Der Bayerische Staatsminister der
Justiz
Prof. Dr. Winfried Bausback

Es gilt das gesprochene Wort

Vortrag von Herrn Staatsminister am 28. April 2014 an der Hochschule Aschaffenburg zum Thema "Datenschutz, Grundrechte und öffentliche Sicherheit - ein unauflösbarer Widerspruch?"

Telefon: 089/5597-3111
Telefax: 089/5597-2332
e-mail: presse@stmj.bayern.de
Internet: www.justiz.bayern.de
Prielmayerstraße 7
80335 München

Übersicht

1. Einführung
2. Begrüßung
3. Grundrechte
4. Bedeutung der Grundrechte für den Datenschutz im Verhältnis Bürger/Staat
    a) Abwehrrecht
    b) Volkszählungsurteil/Recht auf informationelle Selbstbestimmung
    c) Online-Durchsuchung/IT-Grundrecht
    d) Vorratsdatenspeicherung
5. Grundrechte und ausländische Nachrichtendienste
6. Bedeutung der Grundrechte für den Datenschutz zwischen Privaten
    a) Eigenverantwortung
    b) Schutzpflichten des Staates
    c) Strafrechtsschutz
    d) Bundesdatenschutzgesetz
    e) Stärkung der Medienkompetenz
    f) Datenschutz durch Technik
    g) EU-Datenschutzgrundverordnung
    h) Internationale Standards
7. Fazit und Ausblick

Anrede!

Einführung

Seien wir ehrlich: Wir alle genießen das Internet. Wir alle genießen die phantastischen Möglichkeiten, die es uns für einen Austausch mit Freunden und Bekannten und Menschen weltweit bietet. Wir alle googlen, surfen, um uns leicht und schnell Informationen zu beschaffen oder einzukaufen. Und das Beste: Dank Smartphone und Tablet können wir praktisch jederzeit an jedem Ort online gehen.

Wie immer im Leben gibt es aber auch hier einen Haken: Wir hinterlassen überall Datenspuren. Und im Laufe der Zeit kommen gewaltige Datenmengen zusammen, die potentiell weltweit zugänglich sind.

Telefon: 089/5597-3111
Telefax: 089/5597-2332
e-mail: presse@stmj.bayern.de
Internet: www.justiz.bayern.de
Prielmayerstraße 7
80335 München

Diese Daten können aufgrund der rasanten technischen Entwicklung immer leichter zusammengeführt, gespeichert und ausgewertet werden. Die neue Technik ermöglicht auch neue Kriminalitätsformen - auf Neudeutsch Cybercrime -, die gerade auf den Missbrauch unserer Daten angelegt sind. Den Kriminellen auf den Fersen ist der Staat mit neuen Überwachungsmethoden.

Da wird uns schon mulmig, wenn wir in den Medien lesen, dass ausländische Geheimdienste jeden Monat eine halbe Milliarde Telefon- und Internetverbindungen in Deutschland überwachen sollen. Wir kommen ins Grübeln, wenn wir lesen, dass die Staatsanwaltschaft Verden einen Datensatz von 18 Millionen gestohlenen E-Mail-Adressen einschließlich Passwörtern sicherge-

stellt hat.

Andererseits hat mancher von Ihnen vielleicht auch mit einem diffusen Gefühl der Erleichterung gelesen, dass jüngst der Europäische Gerichtshof die EU-Richtlinie zur Vorratsdatenspeicherung für ungültig erklärt hat.

Anrede!

Begrüßung

Sie sehen also, das Thema meines Vortrags ist hochaktuell. Ich danke Ihnen und insbesondere dem Initiator, Herrn Professor Krepold, für die Gelegenheit, dass ich heute zu dem Thema "Datenschutz, Grundrechte und öffentliche Sicherheit - ein unauflösbarer Widerspruch?" zu Ihnen sprechen darf.

Der Titel meines Vortrags signalisiert es bereits: Hier geht es um eine Grundfrage des freiheitlichen Rechtsstaates. Wir haben einerseits den Datenschutz als Symbol für Privatsphäre, für Selbstbestimmung und Freiheit. Und auf der anderen Seite die Sicherheit, für die der Staat im Interesse eines friedlichen, geordneten Zusammenlebens zu sorgen hat - im Interesse des Gemeinwohls aber auch des Einzelnen.

Besteht da ein Widerspruch? Auf der einen Seite die Freiheit und der Datenschutz und die Sicherheit auf der anderen Seite?

Über das Verhältnis von Freiheit und Sicherheit ist viel Kluges gesagt worden. Wilhelm von Humboldt formuliert im Jahr 1792:

"Ohne Sicherheit ist keine Freiheit". Benjamin Franklin, der amerikanische Staatsmann, erklärte hingegen - etwas vereinfacht formuliert: "Wer Freiheit für Sicherheit aufgibt, wird beides verlieren".

Als Politiker und Staatsrechtler bin ich der festen Überzeugung, dass wir in Deutschland diese beiden Werte - Datenschutz und Sicherheit - sehr gut miteinander verbinden und auch gewährleisten können, wenn wir sie in jedem Einzelfall sorgfältig gegeneinander abwägen und ausbalancieren. Dieser Werteausgleich stellt uns in Zeiten des Internet allerdings vor gewaltige Herausforderungen.

- Ein Grund ist die hochdynamische technische Entwicklung, die mit jedem Fortschritt neue Möglichkeiten und Gefahren mit sich bringt, bei denen der Datenschutz und die Sicherheit in Einklang gebracht werden müssen.

- Ein weiterer Grund ist die weltweite Vernetzung, die dazu führt, dass der Staat über sein Territorium hinaus nur noch begrenzte Möglichkeiten hat, den Datenschutz und die Sicherheit für seine Bürger zu gewährleisten.

Wir dürfen vom Staat deshalb auch keine absolute Sicherheit erwarten. Das ist in der virtuellen Welt nicht anders als im wirklichen Leben.

Auch im wirklichen Leben verlangen wir vom Staat nur das Mögliche. Wir erwarten vom Staat, dass er uns in Deutschland sichere Straßen zur Verfügung stellt und für Verkehrsregeln sorgt. Keiner erwartet, dass der Staat auf deutschen Straßen absolute Unfallfreiheit garantiert - und erst recht nicht auf ausländischen Straßen.

Jeder Autofahrer weiß, dass er für seine Sicherheit verantwortlich ist und er passt auf sich auf, so gut er kann. Mit diesem realistischen Ansatz sollte sich jeder Einzelne von uns auch auf der virtuellen weltweiten Datenautobahn bewegen - wenngleich man einräumen muss, dass die Eigenverantwortung des Einzelnen wegen der technischen Komplexität und der unüberschaubaren Vernetzungsmöglichkeiten an Grenzen stößt.

