ULD

www.datenschutzzentrum.de

ULD • Postfach 71 16 • 24171 Kiel

Herrn Bernd Voß
Schleswig-Holsteinischer Landtag
Vorsitzender des Europaausschusses
Düsternbrooker Weg 70
Landeshaus
24105 Kiel

Schleswig-Holsteinischer Landtag
Umdruck 17/1645

Holstenstraße 98
24103 Kiel
Tel.: 0431 988-1200
Fax: 0431 988-1223
Ansprechpartner/in:
Herr Dr. Weichert
Durchwahl: 988-1200

Aktenzeichen:
LD -61.03/04.129

Kiel, 3. Dezember 2010

Erhalt des neutralen Zugangs zum Internet - Netzneutralität
22. Sitzung des Europaauschusses am 08.12.2010, Tagesordnungspunkt 1

Sehr geehrter Herr Voß,
sehr geehrte Damen und Herren Abgeordnete,

zur Vorbereitung der in der Bezugszeile genannten Ausschusssitzung gebe ich Ihnen hiermit zum genannten Thema vorab Informationen und Einschätzungen mit dem anliegenden Text.

Für Rückfragen stehe ich – auch außerhalb der Ausschusssitzung – gerne zur Verfügung.

Mit freundlichen Grüßen

Thilo Weichert

Netzneutralität und Datenschutz

Thilo Weichert
Landesbeauftragter für Datenschutz Schleswig-Holstein
Leiter des Unabhängigen Landeszentrums für Datenschutz (ULD), Kiel

I. Einleitung

Die Europäische Kommission hat Ende Juni 2010 eine *Konsultation zur Netzneutralität* eingeleitet (Ende am 30.09.2010; Ergebnisse liegen noch nicht vor). Dabei geht es der EU-Kommission um die Klärung der Frage, inwieweit es Internet-Anbietern erlaubt sein soll, beim Verkehr im Netz Differenzierungen vorzunehmen und insbesondere bestimmte Verkehrsarten zu bevorzugen bzw. zu benachteiligen. Motivation der EU-Konsultation ist es, Probleme bzw. Nachteile für die Nutzenden zu vermeiden. Die Verbraucher sollen grds. Zugang zu allen Diensten und Inhalten haben.

Hintergrund der Konsultation und einer in der Netzgemeinde heftig geführten Diskussion ist, dass zunehmend Internet-Dienste angeboten und in Anspruch genommen werden, die *hohe Übertragungskapazitäten* verlangen. Dies gilt z.B. für das Internet-Fernsehen, das Videosharing oder die Internet-Telefonie. Trotz massiven Netzausbaus kann es dadurch zu Datenstaus kommen. Dies gilt für das Festnetz, in stärkerem Maße aber für das mobile Internet. Dies wiederum veranlasst Internet-Diensteanbieter, zwischen schnelleren Premium- und langsameren Normaldiensten zu unterscheiden, wobei als Differenzierungskriterien nicht nur die benötigten Bandbreiten sind, sondern auch die Entgeltlichkeit der Inanspruchnahme des Dienstes oder die Herkunft und Identität des Anbieters des genutzten Dienstes (EU-Kommission, 30.06.2010, IP/10/860, Public consultation on the open internet and net neutrality; künftig „Konsultation").

Die Diskussion über die Netzneutralität wurde lange Zeit vorrangig in den *USA* geführt, wo Geschäftsmodelle, die auf einer Differenzierung im Internet-Verkehr basieren, weiter fortgeschritten sind als in Europa. Die Diskussion erhielt dadurch Schwung, dass der Webanbieter Google sein Interesse bekannt gab, dem TK- und Infrastrukturkonzern Verizon gesondert dafür zu zahlen, dass ihm beim Datentransport Vorfahrt eingeräumt wird.

Die Diskussion ist inzwischen in *Europa und Deutschland* angekommen, spätestens seit der Chef der Telekom René Obermann als Netzbetreiber laut darüber nachdachte, datenintensive Dienste wie z.B. von Google oder Apple stärker zur Kasse zu bitten. Besondere Anforderungen an Netzsicherheit und Übertragungsqualität hätten ihren – besonderen – Preis. Im Vordergrund der Diskussion steht die Befürchtung, dass Innovation und Pluralität im Netz durch wettbewerbsschädigendes Marktverhalten und diskriminierende Preismodelle beeinträchtigt werden.

In der *Politik* wurde bisher die Bedeutung der Netzneutralität immer wieder betont, so z.B. durch US-Präsident Barack Obama. Auch im schwarz-gelben Koalitionsvertrag auf Bundesebene vom Herbst 2009 wird zugesichert, man werde „die Entwicklung ... sorgfältig beobachten und nötigenfalls mit dem Ziel der Wahrung der Netzneutralität gegensteuern". Vergleichbare Bekenntnisse sind aus praktisch allen politischen Lagern auf Bundesebene zu vernehmen.

Das Internet ist inzwischen zu einer gesellschaftlich relevanten Infrastruktur geworden, deren Bedeutung für die gesellschaftliche Kommunikation inzwischen teilweise existenziell ist. Es ergänzt nicht mehr nur bestehende Kommunikationskanäle, sondern verdrängt diese und hat diese teilweise überflüssig gemacht, so dass deren Pflege nicht mehr oder nicht hinreichend betrieben wird. Zur Sicherung der *Kommunikations-Daseinsvorsorge* wird das Internet ähnlich wichtig wie die Bereitstellung von Wasser, Wärme, Strom oder Verkehrsinfrastruktur. Dadurch wird die Frage relevant, inwieweit ein Netzzugang technisch, räumlich, organisatorisch und rechtlich offen und diskriminierungsfrei gewährleistet ist. Und es stellt sich die Frage, inwieweit eine faktische ökonomische und soziale Differenzierung beim Netzzugang (noch) hingenommen werden kann.

