Dirk Fischer
Mitglied des Deutschen Bundestages

Dirk Fischer, MdB • Platz der Republik 1 • 11011 Berlin

Freifunk Hamburg
CCC Hansestadt Hamburg e.V.
Humboldstraße 53-55
22083 Hamburg

Berlin

Platz der Republik 1
11011 Berlin

Unter den Linden 71
Raum 324
Telefon: 030/227-77031
Fax: 030/227-76031
E-Mail:
dirk.fischer@bundestag.de

Wahlkreis

Leinpfad 74
22299 Hamburg
Telefon: 040/477055
Fax: 040/483051
E-Mail:
dirk.fischer.wk@bundestag.de

Berlin, 29.06.2015

Ihr Schreiben vom 12.06.2015

Sehr geehrter Herr Krüger,
sehr geehrter Herr Schmidt,

auch für Ihren Brief zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten, der sog. "Vorratsdatenspeicherung" (VDS), danke ich Ihnen und antworte Ihnen im Namen der Kolleginnen und Kollegen der CDU-Landesgruppe Hamburg.

Als Mitglied des Ausschusses für Verkehr und Digitale Infrastruktur des Deutschen Bundestages bearbeite ich dieses Thema nicht selbst, aber kann Ihnen nach Rücksprache mit der Arbeitsgruppe Recht der CDU/CSU-Fraktion folgende Erläuterungen zur Thematik geben:

Am 27. Mai 2015 hat das Bundeskabinett den Entwurf eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten beschlossen. Eine erste Debatte fand am 12.06.2015 im Deutschen Bundestag statt.

Im Mittelpunkt des geplanten Gesetzesentwurfs des Bundesministers der Justiz und für Verbraucherschutz soll die bessere Bekämpfung terroristischer Straftaten und schwerer Kriminalität stehen. Hier geht es um schwerwiegende Rechtsverletzungen, bei denen es oft keine anderen erfolgversprechenden Ermittlungsansätze gibt. Bundesjustizminister Maas nennt daher das Gesetz „einen fairen Kompromiss zwischen Bürgerrechten und effektiver Strafverfolgung".

Dirk Fischer
Mitglied des Deutschen Bundestages

Der Gesetzentwurf wird erst nach der Sommerpause in 2. und 3. Lesung im Bundestag beraten werden. Zuvor wird er Thema einer intensiven Debatte u.a. im Rechts- und Innenausschuss des Bundestages werden. Auch die zunächst für den 15.06.2015 vorgesehene öffentliche Anhörung im federführenden Ausschuss für Recht und Verbraucherschutz wird erst im September stattfinden.

Nur wenn ganz bestimmte Voraussetzungen in dem Gesetzesentwurf erfüllt sind, die ich Ihnen im Folgenden gerne skizziere, sehe ich mich persönlich imstande, dem Gesetzesvorschlag zuzustimmen.

Die geplante gesetzliche Regelung erfordert eine Abwägung zwischen Freiheits- und Sicherheitsaspekten, deren Gewährleistung gleichermaßen zu den Aufgaben des Staates gehören. Ich versichere Ihnen: Das in der EU-Grundrechtecharta verankerte Grundrecht auf Achtung des Privatlebens und Schutz personenbezogener Daten hat auch für mich einen hohen Stellenwert.

Richtig ist, dass in der angeordneten Speicherung von Verbindungsdaten und im Einzelfall erfolgenden Kenntnisnahme von Kommunikationsdaten ein mittelbarer Grundrechtseingriff liegt, der klare Regeln zu Datensicherheit, Umfang der Datenverwendung, Löschung, Transparenz und Rechtsschutz erfordert und der sorgsam gegenüber der staatlichen Pflicht zur Strafverfolgung bei begangenen Straftaten sowie zum Schutz der Bürger vor Straftaten den Zwecken der Strafverfolgung und Gefahrenabwehr abgewogen werden muss.

