Alexander Dix

Rechtspolitische und technische Maßnahmen für einen effektiven Datenschutz

Die Regierungen der EU-Mitgliedsstaaten sind aufgrund ihrer nationalen Verfassungen wie der europäischen Grundrechtscharta verpflichtet, sich für international wirksame Schutzmechanismen zum Schutz der Vertraulichkeit von Kommunikationsdaten einzusetzen. Alexander Dix weist darauf hin, dass die Regierungen in mehrfacher Weise dieser Verpflichtung nachkommen können: bei der Aushandlung neuer Standards für den Datenaustausch mit den USA; in den aktuellen Verhandlungen um Handels- und Dienstleistungsabkommen; in der Vollendung der europäischen Datenschutzgrundverordnung; in der Weiterentwicklung des nationalen Rechtsschutzes gegenüber den Geheimdiensten. Ein wirksamer Schutz des Kommunikationsgeheimnisses sei dabei nur zu erreichen, wenn sichere Infrastrukturen geschaffen werden. Neben der besseren Durchsetzung geltenden Datenschutzrechts sowie der Entwicklung neuer, internationaler Rechtsstandards sollt der Staat die Entwicklung sicherer Kommunikationstechniken und die Bereitstellung sicherer Netze fördern.

Zwei Eingangsbemerkungen: Es gibt keinen Grund zu resignieren und sich zurück zu lehnen und zu sagen: wir können sowieso nichts machen – erster Punkt. Zweiter Punkt: Es gibt allerdings nicht das *Silver Bullet*. Es gibt nicht die eine ideale Handlungsstrategie, sondern wir sollten mehrgleisig fahren, mindestens eine Doppelstrategie verfolgen. Das sind zum einen die politisch-rechtlichen Maßnahmen. Wir müssen geltendes Recht durchsetzen und darauf dringen, dass das Recht, wo es unzureichend ist, verändert wird – also Rechtspolitik betreiben. Und zweitens muss es technische Maßnahmen geben; allerdings unter einem entscheidenden Vorbehalt: Es wird nie den „Datenschutzknopf" geben, den ihr nur drücken müsst und dann sind alle Probleme gelöst. Das Problem muss vor allem politisch gelöst werden. Aber ich denke, beide Seiten sind wichtig und das will ich kurz erläutern.

Anknüpfend an die bisherige Debatte bin ich mit Wolfgang Hoffmann-Riem und anderen führenden Verfassungsrechtlern der Meinung, dass die Bundesregierung verfassungsrechtlich dazu verpflichtet ist, sich international und europäisch für die Grundrechte der Menschen, insbesondere für das Grundrecht auf vertrauliche Kommunikation einzusetzen. Das bedeutet konkret: Der deutsche Staat muss sich für die Schaffung von sicheren Infrastrukturen engagieren, auch international. Der Infra-

strukturaspekt ist ganz wichtig. Und das kann auch bedeuten, dass man über Dezentralisierung sprechen muss. Das Schengen-Routing ist ein Aspekt, vielleicht nicht der ideale, aber man muss auch darüber nachdenken, wie der Staat weit stärker die Bildung von *peer to peer*-Netzwerken fördern muss.

Das Internet wird heute als Überwachungsinfrastruktur missbraucht. Das öffentlich gemacht zu haben, ist das Verdienst von Edward Snowden, der sich deshalb hohe Verdienste um den Datenschutz erworben hat. Der Staat muss sich jetzt dieser Schutzpflicht stellen und über rechtliche Lösungen, die international verankert werden müssen, nachdenken. Ziel solcher Vereinbarungen muss es sein, das Menschenrecht auf vertrauliche Kommunikation international zu schützten. Das ist ein hohes Ziel. Die Datenschutzbeauftragten haben auf internationaler Ebene bereits dieses Recht eingefordert.[1]