II. Datenschutzrelevanz

Auf den ersten Blick hat diese Diskussion keine direkten Bezüge zum Datenschutz. Weder wurde bisher die Forderung aufgestellt, dass personenbezogene Merkmale von Datenpaketen zur *Differenzierung im Netzverkehr* herangezogen werden sollen, noch wurde der Datenschutz selbst als Differenzierungskriterium ins Spiel gebracht. Dessen ungeachtet verdient die Frage nach der Relevanz der Netzneutralität für den Datenschutz eine nähere Betrachtung und eine adäquate Antwort.

Tatsächlich basieren sämtliche Ansätze der Netz-Differenzierung angesichts dessen, dass es sich bei dem globalen Internet derzeit noch um ein weitgehend *unreguliertes dummes Netz* handelt, auf der Analyse von Datenpaketen hinsichtlich Art, Umfang, Inhalte oder Dienstleister (Deep Packet Inspection). Hinter Anbieterdiskriminierungen können sich Versuche zur Beeinflussung der Meinungsbildung verbergen. So wird berichtet, dass der Internet-Anbieter Freenet den Zugang zu bestimmten Webseiten gesperrt habe, weil diese sich kritisch mit dem Geschäftsgebaren der Firma auseinandergesetzt hätten. Letztlich sind auch Preismodelle und Differenzierungen nach der Kontrollierbarkeit der Kommunikation oder der Identität des Nutzenden vorstellbar. Netzaktivisten kritisieren, dass schon heute manche Flatrates Mogelpackungen seien, weil die Provider selektiv die Geschwindigkeit verlangsamen, ohne dies transparent zu machen. Würde für die Netznutzung generell eine Identifizierungspflicht eingeführt, so würde dies nicht nur die Netzneutralität beeinträchtigen, sondern zugleich einen Eingriff in die tatsächliche wie potenzielle informationelle Selbstbestimmung der Netznutzenden darstellen.

Differenzierungen nach individuellen *Merkmalen der Netznutzenden*, z.B. Alter, Geschlecht, Wohnort, Zahlung, Staatsangehörigkeit, Beruf, können grds. einen legitimen Hintergrund haben. So kann dies dem Jugendschutz dienen, aber auch der inhaltlichen Exklusion, z.B. des spielsüchtigen Spielers von bestimmten Onlinespielen.

Weiterhin kennen wir von anderen Netzwerken der Daseinsvorsorge die Differenzierung nach dem Preis. Da mit der Bereitstellung des Netzes eine kostenträchtige Dienstleistung erbracht wird, kann nicht generell ausgeschlossen werden, hierfür einen Preis zu verlangen. Auch eine *Preisdifferenzierung* nach bestimmten Merkmalen, z.B. den Umfang oder den Grund der Inanspruchnahme, kennen wir aus der Bereitstellung von Wasser, Strom oder Energie. Profit ist ein legitimes Streben der Internet-Anbieter. Profitoptimierung kann diesen Anbietern daher nicht generell untersagt werden.

Schließlich kann auch eine *Identifizierungspflicht* bei spezifischen Internet-Angeboten nicht ausgeschlossen werden. Dies gilt nicht für den Netzzugang selbst sowie die Nutzung allgemeiner Angebote, z.B. Informationsangebote. Demgemäß sieht das Telemediengesetz eine generelle Pflicht zur anonymen oder zumindest pseudonymen Bereitstellung von Diensten vor (§ 13 Abs. 6 TMG). Doch können zwingende Identifizierungen der Nutzenden gerechtfertigt sein, z.B. bei höchstpersönlichen Diensten, zwecks Sicherung der Zahlung oder vertraglichen Zuordnung, bei spezifischen Gefahren, evtl. sogar zum Zweck der Strafverfolgung. Insofern hat die Diskussion über die Vorratsdatenspeicherung auch eine Dimension in Bezug auf die Netzneutralität. Der EU-Kommission ist die Möglichkeit bewusst, dass Datenverkehr auf Inhalte hin überprüft wird, z.B. um rechtlichen Pflichten, insbesondere im Hinblick auf illegale Inhalte, zu genügen (EU-Kommission, Konsultation, S. 6). Die Diskussion über sog. Netzsperren wird intensiv geführt, z.B. im Hinblick auf die Verhinderung von Kinderpornografie im Netz. Eine Inhaltsprüfung berührt in besonderem Maße die Telekommunikationsfreiheit nach Art. 10 GG. Sie ist nach deutschem Verfassungsrecht systematisch verboten und gesetzlich nur im Einzelfall ausnahmsweise erlaubt (vgl. z.B. § 100a StPO). Dies gilt nicht nur gegenüber staatlichen, sondern auch gegenüber privaten Stellen wie den Netzanbietern (§ 85 TKG).

Adressaten der Diskussion über Netzneutralität sind primär die privaten Internet-Netzanbieter und sekundär die sonstigen privaten Internet-Diensteanbieter mit ihren jeweiligen Geschäftsmodellen.

Doch auch öffentliche Stellen sind betroffen und gefordert. Dies gilt zum einen natürlich für die öffentlichen Internet-Dienstleister, soweit sie sich im Wettbewerb zu privaten Dienstleister befinden, erst recht aber für staatliche oder hoheitliche Monopolangebote. Gefordert ist in jedem Fall außerdem der Staat mit seinen Regulierungsmöglichkeiten und -pflichten.

Im Vordergrund der Debatte stehen die *rechtlichen Vorgaben* für die Netz- und Diensteanbieter: Welche Verpflichtungen können und müssen diesen zur Wahrung eines offenen und freien Netzes auferlegt werden, welche Rechte haben diese? Welche Differenzierungen, z.B. nach Transportart, Diensteart oder Inhalt sind legitim und rechtlich zuzulassen, welche nicht? Dabei sind die Grenzen zwischen den reinen Netznutzenden, den Diensteanbietern und den Netzanbietern fließend. Bei dieser Diskussion spielt der Schutz informationeller Selbstbestimmung eine Rolle, wenn wir es bei den Nutzenden oder den Diensteanbietern mit identifizierbaren natürlichen Personen zu tun haben.

