**Freifunk Hamburg**

Beim CCC Hansestadt Hamburg e.V.
Humboldtstraße 53-55
22083 Hamburg

Mobil (A. Schmidt): +49 151 26614250

E-Mail: kontakt@hamburg.freifunk.net

Freifunk Hamburg, CCC Hansestadt Hamburg e.V.

Humboldtstraße 53-55, 22083 Hamburg

Frau/Herr X

Deutscher Bundestag

Platz der Republik 1

11011 Berlin

Hamburg, 14. Juni 2015

**Entwurf eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten**

Sehr geehrte/r Frau/Herr X,

nachdem wir uns in unserem Schreiben vom 15. März bereits äußerst besorgt wegen des "Re­ferentenentwurfs eines Zweiten Gesetzes zur Änderung des Telemediengesetzes" in Bezug auf seine Auswirkungen auf freie Netzwerke an Sie persönlich gewandt haben, sehen wir nun mit mindestens ebenso großer Besorgnis den "Entwurf eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten" des BMJV.

Die in diesem Gesetzesentwurf verwendete Terminologie der "Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten" ist schlicht für ein Synonym der Vorratsdatenspeiche­rung (VDS). Dementsprechend werden wir im Folgenden nur noch von Vorratsdatenspeiche­rung sprechen.

In Hamburg gibt es mittlerweile über 800 öffentliche, unbegrenzt kostenlose und freie WLAN Zugangspunkte[[1]](#footnote-1) über Freifunk, die überwiegend von Privatpersonen, kleinen Gewerbetreibenden und Vereinen betrieben werden. Die Einführung einer Speicherpflicht für Freifunker\_innen widerspricht den Festlegungen des Koalitionsvertrags, der die Förderung ebensol­cher "[...] heterogener, frei vernetzter und lokaler Communities und ihrer Infrastrukturen [...]" in Aussicht stellt (Koalitionsvertrag zwischen CDU/CSU und SPD, Abschnitt Wachstum, Innovation und Wohlstand, Unterabschnitt Digitale Infrastruktur)[[2]](#footnote-2).

Die Speicherung von nutzerbezogenen Daten, wie sie durch den vorliegenden Gesetzentwurf vorgeschrieben wird, ist nicht mit dem Betrieb freier Netze vereinbar. Sie ist technisch und wirtschaftlich für das nach dem "Mitmach-Prinzip" aufgebaute Freifunk-Netzwerk nicht durchführbar und würde das seit Jahren bestehende ehrenamtliche Engagement der Freifunker\_innen mit dem Inkrafttreten des Gesetzes vernichten. Kurzum: Die Wiedereinführung der VDS in der intendierten Form würde das sofortige Aus sämtlicher Freifunk-Pro­jekte nicht nur in Hamburg, sondern deutschlandweit bedeuten. Das betrifft dann ca. 14.000 Zugangspunkte und damit fast alle in Deutschland verfügbaren offenen WLANs (ca. 15.000).

Im Detail sehen wir folgende Probleme mit dem vorliegenden Gesetzesentwurf:

Mit der VDS wird einmal mehr die Totalüberwachung aller Kommunikationswege eingeführt. Nicht nur die einfachen Bürger sind bereits heute von der Überwachung betroffen: Auch Abgeordnete sind betroffen, wie Thomas Jarzombek (CDU) über die Überwachung der Bundestags IT feststellt: "Wir können zu diesem Zeit­punkt nicht sicher sein, dass diese vertraulichen Daten vor Zugriffen geschützt sind." und "Wenn man sich vorstellt, dass wir einmal in weniger demokratischen Zeiten leben könnten, sind die Abgeordneten wie ein offenes Buch"[[3]](#footnote-3). Weiter führt Lars Klingbeil (SPD) an: "Ich frage mich: Wie ist das eigentlich vereinbar mit dem freien Mandat. Es müssen sich ja schließlich auch Bürger vertraulich an uns wenden können". Bei der geplanten Einführung der VDS stellen sich die Probleme des Schutzes von erfassten Daten und eines zukünftigen Miss­brauchspotenziales, sowie der vertraulichen Kommunikation mit Abgeordneten (Daten sollen bei der VDS zumindest mit erfasst werden) in noch größerem Umfang, da sie nicht auf die IT-Infrastruktur des Bundestages beschränkt sind.