Ich bin gleichwohl der festen Überzeugung, dass wir hier in Deutschland mit unserem demokratischen Rechtsstaat und seinen Kontrollmechanismen national hervorragend aufgestellt sind: Unser Grundgesetz - mit seinen weitsichtig formulierten Grundrechten und der starken Stellung des Bundesverfassungsgerichts als Hüterin der Verfassung - bietet auch in Zeiten der digitalen Revolution und der weltweiten Vernetzung, immer wieder eine wohl abgewogene Lösung für den Ausgleich zwischen Freiheit und Datenschutz einerseits und der Sicherheit andererseits.

Grundrechte

Anrede!

Wenn ich mir Ihre Fragestellungen ansehe, so zielen diese bei der Frage nach Datenschutz und Sicherheit auf zwei Beziehungsebenen ab:

- erstens auf das Verhältnis Bürger und Staat und
- zweitens auf das Verhältnis zwischen Privaten, also etwa den Internetnutzern und den Internetdienstleistern. Und gerade dieses Verhältnis - das möchte ich an dieser Stelle vorwegnehmen - ist eine zentrale Herausforderung für den Staat.

Früher dachte man beim Thema Datenschutz eigentlich ausschließlich an Gefahren durch den Staat.

Hintergrund ist vor allem das Szenario vom "Big Brother", dem totalen Überwachungsstaat also, den George Orwell in seinem Buch "1984" skizzierte.

Doch in Zeiten des Internets und der Global Player liegen die Gefahren für den einzelnen Internetnutzer heute weniger beim "Big Brother" Staat als vielmehr bei den neuen privaten Freunden: den namhaften Betreibern privater Suchmaschinen, "CLOUD"-Anbietern, online-Händlern, Betreibern sozialer Netzwerke, Kreditkartenunternehmen und Smartphone-Apps.

Denn Daten werden nicht zu Unrecht als das "Gold des 21. Jahrhunderts" bezeichnet. Mit den Daten der User lassen sich Milliardengewinne machen.

Und dann gibt es natürlich auch noch die Cyber-Kriminellen.

Anrede!

Grundrechte

Auf diesen beiden Beziehungs- oder vielleicht manchmal besser Gefahrenebenen spielen die Grundrechte eine entscheidende Rolle für den Ausgleich von Datenschutz und Sicherheit:

- Im Verhältnis des Bürgers zum Staat haben die Grundrechte ihre klassische Bedeutung: Sie sichern die Freiheit des Einzelnen. Sie sind ein subjektives Abwehrrecht des Bürgers gegen ungerechtfertigte Eingriffe des Staates. Der Staat ist an die Grundrechte gebunden und muss jeden

Eingriff umfassend rechtfertigen. Jeder staatliche Eingriff in die Freiheit der Bürger bedarf einer Grundlage im Gesetz und muss verhältnismäßig sein. Das heißt: Er darf nur so weit gehen, wie es das Ziel des staatlichen Eingriffs erfordert. Die Grundrechte binden auch den Gesetzgeber. Verletzt der Gesetzgeber ein Grundrecht, so hat jeder einzelne Bürger einen starken Partner: das Bundesverfassungsgericht - das werde ich nachher noch näher ausführen.

- Die zweite Beziehungsebene ist das Verhältnis der Privaten untereinander. Hier haben die Grundrechte eine ganz andere Bedeutung. Die Grundrechte gelten nicht unmittelbar zwischen den Privaten. In einem

freiheitlich demokratischen Rechtsstaat gilt die Privatautonomie. Bürger und Privatunternehmen begegnen sich grundsätzlich auf Augenhöhe in Freiheit und Gleichheit. Sie können grundsätzlich frei bestimmen, was sie tun. Die Grundrechte verpflichten aber den Staat zum Schutz - genauer gesagt zu einem gerechten Ausgleich zwischen den grundsätzlich gleichrangigen berechtigten Interessen der Bürger bzw. Privatunternehmen.

Der Staat muss hier eine Rechtsordnung schaffen, die die Grundrechte des Einzelnen auch gegen andere Privatpersonen und Unternehmen angemessen schützt.

Für den Datenschutz bedeutet das vor allem: Der Staat muss den Einzelnen davor schützen, dass private Dritte ohne sein Wissen oder ohne seine Einwilligung Zugriff auf seine Daten nehmen, sie weiterleiten oder verwerten. Auf diesen Aspekt werde ich im zweiten Teil meines Vortrags eingehen.

Anrede!

Abwehrrecht

Wie steht es also um Datenschutz, Grundrechte und Sicherheit im Verhältnis Bürger und Staat? Hier möchte ich zunächst eines klar stellen: Ein freiheitlich demokratischer Rechtsstaat wie die Bundesrepublik Deutschland ist sich seiner Verantwortung gegenüber den Grundrechten - insbesondere dem Datenschutz - sehr genau be-

wusst.

Eingriffe des Staates in die Grundrechte des Einzelnen sind daher nie Selbstzweck - gerade wenn es um staatliche Eingriffe zugunsten der Sicherheit geht. Denn wir alle erwarten zurecht vom Staat, dass er für die Sicherheit der Allgemeinheit und des Einzelnen sorgt. Auch Sie finden es sicher gut, wenn eine Videoüberwachung die Ergreifung von Kofferbombenlegern ermöglicht oder dass mit einer Telefonüberwachung ein Kinderpornohändler gefasst werden kann.

Ein wehrhafter Rechtsstaat muss die Bevölkerung wirkungsvoll vor Straftaten schützen. Solche Schutzmaßnahmen können im Einzelfall auch einen Eingriff in Grundrechte bedeuten.

Und gerade bei dem Thema Datenschutz kommt den Grundrechten und der Rechtsprechung des Bundesverfassungsgerichts eine ganz entscheidende Bedeutung zu. Die Entwicklung des grundrechtlichen Datenschutzes gegen unberechtigte Eingriffe des Staates zeigt die Stärke unseres Grundgesetzes, die Stärke unseres Bundesverfassungsgerichts und die Stärke des Staates der seine verfassungsmäßigen Grenzen achtet.

Das Grundgesetz ist am 23. Mai 1949 in Kraft getreten. Damals war an Internet, Google und Facebook noch gar nicht zu denken, genauso wenig an Themen wie Online-Durchsuchung, automatisierte Kennzeichenerkennung oder Vorratsdatenspeicherung.

Und doch haben das Grundgesetz und das Bundesverfassungsgericht gezeigt, dass die Freiheitsrechte des Einzelnen und die Privatsphäre auch im digitalen Zeitalter vor ungerechtfertigten Eingriffen des Staates bestens geschützt werden können - ohne dass man dauernd die Verfassung ändern müsste.

Anrede!

