Datenleak – Wie reagiert der Rechtsstaat?

2014, 362

Von Dr. Thilo Weichert, Kiel. Der Autor ist Leiter des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein.

Datenleaks können aus Sicht des digitalen Grundrechtsschutzes schlecht, möglicherweise aber auch gut sein. Dieser Grundrechtsschutz geht zwischen Europa und den USA weit auseinander. Aus europäischer Sicht sind die Leaks Snowdens ein Segen, die Leaks der NSA eine Katastrophe.

I. Unabhängiges Landeszentrum für Datenschutz

Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein – ULD, das ich leite, ist in mancher Hinsicht eine ungewöhnliche Dienststelle eines Datenschutzbeauftragten. Zum einen ist meine Dienststelle auch für die Durchsetzung des Rechts auf Aktenzugang in der Verwaltung, also für die Informationsfreiheit zuständig. Besonders ist beim ULD zudem dessen präventive Ausrichtung. Das ULD kontrolliert nicht nur öffentliche und private Datenverarbeiter, sondern es berät diese sowie die Bürgerinnen und Bürger und führt in einer eigenen Datenschutzakademie Aus- und Fortbildungen durch. Zum Portfolio des ULD gehören außerdem die Durchführung von Datenschutzforschung – oft in Kooperation mit internationalen Institutionen der Wissenschaft, der Wirtschaft und der Verwaltung – sowie die Durchführung von Datenschutzaudits und die Vergabe von Datenschutz-Gütesiegeln. Damit wird die Konformität von Verfahren und Produkten mit den Regelungen zum Schutz informationeller Selbstbestimmung förmlich geprüft und bestätigt.

II. Datenleaks?

Datenleaks sind nichts grundsätzlich rechtsstaatlich Schlechtes. Sie können eine Verletzung allgemeiner Persönlichkeitsrechte, des Rechts auf Privatheit, den Bruch von Betriebs- und Geschäftsgeheimnissen darstellen. Sie können aber auch dem Schutz der Privatheit, der Durchsetzung von demokratischer Transparenz und der Informationsfreiheit dienen. Dies war und ist zweifellos der Fall bei den Enthüllungen von *Edward Snowden* über die übermäßige Internetüberwachung durch den US-amerikanischen und den britischen Geheimdienst, die National Security Agency – NSA – und das Government Communications Headquarters – GCHQ. Bei seinem Whistleblowing, der Offenlegung eines gewaltigen Überwachungsskandals, hat er bisher erfolgreich darauf geachtet, dass Personen keinen Schaden erleiden.

Diese Feststellung gilt nicht in gleichem Maße für das Datenleak von *Bradley/Chelsea Mannings*, dessen zweifellos wichtige Informationen teilweise ungefiltert und journalistisch nicht aufbereitet der globalen Internetöffentlichkeit über Wikileaks zur Verfügung gestellt wurden.

Es gibt auch schädliche Datenleaks, die bisher nicht auf den geballten Widerstand von Rechtsstaaten stoßen. Dies gilt zB für die von Betroffenen nicht genehmigten Datenzugriffe durch Internetfirmen wie Google, Apple oder Facebook, die damit gewaltige grundrechtswidrige Geschäftsmodelle aufgebaut haben.

Eindeutig illegal sind die Leaks durch Hacker-Angriffe von Kriminellen auf Portale, Webseiten, Unternehmens-, Behörden- und Privatrechner, bei denen es um wirtschaftliche Bereicherung durch Spionage, teilweise aber auch um Datensabotage geht. Nicht weniger illegal nach europäischem Verständnis, aber erheblich schwerer zu bekämpfen sind vergleichbare staatliche Datengriffe, wie sie im Detail über die NSA und den GCHQ bekannt geworden sind. Diese zielen letztlich auf die Totalüberwachung des Internet ab.

Wir dürfen nicht aus dem Blick verlieren, dass vergleichbare Angriffe durch die Geheimdienste anderer Staaten erfolgen, etwa des Irans, von China, Russland oder Syrien. Deren Überwachungsmaßnahmen zielen auch auf die politische Opposition und verletzen damit die digitalen demokratischen Grundfreiheiten der Menschen.