Man muss der Bundesregierung immerhin zu Gute halten, dass sie eine Initiative unter anderem mit der brasilianischen Regierung unterstützt hat, die zur Verabschiedung einer Resolution zum Recht auf Privatheit im digitalen Zeitalter durch die Generalversammlung der Vereinten Nationen am 18. Dezember 2013 geführt hat.[2] Das ist ein sehr allgemeiner Text, der auch noch auf amerikanischen Druck hin verwässert wurde. Aber es ist wichtig: mit dieser Resolution ist das Thema endgültig auf der internationalen Bühne angekommen. Das Thema muss dort bleiben und das Ziel muss, auch das ist eine alte Forderung der Datenschutzbeauftragten, eine internationale Konvention zum Datenschutz sein, die sicherlich nicht von heute auf morgen gemacht werden kann. Das ist ein langwieriger Prozess. Aber auch da warne ich vor Resignation. Nur weil das alles so schwierig und kompliziert ist, sollten wir nicht einfach den Griffel fallen lassen und denken, das nützt alles nichts, das wird nie dahin kommen. Wir müssen dafür arbeiten!

Und wir sollten auch gegenläufige Tendenzen erkennen. Gerade gegenwärtig wird viel berichtet über die Verhandlungen zu einem internationalen Abkommen für den freien Handel mit Dienstleistungen (*Trade in Services Agreement* – TISA). Dieses Abkommen soll offenbar den Finanzdienstleistern die Befugnis einräumen, relativ unbegrenzt international personenbezogene Daten über Finanztransaktionen in jeden anderen Staat übermitteln zu können. Das läuft im Grunde einer wichtigen Vorschrift im GATS-Abkommen, also dem weltweiten Abkommen für den freien Welthandel, zuwider. Das GATS-Abkommen sieht ausdrücklich vor: Datenschutzbestimmungen sind keine nicht-tarifären Handelshemmnisse. Das ist ein technischer Begriff aus dem internationalen Handelsrecht. Die Regelung im GATS-Abkommen bedeutet sinngemäß: Kein Staat darf argumentieren, dass Datenschutzbestimmungen den freien Welthandel behindern; sondern Datenschutz ist Teil des weltweiten *ordre public*, eines allgemeingültigen Mindeststandards. Deshalb müssen sich Deutschland und die Europäische Union auf den Standpunkt stellen, dass das hiesige Datenschutzniveau nicht abgesenkt werden darf mit dem Hinweis, es beeinträchtige den freien Welthandel. Insofern gefährden die Verhandlungen über dieses Freihandelsabkommen über Dienstleistungen, die außerhalb des GATS-Abkommens stattfinden, das europäische Datenschutzniveau. Die Europäische Union hat immerhin schon angekündigt, dass sie das so auch nicht hinnehmen will. Speziell im transatlantischen Verhältnis ist das ein wichtiger Punkt.

Transatlantischer Datenschutz

Die meisten Diskussionen drehen sich natürlich im Moment um die Frage, unter welchen Voraussetzungen personenbezogene Daten aus Europa in die USA übermittelt werden dürfen, unabhängig von der Ausspähung durch Nachrichtendienste. Da ist das Stichwort *Safe-Harbor-Abkommen* zu nennen. Die Europäische Kommission hat nach den Veröffentlichungen von Edward Snowden im November 2013 dreizehn Forderungen formuliert – sie hat es nicht Forderungen genannt, sondern höflicher: Empfehlungen – an die amerikanische Regierung, die bis zum Sommer dieses Jahres umgesetzt werden müssten. Das Ergebnis ist offen. Es gibt widersprüchliche Informationen, welchen Stand diese Verhandlungen erreicht haben. Die damalige Kommissarin Reding hat erklärt, man sei schon ziemlich weit. Es gehe im Grunde um ein neues *Safe-Harbor-Abkommen*, das ein angemessenes Datenschutzniveau in den Vereinigten Staaten sicher stellen soll. Nach Frau Reding ginge es nur noch um einen Punkt, nämlich den Rechtsschutz europäischer Bürger in den Vereinigten Staaten. Da sperren sich die Amerikaner nach wie vor, Europäern die gleichen Rechte vor amerikanischen Gerichten einzuräumen wie US-Amerikanern. Ich halte das nicht für einen kleinen Punkt. Aber es gibt auch andere Informationen aus der Kommission auf Arbeitsebene: Dort wird gesagt, die US-Regierung weigere sich nach wie vor, den Zugriff der Nachrichtendienste auf diese Daten in irgendeiner Weise zu beschränken. Das ist genau das K.o.-Kriterium: eine der Forderungen der EU Kommission lautete nämlich, genau den Zugriff von Sicherheitsbehörden – nicht nur Nachrichtendiensten, sondern ganz allgemein Sicherheitsbehörden (aber die NSA ist natürlich die große Spinne im Netz) – auf das erforderliche Maß zu beschränken. Das Problem ist die Maßlosigkeit, der totale Überwachungsanspruch, der von diesen Einrichtungen reklamiert wird. Das muss eingegrenzt werden; und solange das nicht geschieht, darf auch der Datenverkehr in die USA nicht so weiter laufen wie bisher.

