

WIEN / 23. September 2018

# Stellungnahme zur Novelle des Telekommunikations- gesetzes 2003 (257 d.B., XXVI. GP)

**Kritikpunkte am Entwurf des  
Ministerrates**

**Für epicenter.works**

Mag.<sup>a</sup> Angelika Adensamer, MSc  
Ing. Dr. Christof Tschohl

 **EPICENTER  
WORKS**  
for digital rights



# NEUE FORM DER VORRATSDATENSPEICHERUNG DROHT

Die Grundrechtsorganisation epicenter.works hat bereits Ende Juli im Begutachtungsprozess zur Novelle eine Stellungnahme abgegeben<sup>1</sup>. Im Ministerratsentwurf sind im Vergleich zur Version, die in Begutachtung war, einige problematische Passagen enthalten, die auf eine neue Form der Vorratsdatenspeicherung hinauslaufen können. Konkret geht es um Bestimmungen, die IP-Adressen als Stammdaten definieren und Speicherverpflichtungen dafür vorsehen. Anbieter von Kommunikationsdiensten müssen nach diesen Bestimmungen dynamische IP-Adressen auf Ersuchen von Behörden zur Aufklärung eines konkreten Verdachts einer Straftat (ohne weitere Einschränkung z.B. nach der Schwere der Straftat) herausgeben. Dafür ist keine gerichtliche Bewilligung oder staatsanwaltschaftliche Anordnung nötig.

Vorratsdatenspeicherung ist eine anlasslose Massenüberwachung, die nach einem Urteil des Europäischen Gerichtshofes unzulässig ist. Dieses richtungsweisende Urteil aus dem April 2014<sup>2</sup> muss auch in diesem Zusammenhang beachtet werden.

epicenter.works warnt eindringlich vor einer Einführung einer neuen Form der Vorratsdatenspeicherung und fordert die Bundesregierung auf, die entsprechenden Passagen so zu formulieren, dass diese verhindert wird.

## Inhaltsverzeichnis

Neue Form der Vorratsdatenspeicherung droht.....	2
Stellungnahme zum Bundesgesetz, mit dem das Telekommunikationsgesetz 2003 geändert wird.....	3
Problematische Definition von IP-Adressen als Stammdaten.....	3
Z 87: IP-Adressen als Stammdaten (§ 92 Abs 3 Z 16a TKG).....	3
Speicherung von IP-Adressen.....	4
Z 104: Speicherung von IP-Adressen (§ 99 Abs2 TKG).....	4
Keine Vorratsdatenspeicherung durch die Hintertür!.....	4

1 epicenter.works: Stellungnahme zum Telekommunikationsgesetz 2003: <https://epicenter.works/document/1266>

2 Siehe: <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A62012CJ0293>

# STELLUNGNAHME ZUM BUNDESGESETZ, MIT DEM DAS TELEKOMMUNIKATIONSGESETZ 2003 GEÄNDERT WIRD

Der der exakte Titel Regierungsvorlage, die das BMVIT (Bundesministerium für Verkehr, Innovation und Technologie) am 05. September 2018 vorgelegt hat, lautet: *Bundesgesetz, mit dem das Telekommunikationsgesetz 2003, das Funkanlagen-Marktüberwachungs-Gesetz, das Funker-Zeugnisgesetz 1998, das Postmarktgesetz, das Gebäude- und Wohnungsregister-Gesetz und das KommAustria-Gesetz geändert werden*. Der Text ist auf der Website des österreichischen Parlaments zu finden.<sup>3</sup> Die in diesem Dokument aufgeführten Kritikpunkte beziehen sich ausschließlich auf die Passagen, die die Definition von IP-Adressen als Stammdaten und ihre Speicherung regeln.

