensurmittel?, in: ZD-Aktuell 2017, 05623.

36 Vgl. BVerfG, Urteil vom 27. 02.2008 - 1 BvR 370/07 - Rn. 203, 236.

37 Vgl. https://www.wired.de/collection/life/ein-uber-ingenieur-gibt-uns-einblick-nordkoreas-internet

38 Vgl. *Brodnig, Ingrid* 2014, Der unsichtbare Mensch: Wie die Anonymität im Internet unsere Gesellschaft verändert, zu Fn. 244 f.

39 Vgl. ebd., zu Fn. 247 f.

40 Vgl. ebd., zu Fn. 252 f.

---

https://www.humanistische-union.de/publikationen/vorgaenge/225-226/publikation/das-recht-auf-anonymitaet-im-digitalen-raum-1/
Abgerufen am: 05.02.2023