Humanistische Union

Identität- oder Kosumschutz im Internet?

Das Grundrecht auf freie Entfaltung der digitalen Persönlichkeit

aus: Vorgänge 184 (Heft 4/2008), S.20-29

1. 25 Jahre Volkszählungsurteil - eine Erfolgsgeschichte (bis jetzt!)

Seit genau 25 Jahren gilt „Datenschutz" als Grundrecht, abgeleitet aus der Menschen-würde und dem Persönlichkeitsrecht. Zur Geburtsstunde des „Grundrechts auf informationelle Selbstbestimmung" am 15.12.1983 formulierten dessen Eltern, die damaligen Richterinnen des ersten Senats des Bundesverfassungsgerichts: „Mit dem Recht auf informationelle Selbstbestimmung ist eine Gesellschaftsordnung nicht vereinbar, in der die Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß." Der Einzelne muss „grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten bestimmen." Auf dem sog. Volkszählungsurteil wurzelt das bundesdeutsche Datenschutzrecht, das ob seines weitgehenden Schutzes auch grenzüberschreitend hohes Ansehen genießt. Das ist sicher ein Verdienst richterlicher Rechtsfortbildung.

Man darf aber auch daran erinnern, dass das Grundrecht auf informationelle Selbstbestimmung nicht „deus ex machina" vom Bundesverfassungsgericht geschenkt, sondern von der damaligen Generation der 18 bis 35jährigen geradezu erzwungen wurde. Wegen der bevorstehenden Volkszählung war Anfang der 80er Jahre ein ganzes Land in Aufruhr. Diese schürte bei einem nicht unerheblichen Teil der Bevölkerung die Angst, zu einem „gläsernen Bürger", zum Spielball eines „Überwachungsstaates" degradiert zu werden. In heftig geführten Demonstrationen (beileibe keine „Lichterketten"), polemischen Kampagnen und nicht zuletzt durch zivilen Ungehorsam wurde das neue Bürgerrecht auch *erkämpft*. Mit anhaltendem Erfolg: Das Bundesverfassungsgericht hat die Persönlichkeitsrechte des Bürgers vor staatlichen Zugriffen stets umfassend geschützt. Auch als in Reaktion auf „9/11" beim Kampf gegen den Terrorismus eine vehemente „informationelle Aufrüstung" der staatlichen Sicherheitsbehörden erfolgte, hat das Bundesverfassungsgericht in mehreren Urteilen das Sammeln von Daten erschwert (Lauscheingriff, präventive Telekommunikationsüberwachung, Rasterfahndung, Kennzeichenerfassung oder Online-Durchsuchung).

In seiner letztjährigen Entscheidung zur sog. Online-Durchsuchung ging das Bundesverfassungsgericht noch einen Schritt weiter. Als es erkennen musste, dass die her-kömmlichen dogmatischen Strukturen des grundrechtlichen Persönlichkeitsschutzes angesichts der Gefahren durch den Einsatz moderner destruktiver Techniken und den Möglichkeiten der Datensammlung und -verknüpfung nicht mehr ausreichen, hat es — wie schon im Jahre 1983 - aus dem Menschwürdegrundsatz und dem allgemeinen Persönlichkeitsrecht ein „neues" Grundrecht modelliert: Das dogmatisch wie sprachlich noch etwas sperrige „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme". Dadurch wurde den staatlichen Sicherheitsbehörden ein enges rechtsstaatliches Korsett an verfahrensrechtlichen und materiellen Anforderungen bei der heimlichen Ausforschung privater Rechner angelegt.

Der Schutz des unantastbaren Kernbereichs der privaten Lebensgestaltung erstreckt sich auch auf den „virtuellen Raum" (der dadurch allerdings nicht gleichsam zum Refugium einer privaten Wohnung avanciert, Heckmann 2008). Das war zu erwarten. Bahnbrechendes ist dagegen eher zwischen den Zeilen des Urteils und verstreut in einigen „obiter dicta" herauszulesen: Augenscheinlich will das Gericht in dem

„neuen Grund-recht" nicht nur ein Gebot staatlicher Zurückhaltung erkennen, sondern auch die staatliche Pflicht, den Bürger vor Zugriffen Dritter zu schützen. Einen Bürger, den das Gericht als zutiefst schutzbedürftig ansieht angesichts allgegenwärtiger Bedrohungen durch und in informationstechnischen Systemen. Die Diskussion um eine mittelbare Drittwirkung dieses Grundrechts, um staatliche Schutzpflichten zur *Gewährleistung* von Vertraulichkeit und Integrität der elektronischen Kommunikation ist entfacht.

