Schleswig-Holsteinischer Landtag
Umdruck 18/563

Polizeiliche Kriminalprävention der Länder und des Bundes
- Zentrale Geschäftsstelle -
Landeskriminalamt Baden-Württemberg
Taubenheimstr. 85
70372 Stuttgart
Tel.: 0711 / 5401-2060
Mobil: 0162 2530 666
Fax: 0711 / 2268000
Mail: Andreas.Mayer@polizei.bwl.de
o. propk@polizei.bwl.de

An den
Innen- und Rechtsausschuss

per E-Mail 21. Dezember 2012

Bundesratsinitiative zur Stärkung der Freiheit und der Privatsphäre im Internet

Sehr geehrte Frau Schönfelder,

ich bedanke mich sehr herzlich für Ihr Schreiben vom 27.11.2012 und der damit verbundenen Möglichkeit, zu den einzelnen Eckpunkten einer möglichen Bundesratsinitiative Stellung zu nehmen.

Aus Sicht und als Vertreter der polizeilichen Kriminalprävention ist es mir allerdings nur eingeschränkt möglich, die einzelnen Eckpunkte im Detail zu bewerten. Lassen Sie mich daher zu den aufgeworfenen Fragen bzw. Forderungen gemäß Anlage nur kurz Stellung beziehen. Bei dieser Stellungnahme handelt es sich um eine persönliche Einschätzung, die nicht mit dem Gremienverbund der Polizeilichen Kriminalprävention der Länder und des Bundes abgestimmt ist.

Die vorgeschlagenen Gesetzesanpassungen bedürften über meine Stellungnahme hinaus sicherlich noch einer eingehenderen juristischen Prüfung und Folgenabschätzung. Insofern hielte ich die Rechtsabteilung des Bundskriminalamts bzw. den Unterausschuss Recht und Verwaltung (UA RV) des Arbeitskreises II - Innere Sicherheit für weitere, zur Auskunft geeignete Stellen.

Mit freundlichen Grüßen
gez.
Andreas Mayer

:

Polizeiliche Kriminalprävention der Länder und des Bundes
Zentrale Geschäftsstelle
Az.: 031-SH-18/195

Antrag der Fraktion der PIRATEN „Bundesratsinitiative zur Stärkung der Freiheit und der Privatsphäre im Internet“

Stellungnahme:

Das Programm Polizeiliche Kriminalprävention der Länder und des Bundes (ProPK) verfolgt das Ziel, die Bevölkerung, Multiplikatoren, Medien und andere Präventionsträger über Erscheinungsformen der Kriminalität und Möglichkeiten zu deren Verhinderung aufzuklären. Dies geschieht unter anderem durch kriminalpräventive Presse- und Öffentlichkeitsarbeit und durch die Entwicklung und Herausgabe von Medien, Maßnahmen und Konzepten, welche die örtlichen Polizeidienststellen und andere Einrichtungen, zum Beispiel Schulen, in ihrer Präventionsarbeit unterstützen.

Der Antrag der Fraktion der PIRATEN bezieht sich auf Themenkomplexe die aktuell diskutiert werden und teilweise sehr facettenreich sind. Dies wird in den Eckpunkten des Antrags konkretisiert. In der zur Verfügung stehenden Zeit und ohne Beiziehung einer feinjuristischen Prüfung war eine umfassende Sachstandsdarstellung / Beantwortung nicht zu erarbeiten. Insofern konnte die nachfolgende Stellungnahme zu den dargestellten Punkten nur verkürzt ausfallen.

Zu 1.: Verantwortlichkeit von Telekommunikationsanbietern:

Der Antrag verfolgt die Gleichbehandlung von Telekommunikationsdiensten und dem Angebot von Internetzugängen. Dem ist nicht zu folgen.
Internetzugänge sollen der Öffentlichkeit völlig verantwortungsfrei und damit unkontrolliert zur Verfügung gestellt werden dürfen. Damit entfiele jede zivil- oder strafrechtliche Verantwortlichkeit eines Internetzugangsanbieters, die ohnehin heute schon begrenzt ist (siehe auch Ziffer 2). Insbesondere wird hierdurch auch eine Identifizierungs- und Protokollierungspflicht in Frage gestellt. U. U. würde hierdurch die Feststellung / Ermittlung eines Straftäters schon im Ansatz unmöglich gemacht.