## Problematische Definition von IP-Adressen als Stammdaten

### Z 87: IP-Adressen als Stammdaten (§ 92 Abs 3 Z 16a TKG)

Mit dem vorliegenden Entwurf sollen nun auch dynamische IP-Adressen als Stammdaten iSd § 92 Abs 3 Z 3 TKG definiert werden und damit der Auskunftspflicht nach § 76a Abs 1 StPO unterliegen (siehe auch die Erläuterungen zum vorliegenden Entwurf, S. 16). So werden nach § 90 Abs 7 TKG iVm § 76a Abs 1 StPO Anbieter von Kommunikationsdiensten nun verpflichtet, auch dynamische IP-Adressen auf Ersuchen von kriminalpolizeilichen Behörden, Staatsanwaltschaften und Gerichten, zur Aufklärung eines konkreten Verdachts einer Straftat (ohne weitere Einschränkung z.B. nach der Schwere der Straftat) herauszugeben. Hierzu ist keine gerichtliche Bewilligung oder staatsanwaltschaftliche Anordnung notwendig. In dieser Form ist diese Befugnis jedenfalls unverhältnismäßig. Damit werden die Befugnisse nach der StPO massiv ausgeweitet, ohne dass dies im Kontext der gesamten StPO verhandelt wurde.

Wir kritisieren, dass die Definition von dynamischen IP-Adressen als Stammdaten erst nach dem abgeschlossenen Begutachtungsverfahren in den Text eingeflossen ist. Damit wurde eine Debatte über diese folgenreiche Änderung verunmöglicht.

Dagegen wird eine Auskunft von dynamischen IP-Adressen nach § 90 Abs 7 TKG iVm § 53 Abs 3a Z 1 SPG auch weiterhin nicht möglich sein, da IP-Adressen unter die Voraussetzungen der § 53 Abs 3a Z 2 und Z 3 fallen und daher e contrario nicht unter Z 1 fallen.

Auch eine Auskunft nach § 90 Abs 6 TKG ist weiterhin über dynamische IP-Adressen nicht möglich, da an dieser Stelle ausdrücklich auf Stammdaten im Sinne von § 92 Abs 3 Z 3 lit a bis e abgestellt wird, worunter auch nach dem vorliegenden Entwurf dynamische IP-Adressen nicht fallen werden.

Nach der heutigen Rechtsauffassung unterliegen dynamische IP-Adressen, die als Zugangs- und Verkehrsdaten gelten (siehe OGH 4Ob41/09x vom 14.07.2009, 5.3.2. mwN), jedenfalls dem Kommunikationsgeheimnis nach § 93 TKG. Dass IP-Adressen nun zusätzlich auch als Stammdaten gelten, ändert grundsätzlich an dieser Rechtslage nichts. Dies sollte aber aufgrund der hohen Sensibilität von dynamischen IP-Adressen für diese eindeutig klargelegt werden.

<sup>3</sup> Text der Regierungsvorlage: <https://www.parlament.gv.at/PAKT/VHG/XXVI/II/00257/index.shtml>

Dynamische IP-Adressen können intime Einblicke und das Leben und die Persönlichkeit von Personen bieten und ihr Schutz kann im Hinblick auf die Judikatur zu Art 8 EMRK nicht geschwächt werden (siehe zB Benedik vs. Slowenien, EGMR 24.4.2018<sup>4</sup>, Big Brother Watch vs. UK, 13.9.2018, Rz 356<sup>5</sup>). Vor nicht einmal zwei Wochen, am 13. September 2018 hat nun auch der EGMR in seiner Entscheidung Big Brother Watch vs. UK festgestellt, dass Verkehrsdaten nicht völlig von den Voraussetzungen, Kontroll- und Schutzmechanismen, die für Inhaltsdaten gelten, ausgeschlossen werden können (s Big Brother Watch vs. UK, 13.9.2018, Rz 357). Im Lichte dieser Rechtsprechung erscheint die mit dem vorliegenden Gesetzesvorschlag erzielte Ausweitung des § 76a StPO ohne Richtervorbehalt und sogar ohne die zwingende Voraussetzung einer Anordnung durch die StA grundrechtswidrig.