II. Datenschutz in der digitalen Welt: Ein Widerspruch?

Datenschutz im 21. Jahrhundert bedeutet mehr als den orwellschen Kampf gegen die „Hydra Staat". Der Bürger muss dabei auch „vor sich selbst" und seinesgleichen geschützt werden: Das Internet hat die Kommunikations- und Informationsformen der Gesellschaft revolutioniert. Dabei ist das Modell des world wide web auf den ständigen (unbemerkten) Austausch von Informationen aller Art ausgelegt; die Preisgabe persönlicher Daten ist quasi die Eintrittskarte zur virtuellen Welt, persönliche Daten avancieren zur grenzüberschreitend gültigen Währung. Über sog. Kundenkarten, Preisaus-schreiben, Ausspähung des Surfverhaltens u.a werden personenbezogene Daten über Kaufverhalten, Konsumgewohnheiten und vieles mehr zusammengetragen, um sie zu kommerziellen Zwecken weiter zu verwenden. Selbst Arbeitgeber lassen durch gezielte Recherchen im Internet überprüfen, ob Bewerber die vorausgesetzte persönliche Integrität und die für den Betrieb erforderliche „Richtlinienkonformität" aufweisen. Dabei ist die Sensibilität in der Bevölkerung, was den Schutz ihrer persönlichen Daten vor privaten Datensammlern angeht, inhomogen und von den unterschiedlichsten Motiven beeinflusst. Tendenziell scheint eher eine gewisse „Sorglosigkeit" und „Vertrauensseeligkeit" feststellbar. Während staatliche Überwachung nach wie vor als Schreckensszenario taugt, werden an private Akteure teils Unmengen an persönlichen Informationen freiwillig preisgegeben.

Ob und in welchem Umfang der Staat, wie es das Bundesverfassungsgericht angedeutet hat, schützend eingreifen muss (falls er dazu überhaupt in der Lage ist!), bleibt nun zu hinterfragen. Anders als im Jahre 1983 geben dabei die Stimmen aus der Bevölkerung wenig Anhaltspunkte. Im Gegensatz zu den von 1968 geprägten Volkszählungsgegnern (die man noch immer sehr deutlich vernehmen kann) sind die Stimmen der „digital natives" in der politischen Diskussion kaum hörbar. Doch gerade die Bedürfnisse dieser Generation, die sich - nach den Worten von Sascha Lobo - „zu einer digitalen Gesellschaft mit digitaler Persönlichkeit" entwickelt - gilt es zu berücksichtigen. Nur mit dem Ohr am Puls der Zeit (also im Netz) ist der Staat in der Lage, die Persönlichkeitsrechte der Betroffenen angemessen zu schützen.

III. Ursachen der zunehmenden Persönlichkeitsrechtsgefährdung in der digitalen Welt

Im Prinzip gibt es fünf typische Ursachen dafür, dass die Privatsphäre und das Persönlichkeitsrecht in den heutigen technischen Umgebungen zunehmend gefährdet werden:

Erstens werden immer mehr digitalisierte persönliche Daten erzeugt und über informationstechnische Systeme verfügbar. Während es früher eines gezielten Einbruchs oder eklatanten (soziale Kontrolle überwindenden) Vertrauensbruchs bedurfte, um persönliche Informationen wie Briefe, Bilder oder Vorlieben zu erlangen und (beliebigen) Dritten zugänglich zu machen, werden sie (heute) geneigten Tätergruppen gleichsam „auf dem Silbertablett" gereicht. Sei es, dass man diese Daten auf unzureichend gesicherten Speichermedien (Rechnern, mobilen Geräten) vorhält, sei es, dass sie freiwillig im Internet

hinterlassen werden. So vereinen sich Sorglosigkeit der Nutzer und Skrupellosigkeit der Täter in verhängnisvoller Weise.