Zu 2. Schutz der Meinungs- und Informationsfreiheit im Internet

Die Entfernung und Sperrung von Inhalten im Internet durch einen Internet-Dienstleister aufgrund von Rechtsverletzungen soll an eine richterliche Entscheidung geknüpft werden. Dies erscheint praxisfern und dürfte tatsächlich nicht handhabbar sein. Internet-Dienstleister haben nach bestehender Rechtslage nicht nur Rechte, sondern auch wichtige Pflichten.

Zur Erläuterung:

Aufgrund der vielen verschiedenen Nutzungsarten des Internets, lassen sich drei verschiedene Formen unterscheiden, in denen ein Provider (Internet-Dienstleister) im World Wide Web agiert:

1. der Content Provider (Inhaltsanbieter), er stellt eigene Inhalte im Internet zur Verfügung.
2. der Host Provider, der als Service Provider (Dienstleistungsanbieter) anderen Personen auf einem Server Speicherplatz zur Verfügung stellt, damit diese eigene Inhalte ins World Wide Web einstellen können.
3. der Access Provider (Zugangsanbieter), der Dritten lediglich den Zugang zum Internet ermöglicht.

Häufig werden Onlinedienste wie z. B. T-Online, mehrere der oben genannten Funktionen erfüllen, so dass ihre Dienste die verschiedenen Provider-Typen beinhalten und nicht isoliert betrachtet werden können.

Content Provider haften, wie bei anderen Medien, voll für die von ihnen bereit gestellten Informationen. Hierzu zählen auch Informationen von Dritten, die sich der Diensteanbieter erkennbar zu Eigen macht. Werden fremde Inhalte ohne Kennzeichnung als eigene Inhalte übernommen, kann sich der Website-Betreiber nicht darauf berufen, dass er für diese Inhalte nicht verantwortlich wäre.

Der Access Provider ist für durchgeleitete Informationen nach dem Gesetz weitestgehend von einer Haftung freigestellt. So besteht gerade keine Verantwortlichkeit, wenn der Access Provider den Zugang zur Nutzung fremder Informationen weder vermittelt, die Übermittlung der Informationen nicht veranlasst, die dem Adressaten übermittelten Informationen nicht ausgewählt noch die betreffenden Informationen ausgewählt oder verändert hat. Darüber hinaus haftet der Access Provider ebenfalls nicht, wenn er seinen Kunden den Zugriff auf rechtswidrige Inhalte im Internet ermöglicht.

Eine Ausnahme besteht allerdings dann, wenn ein Access Provider gezielt mit anderen Anbietern, beispielsweise mit Sitz im Ausland, zusammenwirkt, um eine Haftung für verbotene Inhalte zu umgehen, die auf Servern im Ausland gespeichert sind. Ermöglicht in diesem Fall der Zugangsprovider seinen Kunden den Zugang auf diese Daten, haftet der Provider auch für die rechtswidrigen Inhalte, obwohl er nur den Zugang bereitstellt.

Hatte der Host Provider keine Kenntnis von den Rechtsverstößen und waren diese auch nicht offensichtlich, ist auch der Host Provider von einer Haftung befreit.

Darüber hinaus besteht keine Haftung, wenn der Host Provider, sobald er von den rechtswidrigen Inhalten Kenntnis erlangt, die rechtswidrigen Informationen entfernt oder den Zugang zu diesen Inhalten sperrt.

Dies erscheint zumutbar.

