JONAS BREYER
RECHTSANWALT
DATENSCHUTZBEAUFTRAGTER

Rechtsanwaltskanzlei Breyer
Schiersteiner Straße 37a
65187 Wiesbaden

Jonas Breyer
Rechtsanwalt
Datenschutzbeauftragter

T +49 611 141 056 89
F +49 611 141 056 90

jbreyer@ra-breyer.de
www.ra-breyer.de

Kanzlei Breyer • Schiersteiner Straße 37a • 65187 Wiesbaden
Deutscher Bundestag
Ausschuss für Inneres und Heimat
Platz der Republik 1
11011 Berlin

22.01.2021

BT-Anhörung am 25.01.2021 (Bestandsdatenauskunft)

Sehr geehrte Damen und Herren,

nachfolgend übersende ich meine erbetene

Sachverständigen-Stellungnahme

im Rahmen der öffentlichen Anhörung zum Gesetzentwurf der Fraktionen der CDU/CSU und SPD „Entwurf eines Gesetzes zur Anpassung der Regelungen über die Bestandsdatenauskunft an die Vorgaben aus der Entscheidung des Bundesverfassungsgerichts vom 27. Mai 2020“ (BT-Drs. 19/25294).

Infolge der Kurzfristigkeit kann die Stellungnahme nur kursorischer Art sein.

Im vorgenannten Verfahren vor dem Bundesverfassungsgericht (1 BvR 1873/13 u. a.) habe ich die Beschwerdeführer anwaltlich vertreten. Der Regierungsentwurf behebt die rechtlichen Mängel auch im zweiten Anlauf nicht vollständig, sondern schafft stattdessen neue behördliche Befugnisse. Eine weitere Verfassungsbeschwerde ist daher absehbar.

Generell ist mit dem Bundesverfassungsgericht daran zu erinnern, dass der Schutz der Vertraulichkeit von Bestandsdaten von hoher Bedeutung ist, weil durch die Identifizierung eines Telefon- oder Internetnutzers die Anonymität der Telekommunikation durchbrochen wird. Durch die Identifizierung von Telefon- oder Internetkennungen lassen sich mittelbar Umstände und Inhalte von Telekommunikationsvorgängen individualisieren, etwa dann, wenn Inhalt oder Zeitpunkt eines bestimmten Anrufs, der unter der abgefragten Nummer geführt wurde, der Behörde durch Vorermittlungen bekannt ist (BVerfG, Beschl. v. 24.01.2012 – 1 BvR 1299/05, „Bestandsdatenauskunft I“, Rn. 114). Als Daten, die die Grundlagen von Telekommunikations-vorgängen betreffen, liegen Bestandsdaten deshalb im Umfeld verfassungsrechtlich besonders geschützter Informationsbeziehungen, deren Vertraulichkeit für eine freiheitliche Ordnung essentiell ist (BVerfG a. a. O., Rn. 137). Dem genügt der vorgelegte Regierungsentwurf nicht.

1. Konkrete Gefahr (Art. 1 [BVerfSchG], 3 [MADG] und 4 [BNDG])

In Bezug auf die Nachrichtendienste des Bundes (Art. 1, 3 und 4 des Änderungsgesetzes) fehlt das Erfordernis einer konkreten oder zumindest drohenden Gefahr für ein spezifiziertes Rechtsgut (Rn. 146 ff. der Entscheidung v. 27.05.2020 – 1 BvR 1873/13 u. a., „Bestandsdatenauskunft II“, nachfolgend „Entscheidung“). Der Entwurf stellt nur auf die vage formulierten Aufgaben der Nachrichtendienste ab. Die amtliche Begründung führt dazu aus, die Nachrichtendienste bezweckten ohnehin den Schutz besonders gewichtiger Rechtsgüter. Diese geringen Anforderungen an den zu normierenden Rechtsgüterschutz lässt das Bundesverfassungsgericht aber nur dann genügen, wenn die

> *„Auskunft zur Aufklärung einer bestimmten, nachrichtendienstlich beobachtungsbedürftigen Aktion oder Gruppierung im Einzelfall geboten ist“,*

weil damit ein

> *„wenigstens der Art nach konkretisiertes und absehbares Geschehen vorausgesetzt“*

werde (Rn. 151 der Entscheidung). Ein solches konkretes Geschehen ergibt sich nicht pauschal aus der allgemeinen Aufgabenbeschreibung gemäß § 3 Abs. 1 BVerfSchG und den fachrechtlichen Parallelvorschriften. Ebenso wenig wird eine Störereigenschaft vorausgesetzt. In eine ähnliche Richtung gehen auch die Bedenken des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI), denen ich mich anschließe.