Das führt zu einem weiteren Verhandlungsstrang über ein allgemeines, generelles Datenschutzabkommen zwischen Europa und den USA. Der Abschluss eines solchen Abkommens ist aus meiner Sicht eine zentrale Voraussetzung für das transatlantische Freihandelsabkommen (TTIP). Das Freihandelsabkommen beschäftigt sich *formal* zwar nicht mit dem Datenschutz, weil der Datenschutz gar nicht zur Diskussion stehen darf in Freihandelsverhandlungen. Aber eine Forderung müsste sein: Solange Europa und die USA sich nicht über ein solches Rahmendatenschutzabkommen verständigt haben, darf es auch kein Freihandelsabkommen geben. Diese Forderung wird auch aus dem Europäischen Parlament mittlerweile erhoben.

Die Datenschutzbehörden in Europa haben auch eine Handlungsoption, über die man sprechen muss; die ist lange Zeit vergessen oder in den Hintergrund gedrängt worden. Das *Safe-Harbor-Abkommen* entspricht einer Art Selbstverpflichtung amerikanischer Datenverarbeiter. Die Europäische Kommission hat bei Abschluss des *Safe-Harbor-Abkommens* entschieden: Mit dem Abkommen wird ein angemessenes Datenschutzniveau zwar im Grundsatz anerkannt, aber die europäischen Aufsichtsbehörden haben das Recht, den Datenverkehr jedenfalls zeitweise im Einzelfall zu unterbinden, wenn sie Anhaltspunkte dafür haben, dass die Grundlagen dieser Selbstverpflichtung

entfallen sind; dass im Grunde etwas passiert, was bei Abschluss des *Safe-Harbor-Abkommens* so niemand wirklich auf dem Schirm hatte. Und in dieser Situation sind wir jetzt.

Der *Google*-Chef Larry Page hat im Zusammenhang mit den Überwachungspraktiken der NSA gesagt: Es ist schwierig, in einem demokratischen Staat miteinander umzugehen, wenn wir nicht wissen worüber wir reden. Und genau das war bei Abschluss des *Safe-Harbor-Abkommens* der Fall: Niemand konnte sich seinerzeit vorstellen, welches unglaubliche Ausmaß die Ausspähung durch amerikanische und britische Nachrichtendienste tatsächlich schon damals angenommen hat. Und das ist seitdem eher mehr geworden. Deshalb müssen die europäischen und auch die deutschen Datenschutzbehörden die Frage prüfen, ob sie von ihrer Befugnis zur Aussetzung einzelner Datenübermittlungen in die USA Gebrauch machen wollen. In Deutschland haben sie bereits erklärt, das prüfen zu wollen. Sie warten jetzt im Moment noch ab, wie die amerikanische Seite auf die Forderungen der Europäer hier reagiert, ob es zu einer echten substanziellen Verbesserung beim *Safe-Harbor-Abkommen* kommt.