III. Netzneutralität nach Verfassung und Gesetz

Der Begriff der Netzneutralität ist dem deutschen Recht bisher fremd. Hintergrund sind zum einen die *Gewährleistungspflichten* des Staates für die Bereitstellung und Erhaltung gemeinwohlbezogener Versorgungsnetze. Aus Art. 87 f. Abs. 1 GG lassen sich für die Telekommunikation spezifische staatliche Gewährleistungspflichten als Ausdruck seiner Infrastrukturverantwortung ableiten. Beim Internet begründet sich diese Gewährleistungspflicht auch aus den Grundrechten; ihm kommt auch die Aufgabe der Grundrechtsverwirklichung zu. In unserer globalen Informationsgesellschaft ist das Internet ein Instrument zur Verwirklichung der in Art. 5 GG garantierten Grundrechte der Meinungsäußerungs- und der Informationsfreiheit sowie der Pressefreiheit. Doch auch im Hinblick auf die Verwirklichung weiterer Grundrechte, insbesondere der Sicherstellung der Berufsausübung (Art. 12 GG) sowie der Eigentumsnutzung (Art. 14 GG), kommt dem Internet eine zunehmend wichtige Funktion zu. Es ist davon auszugehen, dass künftig das Internet für die Verwirklichung vieler weiterer Grundrechte grundlegend sein wird; in der Informationsgesellschaft wächst den Grundrechten eine digitale Dimension zu.

Dies gilt auch und insbesondere für das *allgemeine Persönlichkeitsrecht* in seiner spezifischen Ausgestaltung des Grundrechts auf informationelle Selbstbestimmung. Da das Internet für die Wahrung des Datenschutzes eines zunehmenden Teils der Bevölkerung Relevanz erhält, obliegen dem Staat insofern Bereitstellungs-, Sicherungs-, Schutz- und Regulierungspflichten.

Der Begriff der Netzneutralität ist nichts anderes als ein *netzbezogenes Diskriminierungsverbot*. Nach Art. 3 Abs. 1 GG sind alle Menschen vor dem Gesetz gleich. Art. 3 Abs. 3 GG begründet spezifische Diskriminierungsverbote (hinsichtlich Geschlecht, Abstammung, Rasse, Sprache, Heimat und Herkunft, Glauben, religiöser oder politischer Anschauung). Ähnliche Gewährleistungen enthält die seit 01.12.2009 in Kraft befindliche Europäische Grundrechtecharta (Art. 20 ff. EU-GR-Charta).

Adressat des Auftrags zur Gleichbehandlung und zur Nichtdiskriminierung ist primär der Staat. Doch beschränkt sich dieser Auftrag nicht hierauf. Die allgemeine wirtschaftliche Handlungsfreiheit wird auch gegenüber privaten Wirtschaftsunternehmen aus Gleichheitsgründen eingeschränkt, insbesondere wenn der Anbieter Monopolist ist oder eine marktbeherrschende Stellung hat und es sich bei der erbrachten Dienstleistung um eine wichtige Existenzgrundlage für die Konsumenten handelt (sog. Drittwirkung). Insofern kann sich für den Staat zum Schutz der Netzneutralität eine gesetzliche Handlungspflicht ergeben.

Besteht dagegen für den Konsumenten auf dem Markt ein umfangreiches, *pluralistisches Angebot*, so hat der Anbieter die Freiheit der Auswahl seiner Vertragspartner und die Möglichkeit einer Diskriminierung wegen bestimmter Merkmale. Individuelle subjektive Diskriminierung ist in der analogen Welt grds. eine Form der Freiheitsbetätigung. Die Ausrichtung eines Angebots am Preis ist hierbei eines der am weitesten verbreiteten und akzeptierten Differenzierungskriterien. Die Sicherung der Pluralität von Angeboten und damit der Neutralität des Gesamtangebotes eines Marktes obliegt vorrangig dem Kartellrecht, über das die Entstehung von Monopolen verhindert werden soll.

In den *USA* findet bereits eine intensivere Diskussion über Netzneutralität – im Sinne einer neutralen Datenübermittlung im Internet – statt. Das Netz soll unwissend, d.h. v.a. dienste- und applikationsneutral, Datenpakete transportieren. Für die Regulierung des Telekommunikationsmarktes ist in den USA die Federal Communications Commission (FCC) zuständig. Diese hat Gruppen von Anwendungsfällen für die Netzneutralität entwickelt, die für die deutsche und europäische Diskussion fruchtbar gemacht werden können.

Im Vordergrund stehen vier *Grundsätze der FCC*. Danach sind die Verbraucher berechtigt,
- je nach ihrer Wahl Zugang zu legalen Internet-Inhalten zu erhalten,
- alle Dienste und Applikationen ihrer Wahl zu nutzen, wobei sie jedoch den Bedürfnissen der Strafverfolgung Rechnung tragen müssen,
- alle legalen Endgeräte ihrer Wahl anzuschließen und zu nutzen, soweit dies nicht das Netz schädigt,
- Netz-, Dienste-, Service- und Internet-Anbieter in einem Wettbewerbsverhältnis vorzufinden.

Die FCC akzeptiert Vorbehalte bzw. *Differenzierungen*, die sich aus der Kapazität des Netzes sowie aus der Verträglichkeit mit gesellschaftlichen und v.a. rechtlichen Anforderungen ergeben. Ein Anwendungsfall, der letztlich wegen politischen Einlenkens nicht rechtlich durchgesetzt werden musste, bezog sich auf ein Musikkonzert 2007, aus dem die Telefongesellschaft AT&T als Webcast-Sponsor zensierend und diskriminierend eine Passage herausschnitt, in der der damalige Präsident Bush wegen unzureichender Hilfen nach dem Hurrikan „Katrina" kritisiert wurde. Ein aktueller Fall ist das Abschalten des Wikileaks-Angebots durch den Internet-Konzern Amazon auf Veranlassung der US-Regierung, nachdem der Inhaltsanbieter bisher nicht öffentliche Botschaftsdepeschen ins Netz gestellt hatte.