Als Folgeänderung sind auch die korrespondierenden Übermittlungsregelungen anzupassen.

2. Konkrete Gefahr bei IP-Adressen (Art. 1 [BVerfSchG], 3 [MADG] und 4 [BNDG])

Die Vorschriften für die Nachrichtendienste ermöglichen Bestandsdatenauskünfte auch dann, wenn sie anhand von dynamisch zugeteilten IP-Adressen erteilt werden. Dabei wird auf das Vorliegen einer konkreten Gefahr verzichtet. Wegen des „erhöhten Eingriffsgewichts“ einer solchen Abfrage ist das aber erforderlich und zwar auch für Nachrichtendienste (Rn. 176 der Entscheidung). Zwar bezieht sich das Bundesverfassungsgericht hierbei auf eine Übermittlungsnorm, im konkreten Fall § 113 Abs. 1 TKG. Die Abrufnorm darf aber nicht darüber hinausgehen, anderenfalls ist bereits die Übermittlung unzulässig (Rn. 201 der Entscheidung). Der Entwurf treibt damit sowohl Behörden als auch Diensteanbieter in den Rechtsverstoß.

3. „Mitwirkung an der Mitwirkung“ (Art. 1 [BVerfSchG], 3 [MADG] und 4 [BNDG], 6 [BPolG], 7 [BKAG], 8 [StPO] und 11 [ZFdG])

Der Gesetzentwurf verpflichtet in mehreren Vorschriften, nicht nur bezüglich der Nachrichtendienste, auch diejenigen, die an der Erbringung von Telekommunikationsdiensten „mitwirken“. Wer an Telekommunikationsdiensten mitwirkt, ist aber bereits Telekommunikationsanbieter (§ 3 Nr. 6 TKG). Der Entwurf regelt insoweit eine „Mitwirkung an der Mitwirkung“.

4. Unbestimmte Eingriffsschwellen (Art. 6 [BPolG], 7 [BKAG], 11 [ZfdG], 12 [TMG] und 13 [TKG])

Der Entwurf knüpft an mehreren Stellen die Bestandsdatenauskunft, auch anhand von dynamischen IP-Adressen, an bedrohte

- Rechtsgüter von erheblichem Gewicht,
- Rechtsgüter von hervorgehobenem Gewicht,
- gewichtige Rechtsgüter und
- besonders gewichtige Rechtsgüter.

Diese Terminologie wird zwar vom Bundesverfassungsgericht aus verfassungsrechtlicher Perspektive verwendet, worauf auch die amtliche Begründung verweist (Seite 51). Auch nach der Rechtsprechung des Bundesverfassungsgerichts ist die Zuordnung einzelner Rechtsverstöße zu den jeweiligen Rechtsgütern aber unkonturiert und für den Rechtsanwender unklar. Dabei sollte das Rechtsgut gerade bei den nicht nachrichtendienstlichen Gefahrenabwehrbehörden einzugrenzen sein. Teilweise spricht der Entwurf sogar nur von einer „Gefahr", ohne irgendein Rechtsgut zu nennen, etwa in § 40 BKAG-E. Entsprechendes gilt für Straftaten von „erheblicher Bedeutung".

Es ist nicht Aufgabe der Gerichte, sondern des Gesetzgebers, zu prüfen und zu artikulieren, wofür er die begehrten Bestandsdatenauskünfte benötigt. Dabei kann er zur Vereinfachung auf bestehende Kataloge wie § 100a Abs. 2 StPO zurückgreifen. Kann der Gesetzgeber nicht artikulieren, wozu er die Daten benötigt, sind sie auch nicht erforderlich und die Regelungen sind nicht nur dysfunktional, da unbestimmt, sondern auch unverhältnismäßig.