Zu 3. Begrenzung der „Störerhaftung“ und Ausschluss privatpolizeilicher Überwachungspflichten

Nach hier vorliegenden Erfahrungen erfolgen Löschungen und Sperrungen rechtswidriger Inhalte im Internet durch Internet-Dienstleister (Provider oder auch Plattformbetreiber) auf Antrag und sind zumeist rechtmäßig. Die Meinungs- und Informationsfreiheit wird nach hiesiger Auffassung hierdurch nicht unzumutbar eingeschränkt.

Eine Filterung von als rechtswidrig erkannten Inhalten entspräche in besonderem Maße dem Grundgedanken der Prävention. Hierfür gibt es auch technische Möglichkeiten, die dies unterstützen (diese sind zum Teil umstritten). Eine „vorsorgliche“ Rechtsmäßigkeitsprüfung durch Telemedienanbieter findet nach hiesiger Einschätzung nur sehr begrenzt statt und ist häufig aufgrund enormer Datenmengen, die täglich versandt oder hochgeladen werden, nur eingeschränkt möglich.

Zu 4. Telemediennutzungsgeheimnis

Ein Telemediennutzungsgeheimnis hat nicht nur eine nationale, sondern auch eine internationale Dimension. Zum einen kann der Argumentation durchaus gefolgt werden. Zum anderen erfolgt jede Eingabe und Preisgabe von Daten, insbesondere von personenbezogenen Daten eines Nutzers, freiwillig und unter Hinnahme zumindest einer Einschränkung des Rechts auf informationelle Selbstbestimmung.

Von grundlegender Bedeutung für die Bewertung der Grundrechtsrelevanz von Internetermittlungen durch die Polizei und damit auch der Reichweite eines Telemediennutzungsgeheimnisses erscheint die Entscheidung des BVerfG zur Online-Durchsuchung vom 27.2.2008. Darin heißt es: „Nimmt der Staat im Internet öffentlich zugängliche Kommunikationsinhalte wahr oder beteiligt er sich an öffentlich zugänglichen Kommunikationsvorgängen, greift er grundsätzlich nicht in Grundrechte ein.“ Die §§ 161, 163 StPO als allgemeine Ermächtigungsgrundlagen sind mithin für die Erhebung aller Daten ausreichend, die jedermann zugänglich und damit offen sind.

Insofern zielt ein Telemediennutzungsgeheimnis, angelehnt an die Begründung, die auch die „Offenlegung gegenüber staatlichen Stellen“ anprangert, lediglich darauf ab, staatliche

Stellen in ihrer Aufgabenerfüllung zu behindern. bzw. die Erfüllung deren Aufgaben zu verhindern.
Je nach Art der Nutzung des Internets (z. B. Mailverkehr) sind heute schon die Voraussetzungen des § 100 a StPO - Telekommunikationsüberwachung - zu erfüllen. Für Daten die sich in "geschützten" Bereichen befinden, greifen zum Teil andere Rechtsgrundlagen, die ebenso höhere Voraussetzungen für ein polizeiliches Tätigwerden erfordern (z. B. § 110 a StPO).

Zu 5. Internet-Protokolladressen

Die Einschränkungsvorschläge der Nutzung von IP-Adressen („…unkontrollierte Sammlung, Auswertung …“) erscheinen begrüßenswert, dürften jedoch ins Leere laufen, da eine solche nationale Regelung im Kontext einer globalen, virtuellen Welt keine spürbare Wirkung entfalten dürfte.

Zu 6. Internet-Nutzungsprofile

Die Erstellung personenbezogener Nutzungsprofile durch die Internet- und Privatwirtschaft ist zwischenzeitlich Teil einer üblichen Marketing-Strategie, insbesondere auch von Unternehmen, die international und damit grenzübergreifend „am Markt sind“. Ein nationales Verbot (wenn auch oberflächlich wünschenswert) liefe ins Leere und würde gegebenenfalls zu Wettbewerbsverzerrungen führen.