Gemäß *Planungen* von September 2009 zieht die FCC zwei weitere Prinzipien in Erwägung:
- das Diskriminierungsverbot für Breitbandanbieter gegenüber legalen Internet-Diensten und -Anwendungen durch Blockaden oder Verlangsamung, es sei denn, Netzüberlastungen, Rechts- oder Qualitätsanforderungen (Quality of Service) machen dies nötig,
- die Pflicht zur Transparenz der Netzmanagement-Praktiken der Netzanbieter.

Im April 2010 wurden die Bestrebungen der FCC zur Sicherung der Netzneutralität in Frage gestellt, als ein Berufungsgericht der FCC Auflagen zur Regulierung untersagte, weil es keine klaren rechtsstaatlichen Regelungen hierfür gebe.

Auch im *europäischen Rahmen* spielen bei der Realisierung von Netzneutralität Transparenz und Dienstequalität zentrale Rollen. Die TK-Universalrichtlinie fordert vergleichbare, angemessene und aktuelle Endnutzerinformationen über die Qualität ihrer Dienste für die Verbraucher (Art. 20, 21 Richtlinie 2009/136/EG vom 25.11.2009 zur Änderung Richtlinie über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten).

Im *Allgemeinen Gleichbehandlungsgesetz* (AGG) hat der Neutralitäts- bzw. Gleichheitsgedanke Einzug ins Privatrecht und ins Verbraucherrecht gefunden. Diskriminierungsverbote bestehen hinsichtlich Rasse ethnischer Herkunft, Geschlecht, Religion und Weltanschauung, Behinderung, Lebensalter und sexueller Identität. Klassische Anwendungsfälle sind Massen- und Distanzgeschäfte, bei denen keine individuelle Geschäftsbeziehung besteht und der Bewertung der Vertragspartner nach bestimmten Eigenschaften, Merkmalen und Scores (mathematisch-statistische Berechnung auf der Basis mehrerer Merkmale) eine besondere Bedeutung zukommt. Typisch hierfür sind Verträge im Telekommunikations- und Telemedienbereich. Hierbei spielt der Einsatz von Informationstechnik eine zentrale Rolle.

Gesetzliche Antworten auf mögliche digitale Diskriminierungen sind noch wenig entwickelt. Tatsächlich finden sich insofern keine dezidierten Regelungen im allgemeinen Zivilrecht, im Verbraucher-, im Wettbewerbs- oder im Telekommunikationsrecht. Eine Ausnahme ist das Daten-

schutzrecht. In § 6a Bundesdatenschutzgesetz (BDSG) werden automatisierte belastende, d.h. diskriminierende, Einzelentscheidungen auf der Basis von Merkmalen oder statistischen Berechnungen verboten, soweit nicht Transparenz und die Möglichkeit der Einflussnahme durch die Betroffenen gewährt werden. In § 28b BDSG werden Wahrscheinlichkeitswerte (Scores) in privatrechtlichen Vertragsverhältnissen materiellrechtlichen Anforderungen unterworfen (Wissenschaftlichkeit, Relevanz, Transparenz). Durch Erklären eines Widerspruchs kann ein Marktteilnehmer die Nutzung des Scores ausschließen (§ 35 Abs. 5 BDSG).

Datenschutz kann ein *Qualitätsmerkmal* für Netzdienste (Quality of Service) sein. Entsprechende normative Vorgaben im Interesse des Verbraucherschutzes bzw. generell des Grundrechtsschutzes bestehen heute noch nicht; sie können eine Ungleichbehandlung von Netzdiensten rechtfertigen.

IV. Datenschutz nach Verfassung und Gesetz

Das Grundrecht auf informationelle Selbstbestimmung gewährt bzgl. der Verarbeitung von Daten natürlicher Personen deren Wissen und deren Bestimmenkönnen hierüber. Es beinhaltet die Befugnis der Person, grds. selbst festzulegen, „wer was wann und bei welcher Gelegenheit über sie weiß" (BVerfG NJW 1983, 419, 422). Hierbei geht es um die Verwirklichung der *allgemeinen Persönlichkeitsrechte* und speziell der demokratischen, sozialen und ökonomischen Freiheitsrechte in ihrer informationellen Dimension. Als besonderes Grundrecht hat das BVerfG 2008 das Recht auf Gewährleistung der Integrität und Vertraulichkeit der eigenen informationstechnischen Systeme als spezifische digitale Privatsphäre abgeleitet (BVerfG NJW 2008, 822). Auch dieses Grundrecht hat Netzrelevanz, da sich die selbstgenutzten IT-Anwendungen nicht mehr auf die eigenen Rechnersysteme beschränken, sondern Internet-Nutzungen einschließen.

Soweit die digitalen Grundrechte sich auf die Abwehr von Angriffen durch öffentliche oder private Stellen beziehen, spielen Gleichbehandlung und Diskriminierungsfreiheit keine wesentliche Rolle. Da jedoch diesen Grundrechten auch eine *Gewährleistungsfunktion* zukommt, ist der gleiche freie Zugang zu IT-Netzen und deren Nutzung relevant. Über die staatlichen Gewährleistungspflichten und die Drittwirkung des digitalen Grundrechtsschutzes sind sowohl der Staat wie auch vor allem marktbeherrschende Unternehmen in der Pflicht, diese Grundrechte nicht nur zu respektieren, sondern auch – im Rahmen des Möglichen und Zumutbaren – zu verteidigen und deren diskriminierungsfreie Inanspruchnahme zu sichern. Grundrechte in der digitalen Welt, insbesondere das Recht auf informationelle Selbstbestimmung als Generalgrundrecht, haben somit gleichheitsrechtliche Ausprägungen. Es kann unterschieden werden zwischen informationellen Diskriminierungsverboten und zulässiger bzw. sogar rechtlich geforderter Ungleichbehandlung.