Ein letzter rechtlicher Punkt ist die europäische Datenschutzgrundverordnung, die allerdings leider im Moment auf der Stelle tritt. Die Behandlung im Europäischen Rat bei den Regierungen geht nicht wirklich voran, oder nur in Trippelschritten. Da spielt die britische Regierung eine bremsende Rolle, und sie wird leider unterstützt von der Bundesregierung. Das ist ein erheblicher Mangel. Diese Datenschutzgrundordnung sollte einen einheitlichen Rechtsrahmen in Europa für den Datenschutz für die gesamte Wirtschaft formulieren, an den sich auch amerikanische und andere außereuropäische Unternehmen halten müssen. Ich bin davon überzeugt, dieser Rechtsrahmen wird früher oder später kommen. Aber je später er kommt, desto schlechter!

Europäischer Datenschutz

Mittlerweile hat der Europäische Gerichtshof (EuGH) schon bestimmte Teilprobleme aus diesem Paket nach der geltenden Datenschutzrichtlinie entschieden. In der kürzlichen *Google*-Entscheidung[3] hat er klar gesagt: Wer von außerhalb Europas in Europa Geschäfte machen will, der hat sich an europäisches Datenschutzrecht zu halten. Das war im Grunde schon immer eine Selbstverständlichkeit. Der *US Supreme Court* hat stets von europäischen Unternehmen verlangt, dass sie sich in den USA an amerikanisches Recht halten sollen. Das wird jetzt erfreulicherweise vom Europäischen Gerichtshof auch bestätigt. Außerdem hat der EuGH das Recht auf Vergessen aus der Datenschutzrichtlinie abgeleitet, das in der Datenschutzgrundverordnung enthalten ist. In gewisser Weise ist damit die Verordnung schon ein bisschen vorweg genommen. Ich teile aber nicht die Auffassung, dass diese Grundverordnung damit überflüssig sei, weil der Gerichtshof schon die wichtigen Fragen entschieden habe. Es gibt nämlich noch viele ungeklärte Fragen, die der europäische Gesetzgeber beantworten muss, etwa Fragen der Abstimmung: Wie sollen sich europäische Datenschutzbehörden auf eine einheitliche Auslegung des künftigen europäischen Datenschutzgesetzes verständigen? All das muss noch geklärt werden. Aber wenn der politische Wille da wäre,

dann könnte man sich sehr schnell darauf verständigen. Das Europäische Parlament hat im April 2014 auf Vorarbeiten von Jan Philipp Albrecht bereits einen einheitlichen Standpunkt nahezu einstimmig beschlossen. Wenn wir in einem demokratischen europäischen Staat leben würden, wäre dieses Gesetzgebungsverfahren schon beendet. Das ist jetzt eine ketzerische Bemerkung, weil der europäische Gesetzgebungsprozess so nicht organisiert ist. Da haben die Regierungen der Mitgliedsstaaten noch ein wesentliches Wort mitzureden, und da hakt es im Moment. Die Regierungen müssen sich einigen mit dem Parlament und der Kommission. Es ist dringend erforderlich, dass das schnell passiert.

Nationaler Datenschutz

Zu den Befugnissen der Datenschutzbeauftragten bei der Kontrolle der Geheimdienste will ich einen Satz von Adalbert Podlech zum Stichwort Kontrolle zitieren: „Nur kontrollierte Macht kann regelgeleitete Macht sein“, hat er einmal gesagt. Persönlich ist er auch sehr skeptisch, ob man Nachrichtendienste überhaupt in einem demokratischen Staat kontrollieren kann. Aber wenn man schon Regeln macht, dann sind diese Regeln wertlos, wenn es keine effektive Kontrolle gibt. Das ist ein entscheidender Satz.