Volkszählungsurteil - "Grundrecht auf informationelle Selbstbestimmung"

Ausgangspunkt für den modernen Datenschutz ist die Entscheidung des Bundesverfassungsgerichts zum sogenannten "Volkszählungsurteil" vom 15. Dezember 1983. Diese Entscheidung wird völlig zurecht als "Magna Charta" des Deutschen Datenschutzrechts bezeichnet.

Denn in diesem Urteil hat das Bundesverfassungsgericht aus dem Grundgesetz erstmals ein "Grundrecht auf informationelle Selbstbestimmung" abgeleitet. Im Jahr 1983 sollte in der Bundesrepublik Deutschland eine Volkszählung durchgeführt werden, d.h. eine statistische Erfassung von Informationen wie Namen, Anschrift, Art des Lebensunterhalts, des Berufs und anderer ähnlicher Daten.

Vielleicht lag es gerade an dem bereits genannten Buch von George Orwell "1984", dass die Menschen damals die Gefahr eines aufkommenden Überwachungsstaates durch den sogenannten "Big Brother" sahen. Faktisch war die Bedrohung allerdings überschaubar: Die Computertechnologie stand noch in den Anfängen.

Datenverarbeitung erfolgte weitgehend durch zentrale, aus heutiger Sicht vergleichsweise langsame Großrechner mit nur sehr geringer Speicherkapazität. Ich bin mir sicher, dass jedes Smartphone, das Sie heute bei sich haben, leistungsfähiger ist.

Das Bundesverfassungsgericht hat damals aus Art. 1 Abs. 1 des Grundgesetzes - also dem Schutz der Menschenwürde - in Verbindung mit Art. 2 Abs. 1 des Grundgesetzes - d.h. dem Schutz der allgemeinen Handlungsfreiheit - das sog. "Recht auf informationelle Selbstbestimmung" hergeleitet.

Die herausragende Bedeutung des Persönlichkeitsschutzes hatte das Gericht schon früher unterstrichen: In der sog. "Mikrozensus"-Entscheidung aus dem Jahr 1970 hat es dem Staat untersagt, einen Menschen zwangsweise in seiner ganzen Persönlichkeit zu registrieren und zu katalogisieren. Im sog. Elfes-Urteil aus dem Jahr 1957 hat es einen für den Staat unzugänglichen Bereich individueller Privatheit als Ausdruck der Menschenwürde festgelegt.

Neu war an dem sog. Volkszählungsurteil, dass das Bundesverfassungsgericht das aus Art. 1 und Art. 2 des Grundgesetzes hergeleitete allgemeine Persönlichkeitsrecht an die modernen Bedingungen der automatischen Datenverarbeitung angepasst hat.

Karlsruhe hat klargestellt, dass die freie Entfaltung der Persönlichkeit den Schutz des Einzelnen gegen die unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraussetzt.

Das Grundrecht auf informationelle Selbstbestimmung gewährleistet dem Einzelnen die Befugnis, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Das Bundesverfassungsgericht hat dabei ausdrücklich festgestellt, dass die Persönlichkeit des Einzelnen und die Ausübung seiner Freiheitsrechte gefährdet sind, wenn der Einzelne nicht mehr überschauen kann, wer in einer Gesellschaft was und wann und bei welcher Gelegenheit über ihn weiß.

In seinem Volkszählungsurteil hat das Bundesverfassungsgericht allerdings auch die Grenzen des Grundrechts auf informationelle Selbstbestimmung aufgezeigt. Es hat dem Einzelnen kein eigentumsgleiches Recht an "seinen Daten" eingeräumt und damit Forderungen wie "meine Daten gehören mir" eine Absage erteilt. Da der Mensch Teil einer miteinander kommunizierenden Gemeinschaft ist, können auch personenbezogene Informationen nicht ausschließlich dem Betroffenen allein zugeordnet werden.

Das bedeutet zugleich, dass der Einzelne Einschränkungen seines Rechts auf informationelle Selbstbestimmung im überwiegenden Allgemeininteresse hinnehmen muss.

Eingriffe des Staates bedürfen dann aber einer hinreichend bestimmten gesetzlichen Grundlage, die den Verwendungszweck der zu erhebenden Daten spezifisch und präzise festlegt. Das Bundesverfassungsgericht forderte ferner verfassungsrechtliche Schutzvorkehrungen wie Aufklärungs-, Auskunfts- und Löschungspflichten sowie die Beteiligung eines unabhängigen Datenschutzbeauftragten. Das Volkszählungsurteil mit seinen klaren Vorgaben führte im Jahre 1990 zu einer Neufassung des aus dem Jahr 1977 stammenden Bundesdatenschutzgesetzes.

Das Urteil war ein Meilenstein für den Datenschutz. Die Entscheidung hat das Bewusstsein geschaffen, dass mit personenbezogenen Daten sensibel umgegangen werden muss.

Anrede!

Weitere Entwicklung: neue Maßnahmen gegen organisierte Kriminalität und Terrorismus sowie neue Entwicklung der Informations- und Kommunikationstechnologie

In den Folgejahren wurde der grundrechtliche Datenschutz gegen staatliche Eingriffe in mehreren Entscheidungen weiter präzisiert. Hintergrund waren Gesetze für neue Ermittlungsmethoden zur Bekämpfung der organisierten Kriminalität und des internationalen Terrorismus. Als Beispiele möchte ich hier die "Online-Durchsuchung" und die Vorratsdatenspeicherung nennen.

Anrede!

Online-Durchsuchung

Nach den Terroranschlägen vom 11. September 2001 in den USA und vom 11. März 2004 in Madrid kam es am 27. Februar 2008 zu einer weiteren wichtigen Entscheidung des Bundesverfassungsgerichts - und zwar zur sog. Online-Durchsuchung. Darunter versteht man den heimlichen Zugriff auf einen Rechner mittels einer Spionagesoftware, die es ermöglicht, sämtliche Daten auf dem Rechner zu lesen und zwar auch solche, die verschlüsselt kommuniziert oder hinterlegt werden - ein Trojaner also.

Die Verfassungsbeschwerde richtete sich gegen das Verfassungsschutzgesetz des Landes Nordrhein-Westfalen.

In dieser Entscheidung hat das Bundesverfassungsgericht anerkannt, dass der einzelne Nutzer aufgrund der rasanten technischen Entwicklung der weltweiten Vernetzung seine Daten gar nicht mehr selber beherrschen und schützen kann. Seine Eigenverantwortung stößt an Grenzen.

Er versteht die informationstechnischen Systeme immer weniger und durchschaut auch nicht ihre technischen Arbeitsabläufe. Ihm bleibt also nichts anderes übrig als auf das ordnungsgemäße Funktionieren seiner Hard- und Software zu vertrauen sowie darauf, dass sie nicht von außen manipuliert werden.

