Schleswig-Holsteinischer Landtag
Umdruck 18/1546

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit
Klosterwall 6 (Block C), D – 20095 Hamburg

Schleswig-Holsteinischer Landtag
Innen- und Rechtsausschuss
Düsternbrooker Weg 70
24105 Kiel

Nachrichtlich:
ULD Dr. Thilo Weichert
Mail@datenschutzzentrum.de

Klosterwall 6, Block C
D – 20095 Hamburg
Telefon: 040 - 428 54 - 40 41 Zentrale - 40 40
Telefax: 040 - 428 54 - 40 00
Ansprechpartner: Prof. Dr. Caspar
E-Mail*: Johannes.Caspar@datenschutz.hamburg.de

Az.: D /

Hamburg, den 29. Juli 2013

Bundesratsinitiative zur Stärkung der Freiheit und Privatsphäre im Internet
Antrag der Fraktion der Piraten, Drucksache 18/195

Sehr geehrte Frau Schönfelder,

zunächst darf ich mich für die Gelegenheit zur Stellungnahme zu der o.g. Bundesratsinitiative bedanken. Im Wesentlichen werde ich mich auf die zentralen Fragestellungen, die sich mit Blick auf datenschutzrechtliche Aspekte ergeben, beschränken.

1. Haftungsbegrenzung des Telemediengesetzes auf Telekommunikationsdienste (z.B. offene Internetzugänge)

   Bei der Verbesserung der kommunikativen Infrastruktur durch Schaffung offener WLANs in Deutschland erweist sich das Haftungsrisiko von Betreibern offener Funknetze als durchweg kontraproduktiv. Das liegt im Wesentlichen an der weitgehend übereinstimmenden Rechtsprechung zur Störerhaftung von WLAN-Betreibern. Danach können Privatpersonen auf Unterlassung in Anspruch genommen werden, soweit ihr nicht ausreichend gesicherter WLAN-Anschluss von unberechtigten Dritten für Urheberrechtsverletzungen im Internet genutzt wird (BGH, vom 12. Mai 2010 – I ZR 121/08). Ist danach der Betrieb eines nicht ausreichend gesicherten WLAN-Anschlusses adäquat kausal für Urheberrechtsverletzungen, die unbekannte Dritte unter Einsatz dieses Anschlusses begehen, wird der Betreiber als Störer angesehen.

Um künftig die Bereitschaft zur Bereitstellung von offenen WLANs deutschlandweit zu stärken, sind gesetzliche Vorgaben, die die technischen Vorkehrungen der Betreiber der öffentlichen Netze gegenüber missbräuchlicher Anwendung konkretisieren und Haftungs- sowie Abmahnrisiken ausschließen bzw. abmildern, erforderlich. Auch wenn nach Maßgabe der gegenwärtigen Rechtsprechung die Betreiber der nicht ausreichend gesicherten WLAN-Anschlüsse nicht auf Schadensersatz, sondern lediglich auf Unterlassung in Anspruch genommen werden können, verhindern die damit verbundenen Abmahnrisiken eine Verbesserung der Infrastruktur durch offene WLANs. Insoweit wird die vorgeschlagene Verantwortungsbegrenzung von Anbietern öffentlicher WLANs begrüßt.

2. Schutz der Meinungs- und Informationsfreiheit im Internet

Der Vorschlag zu 2. sieht zum Schutz der Meinungs- und Informationsfreiheit im Internet vor, dass auf Seiten der Internetdienstleister eine Pflicht zur Entfernung oder Sperrung fremder Informationen wegen der angeblichen Verletzung privater Rechte in Zukunft nur dann eingreifen soll, wenn der Anspruchsteller eine vollstreckbare Gerichtsentscheidung, die sich gegen den Verantwortlichen oder den Anbieter richtet, vorlegt. Darüber hinaus soll der Diensteanbieter, wird er unmittelbar in Anspruch genommen, von den Kosten der erstinstanzlichen gerichtlichen Prüfung freigehalten werden.

