Schleswig-Holstein
Der echte Norden

Schleswig-Holsteinischer Landtag
Umdruck 18/7405

Schleswig-Holstein
Ministerium für Wirtschaft, Arbeit, Verkehr und Technologie

Ministerium für Wirtschaft, Arbeit, Verkehr und Technologie Postfach 71 28 | 24171 Kiel

Staatssekretär

An die
Vorsitzende
des Innen- und Rechtsausschusses
des Schleswig-Holsteinischen Landtages
Frau Barbara Ostmeier, MdL
Landeshaus
24105 Kiel

14. Februar 2017

Sehr geehrte Frau Vorsitzende,

in der Sitzung des Innen- und Rechtsausschuss am 01.02.2017 wurde Ihnen eine schriftliche Stellungnahme zum Antrag der Fraktion der PIRATEN „Bundesratsinitiative zur Stärkung der Freiheit und der Privatsphäre im Internet“ (Drucksache 18/195) zugesagt. Bei der Erstellung der Stellungnahme wurde die Rechtsauffassung des zuständigen Bundesministeriums für Wirtschaft und Energie (BMWi) berücksichtigt.

Die Stellungnahme erfolgt anhand der einzelnen Eckpunkte des Antrags:

1. „Erstreckung von Haftungsbegrenzungen des Telemediengesetzes auf Telekommunikationsdienste (z.B. offene Internetzugänge);“

Das BMWi stellt hierzu fest, dass die Regelungen des Zweiten Gesetzes zur Änderung des Telemediengesetzes (TMG) vom 27.07.2016 für alle Diensteanbieter gelten. Soweit noch Regelungslücken bestehen, sollen diese durch die vom BMWi infolge des EuGH-Urteils vom 15.09.2016 geplante erneute Änderung des TMG geheilt werden (siehe auch Antwort der Landesregierung auf die Kleine Anfrage des Abgeordneten Dr. Patrick Breyer (PIRATEN) vom 31.01.2017 – Drucksache 18/5059).

2. „Anbieter von Durchleitungs- und Speicherdiensten sind zur Entfernung oder Sperrung fremder Informationen wegen angeblicher Verletzung privater Rechte nur verpflichtet, wenn der Anspruchsteller eine entsprechende (vorläufig) vollstreckbare Gerichtsentscheidung vorlegt; die Diensteanbieter sind von den Kosten der erstinstanzlichen gerichtlichen Prüfung freizuhalten (Schutz der Meinungs- und Informationsfreiheit im Netz);“

Nach der vom BMWi geplanten Änderung des TMG (siehe Stellungnahme zu Ziffer 1) sollen die Diensteanbieter möglichst von allen Kosten, zumindest aber von den außergerichtlichen freigehalten werden.
Das weitere Thema der Entfernungsverpflichtung erst nach gerichtlicher Anordnung betrifft die Hostproviderhaftung nach § 10 TMG: Danach ist der Hostprovider zur Entfernung verpflichtet, sofern die Rechtswidrigkeit offensichtlich ist. Dies ist aber für die Hostprovider nicht immer erkennbar. Die verpflichtende Einschaltung der Gerichte erscheint zu aufwändig. Deswegen ist das BMWi bemüht, die EU-Kommission zu einer gesetzlichen Konkretisierung der Anforderungen an die Entfernungsverpflichtungen zu bewegen (gesetzliche Regelung des „notice and take down“ – Verfahrens).

3. „Anbieter von Durchleitungs- und Speicherdiensten müssen keine Rechtsverletzungen verhindern, für die sie nicht verantwortlich sind (Begrenzungen der „Störerhaftung“); Diensteanbieter müssen nur bereits vorhandene rechtsverletzende Inhalte entfernen oder sperren und nicht mögliche zukünftige rechtsverletzende Inhalte von denen sie keine Kenntnis haben (Ausschluss privatpolitischer Überwachungspflichten);“

Es wird auf die Stellungnahme zu Ziffer 2 verwiesen sowie auf die Antwort der Landesregierung auf die Kleine Anfrage des Abgeordneten Dr. Patrick Breyer (PIRATEN) vom 31.01.2017 – Drucksache 18/5059, in der die durch das BMWi beabsichtigte Änderung des TMG (weitgehende gesetzliche Abschaffung der Störerhaftung) erläutert wird.
Aus Sicht des BMWi erscheint der generelle gesetzliche Ausschluss der Verhinderung künftiger Rechtsverletzungen problematisch: Eine generelle Überwachungspflicht sei nicht gewollt, sehr wohl aber der Einsatz einfacher technischer Überwachungsmaßnahmen.