Mit seinem Urteil zur Online-Durchsuchung hat das Bundesverfassungsgericht wiederum aus Art. 1 Abs. 1 des Grundgesetzes in Verbindung mit Art. 2 Abs. 1 des Grundgesetzes ein neues Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität der eigenen informationstechnischen Systeme entwickelt, das verkürzt als IT-Grundrecht bezeichnet wird.

Das Bundesverfassungsgericht sah die Gefahr, dass man sich mit einem heimlichen Zugriff auf einen Rechner ein umfassendes Bild über die Persönlichkeit des Menschen machen kann. Der einzelne Nutzer könne auch gar nicht mehr kontrollieren und steuern, welche Information das System überhaupt über ihn speichert.

Das Grundrecht auf informationelle Selbstbestimmung reichte somit nicht aus, um auch das für den Persönlichkeitsschutz wichtige Vertrauen in die Funktionsfähigkeit der eigenen, zur Kommunikation eingesetzten informationstechnischen Systeme zu schützen.

Das Bundesverfassungsgericht entschied sich deshalb für eine Vorverlagerung des grundrechtlichen Schutzes bereits gegen die Infiltration - also noch bevor überhaupt ein Zugriff auf bestimmte Daten erfolgt: Denn der heimliche behördliche Zugriff unterläuft die informationelle Selbstbestimmung, also den Selbstschutz durch Verschlüsselung oder Nutzung von Passwörtern.

Das Bundesverfassungsgericht stellte insbesondere für die Frage der Verhältnismäßigkeit solcher staatlichen Eingriffe hohe Hürden auf und formulierte strenge Anforderungen an die Erhebung und Verwertung der aufgrund der Infiltration gewonnenen Daten und Informationen. Es stellte weiterhin hohe Anforderungen an die Rechtfertigung einer Online-Durchsuchung für die Strafverfolgung und forderte insoweit ein überragend wichtiges Rechtsgut wie den Schutz von Leib, Leben und Freiheit oder solcher Allgemeingüter, die die Grundlagen des Staates oder der Existenz der Menschen berühren - namentlich Angriffe auf existenzsichernde öffentliche Versorgungseinrichtungen wie z.B. Staudämme.

Hohe Forderungen wurden auch im präventiven Bereich an die Art und Intensität der Gefährdung gestellt und eine hinreichende Eintrittswahrscheinlichkeit für diese Gefahr gefordert. Schützend stellte sich das Bundesverfassungsgericht auch vor den Kernbereich der privaten Lebensgestaltung.

Da für die staatlichen Behörden nicht von vorneherein absehbar ist, ob sie mit der Infiltration in diesen Kernbereich eingreifen, hat das Bundesverfassungsgericht zwischen der Erhebung und der Auswertung der Daten differenziert. Eine Datenerhebung sei zu unterlassen, wenn Anhaltspunkte dafür bestehen, dass der Kernbereich der privaten Lebensgestaltung berührt werden kann.

Auch bei der Entscheidung zur Online-Durchsuchung hat das Bundesverfassungsgericht deutlich gemacht, dass es sehr präzise und mit viel Augenmaß den Datenschutz gegen die öffentliche Sicherheit abwägt.

Anrede !

Vorratsdaten-speicherung

Als letztes Beispiel für den Datenschutz im Verhältnis Bürger/Staat möchte ich die Entscheidung des Bundesverfassungsgerichts zur sog. Vorratsdatenspeicherung vom 2. März 2010 anführen und auch kurz auf die Entscheidung des Europäischen Gerichtshofs vom 8. April 2014 eingehen.

Zum einen ranken sich um diese Entscheidungen viele Missverständnisse, zum anderen zeigt sich hier, dass neben dem Bundesverfassungsgericht auf nationaler Ebene jetzt auch der EuGH auf europäischer Ebene für einen starken Grundrechtsschutz sorgt.

Ausgangspunkt für das Tätigwerden des Gesetzgebers war auch hier die Terroranschläge vom 11. September 2001, bei dem die Täter im Vorfeld über Telefon, E-Mail und Internet kommunizierten. Der Gesetzgeber schuf daher im Telekommunikationsgesetz eine Verpflichtung für die privaten Telekommunikationsdiensteanbieter, Verkehrsdaten des Telefonverkehrs, des Internetzugangs und der E-Mail-Kommunikation zu speichern - und zwar ohne besonderen Anlass.

Die Strafverfolgungsbehörden sollten nach der Strafprozessordnung nur unter engen gesetzlichen Voraussetzungen bei einem Anfangsverdacht für schwere Straftaten auf diese Daten bei den privaten Telekommunikationsdiensteanbietern zugreifen können. Eine anlasslose Herausgabe oder Rasterung gespeicherter Verkehrsdaten an die Strafverfolgungsbehörden war damit ausgeschlossen.

Zum besseren Verständnis möchte ich hiermit klarstellen, dass es bei den Verkehrsdaten, die gespeichert werden sollen, nicht um die Inhalte der Kommunikation geht, sondern nur die äußeren Verkehrsdaten - also wer wann wie lange mit wem kommuniziert hat.

Das sind die Telefonnummern, der Beginn und das Ende einer Verbindung, beim Mobilfunkverkehr die Funkzelle und bei der Internet- und E-Mail-Kommunikation die IP-Adresse. Diese Daten fallen bei den privaten Kommunikationsdienstleistern technisch ohnehin an. Sie werden aber wegen der inzwischen weit verbreiteten Flatrates heute kaum noch gespeichert. Es sollten also keine zusätzlichen Daten erhoben, sondern nur ihre sechsmonatige Speicherung gesichert werden.

Das Bundesverfassungsgericht hat in seiner Entscheidung zur Vorratsdatenspeicherung im Jahr 2010 die Neuregelungen im Telekommunikationsgesetz für verfassungswidrig erklärt.

Es sah darin einen nicht gerechtfertigten Eingriff in das Grundrecht des Art. 10 des Grundgesetzes, der das Brief-, Post- und Fernmeldegeheimnis schützt.

Zwar sei die sechsmonatige vorsorgliche anlasslose Speicherung von Telekommunikationsverkehrsdaten durch private Dienstanbieter nicht schlechthin unvereinbar mit diesem Grundrecht. Die gesetzlichen Regelungen seien jedoch nicht verhältnismäßig. Zum einen müsse angesichts der Schwere des Eingriffs ein besonders hoher Standard an Datensicherheit gewährleistet werden.

Der Abruf und die Nutzung solcher Daten durch staatliche Behörden seien zur Ahndung von Straftaten zulässig, die überragend wichtige Rechtsgüter bedrohen, oder zur Abwehr einer konkreten Gefahr für solche Rechtsgüter. Auch müsse der Gesetzgeber Vorkehrungen für die Transparenz der Datenverwertung sowie für einen effektiven Rechtsschutz treffen.