Hinsichtlich der *Diskriminierungsverbote* sei zunächst auf das AGG verwiesen und die dort genannten, nicht oder nur begrenzt nutzbaren Merkmale: Geschlecht, Abstammung, Rasse, Sprache, Heimat und Herkunft, Glaubens, religiöse oder politische Anschauung. Eine weitere Kategorie ergibt sich direkt aus der Grundrechtsgewährleistung und dem Rechtsstaatsprinzip: die aktive Wahrnehmung von subjektiven Rechten, u.a. von Datenschutzrechten, d.h. der Ansprüche auf Auskunft, Widerspruch, Berichtigung, Löschung, Sperrung, Gegendarstellung und Petition. Ein Anspruch auf weitgehende diskriminierungsfreie Grundrechtsausübung besteht weiterhin bzgl. politischer Rechte, also der Meinungsfreiheit, der politischen und gewerkschaftlichen Vereinigungsfreiheit, der Versammlungsfreiheit und der Religionsfreiheit. Die legale Inanspruchnahme dieser Rechte kann in keinem Fall eine Schlechterstellung im Netzverkehr rechtfertigen.

Hinsichtlich *sonstiger Freiheitsrechte*, insbesondere der Ausübung der Berufsfreiheit und des Eigentumsrechts, können netzspezifische Anforderungen Grenzziehungen nötig machen. Generell gilt, dass hinsichtlich des jeweils verfolgten Zwecks eine erforderliche und verhältnismäßige Grundrechtsbegrenzung erfolgt. Regelmäßig werden die Begrenzungen der Freiheitsrechte sich nicht direkt auf die Netznutzung beziehen, sondern sich wegen sonstiger rechtlicher Begrenzungen indirekt ergeben. Sind diese Begrenzungen gesetzlich begründet und rechtlich geboten, so ergibt sich hieraus eine gerechtfertigte Ungleichbehandlung. Derartige zulässige und gesetzlich gedeckte

Diskriminierungszwecke sind z.B. die der Strafverfolgung oder der Gefahrenabwehr, die Aufrechterhaltung der Netzfunktionalität, aber auch der Verbraucherschutz oder die Erreichbarkeit und Funktionsfähigkeit öffentlicher Einrichtungen.

Gesetzlich festgelegt werden können auch *besondere Datenschutzgründe* zur Bevorzugung im Netzverkehr, die eine Positivdiskriminierung zur Folge haben. So ist z.B. eine Bevorzugung von Netzverkehr vorstellbar, dessen Gesetzeskonformität in einem formellen Verfahren nachgeprüft und bestätigt wurde. Gerade angesichts des gewaltigen Vollzugsdefizits im Datenschutz kann hierin eine geringer eingreifende Maßnahme gegenüber einer generellen Lizenzierungspflicht gesehen werden. Einen derartigen Regelungsansatz, beschränkt auf das Vergaberecht, verfolgt § 4 Abs. 2 Landesdatenschutzgesetz Schleswig-Holstein (LDSG SH), der einen vorrangigen Einsatz von IT-Produkten vorsieht, „deren Vereinbarkeit mit den Vorschriften über den Datenschutz und die Datensicherheit in einem förmlichen Verfahren festgestellt wurde". Denkbar ist auch eine Bevorzugung bei nachweislicher Übererfüllung der Datenschutzpflichten. Solche Zertifikate (Auditzeichen/Gütesiegel) stehen derzeit im Rahmen der Einrichtung einer Stiftung Datenschutz auf Bundesebene als Marktinstrumente zur Diskussion.

Ob Datenschutzzertifikate zur *Zugangsvoraussetzung zum Netz* gemacht werden sollen und können, muss in Frage gestellt werden. Das Internet ist nicht per se ein Instrument der Gefahr und der (z.B. Datenschutz-) Kriminalität, sondern eine Plattform zur vielfältigen Verwirklichung von Freiheiten in der digitalen Welt. Eine Besonderheit fast sämtlicher Internet-Anwendungen ist, dass diese neutral in dem Sinne sind, dass sie für nützliche wie für schädliche Zwecke, zum Guten wie zum Schlechten genutzt werden können. Dies ändert aber nichts an der Notwendigkeit der Festlegung spezifischer Netznutzungsregelungen, bei der privilegierte Nutzungen an spezifische Anforderungen geknüpft werden, so wie dies z.B. nach dem De-Mail-Gesetz hinsichtlich einer gesicherten E-Mail-Kommunikationsstruktur der Fall sein soll.

Nach den Regelungen des BDSG erfolgt *Datenschutzkontrolle* grds. anlasslos bzw. ist anlasslos möglich (§ 38 Abs. 1 BDSG). Dieses Prinzip ist erforderlich, weil eine Vielzahl von Verletzungen des Datenschutzes und der Datensicherheit anders nicht festgestellt und geahndet werden können. Insofern ist es denkbar, dass zertifizierten Internet-Anwendungen auch im Hinblick auf Datenschutzprüfungen Vorfahrt eingeräumt wird, soweit das Zertifikat einen adäquaten Ausgleich zum Risiko des jederzeitigen Geprüftwerdens darstellt. Angesichts des derzeit bestehenden gewaltigen Vollzugs- und Kontrolldefizits gehen aber heute solche Netzprivilegierungen noch an der Realität vorbei. Es stellt sich eher die Frage, inwieweit es einen Verstoß gegen die Netzneutralität darstellt, dass umfassende und weit verbreitete Datenschutzverstöße unsanktioniert bleiben und hinsichtlich der Sanktionen mit Beanstandung, Veröffentlichung, Auflage, Bußgeld oder gar Verbot eine weit auseinanderklaffende Praxis besteht.

