DATENSICHERHEIT

Rechtliche Rahmenbedingungen und Möglichkeiten

THORSTEN FELDMANN || Die physische Sicherheit von Datenströmen und informationstechnischen Systemen ist in rechtlicher Hinsicht sowohl in den europäischen und deutschen Grundrechten als auch in einfachen Gesetzen und Umsetzungsrichtlinien angelegt. Vorschriften zur Datensicherheit müssen dabei verschiedene Bedürfnisse bedienen.

Zunächst erfordert und bedingt die fortschreitende Digitalisierung einen kraftvollen, auch rechtlichen Schutz von Informationen gegen unrechtmäßige Zugriffe. Im Lichte jüngerer Abhöraktionen nationaler und ausländischer Dienste wird man aber die Frage zu diskutieren haben, wann ein „rechtmäßiger" Zugriff vorliegt, der eine Überwindung von Datensicherheitsmaßnahmen rechtfertigt. Zugleich belegen Datenskandale im privaten Sektor, namentlich unbeabsichtigte Datenverluste und Hacks von Konkurrenten, Politaktivisten und Randalierern, dass es allen Anstrengungen zum Trotz offenbar einen absoluten Schutz gegen unberechtigte Informationszugriffe nicht geben kann. Auch aus dieser Erkenntnis müssen Gesellschaft und Recht, vor allem auch für den privaten Rechtsverkehr, Konsequenzen ziehen.

Der vorliegende Beitrag versucht sich an einer Bestandsaufnahme der geltenden juristischen Rahmenbedingungen und unternimmt einen Ausblick, in welche Richtung sich das Recht der Datensicherheit entwickeln sollte.

GEMEINSCHAFTSRECHT UND VERFASSUNGSRECHT

Als beschreibender Begriff für einen physischen und damit technischen Schutz von Daten darf Datensicherheit nicht mit dem Datenschutz verwechselt oder gleichgesetzt werden. Das geltende Datenschutzrecht schützt Daten nicht um ihrer selbst willen, sondern soll den Einzelnen nach Möglichkeit davor bewahren, dass er durch den Umgang Dritter mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.[1] Die Datensicherheit kann zwar Teil des geltenden Datenschutzrechtsrahmens sein, etwa mittels der Vorgaben zu den technischen und organisatorischen Maßnahmen in § 9 Bundesdatenschutzgesetz (BDSG). Sie geht jedoch zugleich über das bloße Datenschutzrecht hinaus, da sie sich, anders als die Vorgaben des BDSG, nicht notwendigerweise nur auf personenbezogene Daten beziehen muss. Generelles Ziel der Datensicherheit ist es, dass Daten, seien diese nun personenbezogen oder nicht, weder durch äußere Einflüsse noch durch fehlerhaftes oder missbräuchliches Verhalten beeinträchtigt werden.

Das Schutzgut Datensicherheit wird sowohl von europäischen als auch von nationalen Vorschriften adressiert: So bestimmt etwa Art. 8 Abs. 1 der Charta der Grundrechte der Europäischen Union (Charta), dass jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten hat. Auch hier bezieht sich der Schutzbereich dieses Grundrechts dem Wortlaut nach nur auf den Datenschutz. Der Gerichtshof der Europäischen Union (EuGH) legt die Norm aber dynamisch aus und entnimmt ihr zugleich Anforderungen für die Datensicherheit. So hatte der EuGH in seiner Ent-

scheidung zur Aufhebung der Vorratsdatenrichtlinie festgestellt, dass die mit dem Unionsrecht unvereinbar erklärte Richtlinie keine hinreichenden, den Anforderungen von Art. 8 Charta entsprechenden Garantien dafür bietet, die auf Vorrat gespeicherten Daten wirksam vor Missbrauchsrisiken sowie vor jedem unberechtigten Zugang zu ihnen und jeder unberechtigten Nutzung schützen zu können.[2] Nach Ansicht des EuGH spielen Datensicherheitsgesichtspunkte also durchaus eine wichtige Rolle bei der Frage des Schutzes personenbezogener Daten und einer möglichen Verletzung von Grundrechten. Ebenfalls nimmt der EuGH in seiner Entscheidung auf Art. 17 der europäischen Datenschutzrichtlinie (RL 95/46/EG) Bezug, der Anforderungen an die technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten aufstellt[3] und durch § 9 BDSG in nationales Recht umgesetzt ist.