## Speicherung von IP-Adressen

### Z 104: Speicherung von IP-Adressen (§ 99 Abs2 TKG)

Mit dieser neuen Bestimmung sollen Betreiber eines öffentlichen Kommunikationsnetzes verpflichtet werden, zu Zwecken der Verrechnung von Entgelten IP-Adressen *„die eindeutige Zuordenbarkeit eines Kommunikationsvorgangs zu einem Teilnehmer, dem eine IP-Adresse zu einem bestimmten Zeitpunkt unter der Angabe der zugrundeliegenden Zeitzone zugeteilt war, sicherzustellen.“*

Soweit diese Zuordenbarkeit aber für die Verrechnung von Entgelten nicht notwendig ist – was regelmäßig der Fall sein wird – muss sie auch in Zukunft nicht gegeben sein. Es sollte daher gesetzlich klargestellt werden, dass auch weiterhin keine Verpflichtung besteht, dynamische IP-Adressen, zu speichern, wenn diese nicht für die Zwecke der Verrechnung notwendig sind (und daher keine Speicherverpflichtung nach § 100 Abs 1a TKG besteht) noch andere handelsrechtliche oder steuerrechtliche Speicherverpflichtungen bestehen, da sie für die Erfüllung der Vertrags- und damit einhergehenden gesetzlichen Pflichten nicht notwendig sind.

Ebenso muss klargestellt werden, dass die Löschverpflichtung nach § 99 Abs 1 TKG, die normiert, dass nach der Beendigung der Verbindung Verkehrsdaten unverzüglich zu löschen oder zu anonymisieren sind, auch nach diesem Entwurf noch für dynamische IP-Adressen gelten würde, da mit der Eigenschaft als Stammdatum die als Verkehrsdatum nicht automatisch verloren geht (arg: „(...) handelt es sich *zugleich* um ein Stammdatum (...)“ so der „sinngemäß“ geltende letzte Halbsatz des § 92 Abs 3 Z 16 TKG).

# KEINE VORRATSDATENSPEICHERUNG DURCH DIE HINTERTÜR!

### Klarstellung dringend nötig

Die in dieser Stellungnahme angesprochenen Unklarheiten müssen dringend beseitigt werden. Ansonsten besteht die Gefahr, dass der bestehende Schutz des Telekommunikationsgeheimnis im Hinblick auf dynamische IP-Adressen völlig ausgehöhlt wird und aufgrund der Definition der

4 Judgment Benedik v. Slovenia - police's accessing subscriber info via dynamic IP address: <https://hudoc.echr.coe.int/app/conversion/pdf?library=ECHR&id=003-6069932-7814155&filename=Judgment%20Benedik%20v.%20Slovenia%20-%20police%27s%20accessing%20subscriber%20info%20via%20dynamic%20IP%20address.pdf>

5 Big Brother Watch and Others v. the United Kingdom - complaints about surveillance regimes: <https://hudoc.echr.coe.int/app/conversion/pdf?library=ECHR&id=003-6187848-8026299&filename=Big%20Brother%20Watch%20and%20Others%20v.%20the%20United%20Kingdom%20-%20complaints%20about%20surveillance%20regimes.pdf>

dynamischen IP-Adressen als „Stammdaten“ kein Schutz und keine Grenzen mehr bestehen. Besonders problematisch wäre ein Verständnis, wonach allein durch das Schlagwort „Stammdaten“ eine 7-jährige (handelsrechtliche oder steuerrechtliche) Aufbewahrungspflicht angenommen wird. **Damit würde eine 7-jährige Vorratsdatenspeicherung der Internetnutzung sozusagen durch die Hintertür eingeführt. Entsprechende Abgrenzungen sind daher aus rechtsstaatlicher Sicht dringend geboten.**