Insofern soll auf das Instrument des § 38a BDSG verwiesen werden, das die aufsichtliche Genehmigung von *Branchenverhaltensregeln* im Bereich des Datenschutzes vorsieht. Hierbei handelt es sich um eine Form gesetzlich regulierter Selbstregulierung. Solche durch Branchenverbände entwickelte Netznormen (hier für den Datenschutz) sind nur in Ausfüllung gesetzlich vorgegebener Regelungen vorstellbar. Anderenfalls könnten diese Gefahr laufen, bestimmte Netzangebote durch Branchenverbände beherrschende Unternehmen zu bevorzugen oder zu benachteiligen. Das Instrument der (datenschutzrechtlichen) Verhaltensregel soll Praxis- und Techniknähe sowie zugleich Technikoffenheit und Entwicklungsfähigkeit gewährleisten, ohne Kartellentwicklungen zu begünstigen. Ein erster Ansatz einer solchen Verhaltensregel ist der aktuelle Vorschlag des BITKOM für einen Verhaltenskodex für Internet-Panoramadienste.

Ähnliche Effekte wie Verhaltensregeln sind durch *Standardisierungen* möglich. Datenschutzstandardisierungen befinden sich derzeit noch in einem sehr frühen Stadium. Deutschland nimmt insofern weltweit national wie auch in internationalen Standardisierungsorganisationen wie ISO/IEC eine führende Rolle ein. Standardisierungen müssen einem Gemeinwohlziel dienen. Dies kann die Interoperabilität sein, aber auch ein bestimmtes Schutzniveau für Nutzende oder Verbraucher, z.B. in

Bereich Datenschutz und Datensicherheit. Bei der Standardisierung muss jedoch darauf geachtet werden, dass Raum für Innovationen verbleibt. Nicht entwicklungsoffene Standards können dazu führen, dass u.U. besonders innovative, Datenschutz fördernde Anbieter und deren Technologie sich auf dem Markt nicht etablieren können.

Nicht nur Vollzugsdefizite, auch *Regulierungsdefizite* können zu massiven Beeinträchtigungen der Netzneutralität führen. Auch insofern ist Datenschutz ein anschauliches Beispiel – im nationalen, europäischen wie auch globalen Rahmen. Weltweit bestehen derzeit noch keine normativ verbindlichen Datenschutzstandards. Erkennt man an, dass Datenschutz ein legitimes Anliegen im Netz ist, so führt das Fehlen gemeinsamer hoher Datenschutzstandards zur teilweisen Missachtung dieses Anliegens. Nationale Grenzen sind keine kommunikativen Grenzen. Da das Angebot im globalen Netz zudem nur schwer territorial begrenzt regulierbar ist, führen Regulierungsdefizite in Staaten mit keinem oder einem geringeren Datenschutz zwangsläufig zu faktischen Diskriminierungen.

Exemplarisch für dieses Phänomen sind die niedrigen bis nichtexistenten Datenschutzstandards in den USA und die daraus resultierende Missachtung deutscher oder europäischer Datenschutzstandards durch *US-Anbieter* wie z.B. Google, Apple oder Facebook. Besonders schwerwiegend wirkt sich dies dann aus, wenn der ausländische Anbieter ohne Datenschutzbindung zugleich Monopolist ist oder einem Oligopol von Anbietern angehört. Dies ist z.B. in Deutschland auf dem Suchmaschinenmarkt der Fall, wo Google einen Marktanteil von über 90% innehat. Derartige Angebote verstoßen zwar durch ihre Missachtung des Datenschutzes nicht selbst direkt gegen das Gebot der Netzneutralität, doch können sie ihre Marktmacht missbrauchen zur Verletzung der Netzneutralität, etwa indem der Zugang datenschutzkonformer Angebote zum Markt verhindert wird. Dies wäre z.B. der Fall, wenn der Suchmaschinenanbieter Google das datenschutzkonforme und zertifizierte Angebot der Metasuchmaschine www.ixquick.com von einer Nutzung ausschlösse.

Auch die Intransparenz des Suchmaschinenranking und die Bevorzugung von „befreundeten" Seiten bzw. zahlenden Angeboten beim Ranking entfalten diskriminierende Wirkungen und vertiefen die jeweiligen Datenschutzverstöße der Suchmaschinenanbieter. Eine solche Perpetuierung von Datenschutzverstößen lässt sich auch beim Phänomen des „umfriedeten Gartens" (*walled garden*) feststellen, für das Facebook ein anschauliches Beispiel ist: Das Unternehmen ignoriert sehr weitgehend die Grundsätze des Datenschutzes. Dies ist für die Nutzenden dadurch besonders gravierend, dass Facebook die Nutzenden durch seine Angebote und Anreize dazu zu animieren versucht, die von Facebook beeinflussten Dienste nicht zu verlassen. Dieser Effekt kann auch durch den Einsatz von Techniken erreicht werden, die mit der außerhalb des „Gartens" nicht kompatibel sind. Dieses Phänomen ist beim US-Anbieter Apple festzustellen.

Besteht *Pluralität verschiedener Angebote* auf einem Netzmarkt, so sollte sich der Staat hinsichtlich eigener Interventionen zurückhalten. In dieser Situation ist er aber nicht durch den Grundsatz der Netzneutralität daran gehindert, datenschutzfördernd in der Form im Markt zu intervenieren, dass datenschutzfreundliche Angebote ausgezeichnet werden oder dass deren Entwicklung und Einführung finanziell unterstützt wird. Der Staat ist auch nicht gehindert, mit datenschutzfreundlichen Produkten selbst auf dem Markt präsent zu sein, solange dies für die Einführung datenschutzfördernder Technologien erforderlich scheint.

