Der Bayerische Staatsminister der
Justiz
Prof. Dr. Winfried Bausback

Es gilt das gesprochene Wort

Vortrag des Herrn Staatsministers am 26. März 2015 bei der Eröffnung einer Datenschutzkonferenz in Starnberg

zum Thema "Datenschutz und Cybercrime - eine Gratwanderung zwischen Freiheit und Sicherheit"

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

Anrede!

Einführung

Seien wir ehrlich: Wir alle genießen das Internet mit seinen phantastischen Möglichkeiten, die es uns bietet. Wir alle googeln, surfen, um uns leicht und schnell Informationen zu aktuellen Themen zu beschaffen. Wir nutzen das Internet zum Online-Einkauf und wickeln Überweisungen online vom Sofa aus ab, ohne ein Geschäft oder eine Bank betreten zu müssen. Und das Beste: Dank Smartphone und Tablet können wir praktisch jederzeit an jedem Ort weltweit online gehen.

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

Wie so häufig im Leben gibt es aber auch hier **einen Haken**:

Wir hinterlassen überall **Datenspuren**. Und im Laufe der Zeit kommen gewaltige Datenmengen zusammen, die potentiell ebenfalls weltweit zugänglich sind. Diese Daten können aufgrund der rasanten technischen Entwicklung immer leichter zusammengeführt, gespeichert und ausgewertet werden.

Die in den letzten Wochen diskutierten **Änderungen der Geschäftsbedingungen von Facebook** haben dies wieder einmal deutlich vor Augen geführt:

Danach kann Facebook geräteübergreifend auf nahezu alle Daten zugreifen, sie verknüpfen und auswerten.

Aber auch, wenn wir in den Medien lesen, dass **ausländische Geheimdienste** jeden Monat eine halbe Milliarde Telefon- und Internetverbindungen in Deutschland überwachen sollen, kann es uns mulmig werden.

Das Internet hat aber auch noch eine andere dunkle Seite: Die digitalen Techniken ermöglichen **immer neue Kriminalitätsformen** - auf Neudeutsch Cybercrime -, die gerade auf den **Missbrauch unserer Daten** angelegt sind und ohne diese Technik gar nicht möglich wären.

Dies gilt vor allem für die Fälle des Hacking, der Datenveränderung oder den Diebstahl von digitalen Identitäten, um diese etwa zum Computerbetrug zu verwenden. Aber auch Phishing, Skimming und der Aufbau und Betrieb von Botnetzen bis hin zu Denial of Service-Attacken mit gezielten Angriffen auf Rechnersysteme sind hier zu nennen.

In gleicher Weise verlagern sich altbekannte Tatbegehungsweisen von der realen in die virtuelle Welt. So erfolgt der klassische Betrug statt an der Haustüre nun über Ebay oder über Fakeshops im Internet. Auch Kinderpornografie wird nicht mehr unter dem Ladentisch verbreitet, sondern nur noch über entsprechende Newsgroups oder Foren im Internet.

Besonders erschreckend ist aktuell die Entwicklung zu "crime as a service", einer service-basierten Kriminalitätsindustrie. Man kauft sich die für die Begehung einer Straftat notwendigen Werkzeuge und Komponenten im virtuellen Untergrund über entsprechende Foren einfach zusammen.

Es verwundert daher nicht, dass es in den letzten fünf Jahren hier zu einer **Verdoppelung der registrierten Verfahren** gekommen ist. Und zudem ist die Dunkelziffer sehr hoch, da in der Statistik viele Fälle - etwa Straftaten mit Auslandsbezug - gar nicht erfasst sind.

Beunruhigend ist auch die Tendenz zu immer gefährlicheren und häufigeren Großangriffen auf Informationssysteme im öffentlichen und privaten Sektor. Gleichzeitig sind die Angriffe mit immer ausgefeilteren Methoden verbunden, bei denen kriminelle Handlungen in verschiedenen Stufen erfolgen.

Anrede!

Ihnen als ausgewiesene Experten muss ich es nicht sagen: Die Themen Datenschutz und Cybercrime sind hochaktuell. Dabei geht es hier um Grundfragen des freiheitlichen Rechtsstaates. Wir haben **einerseits** den **Datenschutz** als Symbol für Privatsphäre, für Selbstbestimmung und **Freiheit**.

Und **auf der anderen Seite die Bedrohung der 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 auf der anderen Seite die Sicherheit?

Über das Verhältnis von Freiheit und Sicherheit ist viel Kluges gesagt worden. Wilhelm von Humboldt formulierte 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 Internets allerdings vor gewaltige **Herausforderungen**.