Klare Regeln zu Datensicherheit, Umfang der Datenverwendung, Löschung, Transparenz und Rechtsschutz werden erforderlich sein. Ein diffuses Gefühl von Bedrohung und Überwachung wäre freiheitswidrig und darf nicht entstehen.

Entscheidend wird daher sein, dass eine Regelung getroffen wird, welche die Nutzung der gespeicherten Verbindungsdaten in einer sprachlich unmissverständlichen Weise **unter Beachtung der Maßgaben des EuGH und des BVerfG** regeln wird.

Praktiker aus den Ermittlungsbehörden sowie die meisten Innenminister der Länder weisen auf die Notwendigkeit der Speicherung von Verbindungsdaten hin. Bei der Aufklärung von Gewaltverbrechen, bei denen das Internet als Tatmittel genutzt wurde, zum Beispiel bei Kinderpornographie, sollen die gespeicherten Verbindungsdaten in besonderem Maße helfen. Das gleiche gilt bei der Verfolgung schwerer Straftaten, wie Mord, Totschlag oder Vergewaltigung, und terroristischer Verbrechen, zur Namhaftmachung von Mitgliedern terroristischer Netzwerke oder von solchen in der Organisierten Kriminalität.

Dirk Fischer
Mitglied des Deutschen Bundestages

In diesen Fällen ist die aufgezeichnete IP-Adresse oftmals der erste und zunächst einzige erfolgversprechende Ermittlungsansatz für weitere Maßnahmen und daher unverzichtbar. In erster Linie ist die Vorratsdatenspeicherung nicht allein eine Frage der Prävention, sondern sie ist ein Instrument für die bessere Ermittlung nach einer (repressiv). Die Auswertung der Kommunikationsverbindungsdaten kann die Strafverfolgungsbehörden in die Lage versetzen, zum Beispiel die Hintermänner, Gehilfen und ganze kriminelle Netzwerke zu ermitteln. Gelingen solche Ermittlungen, können auch weitere Straftaten verhindert werden.

Nach statistischen Erhebungen des Bundeskriminalamts aus dem Jahr 2010 zu über 1.000 Auskunftsersuchen bei Kommunikationsanbietern, waren die Daten in 80 Prozent der Fälle nicht verfügbar. Das führte dazu, dass bezogen auf diese 1.000 Fälle Straftaten in rund 56 Prozent der Fälle gar nicht, in 18 Prozent der Fälle nur unvollständig und in 25 Prozent der Fälle stark verspätet aufgeklärt werden konnten. Auch wenn neuere statistische Auswertungen nicht vorliegen, hat sich an der Situation seitdem nichts geändert. Die Vorratsdatenspeicherung würde die Aufklärung also erheblich erleichtern, in vielen Fällen überhaupt erst möglich machen.

Die CDU/CSU-Bundestagsfraktion will die Bürger bestmöglich schützen und befürwortet daher eine gesetzliche Grundlage für die Speicherung von Verbindungsdaten. Es geht dabei vor allem um Daten, die die Telekommunikationsunternehmen schon heute zum Beispiel für die Telefonrechnung speichern. Die Übermittlung und Verwendung dieser Daten durch staatliche Ermittlungsbehörden darf nur anlassbezogen erfolgen. Sie setzt den Verdacht einer gesetzlich definierten Straftat oder konkreten Gefahr voraus. Ohne einen solchen Anlass – also in aller Regel - werden die Daten nach der festgesetzten Frist ohne weitere Nutzung schlicht bei den Providern gelöscht; keine staatliche Stelle bekommt sie jemals zu sehen. Damit besteht ein entscheidender Unterschied gegenüber Datensammlungen von Google, Facebook, Payback etc., die die Daten in ihrer Gesamtheit gerade zu dem Zweck erheben, diese umfassend z.B. zu Werbezwecken auszuwerten und möglichst viel über möglichst viele Nutzer zu erfahren.