Kein Verstoß gegen den Gleichheitsgrundsatz und gegen das Gebot der Netzneutralität sind datenschutzrechtliche nationale oder supranationale *Datenschutzregulierungen*, soweit diese nicht dem Marktausschluss oder einer Marktabschottung, sondern dem Schutz informationeller Selbstbestimmung dienen. Insofern stellt der Datenschutz ein berechtigtes und zulässiges Differenzierungskriterium dar. Es ist also unter dem Aspekt der Netzneutralität nicht zu beanstanden, dass in Deutschland und Europa auch an außereuropäische Anbieter hohe Datenschutzanforderungen gestellt werden, die letztlich zu einem Marktausschluss in Europa führen können. Netzneutralität kann es aber gebieten, Diensten, die sich „freiwillig" einem dem europäischen vergleichbaren Datenschutzstandard unterwerfen, gleich zu behandeln wie europäische Anbieter.

V. Technische Rahmenbedingungen für Netzdifferenzierungen

Die Differenzierung beim Netztransport setzt im Rahmen des Daten-Verkehrsmanagements eine *Analyse der transportierten Datenpakete* nach den jeweiligen Differenzierungsmerkmalen voraus. Soweit bei der Differenzierung nach rein quantitativen Merkmalen, etwa dem Umfang eines Datenpaketes, vorgegangen wird, ergeben sich vorrangig wirtschaftliche und kaum datenschutzrechtliche Fragestellungen. Soll jedoch eine Differenzierung nach qualitativen Merkmalen vorgenommen werden, so setzt dies regelmäßig die Beeinträchtigung der Datensatzintegrität voraus; zugleich steigt die Gefahr der Beeinträchtigung der Freiheitsrechte im digitalen Raum. Es ist die Rede von einer „Deep Packet Inspection", bei der Merkmale wie Absender und Empfänger, Kostenpflichtigkeit, Datenformat, Diensteanbieter, ja Dateninhalte erfasst, ausgewertet und für die Entscheidung über den Netztransport genutzt werden können. Derartige Formen der Differenzierung greifen in die Grundrechte ein, insbesondere in das Grundrecht auf informationelle Selbstbestimmung und in die Telekommunikationsfreiheit der Nutzenden. Zwar gibt es bei diesen Formen der Differenzierung mehr und weniger schwere Eingriffe. Die größte Eingriffstiefe wird bei einer Inhaltsanalyse erreicht, gefolgt von einer Verkehrsdatenanalyse des jeweiligen Datenpakets im Hinblick auf den einzelnen Nutzenden. Aus grundrechtlicher Sicht stark einschneidend sind auch Differenzierungen nach der Identität des Diensteanbieters. Eine geringere Grundrechtsrelevanz haben dagegen objektivierte Selektionen nach Transportart, Dienstart und Datenformat.

Die grundrechtliche Bewertung der Paketanalyse hängt von der Art und Weise der technischen *Durchführung der Verkehrslenkung* ab. Grundsätzlich ist es denkbar, dass grundrechtskonforme Diskriminierungstools zum Einsatz kommen. Voraussetzung ist, dass bei der Konzeption und Realisierung der Werkzeuge auf Wahrung des Grundsatzes der Datensparsamkeit geachtet wird. Nur solche Merkmale dürfen erfasst und genutzt werden, die als gerechtfertigte Differenzierungskriterien geeignet und verhältnismäßig sind.

Um dieses Ziel zu erreichen, müssen technische, organisatorische und diese absichernde rechtliche *Vorkehrungen* getroffen werden. In jedem Fall ist das Prinzip der Datensparsamkeit zu beachten. Die Vertraulichkeit und Integrität der jeweiligen Datenpakete muss gewahrt bleiben. Hierbei können Instrumente der Verschlüsselung und der digitalen Signatur verwendet werden. Verkehrsdaten können anonymisiert oder zumindest pseudonymisiert werden. So ist es z.B. beim Einsatz von Bepreisungswerkzeugen des Cloud Computing als eine stark im Kommen befindliche Internet-Anwendung äußerst wünschenswert, dass den Cloud-Anbietern die Identität der Cloud-Nutzenden verborgen bleibt. Um insofern die nötige Vertrauenswürdigkeit der Differenzierungstools zu erlangen, dürfte regelmäßig kein Weg an einer unabhängigen vertrauenswürdigen und transparenten Zertifizierung vorbeigehen.

VI. Transparenz

Informationelle Selbstbestimmung setzt das Wissen der Betroffenen über die sie betreffende Datenverarbeitung voraus. Insofern ist Transparenz eine Grundvoraussetzung für den Datenschutz. Angesichts der Komplexität und der gesellschaftlichen Relevanz der Informationsverarbeitung beschränkt sich der Transparenzbedarf nicht auf die Betroffenen selbst, sondern schließt die *allgemeine Öffentlichkeit* mit ein.

Der politische, ökonomische, technische und rechtliche *öffentliche Diskurs* mit Interessierten, Kompetenten und Engagierten kann als Korrektiv für die oft unzureichende Medienkompetenz der Betroffenen wirken. Der Transparenzbedarf erstreckt sich auf den normativen Rahmen, die Datenverarbeitungspraxis, auf die Praxis der Aufsichtsbehörden und der Gerichte sowie auf die Wissenschaft. Hinsichtlich Netzthemen finden wir ein kritisches Potenzial in der sog. Netzgemeinde, im Wissenschaftsbetrieb und bei der Presse bzw. den Medien. Institutionell sind vor allem Datenschutzbehörden und Verbraucherschutzorganisationen aufgerufen, das gesellschaftliche Interesse an der Wahrung und Verteidigung informationeller Selbstbestimmung zu vertreten.