Meinungs- und Informationsfreiheit stehen gerade im Internet auch in einem grundsätzlichen Spannungsverhältnis zu den Persönlichkeitsrechten Betroffener. Die Lasten der Ahndung der Verletzung von zivilrechtlichen Persönlichkeitsrechten auf die Rechteinhaber zu verteilen, um pauschal Nutzerinnen und Nutzer sowie die Diensteanbieter von der Verantwortung für die eingestellten und vermittelten Inhalte zu entlasten, kann aus datenschutzrechtlicher Sicht nicht geteilt werden.

Die Verteilung der Risiken zwischen den für die Meinungsäußerung Verantwortlichen und den Anbietern von Internetdienstleistungen einerseits sowie den von Eingriffen in ihr Persönlichkeitsrecht Betroffenen dürfen nicht einseitig verschoben werden. Die Vollzugspraktik bei der Umsetzung z.B. berechtigter datenschutzrechtlicher Löschungsansprüche zeigt, dass Betroffene gegenüber Diensteanbietern und den Nutzerinnen und Nutzern eine effektive Wahrnehmung ihrer Rechte nur schwer realisieren können. Die Erhöhung der Anforderungen an die Umsetzung z.B. datenschutzrechtlicher Löschungsansprüche wäre aus hiesiger Sicht daher nicht zu empfehlen und würde der weiteren Absenkung des Schutzes europa- und verfassungsrechtlich

garantierte Rechte auf Schutz der digitalen Persönlichkeit Vorschub leisten. Dies gilt insbesondere auch in Anbetracht des Zusammenwirkens von Nutzerinnen und Nutzern und den Dienstanbietern bei der Nutzung personenbezogener Daten Dritter, wie z.B. in den Fällen der auto-suggest-Funktion bei Suchmaschinen (vgl. BGH Urt. v. 14. 05. 2013, VI ZR 269/12), der Veröffentlichung von Fotos Dritter und die biometrische Auswertung dieser oder der Nutzung von E-Mail-Adressen für das sogenannte „Friend-finding“. Für Betroffene ist es in diesen Fällen bereits heute überaus schwierig, die datenschutzrechtliche Verantwortung eindeutig zuzuweisen, um wirksam gegen Verstöße vorgehen zu können.

Verschärft wird diese Situation noch dadurch, dass in der Praxis des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit häufig Fallgestaltungen zu bearbeiten sind, in denen Betroffene ihre Rechte gegen die Veröffentlichung personenbezogener Daten bzw. gegen Eingriffe in Persönlichkeitsrechte gegenüber Anbietern von Telemedien verfolgen müssen, obwohl diese nicht Urheber sind. Grund hierfür ist, dass einer direkten Geltendmachung von Ansprüchen unmittelbar gegenüber den für eine Veröffentlichung Verantwortlichen häufig entgegensteht, dass diese nicht ermittelt werden können oder sich der Rechtsdurchsetzung faktisch entziehen. Betroffene haben somit keine andere Wahl als sich an die Intermediäre im Internet, insbesondere an Betreiber von Suchmaschinen, sozialen Netzwerken, Bewertungsportalen oder Blogs, zu wenden.

In vielen Fällen wird dabei die Unterstützung der staatlichen Ausfsichtsbehörden für den Datenschutz gesucht. In der Vollzugspraxis des HmbBfDI gelingt es oft durch Kommunikation mit den Internet-Anbietern, den Betroffenen bei Rechtsverletzungen durch Dritte unbürokratisch zu helfen. Gerade mit Blick auf die zahlreichen Schwierigkeiten, die der einzelne Nutzer hat, um seine Rechte in der digitalen Welt durchzusetzen, ist diese Hilfe durch Datenschutzbehörden von großer Bedeutung. Die Forderung, künftig für die Löschung oder Sperrung fremder Informationen im Falle der Rechtsverletzung durch den Anspruchsteller eine vollstreckbare Rechtsentscheidung vorlegen zu müssen und zudem die Kosten gegenüber dem Dienstleistungsanbieter zu übernehmen, stellt aus hiesiger Sicht eine Verschlechterung der Rechtsverfolgungsmöglichkeiten Betroffener gerade auch gegenüber Internetdienstleistern dar. Die Umsetzung datenschutzrechtlicher Individualrechte durch die Betroffenen sollte im Gegensatz dazu eher erleichtert und nicht durch weitete Anforderungen gänzlich unmöglich gemacht werden. Das gilt gerade für die ohnehin schwierige Durchsetzung von Individualrechten Einzelner gegenüber international agierenden und über wirtschaftlich fast unbegrenzte Ressourcen verfügenden Unternehmen.