4. „Erstreckung des Fernmeldegeheimnisses auf die Nutzung von Telemediendiensten (Telemediennutzungsgeheimnis); Offenlegung von Informationen über den Inhalt der persönlichen Internetzugang gegenüber Behörden nur unter den Voraussetzungen, die für das Abhören von Telefonaten gelten;“

Das BMWi weist darauf hin, dass das derzeitige Fernmeldegeheimnis in § 88 Telekommunikationsgesetz (TKG) eine Umsetzung des Art. 5 der E-Privacy-RL ist. Die zukünftige E-Privacy-Verordnung wird einen entsprechenden Artikel 5 beinhalten, der alle Kommunikationsdaten umfasst und – wenn die Verordnung so kommt – das in § 88 TKG geregelte Fernmeldegeheimnis ersetzen wird. Die Regelung erfasst aber nicht die Mediennutzung im Einzelnen, soweit diese bei Telemedien protokolliert wird. Hier gilt der Datenschutz des TMG (ab 2018 der Datenschutz-Grundverordnung). Grundsätzlich darf der Diensteanbieter Auskünfte über die Mediennutzung an Strafverfolgungs- und Sicherheitsbehörden erteilen, wenn solche Auskunftsrechte in den Rechtsgrundlagen dieser Behörden geregelt sind. Solche Auskunftsrechte bestehen beispielsweise in § 8a BVerfSchG, auf den die Gesetzes anderer Sicherheitsbehörden dann verweisen. Das Bundesamt für Verfassungsschutz darf im Einzelfall bei Telemedienanbietern Auskunft über die vom Nutzer in Anspruch genommenen Teledienste einholen. Ein Mediennutzungsgeheimnis müsste im Kontext der Sicherheitsgesetze unter Federführung des BMI geprüft werden.

5. „Klarstellung, dass der gesetzliche Datenschutz auch für Internet-Protokolladressen gilt, die von Telemedienanbietern gesammelt werden;“

Der EuGH hat in der Rechtssache C - 582/14 Patrick Breyer / Bundesrepublik Deutschland am 19. 10. 2016 entschieden, dass das Aufzeichnen und Speichern der IP-Adressen durch Bundesbehörden zwar den Regelungen des TMG unterliegen und grundsätzlich personenbezogene Daten darstellen, aber die Einrichtungen des Bundes, die Online-Mediendienste anbieten, ein berechtigtes Interesse daran haben könnten, die Aufrechterhaltung der Funktionsfähigkeit der von ihnen allgemein zugänglich gemachten Websites über ihre konkrete Nutzung hinaus zu gewährleisten. Im Übrigen richte sich der Datenschutz nach den Vorschriften des TMG, wie auch der Kläger Breyer betonte. Ergänzend könnte überlegt werden, ob nicht IP-Protokolladressen unter Heranziehung von Erwägungsgrund 26 und Art. 4 Nr. 1 Datenschutz-Grundverordnung (DSGVO) als personenbezogenes Datum nach allg. Datenschutzrecht zu behandeln wären. Nach Art. 4 Nr. 1 DSGVO sind personenbezogene Daten alle Informationen, die sich auf eine identifizierbare Person beziehen. Dies kann direkt oder indirekt mittels Zuordnung zu Standortdaten, einer Online-Kennung oder mehreren Merkmalen erfolgen. Nach dem additiv heranzuziehenden Erwägungsgrund 26 sollen „bei der Entscheidung, ob eine Person bestimmbar ist, alle Mittel berücksichtigt werden, die vernünftigerweise entweder von dem Verantwortlichen für die Verarbeitung oder von einem Dritten eingesetzt werden könnten, um die betreffende Person zu bestimmen“. Dies lässt sich so verstehen, dass es unter Umständen ausreicht, wenn ein Dritter den Personenbezug herstellen kann. Folglich erscheinen IP-Adressen europarechtlich immer als personenbezogene Daten, da zumindest der Access Provider für den Zeitraum der IP-Adressdatenspeicherung eine solche Zuordnung vornehmen kann (vgl. die Stellungnahmen der Europäischen Art. 29 -Gruppe: Opinion 4/2007 on the concept of personal data and the Opinion on data protection issues related to search engines , S. 15 f. und Opinion 1/2009 on the proposals amending Directive 2002/58/EC on privacy and electronic communications (e-Privacy Directive), S. 8). Es ist daher anzunehmen, dass die Speicherung von Internet-Protokolladressen grundsätzlich als Speicherung von personenbezogenen Daten zu bewerten ist und sich diese Einschätzung durch Umsetzung der DSGVO nicht ändern wird. Die weiteren datenschutzrechtlichen Anforderungen richten sich hier konkret nach dem TMG.