Transparenz erfüllt auch eine wichtige Funktion zur Wahrung der *Netzneutralität*. Ungleichbehandlung und Diskriminierung gedeihen am besten im Dunkeln. Die öffentliche Diskussion über die Rahmenbedingungen der Netznutzung ist der sicherste Garant für Gleichbehandlung durch Wirtschaft wie Verwaltung. Die Verbraucher, die Konkurrenz, die Politik und die öffentliche Meinung benötigen die für die Beurteilung des Netzgeschehens relevanten Informationen. Daher ist es nachvollziehbar, dass in den USA Transparenz als einer der Grundpfeiler zur Netzneutralität anerkannt ist. Auch in der EU ist der Grundgedanke eingeführt, wenngleich noch nicht in zureichendem Maße rechtlich sichergestellt (EU-Kommission, Konsultation, S. 3 f.). Die nationalen Regelungen hinken insofern weiter hinterher. Während Verbraucherinformationen in anderen Segmenten der Öffentlichkeit in großem Umfang zur Verfügung gestellt werden, besteht in Hinblick auf die Informationstechnik generell und den Netzbetrieb starker Nachholbedarf. Dies ist auch dem Umstand geschuldet, dass die Netzstrukturen noch jung und im starken Wandel sind und sich weitgehend außerhalb staatlicher Regulierung, Planung und Beeinflussung befinden.

Markttransparenz setzt aber nicht zwangsläufig aufsichtliches Handeln voraus. Sie kann auch direkt die *Marktteilnehmer* adressieren. Die privaten Netzstrukturen sind kein Grund zum Verzicht auf Transparenzanforderungen. Dabei können die bestehenden datenschutzrechtlichen Hinweis- und Benachrichtigungspflichten ergänzt werden durch marktrelevante Informationen sowie strukturelle Angaben über den IT-Einsatz. Generell von Relevanz sind Angaben zur Verantwortlichkeit, zur Einschaltung von Dienstleistern, zu eingesetzten Maßnahmen der Datensicherung, zu Art, Zweck und Umfang der Datenverarbeitung und der Datenauswertung und zu den Optionsmöglichkeiten der Nutzenden.

Parallel zur Markttransparenz müssen die *staatlichen Aufsichtsmaßnahmen* für die Öffentlichkeit nachvollziehbar und kontrollierbar sein. Dem dienen z.B. die Tätigkeitsberichte der Datenschutz- und Netzaufsichtsbehörden, deren Öffentlichkeitsarbeit und deren Stellungnahmen gegenüber politischen Entscheidungsträgern. Die demokratische Regulierung der Netze setzt objektive Information über das Netzgeschehen voraus, die von den Aufsichtsbehörden bereitgestellt werden kann und muss.

VII. Schlussfolgerungen

Die derzeit geführte Diskussion über Netzneutralität tendiert dazu, *Aspekte des Datenschutzes* und des Verbraucherschutzes sowie der Verteidigung individueller und demokratischer Grundrechte auszublenden. Sie fokussiert auf die Geschäftsmodelle und das wirtschaftliche Handeln der Netz- und der Diensteanbieter. Tatsächlich besteht ein enger Zusammenhang zwischen wirtschaftlichem Handeln im Netz, demokratischer Kultur der Informationsgesellschaft, dem Schutz digitaler Freiheiten und vor allem des Rechts auf informationelle Selbstbestimmung.

Datenschutz und Netzneutralität stehen nicht unvermittelt nebeneinander, sondern haben eine Vielzahl von *Berührungspunkten und Konvergenzen*. So wie dem Datenschutz eine Diskriminierung verhindernde Funktion zukommt, so kommt der Netzneutralität die Funktion der Wahrung der Grundrechte im digitalen Raum zu. Gemeinsame Basis ist die Herstellung größtmöglicher Transparenz über das Netzgeschehen, technisch, organisatorisch und wirtschaftlich. Insofern besteht zur Umsetzung der EU-TK-Universalrichtlinie Handlungsbedarf. Netzneutralität schließt nicht datenschutzrechtliche Regulierung aus, sondern bedingt diese. Datenschutzanforderungen sind noch zu etablierende, äußerst wünschenswerte Qualitätsstandards (Quality of Services). Derzeit verfolgt die EU jedoch noch ein restriktives, auf technische Funktionalität ausgerichtetes Verständnis von Dienstqualität, das lediglich Standards der Datensicherheit mit einschließt (EU-Kommission, Konsultation, S. 4, 8). Neben staatlicher Regulierung bietet sich hierbei regulierte Selbstregulierung der Unternehmen bzw. Unternehmensverbände an, z.B. in Form von Zertifizierungen, Standardisierungen und Verhaltensregeln.

Normativ festgelegte, *sachlich begründete Diskriminierung* im Netz kann für den Zweck des Grundrechtsschutzes nötig sein. Ausgeschlossen sind jedoch Differenzierungen nach den im AGG genannten Merkmalen sowie nach der Wahrnehmung individueller Rechte v.a. nach der Inanspruchnahme der persönlichen demokratischen Grundrechte. Datenpaketanalysen nach diesen Merkmalen verbieten sich aus Gründen des Datenschutzes ebenso wie aus Gründen der Netzneutralität.

Bei einem pluralistischen Angebot können faktische Marktdiskriminierungen durch private Netzanbieter unschädlich sein. Angesichts der *Marktkonzentration* im Internet ist aber eine dauernde kritische Hinterfragung der Politik der Marktakteure nötig sowie die staatliche Bereitschaft, zur Wahrung von Neutralität und Grundrechtsschutz zu intervenieren.

Marktmacht, proprietäre Standards und nutzerbindende Einstellungen und Praktiken einiger US-amerikanischer Anbieter konterkarieren Bestrebungen zur Nutzerneutralität. Durch das Ignorieren von europäischen bzw. deutschen Datenschutzanforderungen stellen sie zugleich eine Gefahr für digitale Bürgerrechte dar. Dem kann und sollte mit klaren Regulierungen auf nationaler wie europäischer Ebene entgegengewirkt werden. Im Vordergrund muss aber der Abbau der heute schon bestehenden Vollzugsdefizite stehen. Wegen der europaweiten Präsenz dieser marktdominierenden Anbieter ist ein koordiniertes Vorgehen der Aufsichtsbehörden wünschenswert.