III. Rechtlicher Datenschutzbestand in Europa

Datenschutzgesetze gibt es in Europa seit den 70er Jahren des letzten Jahrhunderts, ausgehend vom deutschen Bundesland Hessen und von Schweden. Diese Gesetze breiteten sich aus und begründeten eine neue Angst im Bereich der Wirtschaft, dass sie zu Handelshemmnissen führen könnten. Deshalb wurden schon früh internationale Standards für den Datenschutz erarbeitet, bei deren Einhaltung der ungehinderte grenzüberschreitende Datenaustausch weiterhin möglich sein sollte. Dem dienten etwa die OECD-Datenschutz-Leitlinien von 1980 oder auch die Europarats-Konvention aus dem Jahr 1981.

Einen juristischen Durchbruch schaffte das deutsche Bundesverfassungsgericht, als es im Jahr 1983 anlässlich des staatlichen Versuchs der Durchführung einer

Volkszählung feststellte, dass jeder Mensch – abgeleitet aus dem allgemeinen Persönlichkeitsrecht – ein subjektives Grundrecht auf Datenschutz, ein Recht auf informationelle Selbstbestimmung hat.

Auf dieser Grundlage beschlossen die Institutionen der EU im Jahr 1995 die europäische Datenschutzrichtlinie, mit der für die gesamte EU das Prinzip des grundrechtlichen Verbots mit Erlaubnisvorbehalt eingeführt wurde, das inzwischen nicht nur vom EuGH, sondern auch vom Europäischen Gerichtshof für Menschenrechte, auf der Grundlage von Art 8 der Menschenrechtskonvention, anerkannt und durchgesetzt wird.

Einen weiteren Meilenstein zur Gewährleistung von digitalen Grundrechten setzte erneut das deutsche Bundesverfassungsgericht im Jahr 2008, als es anlässlich eines Urteils über die geheimdienstliche Durchsuchung von Privatcomputern ein Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme, also auf eine digitale Privatsphäre, vergleichbar der räumlichen Sphäre der Wohnung oder der sozialen Sphäre der Familie, begründete.

Der Siegeszug des digitalen Rechtsschutzes fand bisher seinen Höhepunkt in der 2009 in Kraft getretenen europäischen Grundrechtecharta, in der in Art 8 ausdrücklich ein Grundrecht auf Datenschutz fixiert ist.

IV. Sonstiger Europäischer Grundrechtsstandard

Der Schutz informationeller Selbstbestimmung ist nur ein – zweifellos zentraler – Bestandteil eines nötigen umfassenderen digitalen Grundrechtsschutzes. Viele dieser schon in nationalen Verfassungen angelegten Sicherungen finden inzwischen auch in der Europäischen Grundrechtecharta ausdrückliche Erwähnung. Dies gilt für die Meinungs- und die Kommunikationsfreiheit, denen im Netz besondere Bedeutung zukommt. Damit eng verknüpft ist die Informationsfreiheit. Gemäß der ganz aktuellen Rsp des EGMR begründet sich aus Art 10 der Europäischen Menschenrechtskonvention ein Anspruch auf Zugang zu Verwaltungsinformationen. Zu den politischen Freiheiten gehören auch ein „digitales Vereinigungs- und Versammlungsrecht". Das Petitionsrecht kann über das Netz wahrgenommen werden. Eine Vielzahl eher analog zu verstehender Freiheiten haben dadurch eine digitale Komponente, dass sie auch vor digitaler Ausforschung und Beeinflussung – zB der Religion, der Familie, des Berufs, der Wohnung oder der Freizügigkeit – schützen. Erwähnt werden muss weiterhin der Gleichbehandlungsgrundsatz, der ein Diskriminierungsverbot enthält. Merkmale über das Geschlecht, die Abstammung, die Herkunft oder den Glauben dürfen auch nicht bei digitaler Auswertung für Zwecke der Diskriminierung genutzt werden.

Die Grundrechte haben zur Folge, dass staatliche Eingriffe nur auf gesetzlicher Grundlage zulässig sind. Gegen Eingriffe kann sich jede Person vor Gerichten zur Wehr setzen, die effektiven Rechtsschutz gewähren müssen. Ergänzend dazu bestehen – insb in Sachen Datenschutz und Informationsfreiheit – unabhängige Kontroll- und Mediationsinstanzen in Form von Beauftragten. Weitere rechtsstaatliche Absicherungen des digitalen Grundrechtsschutzes sind die Unschuldsvermutung, das Recht, sich nicht selbst belasten zu müssen (Nemo Tenetur), das Gebot transparenten Verwaltungshandelns mit dem grundsätzlichen Verbot heimlicher Eingriffe, der Anspruch auf ein faires Verfahren sowie prozessuale Gewährleistungen.