Am Beispiel privater Fotografien lässt sich diese Explosion der digitalisierten Privatsphäre aufzeigen: Im Durchschnitt hat jeder Nutzer 1.788 Bilder auf seinen online (durch Berechtigte oder Unberechtigte) zugänglichen Medien gespeichert, einen Teil davon in sozialen Netzwerken wie StudiVZ oder Facebook. Diese faktische Öffnung der Privatsphäre und die damit einhergehende Entäußerung der Persönlichkeit ist letztlich Folge expliziter Geschäftsmodelle der IT-Branche, die mit ihren innovativen Hard-und Softwareangeboten faszinieren, lancieren und verführen. Gerade was den letztgenannten Punkt betrifft, bedarf es zur Verwirklichung informationeller Selbstbestimmung eines effektiven IT-Verbraucherschutzrechts, welches die legitimen geschäftlichen Interessen (einschließlich des mittelbaren Konsumschutzes) mit dem grundrechtlich garantierten Persönlichkeitsschutz in Einklang bringt. Erste Ansätze (aber auch nur solche) bietet die anstehende Datenschutznovelle mit der Verschärfung des Koppelungsverbots und der Stärkung des Einwilligungsregimes durch „opt-in-Regelungen". Die Frage ist, bis zu welchem Grade man den IT- und Internetnutzer „vor sich selbst" schützen darf und soll, denn, in den Worten von *Roger Clarke*: „Das Recht auf Privatsphäre ist die Freiheit von übermäßiger Einschränkung bei der Konstruktion der eigenen Identität". Bei dieser Gestaltung sollte der Einzelne die Bedienungsanleitung seiner Bausätze verstehen können – was er damit baut, muss ihm aber selbst überlassen bleiben.

Zweitens gibt es immer ausgefeiltere technische Möglichkeiten zur Datenerhebung, Datenverarbeitung und Datenverknüpfung, und zwar durch legale (legitime?) Programme der Privatwirtschaft (z.B. Mashups im web 2.0), legale (legitime?) neuartige staatliche Befugnisse (z.B, die Schüler-ID) sowie illegale Methoden der Internet- und Computerkriminalität (z.B. durch Identitätsdiebstahl). Damit ist die erste Eskalationsstufe erreicht. Die erstgenannte Ursache der Datenhäufung erhält ihre eigentliche Brisanz in Kombination mit dem Gefährdungspotential der nachhaltigen Datenverwendung. Bei-spiele hierfür bieten die Cache-Funktion der Suchmaschinen, verbesserte Suchfunktionen wie die Bildersuche oder frei verfügbare Software, mit deren Hilfe der Kopierschutz von Bildern aufgehoben werden kann. Auf diese Weise werden persönliche Daten von ihrem Urheber und Entstehungsanlass gelöst und entfalten ein Eigenleben. Neu zusammengefügt entsteht das Profil einer digitalen Persönlichkeit, das sich mit den Eigenschaften der realen Persönlichkeit nur teilweise decken mag.

Diese technisch bedingte partielle Wahrnehmung der Person ist auch einer der problematischen Konsequenzen der Befugnis zur Online-Durchsuchung. Zwar hat das Bundesverfassungsgericht diese Eingriffsermächtigung dem Grunde nach unter verfassungsrechtlichen Aspekten gebilligt und werden Verfahrensvorkehrungen wie der Richtervorbehalt nun (beim soeben beschlossenen BKAG) als Bollwerk des Freiheitsschutzes gefeiert. Das tiefer liegende Gefährdungspotential tritt dabei aber (zu Unrecht) in den Hintergrund: Ist der Bürger überhaupt in der Lage, seine durch den kompletten heterogenen Festplatteninhalt in Verbindung mit weiteren Profilelementen gebildete digitale Persönlichkeit so zu konstruieren, dass sie im Blickwinkel der Fahnder seine Unbescholtenheit widerspiegelt? Man muss den Sicherheitsbehörden nicht einmal missbräuchliches Vorgehen vorwerfen. Falsche Bewertungen der Tatsachenlage sind angesichts zufälliger Datenkonstellationen, vielfältiger Manipulationsmöglichkeiten und technischer Wirrungen in Zeiten zunehmender IT-Unsicherheit buchstäblich vorprogrammiert.