Das Bundesverfassungsgericht hat damit klar zum Ausdruck gebracht, dass die Vorratsdatenspeicherung grundsätzlich möglich ist, aber eben nicht so, wie es der Gesetzgeber in der Neuregelung des Telekommunikationsgesetzes gemacht hatte.

Grundlage für diese als verfassungswidrig erklärte Neuregelung des Telekommunikationsgesetzes war eine EU-Richtlinie aus dem Jahr 2006. Diese hat der Europäische Gerichtshof am 8. April dieses Jahres mit weitgehend ähnlicher Begründung wie das Bundesverfassungsgericht wegen des Verstoßes gegen die Grundrechte auf Achtung des Privatlebens und auf Schutz personenbezogener Daten gemäß Art. 7 und 8 der EU-Grundrechtecharta für nichtig erklärt.

Anrede!

Lassen Sie mich hierzu kurz ein paar Ausführungen als Rechtspolitiker machen. Auch die Entscheidung des Europäischen Gerichtshofs ist keinesfalls das Ende der Vorratsdatenspeicherung.

Denn auch der Europäische Gerichtshof hat die Vorratsdatenspeicherung nicht umfänglich für grundrechtswidrig erklärt. Die Entscheidung bedeutet erst recht kein Verbot der Vorratsdatenspeicherung in den Mitgliedsstaaten, sie hat also keine Sperrwirkung.

Sofern persönliche Stellungnahme beabsichtigt:

Nach meiner festen Überzeugung brauchen wir in Deutschland die Vorratsdatenspeicherung, damit wir schwerste Straftaten verfolgen und Leib und Leben der Menschen wirksam schützen können. Als wir die Regelung der Vorratsdatenspeicherung in Deutschland noch hatten, konnten wir Dank der Mindestspeicherfristen zahlreiche schwerste Straftaten aufklären: So konnten etwa im Jahr 2009 einem Sexualstraftäter 25 Taten des schweren sexuellen Missbrauchs von Kindern nachgewiesen werden.

Ohne die Vorratsdatenspeicherung wäre das nicht möglich gewesen, weil der Internetprovider diese Daten heute nicht mehr speichert.

Jetzt ist der Bundesgesetzgeber gefordert, so schnell wie möglich einen Gesetzentwurf vorzulegen, der die verfassungsrechtlichen Vorgaben achtet und den gebotenen Grundrechtsschutz gewährleistet.)

Zwischenfazit

Anrede!

Als Zwischenfazit ist zu dem Komplex Datenschutz, Grundrechte und Sicherheit im Verhältnis zwischen dem Bürger und dem Staat festzuhalten:

Auch in Zeiten der rasanten technologischen Entwicklung und der massiven Bedrohung der Sicherheit vor allem durch den internationalen Terrorismus ist Deutschland kein Orwell 'scher Überwachungsstaat. Wir haben ein hervorragendes Grundgesetz, das die Persönlichkeitssphäre des Bürgers und seine Daten gegen ungerechtfertigte Eingriffe des Staates effektiv schützt. Der Gesetzgeber ist sich der Bedeutung der Grundrechte bewusst und achtet sie.

Anrede!

Datenschutz und ausländische Geheimdienste

Eine Ihrer Fragen bezieht sich auf eine staatliche Überwachung ganz anderer Art - und zwar auf die eingangs genannten Aktivitäten ausländ-

discher Geheimdienste.

Der Deutsche Bundestag hat hierzu am 20. März 2014 einen Untersuchungsausschuss eingesetzt. Ich bitte um Verständnis, dass ich der Arbeit dieses Ausschusses heute hier keinesfalls vorgreifen kann und will.

Ich bin aber gerne bereit, ein paar allgemeine Ausführungen zu den völkerrechtlichen und verfassungsrechtlichen Fragen einer solchen Tätigkeit zu machen. Denn auch insoweit haben vor allem die Grundrechte Relevanz. Es stellt sich hier aber nicht die Frage eines Abwehrrechts gegenüber dem Staat. Denn die Grundrechte des Grundgesetzes binden nicht ausländische Staaten.

Es stellt sich aber sehr wohl die Frage, inwieweit der deutsche Staat verfassungsrechtlich verpflichtet sein könnte, deutsche Bürger vor einem ungerechtfertigten Zugriff ausländischer Nachrichtendienste auf ihre Daten zu schützen.

Hier ist zunächst der Grundsatz der Territorialität zu beachten. Die Hoheitsgewalt der Bundesrepublik Deutschland beschränkt sich auf ihr Staatsgebiet. Wenn ein Deutscher im Ausland von Maßnahmen ausländischer Staaten betroffen ist, hat der deutsche Staat nur begrenzte Schutzmöglichkeiten. Naturgemäß können wir fremden Staaten im Ausland nicht die deutsche Rechtsordnung aufzwingen.

Deutschland kann hier aber beispielsweise darauf hinwirken, dass die Maßnahme nach dem einschlägigen ausländischen Recht geprüft wird. Etwas anderes wäre es freilich, wenn deutsche Staatsbürger auf dem Gebiet der Bundesrepublik von ausländischen Staaten überbewacht werden. Hier kann der Betroffene den Schutz der deutschen Staatsgewalt verlangen, wenn sie ungerechtfertigte Hoheitsakte eines anderen Staates auf dem Gebiet der Bundesrepublik Deutschland zulässt oder gar unterstützt.

Das Völkerrecht kennt kein umfassendes Verbot der Spionage. Klar ist aber auch, dass für eine solche Tätigkeit die Zustimmung des betroffenen Territorialstaates erforderlich wäre.

In den Medien wurde berichtet, dass Bundeskanzler Adenauer 1954 den amerikanischen Truppen das Recht zur eigenen Nachrichtenerhebung eingeräumt habe im Zusammenhang mit dem sog. Truppenvertrag bzw. einem Zusatzabkommen zum Nato-Truppenstatut. Nach neuen historischen Erkenntnissen sollen diese späteren geheimen Zusatzerklärungen für eine weitreichende Telekommunikationsüberwachung der Alliierten umgestaltet worden sein.

Seit dem Inkrafttreten des sog. G10-Gesetzes im Jahr 1968 gibt es für die Alliierten hingegen keine Ermächtigung mehr zu geheimen Datenerhebungen aus nicht öffentlichen Quellen auf deutschem Staatsgebiet. Wenn die Medienberichte also tatsächlich zutreffen sollten, könnte die deutsche Souveränität hier verletzt worden

sein. Kein Verstoß läge hingegen vor, soweit die Nachrichtendienste im eigenen Land gehandelt und den Internetverkehr ausgewertet hätten, der über die dort gelegenen Server und Leitungen lief.