V. USA

Anders die USA, der ein aktives Bekenntnis zur Demokratie nicht abgesprochen werden kann. Doch dort erweist sich die Leugnung digitaler Grundrechte als ein zentraler demokratiefeindlicher Baustein im Interesse der Wahrung politischer und ökonomischer Hegemonie. Diese besteht in einer über viele Jahrzehnte aufgebauten Vormacht der NSA bei der Kontrolle des globalen Informationsnetzes mit dem Ziel der Absicherung der sicherheitspolitischen und militärischen Hegemonie. Dies besteht aber auch in der Abwehr von Grundrechtsbindungen für die eigene IT-Wirtschaft.

Es ist verblüffend, dass sich die herrschende Meinung in den USA zur Digitalisierung des Grundrechtsschutzes immer noch auf dem Stand der 70er Jahre des letzten Jahrhunderts befindet. Bis dahin waren die USA hier weltweit führend, beginnend mit dem Beitrag von *Samuel D. Warren* und *Louis D. Brandeis* zum „Recht auf Privatheit" aus dem Jahr 1890. *Alan F. Westin* skizzierte im Jahr 1967 in seinem Klassiker „Privacy and Freedom" nicht nur die Risiken der Digitalisierung und die dazu erfolgte gesellschaftliche Auseinandersetzung, sondern auch die Ableitungen digitaler Grundrechte aus den Amendments zur US-Verfassung. Er beschreibt darin auch die damaligen politischen Widerstände aus der Wirtschaft und der Sicherheitsadministration hiergegen. Exemplarisch für die herrschende Position in den USA ist der Supreme Court, der Grundrechte analog versteht, Ausländer vom Schutz ausschließt, Sicherheitsbelangen den Vorrang einräumt und private Unternehmen keiner Bindung unterwirft.

VI. Technische Perspektiven

Dieser Dissenz zwischen den USA und Europa wird durch die absehbaren technischen Entwicklungen immer anachronistischer: Durch sog Wearable Computing, zB sog „Smart Watches" oder „Smart Glasses"

rückt die Digitalisierung den Menschen – im wahrsten Sinn des Wortes – immer mehr auf die Pelle bzw auf die Haut und in den Körper. Mit dem „Internet der Dinge" werden die Alltagsumgebungen des Menschen, etwa Wohnung und Auto, aber auch die Lebenswelt der Arbeitens und der Freizeit, digital erfasst. Mit Hilfe von Big Data werden die vorhandenen, teilweise unstrukturierten Daten zusammengeführt und Analysen zugeführt. Diese Analyseergebnisse haben teilweise direkte (analoge) Auswirkungen auf menschliche Lebenswelten, etwa bei der Kreditvergabe (Scoring, Rating) oder bei der Kfz-Sicherheit (Car2Car-Communication).

Technisch ist die digitale Diktatur möglich. Gibt es hiergegen keine rechtsstaatlichen Korrekturmöglichkeiten in Form der Gewährung digitaler Grundrechte, so ist diese Diktatur auch realistisch.

VII. Gegenstrategien

Es gibt schon heute eine Vielzahl von – mehr oder weniger – wirksamen Aktivitäten zur Behebung des konstatierten rechtsstaatlichen Defizits. Eine interessante, öffentlich kaum wahrgenommene Initiative Deutschlands und Brasiliens ist die letztlich einstimmig beschlossene Resolution bei den Vereinten Nationen (UNO) „Schutz der Privatheit im digitalen Zeitalter", die erstmals den digitalen Charakter der Gewährleistungen der allgemeinen Erklärung der Menschenrechte (Art 12) und des Paktes für politische und zivile Rechte (Art 17) herausstreicht. Das Problem der UNO besteht darin, dass darin Überwacherstaaten ein wesentliches Wort mitzusprechen haben, so dass hierüber eine globale Rechtsentwicklung langfristig blockiert werden kann. Deshalb sind parallele europäische Initiativen dringend nötig, bei denen Europa mit einzelnen Staaten oder Staatengruppen Bündnisse eingehen kann und sollte.