Die VDS bezieht sich allerdings nicht nur auf Abgeordnete, sondern natürlich auf alle Einwoh­ner. Berufsgeheimnisträger sollen von der Auswertung der Daten nicht betroffen sein. Ihre Daten werden aber gleichwohl gespeichert und liegen damit prinzipiell für spätere Zugriffe vor, da sich kein sinnvoller Ausschluss der Daten solcher Personen umsetzen lässt. Die Spei­chersysteme „wissen nicht“, dass es sich bei einem Verbindungspartner um einen Berufsgeheimnisträger handelt. Missbrauch ist hiermit Tür und Tor geöffnet, da davon auszugehen ist, dass vorliegende Daten auch genutzt werden. Zudem sind eben diese Berufsgeheimnisträger nicht scharf definiert. Der Begriff Journalist beispiels­weise ist nicht geschützt. Quellenschutz kann deshalb nicht mehr gewährleistet werden, was einen massiven Eingriff in die Pressefreiheit bedeutet. Für potentielle Presseinformanten wird die Hemmschwelle zur Informationsweitergabe erhöht.

Es entstehen lückenlose Bewegungsprofile aller Bürger die in irgendeiner Form elektronische Kommunikation nutzen, sowie deren kompletter sozialer Graph[[4]](#footnote-4). Eindrucksvoll stellen dies die Daten der Abgeordneten Malte Spitz[[5]](#footnote-5), Ton Siedsma[[6]](#footnote-6) und Balthasar Glättli[[7]](#footnote-7) dar.

Der als Kontrollmechanismus angedachte Richtervorbehalt ist ein Placebo. Zunächst bezieht er sich nicht auf die Bestandsdatenauskunft. Allein im Jahr 2014 gab es laut BNetzA 7 Mio Bestandsdatenabfragen von sog. Bedarfsträgern, die sich nicht nur aus Strafermittlungsbehörden zusammensetzen. Das bedeutet eine Bestandsdatenauskunft alle fünf Sekunden. Zudem zeigt die ebenfalls unter Richtervorbehalt stehende Funkzellenabfrage (FZA) sowie die Tele­kommunikationsüberwachung (TKÜ), dass Richter mit schieren Massen an Anfragen überfordert sind (6,5 Mio. Datensätze allein in Berlin zwi­schen 2009 und 2012)[[8]](#footnote-8). In der Rechtspraxis führt dies zum ungeprüften „Durch­winken“ derlei Anfragen.

Das Deutsche Institut für Menschenrechte weist zutreffend darauf hin, dass grausame Attentate, wie jüngst auf die Redaktion des Satiremagazins Charlie Hebdo in Paris geschehen, nur allzu willkommen sind, um tiefgreifende Grundrechtseingriffe zu legitimieren[[9]](#footnote-9). Bitte lassen Sie sich hiervon nicht beeindrucken. Studien, die einen Sicherheitszuwachs durch VDS belegen, existieren nicht. Im Gegenteil hat das Max-Planck-Institut für ausländisches und In­ternationales Strafrecht festgestellt, dass VDS de facto nicht zu mehr Aufklärung geführt hat[[10]](#footnote-10). Auch die Argumentation, durch VDS könnten Terroranschläge verhindert werden, erweist sich - wie die Studie zeigt - bei Lichte betrachtet nicht als wahr. Insgesamt beruht das Sicherheitsargument empirisch be­trachtet ausschließlich auf Spekulationen.