3. Begrenzung der Störerhaftung und Ausschluss privatpolizeilicher Überwachungspflichten

Ebenfalls kritisch ist daher auch die Forderung nach Begrenzung der Störerhaftung mit Blick auf Eingriffe in das informationelle Selbstbestimmungsrecht sowie die Persönlichkeitsrechte Betroffener zu bewerten. Das Internet erhöht den Druck auf den Einzelnen, entweder freiwillig oder als Objekt der Bewertung oder der Kritik, möglicherweise auch der Beleidigung als Teil des globalen Netzes präsent zu sein. Die derzeitige Rechtslage ist hier kaum in der Lage, einen zureichenden Schutz zu gewährleisten. Nicht zuletzt deshalb wird gegenwärtig die Diskussion um ein Recht auf Vergessenwerden und auf Löschung aus Anlass der geplanten EU-Datenschutz-GrundVO auf europäischer Ebene geführt. Ziel ist es, die Grundrechte der Betroffenen gerade im Internet besser zu schützen und den Datenschutz zu stärken. Die Nutzer sollen in die Lage versetzt werden, künftig die Herrschaft über ihre Daten wieder zu erlangen.

Eine Erhöhung der Hürden für Betroffene, ihre Ansprüche durchzusetzen, kann demgegenüber unter den gegebenen Umständen nicht befürwortet werden. So bleibt bislang zwar das Datenschutzrecht neben dem TMG selbständig anwendbar und wird auch nicht durch die eingeschränkte Störerhaftung begrenzt. In der Praxis gilt gegenüber Publikationen im Internet aber in vielen Fällen das sog. Medienprivileg, das bei einer journalistisch-redaktionellen Zweckbestimmung der Daten einer Kontrolle durch die Datenschutzaufsicht ohnehin weitgehend entzieht. Damit sind die Betroffenen hier ausschließlich auf die eigenständige Rechtswahrnehmung beschränkt.

Gegenüber dem bisherigen Rechtsszustand sollte es zu keiner weiteren Absenkung des Schutzes Betroffener kommen: Telemedienanbieter sind danach für fremde Inhalte nach §§ 7ff. TMG von der strafrechtlichen Verantwortung sowie der Haftung auf Schadensersatz ausgeschlossen. Verantwortlich sind sie lediglich eingeschränkt nach Maßgabe der sogenannten Störerhaftung. D.h. die Internetdienstleister dürften unter bestimmten Vorgaben auch dann, wenn sie einen Eintrag weder verfasst noch sich dessen Inhalt zu Eigen gemacht haben, auf Unterlassung in Anspruch genommen werden. Die Störerhaftung legitimiert sich letztlich aus Schaffung der technischen Voraussetzung zur Übermittlung bzw. zum Abruf von Daten. Eine entsprechende Einstandspflicht für Rechtsverletzungen Dritter sieht die Rechtsprechung hier nur unter der einengenden Voraussetzung der Verletzung zumutbarer Verhaltenspflichten vor: Danach ist ein Hostprovider nicht verpflichtet, die von den Nutzern ins

Netz gestellten Beiträge vor Veröffentlichung auf mögliche Rechtsverletzungen vorab zu überprüfen (vgl. § 7 Abs. 2 TMG).