Deutschland und Europa müssen sich zumindest partiell vom Freund- und Partner-Denken befreien und ihre Grundrechtsinteressen vertreten. Dabei kommt der europäischen Position der angenehme Umstand zugute, dass die ökonomischen und politischen Interessen weitgehend mit grundrechtlichen Interessen gleichgerichtet sind: Die Bindung der IT-Industrie an Grundrechtsstandards würde nicht nur rechtlich zu einer Gleichbehandlung der US-amerikanischen mit den europäischen Anbietern führen, sondern faktisch zu einer Verbesserung der Wettbewerbslage der Europäer.

Um die Ernsthaftigkeit des grundrechtlichen Engagements Europas zu demonstrieren, ist eine einfache, weitgehend symbolisch aber zugleich massiv wirkende Aktion wichtig: die Gewährung eines sicheren Aufenthalts für *Edward Snowden*. *Snowden* hat keinen Verrat an demokratischen und freiheitlichen Werten begangen, sondern einen zentralen Beitrag geleistet für einen dringend nötigen Läuterungs- und Selbstreinigungsprozess zum Wiedergewinn teilweise verloren gegangener und teilweise zum Gewinn noch nicht erkannter Werte – nämlicher digitaler Grundrechte. Angesichts einer immer restriktiver werdenden Praxis in den USA bei der Pressefreiheit, der Informationsfreiheit und des Informantenschutzes muss eine Kampagne für digitale Grundrechte zwingend den verstärkten Schutz von Whistleblowern auf nationaler, europäischer und globaler Ebene beinhalten.

Ein Ansatzpunkt zur Durchsetzung von Grundrechten sind die Wirtschaftsbeziehungen. Diese können dazu genutzt werden, einen grundrechtlichen Mindeststandard zu realisieren. Anderenfalls macht sich Europa durch Unterlassen für die Massenüberwachung mitschuldig. Bisher hatte Europa die USA gegenüber sämtlichen anderen Staaten der Welt mit dem Safe-Harbor-Abkommen privilegiert, das einen Datenaustausch ohne effektive Instrumente zur Durchsetzung von Datenschutz vorsieht, weil man in Europa am informationstechnisch bedingten Aufschwung in den USA teilhaben wollte. Inzwischen hat sich dieses Blatt gewendet: Die Fortführung von Safe Harbor würde zu einer massiven ökonomischen Benachteiligung der eigenen Wirtschaft führen. Die Erörterungen über ein Freihandelsabkommen zwischen Europa und den USA müssen zumindest im Hinblick auf den informationellen Handel, der eine zunehmende Rolle spielt, ausgesetzt werden, bis von den USA ein Mindeststandard beim digitalen Grundrechtsschutz zugesichert wird. Dies ist nicht „Datennationalismus", sondern eine Grundvoraussetzung für demokratische und freiheitliche Handelsbeziehungen.

Eine vergleichbare Vorgehensweise sollte bei den Kooperationsabkommen im Sicherheits- und im Finanzbereich praktiziert werden. Die USA haben Europa einseitig Kooperationspflichten beim Austausch von Fluggast- oder Bankdaten auferlegt, zB dem sog Passenger Name Record- und dem sog SWIFT-Abkommen. Europa sollte die Möglichkeit nutzen, gleichberechtigte Datenkooperationen unter Berücksichtigung des Grundrechtsschutzes zu verabreden.

Bei dem Führen eines „transatlantischen Cyber Dialogs" muss Transparenz durch die Beteiligten hergestellt werden; ein Rückgriff auf Whistleblower kann schon kurzfristig nicht genügen. In einem zweiten Schritt bedarf es der Entwicklung von Normen, über die materielle Sicherungen, unabhängige Kontrollen und Rechtsschutz für die Betroffenen hergestellt werden. Hierbei spielt das soeben vom Europaparlament gebilligte einheitliche Datenschutzpaket eine wichtige Rolle, dem eine normative Wirkung über Europa hinaus zukommt. Die dabei geplante

Europäische Datenschutz-Grundverordnung orientiert sich am Marktortprinzip und soll europaweit effektiven Rechtsschutz auch gegenüber US-Unternehmen gewährleisten.