Es muss daher gelingen, die notwendige und gebotene Balance zwischen Freiheit und Sicherheit zu wahren. Bundesverfassungsgericht und der Europäische Gerichtshof haben der Vorratsdatenspeicherung nicht generell eine Absage erteilt, sondern einen Rahmen für eine rechtliche Regelung gesetzt. Die grundrechtssensiblen Vorgaben des Bundesverfassungs-gerichts will die Bundesregierung zügig umsetzen.

Dirk Fischer
Mitglied des Deutschen Bundestages

Die Leitlinien zur Einführung einer Speicherpflicht sehen dementsprechend vor, dass die IP-Adressen und Verbindungsdaten höchstens zehn Wochen gespeichert werden dürfen. Nach Ablauf der Speicherfrist müssen die Daten sofort gelöscht werden. Hält sich ein Provider nicht daran, wird dies mit einem Ordnungsgeld belegt. Komplett von der Speicherung ausgenommen werden sollen E-Mails. Standortdaten sollen maximal vier Wochen gespeichert werden. Auf sie darf nur vereinzelt zugegriffen werden; Bewegungsprofile sind nicht möglich. Die Daten müssen im Inland gespeichert werden. Nur zur Klärung schwerer Straftaten darf auf die Daten zugegriffen werden. Berufsgeheimnisträger werden besonders geschützt. Bei der Speicherung der Daten gilt die höchste Sicherheitsstufe für Provider. Um Strafbarkeitslücken zu schließen, wird zudem die „Datenhehlerei" unter Strafe gestellt werden. Weiterhin ist vorgesehen, dass die Daten nur mit richterlicher Erlaubnis abgerufen werden dürfen. Betroffene sollen zudem grundsätzlich informiert werden. Die Ausnahme von Berufsgeheimnisträgern, die Beschränkung auf sehr schwere Straftaten, sehr klare Regelungen zum Datenschutz und zur Datensicherheit und beschränkte Speicherfristen sind richtig und notwendig.

Hier noch einmal die Fakten im Überblick, was im Rahmen der VDS geregelt werden soll:

- In Zukunft sollen Telekommunikationsunternehmen bestimmte Verbindungsdaten einschließlich Funkzellenangaben (Verkehrsdaten) speichern, insbesondere die Rufnummer der beteiligten Telefonanschlüsse, Zeitpunkt und Dauer eines Anrufs, bei Mobilfunk die Standortdaten sowie wann und wie lange eine IP-Adresse einem bestimmten Computer, Smartphone o.ä. zugeordnet war, d.h. wann von diesem Gerät das Internet benutzt wurde. Nicht gespeichert wird der **Inhalt** von Telefongesprächen, welche Internetseiten aufgerufen wurden oder der Versand und Inhalt von E-Mails oder SMS. Funkzellenangaben sollen nach den vereinbarten Leitlinien nur zu Beginn einer Kommunikation, nicht etwa fortlaufend gesichert werden. IP-Adressen sollen nur punktuell abgefragt werden können, etwa wenn aufgrund von Vorermittlungen bekannt ist, dass sie zum verbotenen Abruf von Daten (z.B. kinderpornografischer Inhalte) genutzt worden sind.
- Die Daten werden grundsätzlich zehn Wochen gespeichert. Die besonders sensiblen Standortdaten lediglich vier Wochen. Nach Ablauf der Fristen müssen die Daten binnen einer Woche gelöscht werden. Für die Speicherung gelten hohe Sicherheitsanforderungen. Bei Verstößen drohen den Unternehmen Geldbußen von 100.000 bis 500.000 Euro.
- Genutzt werden dürfen die Daten von der Staatsanwaltschaft zur Verfolgung einzeln aufgeführter besonders schwerer Straftaten, insbesondere bei terroristischen Taten und anderen Delikten gegen Leib, Leben, Freiheit und sexuelle Selbstbestimmung, also etwa bei Mord, Totschlag oder schwerem sexuellen Missbrauch von Kindern. Außerdem