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

Mit diesem realistischen Ansatz sollte sich jeder Einzelne von uns auch auf der virtuellen weltweiten Datenautobahn bewegen.

Ich bin gleichwohl der festen Überzeugung, dass wir hier in Deutschland mit unserem demokratischen Rechtsstaat und seinen Kontrollmechanismen hervorragend aufgestellt sind.

Anrede!

Grundrechte

Das **Verhältnis von Datenschutz und Sicherheit** spielt sich auf **zwei Beziehungsebenen** ab:

- erstens zwischen Bürger und Staat und

- zweitens 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 Beeinträchtigungen aus der staatlichen Sphäre**. Hintergrund ist vor allem das Szenario vom "Big Brother", dem totalen **Überwachungsstaat**, 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 und von sozialen Netzwerken, aber auch von "CLOUD"-Anbietern, online-Händlern, 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. Da wünscht sich mancher den Staat als großen Bruder, der aufpasst, dass ihm diese neuen "Freunde" nichts tun.

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.

- 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**.

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.

Anrede!

Abwehrrecht

Wie steht es also um Datenschutz, Grundrechte und Sicherheit im Verhältnis Bürger und Staat?

Die Entwicklung des grundrechtlichen Datenschutzes, ausgehend vom "Volkszählungsurteil" im Jahr 1983, mit dem ein Grundrecht auf informationelle Selbstbestimmung geschaffen wurde, zeigt die Stärke unseres Grundgesetzes, die Stärke unseres Bundesverfassungsgerichts und die Stärke des Staates, der seine verfassungsmäßigen Grenzen achtet.

Dies obwohl bei der Schaffung des Grundgesetzes an Internet, Google und Facebook nicht zu denken war, genauso wenig wie an Online-Durchsuchung oder Verkehrsdatenspeicherung.

Anrede!

Das **Volkszählungsurteil war ein Meilenstein** für den Datenschutz.

Die Entscheidung hat das Bewusstsein geschaffen, dass mit **personenbezogenen Daten sensibel umgegangen** werden muss.

In den Folgejahren wurde **der grundrechtliche Datenschutz** gegen staatliche Eingriffe - vor allem in Bezug auf zwei neue Ermittlungsmethoden - **weiter präzisiert**: die "Online-Durchsuchung" und die Verkehrsdatenspeicherung.

Online-Durchsuchung

Mit seinem Urteil zur **Online-Durchsuchung** hat das Bundesverfassungsgericht ein neues Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität der eigenen informationstechnischen Systeme entwickelt, das **verkürzt als "IT-Grundrecht"** bezeichnet wird.

Das Bundesverfassungsgericht stellte mit dieser Entscheidung 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.

Anrede!

Verkehrsdaten-speicherung

Auf die schon angesprochene Entscheidung des Bundesverfassungsgerichts zur **Verkehrsdatenspeicherung** vom 2. März 2010 möchte ich noch etwas näher 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.

Dabei möchte ich zunächst nochmals **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 sollen also **keine zusätzlichen Daten erhoben**, sondern nur ihre sechsmonatige Speicherung gesichert werden.

Das Bundesverfassungsgericht hat in seiner Entscheidung zwar die Neuregelungen im Telekommunikationsgesetz wegen eines nicht gerechtfertigten Eingriffs in das Grundrecht des Art. 10 des Grundgesetzes für verfassungswidrig erklärt.

Aber Karlsruhe hat auch **ganz klar gesagt**: Eine solche sechsmonatige Speicherung von Telekommunikationsverkehrsdaten durch private Dienstanbieter ist **nicht schlechthin unvereinbar** mit den Grundrechten, wenn sie verhältnismäßig ausgestaltet ist!

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 **Verkehrsdatenspeicherung grundsätzlich möglich** ist, aber eben nicht so, wie sie der Gesetzgeber damals geregelt 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 2014 mit weitgehend ähnlicher Begründung wie das Bundesverfassungsgericht wegen eines unverhältnismäßigen 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 der Europäische Gerichtshof hat die Vorratsdatenspeicherung keinesfalls umfänglich für grundrechtswidrig erklärt! Und die Entscheidung bedeutet erst recht **kein Verbot** der Verkehrsdatenspeicherung in den Mitgliedsstaaten, sie hat also **keine Sperrwirkung.**

Nach meiner festen Überzeugung **brauchen** wir in Deutschland **die Verkehrsdatenspeicherung**, damit wir **schwerste Straftaten verfolgen** und Leib und Leben der Menschen wirksam schützen können!