5. Fehlende Erforderlichkeit (Art. 11 [ZFdG], 12 [TMG] und 13 [TKG])

Nach mehreren Normen muss eine Auskunftsverlangen die Abwehr einer Gefahr nur „zum Gegenstand" haben. Richtigerweise muss sie dafür erforderlich sein. Eine Bezugnahme auf die allgemeinen Aufgaben einer Behörde würde eine Vorratsspeicherung ermöglichen und genügt daher nicht (Rn. 197 der Entscheidung).

6. Zeitlich absehbares Geschehen (Art. 6 [BPolG], 7 [BKAG], 11 [ZFdG], 12 [TMG] und 13 [TKG])

In den genannten Vorschriften knüpft der Entwurf Eingriffe daran, dass

> *„Tatsachen den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen, an dem bestimmte Personen beteiligt sein werden".*

Diese abstrakte Formel wurde aus der Entscheidung des Bundesverfassungsgerichts kopiert (etwa Rn. 148 der Entscheidung). Es ist Aufgabe des Gesetzgebers, sie politisch mit Leben zu füllen und den Zeitfaktor, das Geschehen und die beteiligten Personen konkret zu bestimmen. Anderenfalls drohen erhebliche Rechtsunsicherheit und rechtswidrige Datenverarbeitungen.

7. Unklare Übermittlungsregelungen (Art. 12 [TMG] und 13 [TKG])

Der Entwurf lässt den Rechtsanwender darüber im Unklaren, wie sich die neuen Übermittlungsnormen in §§ 15a, b TMG-E zu den bisherigen Übermittlungsregelungen in § 14 TMG verhalten, die ebenfalls Auskünfte zur Gefahrenabwehr und Strafverfolgung regeln.

Daneben verlangt §15a Abs. 2 TMG-E eine „elektronische“ Bestätigung. Es bleibt unklar, ob beispielsweise die elektronische Form nach § 126a BGB oder nach § 3a VwVfG gemeint ist.

Der Entwurf regelt zudem zwar theoretisch, dass eine Übermittlung nur erfolgen darf, wenn die Voraussetzungen der Abrufnorm erfüllt sind (§ 15a Abs. 6 TMG-E). Nur dann ist die Übermittlung zulässig (Rn. 201 der Entscheidung). Mangels Information hat der Diensteanbieter aber keine Möglichkeit, das Vorliegen der Voraussetzungen zu prüfen, was das verfassungsrechtliche Prinzip der Doppeltür aushöhlt. Auch bei einer Beschlagnahme muss ein überprüfbarer Beschluss vorgelegt werden. Die Diensteanbieter sollten bei dieser Prüfung unterstützt werden, zumal es sich gerade im Bereich von Telemedien überwiegend um Kleinunternehmer und Privatpersonen handelt. Es sollte daher nach § 15a Abs. 2 Satz 1 TMG-E folgender Satz eingefügt werden:

> *„Die ersuchende Stelle hat auch die ernstlich in Betracht kommenden rechtlichen Auskunftstatbestände unter Zitierung der jeweiligen Norm dieses Gesetzes und kurz den zur Prüfung erforderlichen Sachverhalt anzugeben sowie gegebenenfalls die gerichtliche Anordnung zu übermitteln.“*

Zwar hat das Bundesverfassungsgericht entschieden, auch das Vorliegen der Übermittlungs-Voraussetzungen müsse durch die jeweilige Abrufbehörde geprüft werden. Das hat das Gericht aber nicht verfassungsrechtlich, sondern nur anhand des fachrechtlichen Status quo in § 113 TKG begründet (Rn. 202 der Entscheidung).

Soweit § 15a Abs. 6 TMG-E eine Prüfung durch „Fachkräfte“ vorsieht, ist dies lebensfern und sollte dies gestrichen werden. Die Vorstellung, dass es sich etwa bei Betreibern von Websites mehrheitlich um große Anbieter wie Facebook handelt, entspricht nicht der Realität.