Ferner muss es auch den Strafverfolgungsbehörden möglich sein, über die Erstellung von Nutzungsprofilen Ermittlungsansätze zu identifizieren, die für die Aufklärung schwerer Straftaten unverzichtbar sind, auch ohne Einwilligung des Nutzers. Je nach Art und Zweck der Nutzung sind dafür unterschiedliche Rechtsgrundlagen erforderlich (s. Ziffer 4).

Zu 7. Schutz vor Ausspionieren des Nutzers durch „Spyware“, „Web-Bugs“ usw.

Der Einsatz von „Spyware“ ohne Rechtfertigungsgrund ist bereits strafbewehrt, z. B. durch § 202 a StGB; daher erscheint eine weitergehende Regelung nicht erforderlich.

Zu 8. Transparenz von Speicherfristen

Die Polizei besteht auf der Gewährleistung von Mindestspeicherungsfristen durch Serviceprovider für anfallende Verkehrsdaten gem. der EU-Richtlinie (2006/24/EG). Derartige Informationen, einschl. der indirekten Ermittelbarkeit von Nutzerdaten, sind sowohl für zivilrechtliche als auch für strafprozessuale Zwecke erforderlich.

Die Forderung nach mehr Transparenz bzgl. der Aufbewahrungsdauer von Nutzer- und damit zweifellos auch von Verkehrsdaten könnte bei der derzeitigen, lückenhaften Gesetzeslage in Deutschland dazu führen, einem potenziellen Straftäter es zu ermöglichen, einen Serviceprovider auszuwählen, der aufgrund äußerst kurzer bzw. entfallender Speicherfristen die größtmögliche Chance bietet, für Rechtsverletzungen weder zivil- noch strafrechtlich belangt werden zu können.

Zu 9. Koppelungsverbot

Das im Antrag beschriebene Koppelungsverbot dient dazu, die Erhebung von personenbezogenen Daten eines Nutzers „für andere Zwecke“ und damit auch auf für Zwecke der Strafverfolgung einzuschränken bzw. über einen kostenpflichtigen Zugang gänzlich zu verhindern. Damit wird eine anonyme Nutzung von Internetdiensten begünstigt bzw. sogar erst ermöglicht. Dies ist aus Sicht einer Strafverfolgungsbehörde, die auch einen kriminalpräventiven Auftrag hat, abzulehnen. Es sei denn, es würden für diese Ausnahmeregelungen getroffen.

Zu 10. Schutz vor unangemessenen Datenverarbeitungs- Einwilligungsklauseln

Hierzu wird nicht näher Stellung genommen, da diese Forderung in erster Linie privatrechtliche Verträge betrifft, über deren Zustandekommen jede/r zunächst eigenverantwortlich selbst entscheidet.

Schlussvermerk:

Insgesamt ist in der Initiative der Versuch einer umfangreichen Deregulierung der Nutzung des Internets zu sehen. Die Initiative steht allerdings in Teilen konträr zu derzeit geltendem Recht. Dem politischen Postulat, dass das Internet kein rechtsfreier Raum sein darf, wird dadurch nicht Rechnung getragen. Würde man einzelne geforderte Punkte - wie vorgeschlagen - umsetzen, so würde man der Anonymität bei der Nutzung des ‚Netzes’ nicht nur zum Vorteil des Nutzers und dessen Persönlichkeitsschutzes Vorschub leisten, sondern auch zum Vorteil der Begehung von Straftaten und potenzieller Straftäter, zum Nachteil von Opfern und des Opferschutzes und zur Verhinderung von straf- und zivilrechtlicher Ermittlungen und Forderungen.

Es wäre zu befürchten, dass die anonyme und damit straflose Vorbereitung und Begehung von Straftaten hierdurch nicht nur begünstigt, sondern in Teilbereichen erst ermöglicht würde. Da dies sicherlich politisch nicht gewollt ist, gilt es, die einzelnen Bereiche der Initiative noch einmal einer genauen, rechtlichen Prüfung zu unterziehen.

gez.
Andreas Mayer