Die Datenschutzbeauftragten, genauer gesagt die Bundesbeauftragte für Datenschutz, haben nach geltendem Recht eine ergänzende Kontrollfunktion neben dem, was die G 10-Kommission macht. Selbst diese eingeschränkten Kontrollbefugnisse sind dem früheren Bundesbeauftragten Schaar vom Bundesinnenminister seinerzeit bestritten worden. Herr Friedrich hatte sich geweigert, bestimmte Informationen, die eindeutig dem Bundesbeauftragten hätten übermittelt werden müssen, offen zu legen – mit fadenscheiniger Begründung. Ich hoffe, dass die jetzige Bundesdatenschutzbeauftragte da nicht locker lässt, sondern weiterhin darauf besteht, dass zumindest die geltenden Kontrollbefugnisse eingehalten werden. Immerhin hat Frau Voßhoff erfreulicherweise schon darauf gedrungen, dass die Stellung der Bundesbeauftragten endlich europarechtskonform in völliger Unabhängigkeit organisiert werden muss – diese völlige Unabhängigkeit gibt es nämlich bisher nicht. Die Bundesbeauftragte ist die einzige Datenschutzbeauftragte in Deutschland, die noch von der Regierung in gewisser Weise abhängig ist. Alle Landesdatenschutzbeauftragten sind bereits völlig unabhängig. Das ist eine Forderung, die wiederum der Europäische Gerichtshof in einem Verfahren gegen Deutschland erhoben hat.

Darüber hinaus bin ich auch der Meinung, dass die Befugnisse der Bundesdatenschutzbeauftragen bei der Kontrolle der Nachrichtendienste noch verstärkt werden sollten. Das haben die Datenschutzbeauftragten auch gefordert, sie haben sich aber zugleich für eine Stärkung der parlamentarischen Kontrolle eingesetzt.[4] Da gibt es verschiedene Modelle. Wir sind nicht der Meinung, dass man sozusagen die Hoffnung aufgeben sollte, überhaupt Nachrichtendienste zu kontrollieren. Man kann es, wenn man es nur will. Aber dann muss man auch die richtigen Instrumente dafür in die Hand nehmen.

Technischer Datenschutz als notwendige Ergänzung

Ich will noch etwas sagen zu den technischen Möglichkeiten eines besseren Datenschutzes. Recht muss ergänzt werden durch Technik. Ohne Technik ist Recht hilflos und umgekehrt. Die beiden müssen zusammengebunden werden. Erstens: Datenschutz ist keine Privatsache; anders als Herr Uhl das zu Beginn der Snowden-Enthüllungen gesagt hatte. Man kann nicht das ganze Überwachungsproblem auf die einzelnen Menschen abwälzen. Deshalb ist es auch keine Lösung, dass sich jede_r einen eigenen Mailserver aufsetzt oder jede_n Programmieren lernen zu lassen. Der Staat hat eine Schutzpflicht. Trotzdem ist es wichtig, die Mittel zum digitalen Selbstschutz zu verbessern. Dafür muss der Staat auch Voraussetzungen schaffen. Er muss zum Beispiel Mittel dafür bereit stellen und Forschungen unterstützen, die einfache Verschlüsselungstechnik endlich zum Standard macht. Ein amerikanischer Experte hat einmal gesagt: ‚Wir brauchen *crypto for grandma*', das heißt Verschlüsselung für die Omi, die an ihrem Computer sitzt, wenn sie denn einen Computer nutzen will. Die muss überhaupt nichts machen. Alles, was sie übers Netz schickt, ist *per se* standardmäßig verschlüsselt. Nur wenn sie ausnahmsweise einmal sagt, jetzt will ich das abschalten, gibt es einen Ausschaltknopf. Verschlüsselte Kommunikation muss *per default* angeschaltet sein; sie muss zum Standard werden. Das ist eine ganz wichtige Forderung.