Wenn es jedoch zu einer rechtswidrigen Datenerhebung auf deutschem Staatsgebiet gekommen sein sollte, stellt sich die Frage, ob die Bundesregierung verpflichtet wäre, gegen die Datenerhebung vorzugehen. Art. 10 Abs. 1 des Grundgesetzes schützt den Telekommunikationsverkehr gegen ungerechtfertigte Zugriffe der deutschen öffentlichen Gewalt.

Daraus folgen auch Schutzpflichten und zwar nicht nur gegen ungerechtfertigte Beeinträchtigung durch Private.

Auch ein Eingriff durch ausländische Staaten könnte grundsätzlich Schutzpflichten auslösen. Hier hat das Bundesverfassungsgericht wiederholt entschieden, dass aus der grundrechtlichen Schutzpflicht des Staates grundsätzlich keine konkrete verfassungsrechtliche Handlungsvorgabe folgt.

Die Verfassung gibt hier somit große Spielräume und begründet keine bestimmte Handlungspflicht des Staates für seine Bürger.

Anrede!

Als Politiker bin ich allerdings der Auffassung, dass Klärungsbedarf besteht! Die Bundeskanzlerin bzw. die Bundesregierung haben bereits mit einem "Acht-Punkte-Programm für besseren

Datenschutz" reagiert. Auch der bayerische Ministerrat hat in seiner Sitzung vom 6. November 2013 ein dreizehn Punkte umfassendes 'Maßnahmenkonzept für Freiheit, Verantwortung und Vertrauen in einer vernetzten Welt' vorgelegt. Darin hat die Staatsregierung klargestellt, dass auf internationaler Ebene - nach einer gründlichen Aufklärung und Analyse der bisherigen Überwachungsmaßnahmen - ein internationaler Datenschutzkodex der Nachrichtendienste vereinbart werden muss. Eckpunkt eines solchen Kodex soll der Verzicht auf das Ausspionieren befreundeter Staaten und auf Wirtschaftsspionage sein. Auch darf es keine anlasslose und allumfassende Überwachung durch die Nachrichtendienste geben. Der Schutz des Kernbereichs der privaten Lebensgestaltung muss in jedem Fall sichergestellt sein. Damit haben wir

in Bayern ein klares Signal zu dieser Frage gegeben.

Wir sollten nun die Ergebnisse des Untersuchungsausschusses abwarten und dann über weitere politische Konsequenzen beraten.

Anrede!

Datenschutz im Verhältnis zwischen Privaten und Schutzpflichten des Staates

Ich komme nun zu dem Bereich, der mir mit Blick auf den Datenschutz die größten Sorgen macht: dem Datenschutz zwischen Privatpersonen.

Der frühere Präsident des Bundesverfassungsgerichts Papier hat es auf den Punkt gebracht - ich zitiere:

"Ich sorge mich jedenfalls mehr davor, dass wir uns zu einer privaten Überwachungsgesellschaft internationalen Ausmaßes verwandeln und dies weitgehend auch noch völlig freiwillig." - Ende des Zitats.

Wenn wir ehrlich sind, nehmen wir in der virtuellen Welt vieles hin, was uns im wirklichen Leben mehr als seltsam vorkommen würde? Denken Sie an das schöne Beispiel des morgendlichen Zeitungskaufs am Kiosk: Wenn Ihnen der Zeitungsverkäufer ungefragt auch noch eine Auto-XY-Zeitung empfehlen würde, weil Sie hierzu in der gestrigen Zeitung einen Artikel gelesen haben, oder gar das passende Medikament zu dem gestrigen Artikel im Wissenschaftsteil, dann wären sie mehr als beunruhigt.

Im Internet hingegen nehmen wir es hin, dass wir ungefragt eine Vielzahl von Werbemails zugeschickt bekommen, obwohl wir mit dem jeweiligen Anbieter bisher keinen direkten Kontakt hatten.

Eigenverantwortung

Für mich stellt sich - noch vor dem durchaus berechtigten Ruf nach den Schutzpflichten des Staates - zunächst die Frage der Eigenverantwortung. Wir sollten auch im Internet im ureigenen Interesse alle Selbstschutzmaßnahmen ergreifen, die wir ergreifen können. Wir sollten unsere Emails konsequent verschlüsseln und uns durchaus einmal die Zeit nehmen, die Datenschutzerklärung eines Internetanbieters genau durchzulesen und bewusst zu entscheiden, ob wir das wirklich alles akzeptieren wollen oder ob

wir nicht lieber auf das Angebot verzichten. Wir sollten auch überlegen, wem wir welche Information von uns preisgeben und ob das das Internet überhaupt wissen sollte.

Ein Beispiel ist das sog. Self Tracking. Inzwischen gibt es einen boomenden Markt für Apps zur Selbstüberwachung. Gesundheitsbewusste Menschen erfassen mit diesen Apps ihre Schrittzahl, ihren Kalorienverbrauch, die Pulsfrequenz, den Blutzucker, das Körperfett oder gar das Schlafverhalten. Hier sollte man sich schon Gedanken machen, wo diese Daten genau gespeichert werden. Man kann nur davor warnen, diese Information über Cloud-Dienste auswerten zu lassen. Denn sonst entpuppt sich das wunderbare Smartphone schnell als gefährlicher Spion in der Hosentasche. Noch brisanter

wird es, wenn Ihre sensiblen Gesundheitsdaten von einem Dritten mit anderen im weltweiten Netz verfügbaren Daten zu einem umfassenden Persönlichkeitsprofil zusammengeführt werden. Deshalb fordern Datenschützer zu Recht, dass die Nutzer möglichst geizig mit ihren Daten im Netz umgehen sollten. Wenn man die freimütige Self-Tracking-Praxis mancher betrachtet und andererseits die vehemente Kritik an der elektronischen Gesundheitskarte, dann fällt schon auf, wie relativ die Sorge um den eigenen Datenschutz manchmal ist.

Grenzen der Eigenverantwortung

Mit der Eigenverantwortung allein ist es freilich nicht getan. Angesichts des rasanten technischen Fortschritts und der weltweiten Vernetzung stößt ein eigenverantwortlicher Selbst-

schutz schnell an seine Grenzen. Denn hier geht es nicht mehr um Inhalte, die wir als Nutzer aktiv und selbstbestimmt im Internet preisgeben, sondern um die nicht durchschaubare Erfassung und Auswertung von Datenspuren, die wir bei jeder Aktion im Internet hinterlassen und gar nicht steuern können.

Solche Spuren können beiläufig anfallen, wenn eine Dienstleistung erbracht wird. Sie kann aber auch gezielt erfasst werden etwa durch Analysesoftware oder Tracking-Cookies zur technischen Beobachtung des Nutzungsverhaltens auf Websites.