Als wir die Verkehrsdatenspeicherung in Deutschland noch hatten, konnten wir Dank der Mindestspeicherfristen zahlreiche schwerste Straftaten aufklären. Und ohne anlasslos gespeicherte Verkehrsdaten gibt es auch für viele Delikte der Cyberkriminalität gar keine Ansatzpunkte für Ermittlungen und damit zur Tataufklärung.

Wir brauchen deshalb **keine Diskussion über das "Ob" einer Verkehrsdatenspeicherung**. Die Notwendigkeit bejahen unsere Fachleute seit Jahren. Wir brauchen vielmehr eine ernsthafte Debatte über das "Wie" – also über eine verfassungs- und rechtsstaatskonforme Ausgestaltung mit Augenmaß. Ich begrüße ausdrücklich, dass sich die **Vernunft nun auch auf Bundesebene einen Weg gebahnt hat.**

Es ist erfreulich, dass zu dem Thema endlich Gespräche zwischen unserem Bundesinnenminister und dem Bundesjustizminister stattfinden und der Kollege **Maas** nunmehr **zeitnah einen Entwurf angekündigt** hat.

Ich hoffe sehr, dass man dabei schnell zu einer guten, tragfähigen Lösung findet! Und ich kann Ihnen versichern, da werde ich "ein Auge drauf haben"!

Damit unseren Staatsanwaltschaften nun endlich die Steine aus dem Weg geräumt werden, die da schon viel zu lange liegen!

Anrede!

Zwischenfazit

Es bleibt letztlich festzuhalten: Auch in Zeiten der rasanten technologischen Entwicklung und der massiven Bedrohung der Sicherheit vor allem durch den internationalen Terrorismus und durch immer neue Formen von Cybercrime ist **Deutschland** selbstverständlich **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.

Und wir haben rechtsstaatliche demokratische Kontrollmechanismen die hinreichenden Grundrechtsschutz gewährleisten.

Anrede!

Datenschutz im Verhältnis zwischen Privaten und Schutzpflichten des Staates

Ich möchte nun auch noch zu dem Bereich kommen, der mir mit Blick auf den Datenschutz die größten Sorgen macht: dem **Datenschutz zwischen Privatpersonen.**

Wenn wir ehrlich sind: Nehmen wir in der virtuellen Welt nicht 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 in unserem ureigenen Interesse alle Selbstschutzmaßnahmen ergreifen, die wir ergreifen können.

Grenzen der Eigenverantwortung

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

Privater Datenschutz ist ein Gestaltungsauftrag für den Staat. Vor allem der **Gesetzgeber** hat hier 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 dem Staat jedoch einen **großen** Einschätzungs-, Wertungs- und **Gestaltungsspielraum**, **wie** er seinen Schutzpflichten nachkommt. Deshalb ist es wichtig, wenn es hier im Bereich des Datenschutzes mit der Europäischen Datenschutzgrundverordnung alsbald zu einer **Festlegung einheitlicher Mindeststandards in der Europäischen Union** kommt.

Mein Haus bringt sich hier selbstverständlich in die Diskussion aktiv ein.

Fazit

Anrede!

Lassen Sie mich zum Schluss folgendes **Fazit** ziehen:

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

Zur **Gewährleistung einer effektiven Strafverfolgung** - etwa im Bereich Cybercrime **brauchen** wir aber auch **Möglichkeiten**, um in angemessenem Umfang in die Datenschutzrechte **einzugreifen**.

Zweitens: Im Verhältnis der Privaten untereinander gewährleisten die Grundrechte eine **angemessene Schutzpflicht** des Staates. Aber:

Einen **absoluten Schutz** kann es angesichts des hochdynamischen technischen Fortschritts und der weltweiten Vernetzung **nicht geben**.

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.

Anrede!

Schluss

In kaum einem anderen Bereich entwickelt sich die Technik und auch das Recht so schnell.

Deshalb ist es **besonders wichtig, dass Staat und Wirtschaft, Juristen und Techniker ständig miteinander im Austausch** sind: Um auf die neuen Probleme und Herausforderungen schnell praktikable Antworten zu finden.

Genau das tun Sie die nächsten zwei Tage in Starnberg.

Ich wünsche Ihnen heute und morgen spannende Diskussionen und gute Gespräche! Auch im Namen unseres **Ministerpräsidenten Horst Seehofer**, den ich heute hier vertrete und von dem ich Sie alle **herzlich grüßen** darf! Vielen Dank für die Aufmerksamkeit!