Dirk Fischer
Mitglied des Deutschen Bundestages

können die Länder ihre Polizeigesetze so ändern, dass deren Polizeien die Daten auch nutzen dürfen, um konkrete Gefahren für höchste Rechtsgüter abzuwehren. Damit unterscheidet sich die VDS entscheidend gegenüber Datensammlungen etwa von Google, Facebook, Payback etc., die die Daten in ihrer Gesamtheit gerade zu dem Zweck erheben, diese umfassend z.B. zu Werbezwecken auszuwerten und möglichst viel über möglichst viele Nutzer zu erfahren.

- Die Daten werden bei den Telekommunikationsunternehmen ohne jegliche besondere Aufbereitung gespeichert und werden nicht bei einer staatlichen Stelle zusammengeführt.
- Die Strafverfolgungsbehörden können nur dann einzelne Daten nutzen, wenn ein Richter oder eine Richterin dies für den konkreten Einzelfall nach Prüfung der gesetzlichen Voraussetzungen erlaubt. Die Datennutzung unterliegt also einem umfassenden Richtervorbehalt. Ohne einen solchen Anlass werden die Daten nach der festgesetzten Frist ohne weitere Nutzung schlicht bei den Providern gelöscht; keine staatliche Stelle bekommt sie dann jemals zu sehen.
- Verbindungsdaten von Berufsgeheimnisträgern werden von dem Abruf ausgenommen, die etwa bei der Kontaktaufnahme zu Telefonseelsorge-Hotlines anfallen. Daten, die bei der Kommunikation mit Personen anfallen, denen die Strafprozessordnung ein Zeugnisverweigerungsrecht einräumt (etwa Geistliche, Rechtsanwälte, Ärzte, Apotheker, Journalisten, Volksvertreter) dürfen von den Strafverfolgungsbehörden nicht genutzt werden. Zufallsfunde unterliegen einem Verwertungsverbot, d.h. sie dürfen in keinem Fall genutzt werden.
- Mit dem Gesetzentwurf wird zudem ein neuer Straftatbestand der „Datenhehlerei" geschaffen, um Daten vor Ausspähung und dem Handel damit zu schützen. Journalistische Tätigkeiten zur Vorbereitung einer konkreten Veröffentlichung sollen nicht als Datenhehlerei eingestuft werden.

Ich betone noch einmal, dass ich einem Gesetz nur zustimmen werde, wenn ganz bestimmte Voraussetzungen gegeben sind, die deutlich machen, dass eine sorgfältige Abwägung zwischen Freiheitsrechten und Pflichten des Staates zur Strafverfolgung vorgenommen wurde.

Der Entwurf wird nun im parlamentarischen Verfahren diskutiert und ggfls. auch verändert und angepasst werden. So wurde bereits beschlossen, das Gesetz bis zum Jahr 2018 zu evaluieren, eine Maßnahme, welche die geplante statistische Erhebung ergänzt.

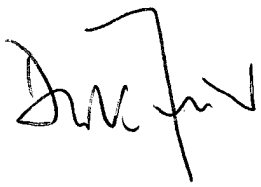
Dirk Fischer
Mitglied des Deutschen Bundestages

Ich bitte daher zu berücksichtigen, dass ich Ihnen in der jetzigen Phase nur über den Referentenentwurf Auskunft geben konnte, um Ihnen schnellstmöglich auf Ihr Schreiben zu antworten.

Weitere Details der Einigung finden Sie auf der Homepage des Bundesministeriums des Innern sowie auf der Homepage des Bundesministeriums der Justiz und für Verbraucherschutz. Für Rückfragen zum weiteren parlamentarischen Verfahren stehe ich Ihnen gerne zur Verfügung.

Mit freundlichen Grüßen

Ihr



Dirk Fischer