Anders ist es jedoch, sobald er Kenntnis von der Rechtsverletzung, etwa durch einen Hinweis eines Betroffenen, erlangt (BGH vom 25.10.2011, VI ZR 93/10 mit weiteren Verweisen auf die vorangegangene Spruchpraxis). Diese Haftung schafft dem Betroffenen, der in vielen Fällen den Verantwortlichen für eine Persönlichkeitsrechtsverletzung gar nicht ausmachen kann, die Möglichkeit, seine Rechte zumindest gegenüber den Internetdienstleistern weiter zu verfolgen.

Schließlich müssen Beschränkungen der geltenden Regelung zur Störerhaftung auch die gemeinschaftsrechtlichen Vorgaben der E-Commerce-Richtlinie der EU beachten. So sieht Art. 14 der Richtline 2000/31/EG vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr“) eine Haftungsfreistellung des Hostproviders nur unter der Voraussetzung vor, dass der Anbieter keine tatsächliche Kenntnis von der durch den Nutzer eingegebenen rechtswidrigen Information hat. Damit ist eine Beschränkung der Störerhaftung, die über das Kriterium der Kenntnisnahme weitergehende Ausnahmen macht, mit dem europäischen Rechtsrahmen nicht vereinbar.

4. Anwendung des Fernmeldegeheimnisses auf die Nutzung von Telemediendiensten (Telemediendienstnutzungsgeheimnis)

Die Erstreckung des Fernmeldegeheimnisses auf die Nutzung von Telemedien wird ausdrücklich unterstützt. Insoweit wäre der Ausbau des bereits in § 7 Abs. 2 Satz 3 TMG enthaltenen Grundsatzes der Verpflichtung der Dienstanbieter auf die Wahrung des Fernmeldegeheimnisses zu begrüßen. Die Nutzung der im Internet angebotenen Dienste stellt für den Einzelnen zur Wahrnehmung seiner kommunikativen Freiheitsrechte eine zentrale Voraussetzung dar. Neben der Nutzung der Kommunikationsmöglichkeiten über die Telemediendienste hat der Staat daher auch für den Schutz vor dem unberechtigten Zugriff und der Auswertung des Nutzungsverhaltens zu sorgen. In der Praxis zeigt sich immer deutlicher, dass vor allem die bei der Nutzung des Internets entstehenden Daten und die Möglichkeit der Verwendung dieser Informationen für Persönlichkeitsprofile einzelner Nutzerinnen und Nutzer eine wachsende Bedrohung für die ungehinderte Wahrnehmung der genannten verfassungsrechtlichen Rechte darstellen.

Auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich daher im Rahmen ihres Eckpunktepapiers „Ein modernes Datenschutzrecht für das 20. Jahrhundert“ für die Einführung eines Mediennutzungsgeheimnisses ausgesprochen. Das Nutzungsverhalten des Einzelnen im Internet ist ein wesentlicher Schlüssel zur Profilbildung von Individuen. Daher sollte ein modernes Datenschutzrecht den Grundsatz einer unbeobachteten Inanspruchnahme elektronischer Dienste garantieren.

5. Internetprotokolladressen

Eine Klarstellung, wonach der gesetzliche Datenschutz auch für Internetprotokolladressen gilt, die von Telemedienanbietern gesammelt werden, wird befürwortet. Zwar sind die Datenschutzbeauftragten des Bundes und der Länder bereits der Auffassung, dass IP-Adressen Daten mit Personenbezug darstellen und damit den Anwendungsbereich des Datenschutzrechts eröffnen. Diese Auffassung hat bislang jedoch keine feste richterrechtliche Bestätigung gefunden. Insoweit würde bereits eine gesetzliche Klarstellung der Rechtssicherheit dienen.

Gleichzeitig ist jedoch auch darauf hinzuweisen, dass die IP-Adresse nur ein Merkmal der personellen Identifizierbarkeit darstellt. Der Einsatz von Cookies oder Browserfingerprints stellen weitere Gefährdungsszenarien dar, die ebenfalls bedacht und bei einer Novellierung des TMG berücksichtigt werden sollten.