Entsprechende Vorschriften wie im TMG-E befinden sich im TKG-E.

8. Nutzungsdaten (Art. 8 [StPO] und 12 [TMG])

Der Gesetzentwurf verpflichtet Anbieter sozialer Netzwerke und anderer Telemediendienste, Auskunft über Bestands- und sogar Nutzungsdaten zu erteilen. Er wird der Tiefe des damit verbundenen Grundrechtseingriffs jedoch nicht gerecht. Möglich ist etwa die Zurückverfolgung der gesamten Aktivitäten eines Benutzers, indem ein Pseudonym in einem Meinungsforum oder sozialen Netzwerk aufgedeckt wird. Gespeichert werden bei solchen Diensten teilweise auch Bestandsdaten wie Krankheiten, sexuelle Orientierung oder Religion, etwa bei Selbsthilfeforen. Denkbar wäre auch eine Verknüpfung anhand sogenannter Browser-Fingerprints, also pseudonym- und sogar personenübergreifender Profile. Anders als in § 100b StPO muss die Stelle nicht einmal einen bestimmten Nutzer nennen, sodass ungezielt Auskünfte über alle Nutzer verlangt werden können. Privilegierungen für Berufsgeheimnisträger oder Presseinformanten fehlen.

Telemedien-Nutzungsdaten beantworten beispielsweise folgende Fragen:

- Welche Internetseiten hat ein Nutzer aufgerufen?
- Welche Suchbegriffe hat er in eine Suchmaschine eingegeben?
- Welche Online-Videos hat er gesehen oder selbst veröffentlicht?
- Welche Artikel welcher politischen Online-Zeitungen hat er abgerufen?
- Welche Nachrichten hat er in einem Online-Chat geschrieben und gelesen?
- Was hat er in einem geschlossenen Aidshilfe- oder Gewerkschaftsforum geschrieben?

Nutzungsdaten sind Telekommunikationsinhalten auch deshalb vergleichbar, weil sie regelmäßig den Inhalt der abgerufenen Informationen erkennen lassen (etwa URLs der gelesenen Internetseiten). Sie können sogar aussagekräftiger sein, da Telefongespräche nicht fixiert werden. Bei der Diskussion über die Praktiken der NSA ist deutlich geworden, dass die im Internet anfallenden „Metadaten“ sogar eine weiter reichende Durchleuchtung unseres Lebens erlauben als eine Auswertung des Inhalts von Individualkommunikation. Ihre automatisierte Zusammenführung ermöglicht die Erstellung umfassender Persönlichkeitsprofile.

Dementsprechend müssen Abruf- und Übermittlungsnormen formell und materiell denselben verfassungsrechtlichen Anforderungen genügen wie die Telekommunikationsüberwachung. Diese ist nur unter engen Voraussetzungen zulässig. Es ist nicht ersichtlich, warum die staatliche Befugnis zur Offenlegung der Internetnutzung weiter reichen dürfte als die Befugnis zur Offenlegung der Telefonnutzung. Im Bereich der Strafverfolgung wären daher die Anforderungen der §§ 100a, b StPO einzuhalten. Im polizeilichen Bereich hat das Bundesverfassungsgericht die Voraussetzungen einer verhältnismäßigen Befugnis zur Telekommunikationsüberwachung bereits geklärt (Az. 1 BvR 668/04), unter anderem bedarf es einer konkreten Gefahr. Im Bereich der Nachrichtendienste wäre eine Öffnung allenfalls unter den Voraussetzungen, in dem Verfahren und nach Maßgabe des G10-Gesetzes denkbar, wobei die Erforderlichkeit nicht ersichtlich ist. Dass verschiedene im Entwurf vorgesehene Abrufnormen an Telemedien- und Telekommunikations-Bestanddaten dieselben Anforderungen stellen, genügt nicht annähernd. Auch fehlt es dem geänderten § 100g StPO an einem abschließenden Straftatenkatalog, wie bei der Telekommunikationsüberwachung erforderlich. Der Kritik des Sachverständigen Prof. Dr. Bäcker ist hier zuzustimmen.