Das können Ermittlungsrichter auch kaum verhindern, beruht ihre Freigabeentscheidung doch auf der gleichen defizitären Tatsachenbasis. Das Dilemma der Rasterfahndung, valide Informationen und belastbare, wirklichkeitsnahe Interpretationen aus einem diffusen Datenmaterial herausfiltern zu müssen, potenziert sich bei der Online-Durchsuchung. Entsprechende Befugnisnormen mögen „am Reißbrett" verfassungskonform (im Sinne ausgleichender Interessenabwägung) gestaltbar sein. In der Rechtswirklichkeit werden sich – wie zuvor bei anderen staatlichen Befugnissen – Vollzugsdefizite zeigen. Dies muss (müsste) der Rechtsstaat mit seinen Steuerungs- und Kontrollinstrumenten aushalten.

Eine solche notwendige Datenherrschaft und Datenkontrolle wird aber - und das ist die *dritte* Ursache der zunehmenden Persönlichkeitsrechtsgefährdung – durch die ITEntwicklung erschwert. Der Staat kann nicht zugleich Datenherrschaft und Datenaskese ausüben. Schon strukturbedingt läuft er außerdem immer ein

Stück dem Gegenstand seiner Regulierungsbemühungen hinterher. Er müsste IT-Sicherheit gewährleisten und kann es mit seinen rechtsstaatlichen, freiheitlichen Mitteln kaum. So ist die Verletzlichkeit der hochkomplexen, hochdynamischen und geradezu auf „Kante genähten" ITInfrastruktur systemimmanent, kommt die Stabilisierung dieses Systems doch einer Luftbetankung bei Mach 2 gleich. Das ist nicht anders bei den privaten ITUmgebungen. Durch die auf den (vermeintlichen) Anforderungen der Nützlichkeit,Bedienungsfreundlichkeit und Kompatibilität aufgesetzte Modellierung von „Plug and play"-Umgebungen wird den Nutzern Herrschaftswissen vorenthalten. So bequem und positiv besetzt („Diese Webseiten machen teure Kauf-Software überflüssig") etwa Cloud Computing und Webspace für jedermann sein mögen, sie verlagern letztlich Teile der Privatsphäre auf die Server mächtiger Anbieter. Die Reduzierung auf bloßes Anwenderwissen ist zwar in hoch industrialisierten Gesellschaften nicht ungewöhnlich. Auch der Passagier eines A 380 muss das Flugzeug nicht fliegen können, solange er ein Ticket lösen kann und den Sicherheitshinweisen der Flugbegleiter folgt. Der Unterschied ist: Der IT-Nutzer hat in Online-Umgebungen die Fähigkeiten eines Passagiers, bekommt dort aber die Rolle und Rechte eines Piloten.

Hier zeigt sich die nächste Eskalationsstufe: Es sind nicht nur zu viele persönliche Daten im Netz verfügbar, die überdies in schädlicher Weise verwendet werden können. Der Einzelne steht diesem Geschehen zum Teil unwissend, zum Teil machtlos gegenüber. Man könnte dem Dilemma entgehen, wenn man sich intensiv mit der Materie beschäftigen würde oder die angebotenen Produkte und Dienstleistungen erst gar nicht nutzen würde. Beides erscheint für den „Durchschnittsnutzer" unrealistisch. Mangelnde Datenkontrolle ist fatal. Es ist schon problematisch, dass sich der Einzelne seiner eigenen Privatheit entäußert. In der digitalen Welt schädigt der sorglose Umgang mit IT aber auch Dritte: sei es durch Zugänglichmachung privaten Bild- und Videomaterials (ohne Einwilligung der Betroffenen) in Webportalen oder durch technische Schwachstellen, über die Rechner gekapert und in Botnetze integriert werden können.

Damit wird der Ruf nach dem Staat lauter. Ist es nicht dessen Aufgabe, für sichere IT-Umgebungen zu sorgen, zumal das Bundesverfassungsgericht in seiner Entscheidung zur Online-Durchsuchung jene staatliche Schutzpflicht betont hat? Doch zeigt sich hier die vierte Ursache einer zunehmenden Persönlichkeitsrechtsgefährdung, nämlich das Versagen klassischer staatlicher Steuerungsinstrumente. Gesetze und Verwaltungsakte, Befehl und Zwang scheinen wirkungslos gegenüber globalen, komplexen und heterogenen Zugriffen auf die digitale Persönlichkeit. Verglichen mit diesem rasanten, unkontrollierten und profitorientierten Datenverkehr wirkt die zwölfspurige Stadtautobahn von Los Angeles zur Rush Hour wie ein Feldweg in der Lüneburger Heide.