Um die informationstechnische Abhängigkeit von den USA abzubauen, müssen und können in Europa eigenständige technische Strukturen aufgebaut werden, wobei Großbritannien außen vor bleiben sollte, wenn dieses Land weiterhin nicht bereit ist, den grundrechtlichen Weg mitzugehen. Unter dem Stichwort „Schengen-Routing" ist geplant, die territoriale Integrität des Internetverkehrs künftig besser zu gewährleisten. Die europäische IT-Industrie kann einen Vorsprung vorweisen in Fragen des Datenschutzes und der Datensicherheit. Diesen gilt es weiter auszubauen durch entsprechende Forschungsförderung wie auch durch freiwillige Angebote und verpflichtende Implementierung. Ende-zu-Ende-Verschlüsselung, Identitätsmanagement, sicheres E-Government sind die Stichworte, mit denen (staatliche) Sicherheitsangebote umschrieben werden können.

Die politische, rechtliche und wissenschaftliche Aufarbeitung der globalen Massenüberwachung ist mit den *Snowden*-Enthüllungen erst am Anfang. Diese Aufarbeitung muss fortgeführt werden. Dies kann in der juristischen Aufarbeitung der Rechtsverletzungen von NSA und GCHQ und von deren Helfershelfern erfolgen – in Form von strafrechtlichen und parlamentarischen Ermittlungen oder zB in Form von grundrechtlichen Prüfungen, etwa durch den EGMR oder den EuGH. Dabei sollten keine falschen Rücksichten genommen werden. Wenn ermittelte Sachverhalte Anklagen vor Strafgerichten oder diplomatische Sanktionen nötig machen, so ist es im Interesse des europäischen Grundrechtsschutzes, diese Schritte zu ergreifen.

Auch auf nationaler Ebene sind rechtliche Korrekturen nötig. Die Diskussionen um die *Snowden*-Enthüllungen haben auch enthüllt, dass das nationale Geheimdienstrecht nicht mehr den Anforderungen eines modernen Grundrechtsschutzes genügt.

VIII. Schlussfolgerungen

Bei der Auseinandersetzung über die NSA-Überwachung ist von europäischer Seite bisher ein Aspekt zu kurz gekommen: Es müsste im wohlverstandenen Interesse der USA liegen, die Existenz und Durchsetzbarkeit digitaler Grundrechte zu akzeptieren. Mittel- und langfristig kann sich eine US-amerikanische Wirtschafts- und Sicherheitspolitik glaubwürdig von der Chinas und Russlands nur absetzen und letztlich durchsetzen, wenn sie ein glaubwürdiges Bekenntnis zu digitalen Grundrechten beinhaltet. Von Vorteil ist, dass die USA eine langjährige bürgerrechtliche Tradition vorweisen kann, die sich nicht nur auf Nichtregierungsorganisationen stützen muss, sondern auch auf eine Opposition, die bisher in Politik, Wissenschaft und Rsp Mindermeinung geblieben ist. Förderlich ist insofern sicher, wenn die Interessenkonflikte zwischen Sicherheitsadministration und IT-Wirtschaft in den USA zunehmen.

Grundvoraussetzung für einen Wandel des Grundrechtsverständnisses in den USA ist, dass dieser nicht allein von außen – also von Europa – aufgezwungen, sondern auch aus „freien Stücken" gegangen wird und auf Einsicht beruht. Die USA unterstützen Demokratie- und Freiheitsbewegungen auf der ganzen Welt. Dies kann und sollte auch Europa tun – auch gegenüber den USA. Derartiges kann, sollte und darf nicht als Einmischung in fremde Angelegenheiten verstanden werden, sondern als Beitrag im transatlantischen Wertedialog.

Die globale Diskussion über digitale Grundrechte kann nur vorankommen, wenn Europa sich seiner eigenständigen Rolle bewusst wird und diese ausfüllt – ökonomisch wie politisch. Diese Rolle darf den Rest der Welt nicht ausblenden, muss vielmehr darauf aufbauend in eine globale grundrechtliche Charmekampagne einmünden. Zumindest mittelfristig sollte das von Anfang klar definierte Ziel darin bestehen, eine internationale digitale Menschenrechts-Charta aufzusetzen.