6. „Verbot der Erstellung von Nutzerprofilen ohne Einwilligung des Nutzers;“

Der § 15 Abs. 3 TMG sieht für pseudonyme Nutzungsprofile entsprechend den geltenden Anforderungen eine Widerspruchsmöglichkeit („opt-out“) vor. Die Regelung war einmal dazu gedacht, Online-Händlern eine Handhabe zu geben, ihre Position auf dem Markt einzuschätzen und ihr Geschäftsmodell zu planen, wie das Offline-Händlern auch möglich ist. Für eine Verschärfung der Regelung sieht das BMWi keine Gründe. Im Übrigen ist Profiling in der Datenschutz-Grundverordnung umfänglich geregelt, so dass ab Mai 2018 kein Handlungsspielraum mehr besteht.

7. „Umsetzung der europäischen Regelung zum Schutz vor Ausspionieren des Nutzers durch „Spyware“, „Web-Bugs“ usw.;“

Das BMWi geht davon aus, dass die EU-Vorgaben ordnungsgemäß umgesetzt worden sind. Im Übrigen werden die Regelungen durch die E-Privacy-Verordnung ersetzt.

8. „Information der Nutzer über die Dauer der Aufbewahrung ihrer Daten;“

Auch hier gilt ab Mai 2018 die Datenschutz-Grundverordnung mit Artikel 13, in der das, was hier gefordert wird, umfänglich geregelt ist.

9. „Stärkung des Rechts auf anonyme Internetnutzung durch ein wirksames Koppelungsverbot;“

Das noch geltende Bundesdatenschutzgesetz enthält in § 28 Abs. 3b die Regelung, dass die verantwortliche Stelle den Abschluss eines Vertrags nicht von einer Einwilligung des Betroffenen in die Verarbeitung seiner Daten abhängig machen darf, wenn dem Betroffenen ein anderer Zugang zu gleichwertigen vertraglichen Leistungen ohne die Einwilligung nicht oder nicht in zumutbarer Weise möglich ist. Eine unter solchen Umständen erteilte Einwilligung ist unwirksam. Der kürzlich von der Bundesregierung beschlossene Entwurf zur Anpassung des Bundesdatenschutzgesetzes (BDSG) an die DSGVO sieht eine solche Regelung nicht mehr vor. Hier gelten ab Mai 2018 die Maßgaben der Datenschutzgrundverordnung zur freiwilligen Einwilligung (insb. Art. 7 Abs. 4 und Erwägungsgrund 43). Danach muss dem Umstand in größtmöglichem Umfang Rechnung getragen werden, ob unter anderem die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrags nicht erforderlich sind. Um sicherzustellen, dass die Einwilligung freiwillig erfolgt ist, sollte diese in besonderen Fällen, wenn zwischen der betroffenen Person und dem Verantwortlichen ein klares Ungleichgewicht besteht, insbesondere wenn es sich bei dem Verantwortlichen um eine Behörde handelt, und es deshalb in Anbetracht aller Umstände in dem speziellen Fall unwahrscheinlich ist, dass die Einwilligung freiwillig gegeben wurde, keine gültige Rechtsgrundlage liefern. Die Einwilligung gilt nicht als freiwillig erteilt, wenn zu verschiedenen Verarbeitungsvorgängen von personenbezogenen Daten nicht gesondert eine Einwilligung erteilt werden kann, obwohl dies im Einzelfall angebracht ist, oder wenn die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung abhängig ist, obwohl diese Einwilligung für die Erfüllung nicht erforderlich ist.

10. „Schutz der Nutzer von unangemessenen Datenverarbeitungs-Einwilligungsklauseln, indem klargestellt wird, dass derartige Klauseln der gerichtlichen Angemessenheitskontrolle (AGB-Kontrolle) unterliegen.“

Ein Gesetz, das als Eckpunkt die Klarstellung erhält, dass bestimmte Klauseln einer gerichtlichen Angemessenheitskontrolle unterliegen, wird seitens der Landesregierung als problematisch gesehen. Ob eine konkrete Klausel der Angemessenheitskontrolle unterliegt, wird von den Gerichten bereits jetzt am Maßstab der §§ 305 ff. BGB im Einzelfall überprüft. Ein Bedürfnis für eine abstrakte gesetzliche Regelung wird nicht gesehen.

Mit freundlichen Grüßen

gez. Dr. Frank Nägele