Dessen müsste sich der Gesetzgeber bewusst werden: Das digitale Leben spielt sich längst in einer neuen Dimension zwischenmenschlicher Kommunikation ab, für die es allenthalben an (Un-) Rechtsbewusstsein und Handlungs- sowie Haftungsmaßstäben fehlt. Da hilft auch der aktuelle Trend, „IT ins Grundgesetz" zu schreiben (Entwurf zur Einfügung eines Art. 91d GG im Rahmen der Föderalismusreform II) und den Datenschutz verfassungsrechtlich zu verankern (Gesetzentwurf der Bundestagsfraktion Bündnis 90/Die Grünen), nicht weiter. Besser als redundante, symbolische Verfassungsgesetzgebung wäre eine breite gesellschaftliche und parlamentarische Debatte über die Verantwortung des Staates, der IT-Wirtschaft und des einzelnen IT-Nutzers zur Gewährleistung einer sicheren und schützenden IuK-Infrastruktur. Und zwar nachhaltiger als die mit kurzer Halbwertszeit versehenen (abstumpfenden) Beteuerungen nach jeder einzelnen der zahlreichen Datenpannen und -skandale alleine im Jahr 2008.

Das ist nicht einfach. Als *fünfte* Ursache der zunehmenden Persönlichkeitsrechtsgefährdung ist nämlich ein Absinken der Hemmschwellen derer zu bemerken, die faktischen Zugriff auf die digitale Persönlichkeit Dritter erlangen. (Vermeintliche) Anonymität und Leichtigkeit des Netzes tragen dazu bei, dass die im realen Raum wenigstens partiell funktionierende soziale Kontrolle im elektronischen Netzwerk weitgehend ausfällt. Dies wird zur größten Herausforderung eines jeden Kontroll- und Steuerungsmodells des Rechtsgüterschutzes im Internet: Einerseits dem Einzelnen Anonymität zum Schutz seiner Privatsphäre zuzusichern, andererseits Äußerungen und Handlungen zurechenbar zu machen. Ob der Weg einer begrenzten Speicherung und Rückverfolgung der IPAdressen dieses Dilemma abzuschwächen vermag, ist weder verfassungsrechtlich noch rechtspolitisch endgültig geklärt. Die sog. Vorratsdatenspeicherung (in

Umsetzung einer EU-Richtlinie) scheint in ihrer Rigorosität und ausgreifenden Reichweite wenig geeignet, gesellschaftlichen Konsens in dieser wichtigen Frage herbeizuführen. Umgekehrt betont der (politisch sicher„unverdächtige") Europäische Gerichtshof für Menschen-rechte (in Sachen K.U. vs. Finnland, Urt, v. 2.12.2008), dass der Deckmantel absoluter Anonymität im Internet die Rechte betroffener Opfer verletzen kann, denen der Staat unter diesen Umständen keinerlei Schutz bieten kann.

IV. 5 Forderungen für eine freie Entfaltung der digitalen Persönlichkeit

1. Mehr Transparenz im Netz!

Nahezu aus allen Lebensbereichen der Bürger sind heutzutage Daten elektronisch gespeichert, die über Web-Applikationen zugänglich sind. Seien es Daten aus staatlichen und privaten Registern, seien es die breiten Datenspuren, die die User selbst im Internet hinterlassen, wenn sie Bankgeschäfte tätigen, Flüge buchen oder sich auf Partnersuche begeben. Durch Verknüpfung dieser Informationen ließen sich regelmäßig umfassende Persönlichkeitsprofile erstellen, aber auch schon einzelne Daten wirken als Spiegel der Seele. Der „gläserne Bürger" — zu Zeiten des Volkszählungsurteil eher Phantom und Schreckgespenst — wäre im digitalen 21. Jahrhundert Realität geworden. Für einen effektiveren Persönlichkeitsschutz ist deshalb mehr *Transparenz* erforderlich. Nur der in-formierte Bürger kann in Kenntnis der Folgen seines Tuns im Netz frei und selbstbestimmt handeln. Der Bürger muss wieder mehr wissen, welche Daten zu welchem Zweck von ihm erhoben werden, was mit ihnen geschieht und welchen Gefahren er sich bei einer Preisgabe der Informationen aussetzt.