Auch die informationstechnischen Systeme sind kaum noch in der alleinigen Herrschaft des Nutzers, wenn sich die Anbieter von Betriebssystem und Apps durch die Nutzungsbedingungen zahlreiche Zugriffsrechte auf Systemfunktionen wie Kontaktlisten, Speicher, Kamera oder GPS einräumen lassen. Hinzukommen Cyber-Kriminelle, die private Daten ausspähen und missbrauchen.

Verantwortung des Staates

Natürlich kann sich hier der Staat nicht heraushalten und das Internet als rechtsfreien Raum dulden. Wie eingangs beschrieben wirken die Grundrechte zwar nicht unmittelbar zwischen den Privaten und geben dem Einzelnen insbesondere kein Abwehrrecht gegenüber den Internetdienstleistern. Sie verpflichten den Staat aber zum Schutz.

Dabei hat der Staat zu beachten, dass sich hier zwei Private in Freiheit gegenüberstehen, die beide Grundrechtsschutz gegenüber dem Staat genießen. Private dürfen grundsätzlich alles tun, was ihnen gesetzlich nicht ausnahmsweise verboten ist.

Im Verhältnis zwischen den Privaten kommt es entscheidend auf die Einwilligung des Betroffenen an. Einwilligung bedeutet allerdings nicht absolute Verfügungsbefugnis im Sinne von "meine Daten gehören mir". Ich kann also nicht bestimmen, wer wann was und auf welche Weise über mich weiß. Ich kann also Informationen nicht wie mein Eigentum zurückfordern und auch nicht verlangen, dass jemand etwas vergisst, was er über mich erfahren hat.

Privater Datenschutz ist hier ein Gestaltungsauftrag für den Staat. Vor allem der Gesetzgeber hat für einen gerechten Ausgleich zu sorgen zwischen den sich gegenüberstehenden Grundrechtspositionen der Privaten - also beispielsweise dem einzelnen Nutzer und dem Internetdienstleister. Das Grundrecht auf informationelle Selbstbestimmung verpflichtet die staatlichen Organe insbesondere, dem Einzelnen Schutz davor zu bieten, dass private Dritte ohne sein Wissen und ohne seine Einwilligung Zugriff auf seine persönlichen Daten nehmen.

Die Grundrechte lassen den Staat jedoch einen großen Einschätzungs-, Wertungs- und Gestaltungsspielraum, wie er seinen Schutzpflichten nachkommt. Maßgeblich ist für den Schutz insbesondere, welches Grundrecht betroffen ist und

wie groß der drohende Schaden für dieses Rechtsgut ist. Der Betroffene hat dabei grundsätzlich aber keinen Anspruch auf ein ganz bestimmtes Handeln des Staates. Er hat vielmehr den von der Verfassung eingeräumten breiten Ermessensspielraum des Gesetzgebers zu akzeptieren.

Anrede!

Strafrechtsschutz

In Deutschland wurde bereits eine Vielzahl von Maßnahmen zum privaten Datenschutz ergriffen - von denen ich hier beispielhaft diejenigen aufgreifen möchte, die Ihre vorab übermittelten Fragen betreffen.

In meinem Zuständigkeitsbereich als Justizminister ist das natürlich vor allem der strafrechtliche Datenschutz gegen den unberechtigten Zugriff Dritter. So wurden etwa gegen das Ausspähen von elektronisch übermittelten oder gespeicherten Daten Strafvorschriften zum Schutz des Betroffenen geschaffen.

Zu nennen sind hier insbesondere die §§ 202 a, 303 a und 303 b des Strafgesetzbuches, die den Einzelnen gegen Angriffe Dritter wie etwa das Ausspähen seiner Daten, Datenmanipulation oder Computersabotage schützen. Und weil das Thema so wichtig ist, gibt es auch bei mir im Justizministerium in der Strafrechtsabteilung ein Referat speziell für Internetkriminalität.

Sie hatten mich vorab gefragt, wo denn der Rechtsstaat bleibe, wenn es um den Missbrauch des Internet als Pranger gehe? - also etwa wenn im Internet jemand zu Unrecht einer Straftat verdächtigt wird und dann mit massiven Folgen überzogen wird, die von einer Beleidigungswelle bis hin zu körperlichen Misshandlungen reichen.

Bei solchen Falschverdächtigungen bis hin zu Gewaltaufrufen via Facebook gilt in der virtuellen Welt nichts anderes in der realen Welt. Hier greifen zunächst die Straftatbestände, die die Ehre schützen, also die Beleidigungsvorschriften nach den §§ 185 ff. des Strafgesetzbuches. Wird gar öffentlich zu Misshandlungen oder bis hin zur Lynchjustiz aufgerufen, so kommt eine Strafbarkeit wegen Auffordern zu einer Straftat gemäß § 111 des Strafgesetzbuches in Betracht oder

aber die Anstiftung zur Körperverletzung oder zu Mord. Solche Internetaufrufe können auch eine strafbare Störung des öffentlichen Friedens durch Androhung von Straftaten gemäß § 126 des Strafgesetzbuches erfüllen. Kommt es dann zur tatsächlichen Misshandlung oder Sachbeschädigung, greifen für die Täter vor Ort insoweit - wie bei sonstigen Fällen auch - insbesondere die Körperverletzungs- oder Totschlagsdelikte bzw. Sachbeschädigung, Hausfriedensbruch, etc.

Die Schwierigkeit liegt hier weniger in den Straftatbeständen, als vielmehr darin, die Täter dingfest zu machen. Geben sich die Täter nicht selbst zu erkennen, wird es für die Strafverfolgungsbehörden häufig schwierig, sie tatsächlich ausfindig zu machen.

Das ist insbesondere dann der Fall, wenn sie bewusst die Anonymität des Netzes ausnutzen. Gerade wenn der Aufruf unter Verwendung einer dynamischen IP-Adresse erfolgte, wird in einem solchen Fall häufig nur die Vorratsdatenspeicherung helfen, um den Täter zu ermitteln. Auch das zeigt, wie wichtig dieses Instrument gerade zur Bekämpfung von Straftaten im Internet wäre.

Verschärft wird die Situation, wenn solche Straftaten auch noch im Ausland begangen werden oder über Server im Ausland. Hier stößt der nationale Rechtsstaat buchstäblich an seine Grenzen. Entsprechende Ermittlungsmaßnahmen können dann nur im Wege der internationalen strafrechtlichen Rechtshilfe erreicht werden.

Anrede!

BDSG

Weitere wichtige Regelungen für den privaten Datenschutz enthält natürlich das Bundesdatenschutzgesetz.