Zwar mögen sich Vorschriften zur Datensicherheit überwiegend aus dem Datenschutzrecht ableiten. Zuweilen ergeben sie sich aber auch aus anderen hochrangigen Erwägungen. Datensicherheit ist nach hier vertretener Auffassung beispielsweise auch ein Bestandteil des vom Gericht erschaffenen „IT-Grundrecht".[4] In seinem Urteil vom 27. Februar 2008 hat das Bundesverfassungsgericht (BVerfG) dem Staat Restriktionen bei der Infiltration stationärer IT-Infrastruktur zum Zwecke der Erkenntnisgewinnung auferlegt und dadurch eine rechtliche Grenze zur Datensicherheit geschaffen, ohne dass es einer zusätzlichen technischen Sicherung bedürfte. Systeme und Daten hinter dieser Grenze sollen also sicher sein. Nach den Leitsätzen des Urteils umfasst das allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 i.V. m. Art. 1 Abs. 1 GG) auch das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Gerade mit Blick auf die Sicherheit von Daten, die in einem informationstechnischen System gespeichert sind, stellte das BVerfG fest, dass das Recht auf informationelle Selbstbestimmung den Persönlichkeitsgefährdungen nicht vollständig Rechnung trägt, die sich daraus ergeben, dass der Einzelne zu seiner Persönlichkeitsentfaltung auf die Nutzung informationstechnischer Systeme angewiesen ist und dabei dem System persönliche Daten anvertraut oder schon allein durch dessen Nutzung zwangsläufig liefert.[5] Denn nach dem BVerfG kann bereits der Zugriff auf ein solches System durch den Staat und dessen Strafverfolgungsbehörden ausreichen, um sich einen großen und aussagekräftigen Datenbestand zu verschaffen, ohne noch weitere Datenverarbeitungsmaßnahmen (die in den Anwendungsbereich des Rechts auf informationelle Selbstbestimmung fallen würden) durchführen zu müssen. Nach Meinung des Gerichts trägt daher das allgemeine Persönlichkeitsrecht dem Schutzbedarf in seiner lückenfüllenden Funktion über seine bisher anerkannten Ausprägungen hinaus dadurch Rechnung, dass es die Integrität und Vertraulichkeit informationstechnischer Systeme gewährleistet.[6]

GESETZLICHE VORGABEN ZUR DATENSICHERHEIT IN DEUTSCHLAND

Der technische Schutz von Daten, seien sie nun personenbezogen im Sinne des BDSG oder nicht, wird auch in einigen Bundesgesetzen verpflichtend vorgeschrieben. So hat nach § 5 Abs. 3 des De-Mail-Gesetzes der Postfach- und Versanddienst die Vertraulichkeit, die Integrität und die Authentizität von Nachrichten zu gewährleisten. Ein akkreditierter Diensteanbieter muss zu diesem Zweck die Erfüllung von zwei Voraussetzungen sicherstellen: erstens, dass die Kommunikation von einem akkreditierten Diensteanbieter zu jedem anderen akkreditierten Diensteanbieter über einen verschlüsselten, gegenseitig authentisierten Kanal erfolgt (Transportverschlüsselung) (§ 5 Abs. 3 S. 2 Nr. 1 De-Mail-Gesetz) und zweitens, dass der Inhalt einer De-Mail-Nachricht vom akkreditierten Diensteanbieter des Senders zum akkreditierten Diensteanbieter des Empfängers verschlüsselt übertragen wird (§ 5 Abs. 3 S. 2 Nr. 2 De-Mail-Gesetz). Relativierend führt § 5 Abs. 3 S. 3 De-Mail-Gesetz jedoch direkt an, dass der Einsatz einer durchgängigen Verschlüsselung zwischen Sender und Empfänger (Ende-zu-Ende-Verschlüsselung) hiervon unberührt bleibt. Die zwingenden Voraussetzungen der Datensicherheit auf dem Übertragungsweg (§ 5 Abs. 3 S. 2 Nr. 1 und Nr. 2 De-Mail-Gesetz) sehen also eine durchgehende Verschlüsselung gerade nicht vor.