Telemedien ersetzen die klassischen Medien immer mehr und sind in vielen Bereichen unseres Lebens unverzichtbar geworden (etwa Internet-Steuererklärung für Unternehmer). Sie sind vielfach Voraussetzung für die Ausübung grundrechtlich geschützter Freiheiten, besonders des Rechts, seine Meinung in Wort, Schrift und Bild frei zu äußern und zu verbreiten und sich aus allgemein zugänglichen Quellen ungehindert zu unterrichten (Art. 5 GG). Nur umfassende Informationen, die man ungehindert und unbefangen zur Kenntnis nehmen kann, ermöglichen eine freie Meinungsbildung und -äußerung für Einzelne wie für die Gemeinschaft. Nur auf der Grundlage eines freien und unbefangenen Informationszugangs kann der Bürger informiert politisch entscheiden und am freiheitlichen demokratischen Gemeinwesen mitwirken.

Der staatliche Zugriff auf Telemediendaten schon nach bisherigem Recht ist Gegenstand einer weiteren Verfassungsbeschwerde (Az. 1 BvR 1732/14). Der Gesetzentwurf sollte bezüglich der Beauskunftung von Telemediendaten grundsätzlich überdacht werden.

9. Abruf von Zugangsdaten (Art. 6 [BPolG], 7 [BKAG], 8 [StPO], 11 [ZfdG] und 12 [TMG])

Der Entwurf versucht erneut, den Behörden Zugangsdaten wie Passwörter zu verschaffen, ohne darzulegen, in wie vielen und in welchen Fällen neben den übrigen Befugnissen ein praktischer Bedarf danach besteht. Da ein Passwort regelmäßig mehrere Dienste schützt (etwa bieten bestimmte Telekommunikationsanbieter unter einem einheitlichen Kundenpasswort zugleich einen Cloud-Speicher an), drohen unzulässige Datenzugriffe.

Außerdem erweist sich der Entwurf auch hier in zahlreichen Fällen als dysfunktional. Es ist den Anbietern nämlich nach Art. 32 DS-GVO (Datensicherheit) untersagt, Passwörter im Klartext zu speichern, sodass diese nicht herausgegeben werden können. Stattdessen werden regelmäßig abgeleitete Hash-Werte gespeichert, deren Rückrechnung mathematisch unmöglich ist. Die Bedenken des BfDI sind insoweit korrekt. Außerdem müssen Anbieter nach Art. 32 DS-GVO für eine regelmäßige Änderung der Passwörter sorgen, sodass ihre Gültigkeit selbst bei Bekanntheit zeitnah abzulaufen droht. Da Art. 32 DS-GVO keine Öffnungsklausel kennt, können die Mitgliedstaaten dies auch nicht ändern. Der deutsche Gesetzgeber kann sich auch nicht dem Anwendungsbereich des europäischen Rechts entziehen. Denn der Europäische Gerichtshof hat im Zusammenhang mit der britischen Vorratsdatenspeicherung entschieden, dass eine alleinige Kompetenz der nationalen Mitgliedstaaten nach Art. 4 Abs. 2 EUV (nationale Sicherheit) jedenfalls dann nicht bestehe, wenn eine Datenverarbeitung zwar staatlichen Sicherheitszwecken diene, sie aber durch verpflichtete Privatanbieter erfolge (EuGH, Urt. v. 06.10.2020 – C-623/17, „Privacy International“, Rn. 30 ff.). Ähnliche Bedenken äußert zutreffend auch der Sachverständige Prof. Dr. Bäcker. Die Befugnisse bieten daher ein großes Schadpotential bei geringem Nutzen und sind als unverhältnismäßig zu streichen.