Ferner kann eine vollständige Datensicherheit nicht garantiert werden. Jedes computertechni­sche System ist - nicht nur theoretisch - angreifbar. Die Datensicherheit wird in die Verant­wortung der (notwendigerweise profitorientiert arbeitenden) Internet-Provider gelegt, die für die Speicherung zuständig sind. Nicht nur das Abgreifen der Daten durch Unbefugte stellt einen schweren Eingriff in die Persönlichkeitsrechte der Betroffenen dar. Auch die Manipula­tionsmöglichkeiten eröffnen Kriminellen die Möglichkeit, das „digitale Leben“ der Betroffe­nen zu verfälschen, die in einem möglichen (straf-)gerichtlichen Verfahren praktisch niemals eine erfolgte Manipulation und damit die Unrichtigkeit der Daten beweisen könnten.

Zuletzt überzeugt die Neuregelung auch vor dem Hintergrund der Entscheidungen des BVerfG und des EuGH nicht. Dass die intendierte Regelung die richterlichen Erwägungen in wesentlichen Teilen außer Acht lässt, wurde in den vergangen Wochen schon häufig erwähnt, allen voran von der Bundesdatenschutzbeauftragten Voßhoff[[11]](#footnote-11). Dies dürfte selbst der Bundes­regierung bekannt sein und sei daher hier nur der Vollständigkeit halber erwähnt.

Vor diesem Hintergrund bitten wir Sie, im anstehenden Beratungs- und Abstimmungsverlauf die vorstehenden Punkte zu berücksichtigen und Ihre Fraktionskolleginnen und -kollegen auf die Gefahren der VDS aufmerksam zu machen. Wir hoffen, dass Freifunker\_innen auch in Zukunft ihr freiwilliges Engagement für die Allgemeinheit fortsetzen dürfen. Dafür bitten wir Sie um Mithilfe. Selbstverständlich stehen wir Ihnen und Ihrer Fraktion jederzeit für per­sönliche Gespräche sowie als Sachverständige zur Verfügung.

Für Freifunk Hamburg mit freundlichen Grüßen,

Leo Krüger Andre Schmidt

1. https://map.hamburg.freifunk.net [↑](#footnote-ref-1)
2. https://www.cdu.de/sites/default/files/media/dokumente/koalitionsvertrag.pdf [↑](#footnote-ref-2)
3. http://www.spiegel.de/politik/deutschland/fall-edathy-unmut-ueber-interne-vorratsdatenspeicherung-im-bundestag-a-969541.htmtl [↑](#footnote-ref-3)
4. Ein sozialer Graph stellt dar, mit welchen Personen eine Person wie oft kommuniziert und zu welchen Gruppen diese Personen zuzuordnen sind. So lässt sich allein aus Metadaten erheben mit welchen Themen sich eine Person beschäftigt und welchen Stellenwert die einzelnen Themen für sie einnehmen. [↑](#footnote-ref-4)
5. http://www.zeit.de/datenschutz/malte-spitz-vorrats­daten [↑](#footnote-ref-5)
6. https://netzpolitik.org/2014/metadaten-wie-dein-unschuldiges-smart­phone-fast-dein-ganzes-leben-an-den-geheimdienst-uebermittelt/ [↑](#footnote-ref-6)
7. https://apps.opendatacity.de/vds/ [↑](#footnote-ref-7)
8. http://www.lto.de/recht/hintergruende/h/funkzellenabfragen-in-berlin-datenschutz/ [↑](#footnote-ref-8)
9. http://www.institut-fuer-menschenrechte.de/aktuell/news/meldung/article/pressemitteilung-zum-europaeischen-datenschutztag-am-28-januar-institut-warnt-vor-neuauflage-der/ [↑](#footnote-ref-9)
10. https://www.mpg.de/5000721/vorratsdatenspeicherung.pdf [↑](#footnote-ref-10)
11. http://www.bfdi.bund.de/DE/Infothek/Pressemitteilungen/2015/15\_VDS.html [↑](#footnote-ref-11)