Auch im Bereich der Telekommunikation hat der Gesetzgeber erkannt, dass Daten potenzielle leichte „Beute“ für Dritte sind, wenn diese gespeichert und übertragen werden. Aus diesem Grund bestimmt § 109 Abs. 1 des Telekommunikationsgesetzes (TKG), dass jeder Diensteanbieter die erforderlichen technischen Vorkehrungen und sonstige Maßnahmen sowohl zum Schutz des Fernmeldegeheimnisses und auch gegen die Verletzung des Schutzes personenbezogener Daten zu treffen hat. Wer ein öffentliches Telekommunikationsnetz betreibt oder öffentlich zugängliche Telekommunikationsdienste erbringt, hat zudem bei den von ihm hierfür eingesetzten Telekommunikations- und Datenverarbeitungssystemen angemessene technische Vorkehrungen und sonstige Maßnahmen zu treffen. Insbesondere sind solche Maßnahmen zu treffen, um Telekommunikations- und Datenverarbeitungssysteme gegen unerlaubte Zugriffe zu sichern und Auswirkungen von Sicherheitsverletzungen für Nutzer oder für zusammengeschaltete Netze so gering wie möglich zu halten.

IT-SICHERHEITSGESETZ

Dass die Datensicherheit nach Ansicht der Bundesregierung eine zentrale Rolle in der Struktur des zukünftigen digitalen Marktes einnimmt, wird in dem Entwurf für das sog. IT-Sicherheitsgesetz deutlich. Ein erster Referentenentwurf wurde im August 2014 vom Bundesinnenministerium veröffentlicht.[7] Das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme soll zum einen dem Zweck dienen, den Schutz der Bürgerinnen und Bürger in einem sicheren Netz zu verbessern. Zudem sollen die geplanten Neuregelungen dazu dienen, den Schutz der Verfügbarkeit, Integrität und Vertraulichkeit datenverarbeitender Systeme zu erhöhen und der gestiegenen Bedrohungslage anzupassen.

Hierzu werden über gesetzliche Verpflichtungen (wie etwa Meldungen an das Bundesamt für Sicherheit in der Informationstechnologie – BSI) die Telekommunikations- und Telemedien-Diensteanbieter, die eine Schlüsselrolle für die Sicherheit des Cyberraums haben, noch stärker in die Verantwortung genommen. Sie sollen verpflichtet werden, IT-Sicherheit nicht nur wie bisher zum Schutz der Vertraulichkeit und zum Schutz personenbezogener Daten, sondern auch zum Schutz von Telekommunikations- und Datenverarbeitungssystemen gegen unerlaubte Zugriffe zu gewährleisten. Besondere Schutzmaßnahmen für „Betreiber kritischer Infrastrukturen“ sollen in einer gesonderten Verordnung geregelt werden. Bei diesen Betreibern kritischer Infrastrukturen und damit den Adressaten der Datensicherheitsverpflichtungen handelt es sich um in der gesonderten Rechtsverordnung näher bestimmte Einrichtungen, Anlagen oder Teile davon in den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen, die von hoher Bedeutung für das Funktionieren des Gemeinwesens sind und durch deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe oder erhebliche Störungen der öffentlichen Sicherheit eintreten würden. Zur Überprüfung der organisatorischen und technischen Vorkehrungen und sonstigen Maßnahmen haben diese Betreiber mindestens alle zwei Jahre die Erfüllung der Anforderungen auf geeignete Weise nachzuweisen. Vorgesehen werden soll eine Möglichkeit für Branchenverbände, selbst Standards zur Konkretisierung der organisatorischen und technischen Vorkehrungen zu entwickeln, die dann durch das BSI anerkannt werden.

WEITERE RECHTLICHE QUELLEN DER DATENSICHERHEIT

Nicht nur gesetzliche Regelungen enthalten Vorgaben zur Datensicherheit. Da gerade die Datensicherheit eine praktische und teilweise hoch-technische Komponente enthält, bedarf es zu einer tatsächlichen und möglichst effektiven Umsetzung der gesetzlich abstrakt definierten Vorgaben (wie etwa „Stand der Technik“) handfester Leitlinien. Einen bekannten und bewährten Katalog solcher praktischer Vorgaben enthält der IT-Grundschutz des BSI.[8] Der IT-Grundschutz ist in verschiedene Kataloge (Bausteine, Gefährdungskataloge, Maßnahmenkataloge) aufgeteilt und bietet mit den in diesen Katalogen aufgeführten Vorschlägen für Umsetzungsmaßnahmen eine einfache Methode, dem Stand der Technik entsprechende Sicherheitsmaßnahmen

zu identifizieren und praxistauglich zu implementieren. Auf diese Weise können nach dem jeweils einschlägigen Gesetz verpflichtete Stellen zumindest den grundlegenden Anforderungen an die Datensicherheit relativ unkompliziert nachkommen.