10. Fehlende Statistik (Art. 12 [TMG] und 13 [TKG])

Der Entwurf regelt keine statistischen Aufzeichnungspflichten, um die Erforderlichkeit manueller Bestandsdatenabfragen zu prüfen, obwohl der Datenzugriff erneut ausgeweitet werden soll. Eine statistische Erfassung der staatlichen Bestandsdatenabfragen ist für eine wissenschaftliche Prüfung und öffentliche Kontrolle der Grundrechtseingriffe unerlässlich. Die Anzahl der getätigten Zugriffe muss der Öffentlichkeit zugänglich gemacht und transparent gemacht werden, damit das Ausmaß der Eingriffe für die Bürger nachvollziehbar sind. Auch die Entwicklung der Nutzung der Zugriffsbefugnisse kann so nachverfolgt werden, und es kann eine übergriffige Nutzung erkannt werden. Dazu ist es notwendig, derartige Daten genau nach Abfragegrund, abfragende Behörde und weiteren Daten aufzuschlüsseln. Zwar ist der Gesetzgeber nicht allgemein verpflichtet, Eingriffe in das Recht auf informationelle Selbstbestimmung statistisch erfassen zu lassen. Im vorliegenden Fall handelt es sich aber um Eingriffe in die Vertraulichkeit von Telekommunikationsverhältnissen, darunter die Identifizierung von Internetnutzern und die Anforderung von Codes zur Überwindung von Zugangssicherungen.

Aus dem verfassungsgerichtlichen Verfahren ist mir bekannt, dass, soweit denn Zahlen rekonstruiert werden konnten, sich etwa in den Jahren 2013 bis 2017 manuelle IP-Abfragen durch das BKA von 2001 auf 17428 Fälle vervielfacht haben, während Zugangsdatenabfragen

in den insoweit beauskunfteten Jahren 2016 bis 2018 durch den BND und den MAD in null Fällen erfolgten (undatierter Schriftsatz der Bundesregierung mit Gerichts-Eingangsstempel vom 24.12.2018). Für automatisierte Abfragen nach § 112 TKG besteht eine solche Statistik.

Dem sollte abgeholfen werden, indem in Anlehnung an den Quick-Freeze-Referentenentwurf des Bundesjustizministeriums eine Statistik über die Identifizierung von Internetnutzern geführt wird, sodass der Gesetzgeber die Entwicklung der Fallzahlen beobachten kann (§ 100k Abs. 4 StPO-Ref-E, „Gesetz zur Sicherung vorhandener Verkehrsdaten und Gewährleistung von Bestandsdatenauskünften im Internet“). Es sollte daher folgender neuer Absatz in die jeweiligen Übermittlungsnormen (TMG, TKG) eingefügt werden:

> *„Über die Übermittlungen nach dieser Vorschrift erstellen der Bund und die Länder entsprechend § 101b der Strafprozessordnung jährlich eine Übersicht, in der anzugeben sind*
>
> 1. *die Anzahl der Verfahren, in denen Bestandsdaten übermittelt wurden,*
> 2. *die Anzahl der Verfahren, in denen Nutzungsdaten übermittelt wurden,*
> 3. *die Anzahl der Internetprotokoll-Adressen, zu denen um Auskunft ersucht wurde,*
> 4. *die Anzahl der Verfahren, in denen Passwörter oder andere Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird, übermittelt wurden,*
>
> *jeweils unterschieden danach, durch welche Behörde und aufgrund welcher genauen fachrechtlichen Abrufvorschrift die Abrufe erfolgten, nach Festnetz-, Mobilfunk- und Internettelekommunikation, weiterhin im Fall der Nr. 3 nach dem Alter. Das Alter bestimmt sich danach, wie viele Tage zwischen dem Zeitpunkt der Anordnung und dem in der Anordnung genannten Zeitpunkt, zu dem die Internetprotokoll-Adresse vergeben war, liegen. In der nach dieser Vorschrift zu erstellenden Übersicht ist das Alter für den Zeitraum bis zu einer Woche taggenau, bis zu einem Monat wochenweise und für darüber hinausgehende Zeiträume monatsweise zu erfassen. Das Bundesamt für Justiz erstellt eine Gesamtübersicht zu den im Berichtsjahr bundesweit durchgeführten Übermittlungen, aufgeschlüsselt nach den vorgenannten Merkmalen, und veröffentlicht diese im Internet.“*

Mit freundlichem Gruß

Jonas Breyer
(Rechtsanwalt)