Mehr Transparenz kann im Netz auf vielfältige Weise geschaffen werden: z.B. durch weitergehende Informationspflichten der Diensteanbieter oder eine allgemeine Aufklärung der Bevölkerung (vielleicht nach dem Vorbild der Fernsehsendung „Der 7. Sinn", die von 1966 bis 2005 über kurze Filmtrailer auf die Gefahren und Anforderungen des Straßenverkehrs aufmerksam gemacht hatte — solche gestiegenen Anforderungen gibt es allemal auf der Datenautobahn). Flankierend könnte die Schaffung von „Wohlfühlräumen" im Netz, also die Kennzeichnung „sicherer" Angebote (etwa durch Datenschutzaudits, Selbstverpflichtung der IT-Wirtschaft, Zertifizierung von „sicheren" Angeboten durch die Datenschutzbeauftragten oder andere Stellen usw.) dem Nutzer aufzeigen, welche Defizite andere Seiten und Angebote aufweisen.

Die Entwicklung verlässlicher und vertrauenswürdiger Kommunikationsstrukturen wird auch von der Bundesregierung gefördert. Technische Dienstleistungen zur sicheren Authentifizierung und zum Identitätsmanagement in E-Government und E-Commerce werden derzeit erforscht und entwickelt. Dabei wird darauf zu achten sein, dass dem Gedanken der informationellen „Selbst"-Bestimmung Rechnung getragen wird, der Bürger also im Rahmen der gesetzlichen Möglichkeiten verständlich vermittelte Wahlmöglichkeiten erhält, welche Daten er zu welchem Zweck preisgibt und welche er verbergen möchte (erste Ansätze hierzu sind beim Konzept der elektronischen Gesundheitskarte erkennbar).

2. Förderung von IT-Kompetenz und Selbstschutz!

Jeder kann Opfer von Datenklau, Persönlichkeitsrechtsverletzungen und anderen Formen der Internetkriminalität werden. Manche allerdings etwas leichter. Hier muss die Vermittlung von IT- und Medienkompetenz in erster Linie ansetzen. Nach der verfassungsgerichtlichen Anerkennung staatlicher Schutzpflichten in diesem Bereich können sich insbesondere die Kultusministerien ihrer Verantwortung zur curricularen Berücksichtigung nachhaltiger (!) Unterrichtsangebote zur Sensibilisierung dieser Gefahren (keine bloßen Computerkurse!) nicht mehr entziehen. Mag da (anwendungsbezogene) technische Verständnis der digital natives auf den ersten Blick beeindrucken, so bedarf auch diese Generation

steuernder Hinweise über die rechtlichen und sozialen Konsequenzen ihres Verhaltens im world wide web.

Angeregt wird ein bundesweites IT-Kompetenz-Barometer, etwa in Form einer öffentlich zugänglichen Datenbank, in der alle diesbezüglichen Unterrichtsangebote abrufbar und vergleichbar sind. Die hierfür notwendige wissenschaftliche Begleitforschung wurde kürzlich am Institut für IT-Sicherheit und Sicherheitsrecht an der Universität Passau initialisiert. Nächste Ausbaustufe wäre dann die Effektuierung des Selbstschutzes. Dieser kann im Netz auf vielfältige Art und Weise erfolgen. Der Markt für „Privacy Enhancing Technologies" (Virenschutz, Verschlüsselungssoftware, Anonymisierungsdienste, Identitätsmanagement-Tools, Rechnertests usw.) wächst ständig, wobei ein effektiver Schutz für die breite Masse „bezahlbar" sein muss. Außerdem darf der grundrechtliche Persönlichkeitsschutz nicht von der technischen Versiertheit und dem individuellen Problembewusstsein der Betroffenen abhängen.

3.Schaffung eines IT-Sicherheitsgesetzes!

Nachdem die Schaffung einheitlicher (grenzüberschreitender) Datenschutzstandards in naher Zukunft unrealistisch ist, muss auch auf technische Entwicklungen gesetzt wer-den. Nach *Lawrence Lessig*, dem als „Elvis des Cyberspace" bezeichneten US-amerikanischen Verfassungsrechtler, wird sich Technologie zu einem wichtigen Teil des Datenschutzes entwickeln. In der Tat könnte zum Beispiel Software, die dem Benutzer die Möglichkeit gibt, durch Voreinstellung selbst zu bestimmen, welche Daten er weitergeben will, und die ihn alarmiert, falls nicht freigegebene Daten abgerufen werden, einen wesentlichen Beitrag zum Schutz der „digitalen Persönlichkeit" leisten. Dass die Wirtschaft dies nicht nur positiv sehen wird, liegt auf der Hand. Allenthalben müssten solche Programme besonders sicher gestaltet werden; würden sie nämlich ihrerseits durch Dritte kompromittiert, wäre die Vortäuschung des Privatsphärestatus geradezu kontraproduktiv.