AKTUELLE FRAGESTELLUNGEN

Trotz aller Anstrengungen: Datensicherheit wird nie ein zu 100 % erreichbares Ziel sein. Dieser Tatsache sollte man sich gewahr werden, wenn man in Zukunft Telekommunikations- und Telemedien-Diensteanbietern zusätzliche Pflichten zum Schutz von informationstechnischen Systemen auferlegen möchte. Auch die Rechtsprechung hat in der Vergangenheit dieses Risiko anerkannt, hieraus jedoch teilweise kaum praxistaugliche Schlüsse für den elektronischen Rechtsverkehr gezogen. Dieser Aspekt angeblich mangelnder Datensicherheit bleibt bisher unterbelichtet. Darunter leidet vor allem auch der private Rechtsverkehr.

So entschied der Bundesgerichtshof (BGH) im Jahr 2011, dass auch wenn den Zugangsdaten für die Internetplattform eBay eine Identifikationsfunktion zukommt, weil das Mitgliedskonto nicht übertragbar und das ihm zugeordnete Passwort geheim zu halten ist, aus diesen Umständen angesichts des im Jahr 2008 (in dem der damalige Sachverhalt spielte) gegebenen und auch zur Zeit des Urteils vorhandenen Sicherheitsstandards im Internet auch bei einem eBay-Account nicht zuverlässig geschlossen werden könne, dass unter einem registrierten Mitgliedsnamen ausschließlich dessen tatsächlicher Inhaber auftritt.[9]

Dies bedeutet, dass stets das latente Risiko besteht, im Internet unwirksame Verträge abzuschließen. § 371 a Zivilprozessordnung (ZPO), der die Beweiskraft elektronischer Dokumente im Zivilprozess regelt, privilegiert allein das gesetzlich geregelte Verfahren der qualifizierten elektronischen Signatur und Nachrichten, die per DE-Mail versendet wurden, was jedoch in der Praxis (vor allem bei Verbrauchern) so gut wie keine Verbreitung findet. Nur beim Einsatz einer qualifizierten elektronischen Signatur soll nach dem Gesetz der Anscheinsbeweis gelten, dass die Erklärung vom Signaturinhaber bzw. einem sicher angemeldeten Nutzer des DE-Mail-Kontos stammt. Ansonsten, also im Fall der „normalen" Internetnutzung oder Versendung einer E-Mail, gilt die freie richterliche Beweiswürdigung nach § 286 ZPO.

Als Folge muss konstatiert werden, dass es derzeit kaum möglich ist, risikolos im Internet Willenserklärungen abzugeben oder Rechtshandlungen vorzunehmen. Vertragsschlüsse, Kündigungen oder ähnliche Erklärungen sind rechtssicher per E-Mail nicht möglich. Es stellt sich daher unweigerlich die Frage, ob der Gesetzgeber und die Rechtsprechung an das Internet und den elektronischen Geschäftsverkehr nicht unbillig hohe Anforderungen an die Datensicherheit im Vergleich zur „Offline-Welt" stellen. Vor allem aber führt diese Minderbewertung der aktuellen technischen Umstände und Gegebenheiten im Internet zu einer Förderung antiquierter Technologien, wie etwa dem Telefax. Ob eine solche Entwicklung im Jahr 2014 noch gewollt sein kann, muss ernsthaft bezweifelt werden.