Eine weitere Möglichkeit wären geografisch begrenzte Routing-Regeln für die internetgestützte Kommunikation – das, was gegenwärtig unter dem Stichwort Schengen-Routing diskutiert wird. Dezentrale Netzstrukturen sollten entwickelt werden. Ich meine, die Technik muss eine größere Bedeutung erlangen und Technik kann auch vom Gesetzgeber unterstützt werden, indem zum Beispiel das Inverkehrbringen von Hard- und Software mit Hintertüren unter Strafe gestellt wird. Das ist eine Forderung, die mit Sicherheit jetzt auf den Tisch muss. Ich will nicht so weit gehen, dass unsichere Hard- und Software strafbar werden sollte – denn das ist das, was Microsoft und andere große Hersteller ständig machen. Die lassen die Nutzer_innen als Versuchskaninchen arbeiten und immer dann, wenn eine neue Sicherheitslücke offenbar (oder von Hacker_innen entdeckt) wird, wird ein Pflaster, ein sogenannter *patch* darüber geklebt. Diese Art der Produktentwicklung ist schon problematisch genug und zeigt die Unsicherheit dieser ganzen Technik. Wenn dann noch Hersteller gezielt und wissentlich Hintertüren in ihre Hard- und Software einbauen lassen, meinetwegen auch auf politischen Druck von Seiten der Regierung, dann sollte es strafbar sein, so etwas zu verkaufen. Es muss natürlich auch strafbar sein, wenn jemand Pakete bei *Amazon* oder *DHL*, bevor der/die Empfänger_in das überhaupt ausgeliefert bekommt, aufmacht und da irgendetwas anschraubt. Das ist doch eine groteske Vorstellung, aber offenbar Realität (s. *TAREX*).

Zivilgesellschaft

Ich denke, es sollte eine internationale Bürgerrechtsbewegung für eine demokratische Informationsökologie geben. Die Humanistische Union ist diejenige Organisation in Deutschland, die dazu prädestiniert ist. Es gibt in den USA eine sehr rege Bürgerrechtsbewegung im Netz. Da gibt es Bündnispartner, mit denen man sich verbünden kann.

Der Text ist die überarbeitete Fassung eines Vortrags auf dem 3. Gustav-Heinemann-Forum der Humanistischen Union am 21. Juni 2014 in Rastatt. Eine Audioaufzeichnung ist auf der Webseite der Humanistischen Union nachzuhören unter http://www.humanistische-union.de/themen/rechtspolitik/ghf/.

DR. ALEXANDER DIX Jahrgang 1951, studierte Rechtswissenschaften in Bochum, Hamburg und London. Er war von 1982 bis 1985 juristischer Referent bei der Stadt Heidelberg und promovierte 1984 zum Dr. jur. an der Universität Hamburg. 1985 wurde er Mitarbeiter des Berliner Datenschutzbeauftragten, von 1998 bis 2005 war er Landesbeauftragter für Datenschutz und für das Recht auf Akteneinsicht des Landes Brandenburg. Seit dem 3. Juni 2005 ist Dix der Beauftragte für Datenschutz und Informationsfreiheit des Landes Berlin. Er ist Vorsitzender der Internationalen Arbeitsgruppe zum Datenschutz in der Telekommunikation („Berlin Group“) und Mitglied der Artikel 29-Gruppe der Europäischen Datenschutzbeauftragten. Dix ist Mitherausgeber des Jahrbuchs für Informationsfreiheit und Informationsrecht.

Anmerkungen:

1 Artikel 29 Datenschutzgruppe, Stellungnahme 04/2014 zur Überwachung der elektronischen Kommunikation zu nachrichtendienstlichen und nationalen Sicherheitszwecken. Brüssel, 10.4.2014 (819/14/DE WP215), abrufbar unter http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_de.pdf#h2-2.

2 Gemeint ist die UN-Resolution 68/167„The right to privacy in the digital age” v. 18.12.2013. Zu dieser Resolution und den weiteren Aktivitäten zum Ausbau des menschenrechtlichen Schutzes auf UN-Ebene siehe den Beitrag von Töpfer in dieser Ausgabe.

3 EuGH, Urteil in der Rechtssache C-131/12 Google Spain SL, Google Inc. / Agencia Espanol de Proteccion de Datos, Mario Costeja Gonzalez. Die Entscheidung ist abgedruckt in der Neue(n) Zeitschrift für Verwaltungsrecht (NVwZ), 2014, S. 857ff. Zu dieser Entscheidung siehe auch den Kommentar von Mandelartz in dieser Ausgabe.

4 S. „Effektive Kontrolle von Nachrichtendiensten herstellen!“, Entschließung der 88. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9.10.2014, abrufbar unter http://www.datenschutz.de/dsb-konferenz/.