6. Internetnutzungsprofile

Das Erstellen von Internetnutzungsprofilen wird derzeit von der Diskussion um die Umsetzung der EU-Privacy-Richtlinie bestimmt. Diese sieht an sich für die Speicherung von Informationen oder den Zugriff auf Informationen, die bereits im Endgerät eines Nutzers gespeichert sind - insbesondere für das Setzen von Cookies - ein Opt-In-Verfahren vor, bei dem der betreffende Nutzer explizit zustimmen muss (Art. 2, Nr. 5 der Richtlinie 2009/136/EG zur Änderung der Richtlinie 2002/58/EG).

Diese Auslegung der Richtlinie ist jedoch nicht unumstritten. In Deutschland ist eine Umsetzung trotz Ablaufs der Umsetzungsfrist bislang nicht erfolgt. In den Mitgliedstaaten gibt es erhebliche Unterschiede bei der Umsetzung: Die EU-Kommission ist offenbar der Ansicht, dass ein Nutzer, der auf den Einsatz von Cookies hingewiesen wird, durch Weiternutzen des Angebots eine konkludente Zustimmung erteilt. Damit

bleibt die so verstandene Regelung im Ergebnis noch hinter dem Opt-In-Erfordernis zurück.

In Deutschland bleibt es derweil bei der Regelung in § 15 Absatz 3 TMG, wonach der Diensteanbieter insbesondere für Zwecke der Werbung pseudonyme Nutzungsprofile erstellen darf, soweit der Nutzer dem nicht widerspricht. Soweit daher im Einzelfall keine personenbezogenen Daten erhoben werden, für die nach § 12 Absatz 1 TMG eine Einwilligung erforderlich wäre, ist ein Setzen von Cookies nur im Rahmen eines Opt-Out-Verfahrens zulässig.

Das von der EU-Privacy-Richtline nach Auffassung der Aufsichtsbehörden für den Datenschutz vorgesehene Opt-In-Verfahren würde demgegenüber die Rechte von Nutzern und Verbrauchern stärken und letztlich auch einer richtlinienkonformen Umsetzung der Richtlinie 2009/136/EG dienen.

7. Schutz vor Ausspionierung des Nutzers durch „Spyware, „Web-Bugs“ u.s.w.

   Soweit die vom EU-Parlament 2009 geänderte Datenschutzrichtlinie für elektronische Kommunikation (Richtlinie 2009/136/EG) vorliegend in Bezug genommen wird, sieht die Änderung der Datenschutzrichtlinie für elektronische Kommunikation künftig vor, dass die Speicherung von Informationen oder der Zugriff auf Informationen, die bereits im Endgerät eines Teilnehmers oder Nutzers gespeichert sind, nur gestattet ist, wenn der betreffende Teilnehmer oder Nutzer auf der Grundlage von klaren und umfassenden Informationen, die er gemäß der Richtlinie 9546/EG u.a. über die Zwecke der Verarbeitung erhält, seine Einwilligung gegeben hat. Diese Regelung ist bislang noch nicht in nationales Recht umgesetzt worden, so dass eine entsprechende Regelung zu begrüßen wäre (s. zuvor unter 6.)

8. Transparenz von Speicherfristen
   Eine Erweiterung der Informationspflicht nach § 13 Absatz 1 TMG auf die konkrete Speicherdauer der Nutzungsdaten wird unterstützt.

9. Koppelungsverbot
   Eine Implementierung des Koppelungsverbots sowie entsprechender rechtlicher Sanktionsmaßnahmen würde die Rechte von Verbrauchern und Nutzern stärken und ist daher zu begrüßen.

10. Schutz vor unangemessenen Datenverarbeitungseinwilligungsklauseln

Gegen einen lediglich deklaratorisch wirkenden Hinweis darauf, dass Datenverarbeitungseinwilligungsklauseln einer gerichtlichen Sicherheitskontrolle der AGB unterliegen, bestehen keine Bedenken.

Für Rückfragen stehe ich Ihnen gern jederzeit zur Verfügung.

Mit freundlichen Grüßen

Prof. Dr. Johannes Caspar