FAZIT

Datensicherheit ist bereits derzeit und wird auch in der Zukunft ein wichtiger, wenn nicht sogar der wesentliche Faktor für die Bereitstellung und Inanspruchnahme informationstechnischer Systeme sein. Bei allem berechtigten Streben nach sicheren Datenverarbeitungssystemen oder Internetverbindungen sollte jedoch nicht eine Richtung eingeschlagen werden, die das Internet per se als risikoreichen und weniger vertrauenswürdigen Raum als die „Offline-Welt" begreift. Ja, das Internet ist kein rechtsfreier Raum und soll dies auch nicht sein. Es sollte aber ebenso wenig ein Raum der Überregulierung werden, der die auch in der Offline-Welt bestehenden Restrisiken ohne jede noch so kleine Ausnahme auszuschließen trachtet und dadurch letzten Endes praktikable Lösungen für eine zumindest halbwegs sichere Kommunikation vereitelt. So muss etwa in Zukunft eine einfache (!) Beweisbarkeit von abgeschlossenen Verträgen möglich sein. Außerhalb der digitalen Welt können Verträge sogar mündlich geschlossen werden, ohne hohe Formvorschriften einhalten zu müssen. Auch Papierdokumente sind nicht fälschungssicher und selbst die Briefpost kann manipuliert werden. Eine rigi-

dere Behandlung der Online-Welt durch eine Regulierung, die strengere technische Voraussetzungen schafft und jedweden theoretischen Missbrauch von vornherein auszuschließen trachtet, bedürfte zumindest einer besonderen Rechtfertigung.

Datensicherheit sollte in Zukunft als ein allgemeines Schutzprinzip verstanden werden, welches in mehrere Richtungen ausstrahlt. Es schützt den Bürger gegenüber dem Staat, ebenso wie den Bürger gegenüber Unternehmen. Daneben muss es auch im Verhältnis zwischen Unternehmen und dem Staat gelten. Zuletzt darf Datensicherheit auch nicht im Verhältnis zwischen Unternehmen außer Acht gelassen werden. In all diesen Beziehungen ist der physische Schutz von Daten und von informationstechnischen Systemen von Bedeutung und sollte es auch in Zukunft sein. Aber es muss praktikabel bleiben und um Akzeptanz beim Anwender werben. Die Definition eines angemessenen Schutzniveaus, das die wesentlichen Bedrohungen und Missbrauchsrisiken auffängt, zugleich aber in der Anwendung praktikabel bleibt und elektronische Handlungen und Erklärungen als rechtsverbindlich anerkennt, wenn sie unter Verwendung von in diesem Sinne datensicherer Infrastruktur vorgenommen werden, sollte der Gesetzgeber im Auge behalten.

THORSTEN FELDMANN, LL.M.

Fachanwalt für Urheber- und Medienrecht,
JBB Rechtsanwälte, Berlin

ANMERKUNGEN

1 § 1 Abs. 1 Bundesdatenschutzgesetz (BDSG); siehe auch Art. 1 Abs. 1 der Richtlinie 95/46/EG (Datenschutzrichtlinie): „Schutz der Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten".

2 EuGH, Urt. v. 8. April 2014 - C-293/12 und C-594/12, Rz. 66.

3 Art. 17 Abs. 1 Datenschutzrichtlinie lautet: „Die Mitgliedstaaten sehen vor, dass der für die Verarbeitung Verantwortliche die geeigneten technischen und organisatorischen Maßnahmen durchführen muss, die für den Schutz gegen die zufällige oder unrechtmäßige Zerstörung, den zufälligen Verlust, die unberechtigte Änderung, die unberechtigte Weitergabe oder den unberechtigten Zugang – insbesondere wenn im Rahmen der Verarbeitung Daten in einem Netz übertragen werden – und gegen jede andere Form der unrechtmäßigen Verarbeitung personenbezogener Daten erforderlich sind."

4 BVerfG, Urt. v. 27. Februar 2014 – 1 BvR 370/07 - , - 1 BvR 595/07 -.

5 BVerfG, Urt. v. 27. Februar 2014 – 1 BvR 370/07 - , - 1 BvR 595/07 -, Rz. 200.

6 BVerfG, Urt. v. 27. Februar 2014 – 1 BvR 370/07 - , - 1 BvR 595/07 -, Rz. 201.

7 Referentenentwurf des Bundesministeriums des Innern, Stand: 18. August 2014, http://www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/Entwuerfe/Entwurf_IT-Sicherheitsgesetz.pdf?__blob=publicationFile, Stand: 9.12.2014.

8 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html, Stand: 9.12.2014.

9 BGH, Urt. v. 11. Mai 2011 – VIII ZR 289/09 -, Rz. 18.