Hinzu kommen rechtliche Forderungen. Damit der Nutzer seine Rechte durchsetzen kann, bedarf es klarer, eindeutiger rechtlicher Regelungen, die dem Wesen der neuen Technologien gerecht werden. Nachdem, wie *Lessig* treffend feststellt, die Architektur des Cyberspace selbst eine Technologie ist, mit der der Internet-Surfer kontrolliert wird, brauchen wir verbindliche Regelungen, die diesen Raum unter Beachtung der Persönlichkeitsrechte seiner Bewohner interessengerecht strukturieren. Die geltenden rechtlichen Regelungen, insbesondere die Datenschutzgesetze des Bundes und der Länder, können dazu nur wenig beitragen. Datenschutzrecht ist heute Technikrecht; das Recht ist von der Technik abhängig. Wir brauchen ein technikkonformes Recht um datenschutzkonforme Technik durchzusetzen.

Nachdem die wesentlichen Regelungen und Grundsätze des geltenden Datenschutzrechts aus der „Vor-Internetzeit" stammen und mit der Anpassung an die EUDatenschutzrichtlinie im Jahre 2001 nur wenige technikspezifische Modifizierungen vorgenommen wurden, ist eine grundlegende Neuregelung unumgänglich. Ob der aufgrund der aufsehenerregenden Datenschutzpannen forcierte Gesetzgebungsprozess die erforderlichen Ergebnisse bringen wird, bleibt abzuwarten. Ebenso dringend wie die Reform der Datenschutzgesetze ist ein Gesetz, das die Parameter für die erforderliche IT-Sicherheit fasst, Verantwortlichkeiten und Haftungsfälle definiert sowie den technischen Rahmen für eine verlässliche Kommunikation im Netz vorgibt.

1. Das Internet muss vergessen lernen!

Die EU-Richtlinien zum Datenschutz (basierend auf den Leitlinien der OECD zum Schutz der Privatsphäre) und natürlich auch die deutschen Datenschutzgesetze sehen als fundamentalen Grundsatz vor, dass nicht mehr benötigte Informationen zu löschen sind. Das Netz aber vergisst nicht. Daten lassen sich nicht einfach löschen, sobald diese ein-mal im Internet erfasst wurden. Zwar ist es kein Problem, elektronisch gespeicherte Informationen zu löschen, auch automatisch. Technisch werden derzeit entsprechende Lösungen erforscht; die „Information mit Verfallsdatum" – wenn dies denn technisch umsetzbar ist – könnte wesentlich zum Datenschutz beitragen. Allerdings hinterlassen die Daten im Netz Spuren (auf Festplatten, Backup-Bändern usw.), sind insoweit rekonstruierbar und werden vor ihrer Löschung ggf. tausendfach durch Dritte kopiert und archiviert. Trotz dieser kaum lösbaren „Vollzugsdefizite" muss darauf hingearbeitet werden, dass mehr

gesammelte Daten gelöscht werden. So hat der Präsident des Bundesverfassungsgerichts *Hans-Jürgen Papier* in einer Festrede auf der Konferenz der Datenschutzbeauftragten von Bund und Ländern am 15.12.2008 treffend festgestellt, dass eine zweckwidrige Verwendung von heute im Internet kommunizierten Daten in der Zukunft geradezu programmiert ist, wenn das Internet nichts vergisst.

Bisher fördert der Staat das „Vergessen" im Internet (aus Gründen einer effektiven Strafverfolgung) nicht gerade. Indem er private Telekommunikationsunternehmen zur „Vorratsdatenspeicherung" verpflichtet, sorgt er im Gegenteil dafür, dass personenbezogene Daten längerfristig gespeichert werden. Das Bundesverfassungsgericht könnte in seiner für 2009 erwarteten Hauptsacheentscheidung die Konturen einer verfassungskonformen Speicherung und Verwendung von Kommunikationsdaten schaffen, auf deren Basis die Abwägung zwischen notwendiger Anonymität (bzw. Vergessen) und notwendiger Zurechenbarkeit erfolgen kann. Am Rande wird dann auch die Kostenfrage zu klären sein, werden die Kosten der Verfolgungs- und Verhinderungsvorsorge doch derzeit noch in fragwürdiger Weise den privaten Providern aufgebürdet (so das VG Berlin in seinen Vorlageentscheidungen vom 17.11.2008 und 08.11.2007 mit Anmerkung Braun, 2008).