Wenn Sie etwa Ihren Namen, Ihre Anschrift und Telefonnummer in elektronischen Verzeichnissen wiederfinden, die die veröffentlichten Datensätze von Telekommunikationsdienstanbietern bezogen haben, so können Sie sich dagegen wehren. Denn die Aufnahme solcher Daten in derart elektronische Verzeichnisse hat zu unterbleiben, "wenn der entgegenstehende Wille des Betroffenen ersichtlich ist" (§ 29 Abs. 3 Satz 1 BDSG).

Wer also eine solche Weitergabe durch den Telekommunikationsanbieter an Anbieter von elektronischen Verzeichnissen unterbinden will, sollte sich an den Telekommunikationsanbieter wenden und einen Widerspruch geltend machen.

Gerade soweit es um den Umgang mit Ihren Daten geht, möchte ich Sie an dieser Stelle ausdrücklich auf das Bayerische Landesamt für Datenschutzaufsicht hinweisen. Bayern hat hier im Jahr 2011 ein deutschlandweit anerkanntes Kompetenzzentrum für Datenschutzfragen geschaffen. Dorthin können Sie sich mit Beschwerden über die Verletzung von Datenschutzvorschriften durch Private wenden - gerade auch wenn es um die Löschung von Daten aus dem Internet geht.

Häufig erscheint es dem Einzelnen aber zu mühsam, den Missbrauch seiner Daten durch ein Unternehmen geltend zu machen. Hier erweisen sich die Verbraucherverbände als starker Partner. Deshalb begrüße ich ausdrücklich die Bestrebungen des Bundes, Verbraucherschutzverbänden bei Datenschutzverstößen ausdrücklich ein Klagerecht einzuräumen. Sie sollen solche Rechtsverstöße künftig für die Verbraucher geltend machen können.

Anrede!

Stärkung der Medienkompetenz

Wichtiger Bestandteil der Erfüllung der staatlichen Schutzpflicht ist natürlich auch die Information der Verbraucher.

Wir müssen die Medienkompetenz des Einzelnen weiter stärken, damit er frühzeitig Risiken im Netz erkennt und weiß, wie er sich davor schützen kann.

Bayern hat auch frühzeitig Maßnahmen ergriffen, um schon Schüler fit zu machen gegen die Risiken des Internets. Bereits seit 2002 werden 120 spezialisierte Beratungslehrkräfte - sog. "MiBs" (Medienpädagogisch-informationstechnische Beratungslehrkräfte) - ausgebildet, die als Multiplikatoren die Lehrkräfte vor Ort unterstützen. Schlagwort ist hier der "Medienführerschein Bayern".

Anrede!

Datenschutz durch Technik

Aber auch bei der besten Ausbildung wird der Selbstschutz der Verbraucher an seine Grenzen stoßen. Deshalb müssen wir auch die IT-Industrie noch stärker in die Pflicht nehmen. Das Schlagwort heißt hier "Datenschutz durch Technik". Grundlage für geschäftlichen Erfolg ist das Vertrauen der Kunden.

Deshalb muss die IT-Industrie ein noch stärkeres Augenmerk auf den Schutz der Privatsphäre und den Datenschutz legen. Die Technik sollte so gemacht sein, dass man die Dienstleistungen auch ohne Preisgabe unnötiger Daten bekommen kann.

Der technische Selbstschutz, wie die E-Mail-Verschlüsselung, sollte möglichst einfach und praktikabel sein. Genauso sollten die Geschäftsbedingungen sein. Sie sollten auch nicht nur pauschal akzeptiert werden können, sondern echte Wahlmöglichkeiten eröffnen.

EU-Datenschutzgrundverordnung

Diese Gedanken werden übrigens von der EU-Datenschutzgrundverordnung aufgegriffen, die derzeit auf europäischer Ebene beraten wird.

Auch sie setzt auf eine Stärkung des sog. "eingebauten" Datenschutzes (Privacy by Design) und datenschutzfreundliche Voreinstellungen (Privacy by Default).

Der Ansatz einer EU-weiten Lösung ist sicher der richtige Weg und ein erster wichtiger Schritt, um den Datenschutz für den Einzelnen im weltweiten Netz international zu stärken. Bayern begrüßt den Ansatz, dass für alle Unternehmen, die in Europa Produkte oder Dienstleistung anbieten, ein einheitliches Datenschutzrecht gelten soll - ganz egal, ob sie in der EU eine Niederlassung oder auch nur einen Server haben. Gerade die Global Player müssen so mit hohen europäischen Datenschutzstandards in die Pflicht genommen werden. In dem Verordnungsvorschlag werden auch das Recht auf Datenübertragbarkeit, das Recht, vergessen zu werden und die Regelung zur Profilbildung näher präzisiert. Höhere Anforderungen werden an die Einwilligung des Verbrauchers als Rechtsgrundlage der Datenverarbeitung gestellt.

Mit dieser Datenschutzgrundverordnung könnte eine wichtige Grundlage für einen einheitlichen effektiven Datenschutz durch Private in ganz Europa geschaffen werden.

Anrede!

Internationale Standards

Über die Ebene der EU hinaus müssen Deutschland und die EU natürlich auch versuchen, konsequent die Mitwirkungsmöglichkeiten auf internationaler Ebene zu nutzen, um möglichst hohe Schutzstandards für unsere Bürger zu erreichen. Gerade wenn es um den weltweiten Datenschutz geht, stößt Deutschland im wahrsten Sine des Wortes an seine Grenzen. Wir können für unsere Bürger die deutschen Schutzstandards nicht weltweit gewährleisten.

Das muss jedem bewusst sein, der die Vorzüge des world wide web für sich nutzt.

Anrede!

Fazit

Lassen Sie mich zum Schluss folgendes Fazit ziehen.

Erstens: Das Grundgesetz hat sich mit seiner Beständigkeit und Flexibilität auch in Zeiten des Internet bewährt. Es gibt die richtigen Antworten, wenn es um Eingriffe des Staates und die Balance zwischen Datenschutz und Sicherheit geht.

Zweitens: Im Verhältnis der Privaten untereinander gewährleisten die Grundrechte eine angemessene Schutzpflicht des Staates. Der Staat muss stets prüfen und entscheiden, ob das, was er bisher getan hat, ausreicht, um den privaten Datenschutz seiner Bürger zu gewährleisten.

Einen absoluten Schutz kann es angesichts des hochdynamischen technischen Fortschritts und der weltweiten Vernetzung nicht geben. Der Staat kann mit seinen Gesetzen faktisch nicht stets auf Augenhöhe mit dem Fortschritt sein. Und gerade dort, wo der Geltungsbereich des Grundgesetzes endet, kann er seine nationale Schutzfunktion ohnehin nicht entfalten.

Deshalb ist auch jeder Einzelne gut beraten, bei jedem Klick im Internet Freiheit und Sicherheit gegeneinander abzuwägen und genau zu überlegen, was er selbst für seinen Schutz tun kann.

Herzlichen Dank für Ihre Aufmerksamkeit!