5. Wertmaßstäbe zur gegenseitigen Achtung der Persönlichkeit schaffen!

Die vermeintliche Anonymität des Netzes hat wie gesehen zu einem Absenken der Hemmschwellen geführt und ist insoweit ein Nährboden für Persönlichkeitsrechtsverletzungen. Anonymität im Netz schützt die Privatheit des distanzierten Betrachters und Empfängers von „One-way-Informationen", ist aber den zivilisatorischen Errungenschaften der zwischenmenschlichen Kommunikation abträglich. Für interaktive oder kommunikative Inhalte ist Anonymität ein Misstrauensfaktor. Ohne die Preisgabe persönlicher Informationen ist Kommunikation oberflächlich (wobei es zunächst irrelevant ist, ob diese Informationen zutreffend sind oder nicht). Der Austausch gemeinschaftsund identitätsstiftender Informationen ist auch für die soziale Kommunikation der Menschen im Internet unumgänglich. Insoweit ist eine neue Balance von Anonymität und Verbindlichkeit in der Netz-Kommunikation gesellschaftlich auszuhandeln.

Soweit man der Anonymität den Vorrang gewährt, müssen für die Verfehlungen der „Nicht-Fassbaren" gegebenenfalls Dritte als Garanten einstehen; man denke etwa an die (in der Rechtsprechung umstrittene) Haftung der Forenbetreiber für ehrverletzende In-halte. Letztlich kann nur eine gestufte Zurechnung beiden Interessen Rechnung tragen. Die Abstufung könnte sich an der bewährten Zurückhaltung bzw. Offenbarung der persönlichen Identität in der realen gesellschaftlichen und rechtlichen Ordnung orientieren. Sie reicht dann von der quasi absoluten Anonymität des privaten (offline!) Konsumverhaltens in der geschützten Wohnung über die relative Anonymität passiven Konsums inder Sozialsphäre („Stadtbummel") bis hin zur Herstellung sozialer, ad hoc zurechenbarer Kontakte und schließlich zur rechtsverbindlichen Schaffung von Vertrauensverhältnissen. Im Internet sind die Dinge zurzeit noch teilweise umgekehrt: Das einfache Surf-verhalten wird quasi kontrolliert, die Begehung von Straftaten ist nicht verfolgbar.

V. Ausblick

Identitäts- oder Konsumschutz im Internet? Am Besten im Prinzip Beides. Es muss auch kein Widerspruch sein. Genau genommen gibt es – was die Zielkonflikte und Interessensbewertungen betrifft – keinen relevanten Unterschied zum realen Raum. Man muss einen Ausgleich schaffen zwischen der legitimen Anonymisierung und der legitimen Zurechnung persönlichen (Fehl-) Verhaltens. Das Bundesverfassungsgericht sprach schon früh von der Gemeinschaftsgebundenheit des Individuums. Dies gilt auch für die digitale Persönlichkeit. Sie ist zweifellos auf vielfache Weise gefährdet. Soweit dies mit rechtlichen Defiziten zusammenhängt, bedarf es besserer rechtlicher Regulierung. Soweit Technologien ein riskantes Eigenleben führen, bedarf es besserer Modellierung der technischen Umgebungen. Und soweit die Defizite und Versäumnisse im Bewusstsein der Gefährdung als solcher liegen, ist es die Pflicht der Politik,

die Menschen behutsam ins 21. Jahrhundert zu führen. Dazu hätte sie bereits neun Jahre Zeit gehabt.

Literatur

Dirk Heckmann, 2008: Der virtuelle Raum als Wohnung, Festschrift für Rolf Stober, 615.
Frank Braun, 2008: Verfassungswidrigkeit der entschädigungslosen Indienstnahme von Telekommunikationsunternehmen, jurisPR-ITR 2/2008; ders., Die Finanzierung polizeilicher Aufgabenerfüllung,
2008, 347.
