SPRECHEN WIR ÜBER
DATENSCHUTZ, VORRATSDATEN & ÜBERWACHUNG

Das Recht, allein gelassen zu werden

Vor fast 130 Jahren haben zwei – berühmt gewordene – amerikanische Bundesrichter, erstmals über das Recht, „allein gelassen zu werden" geschrieben (http://bit.ly/1hOespa). Sie gingen dabei von Fällen aus, in denen Fotografen private Anlässe dokumentierten, ohne dass die Betroffenen davon wussten oder dies wollten. Samuel D. Warren und Louis Brandeis, so hießen die Richter, forderten, verstärkt über das Recht auf Privatleben zu diskutieren, und dabei immer die technischen Entwicklungen und die Medien im Auge zu haben.

Am ältesten ist das Recht auf den Schutz des Briefgeheimnisses. In Österreich wurde es 1867 geregelt. Briefe dürfen grundsätzlich nur nach richterlicher Erlaubnis beschlagnahmt und geöffnet werden.

Der Briefverkehr ist auch durch die Europäische Menschenrechtskonvention im Rahmen des Rechts auf Achtung des Privat- und Familienlebens geschützt. Insgesamt soll dieses Recht jedem Menschen einen privaten Bereich sichern, wo seine Persönlichkeit frei entfaltet werden kann. Der Europäische Gerichtshof für Menschenrechte versteht dieses Recht sehr umfassend und dynamisch. Er hat es auch schon in Fällen herangezogen, wo es z. B. um Videoüberwachung ging.

In Österreich gibt es seit 1975 auch einen ausdrücklichen Schutz des „Fernmeldegeheimnisses". Darunter versteht man heute auch e-mails oder Internet-Telefonie. Wie beim Briefgeheimnis braucht eine Ausnahme davon einen richterlichen Befehl.

Datenschutz wurde in Österreich erstmals 1978 in einem Gesetz geregelt. Dabei ging es vor allem darum die – damals noch recht neue – Datenverarbeitung in Großcomputern und Rechenzentren rechtlich zu regeln. Ein Grundrecht auf Datenschutz gibt es in Österreich aber erst seit dem Jahr 2000!

Was ist Datenschutz?

Das Recht auf Datenschutz ist in Österreich in § 1 des Datenschutzgesetzes 2000 geregelt. Dieses Recht ist Teil der Verfassung. Es umfasst drei Bereiche:

Das Recht auf Geheimhaltung von personenbezogenen Daten,
das Recht auf Auskunft über personenbezogene Daten und
das Recht auf Richtigstellung und Löschung personenbezogener Daten.

Daten sind Angaben oder Informationen „über Sachverhalte". Besonders geschützt sind „personenbezogene Daten". Das sind z. B. Daten über den Gesundheitszustand, Herkunft, Sexualleben, politische Einstellungen, persönliche Vorlieben usw. Das können aber auch Daten über das Erwerbsleben sein.

Wenn ein „schutzwürdiges Interesse besteht", hat jede/r einen Anspruch auf Geheimhaltung. Das betrifft z. B. die Ermittlung von Daten, ihre Verwendung oder die Weitergabe. Ein Eingriff in dieses Recht darf nur erfolgen, wenn ein wichtiges öffentliches Interesse (z. B. Ermittlungen wegen einer Straftat) vorliegt. Weil manche dieser Daten besonders sensibel sind (z. B. Gesundheit oder Sexualleben) muss bei jedem Eingriff sichergestellt werden, dass die Geheimhaltungsinteressen der betroffenen Person gewahrt werden.

Das Datenschutzgesetz regelt genau, wie jemand Auskunft über Daten, die der Staat oder ein Privater (auch Unternehmen) über ihn gespeichert hat, erhalten kann. Es regelt auch eine Verpflichtung, Daten richtig zu stellen oder sogar zu löschen. Für die Einhaltung des Datenschutzes sorgt die Datenschutzbehörde (https://www.dsb.gv.at).

Warum ist Datenschutz so wichtig?

Wir alle nutzen ganz selbstverständlich neue digitale Technologien, wir haben elektronische Kundenkarten, sind auf Facebook, twittern und bewegen uns auf Onlineplattformen. Damit geben viele von uns ein gutes Stück ihrer Privatsphäre preis. Unsere Daten sind heute ein wichtiger Wirtschaftsfaktor geworden, und die Vernetzungsmöglichkeiten ermöglichen ein „Profiling" unseres Privatlebens. Während früher nur Telefonbücher oder vielleicht (einzelne) Zeitungsartikel – sehr mühsam – durchsucht werden konnten, wissen Unternehmen heute oft welche Hobbies wir pflegen, welche Kleidung wir gerne tragen, welche Bücher wir lesen, vielleicht auch wo wir wohnen und wie wir leben. Aber: Unsere Privatsphäre und unsere Daten sind grundrechtlich geschützte Güter. Die Frage ist nur: Wie weit reicht dieser Schutz?

Diese Technologien entwickeln sich sehr schnell. Das Recht kommt da oft nicht mit. Datenschutz ist ein wichtiges Grundrecht und damit Teil des Verfassungsrechts, er ist aber auch Technikrecht und Wirtschaftsrecht. Vor allem ist es aber heute europäisches Recht, weil viele Datenverarbeitungen grenzüberschreitend passieren. Die EU hat in diesem Jahr eine neue Datenschutz-Grundverordnung erlassen, die bis 2018 zu einem völlig neuen österreichischen Datenschutzrecht führen wird. Der Gesetzentwurf dafür ist hier zu finden: http://bit.ly/2tleuOG.

Eine wichtige Neuerung des neuen Datenschutzrechts wird das ausdrückliche „Recht auf Vergessenwerden" sein. Wir alle hinterlassen in der virtuellen Welt Spuren mit unseren persönlichen Daten. Manchmal gezwungen, weil wir Daten bekanntgeben müssen, um bestimmte Dienste zu nutzen, großteils freiwillig. Doch vielen Menschen ist nicht bewusst, wie lange ihre Fußabdrücke sichtbar bleiben.

Das Recht auf Datenschutz soll es da ermöglichen, das jede/r von uns eine Chance hat, über die Informationen, die ihn und sie betreffen, selbst zu bestimmen.

Was sind Vorratsdaten?

Die Daten, die jede/r von uns hinterlässt, können auch große Bedeutung für Ermittlungen der Polizei und der Staatsanwaltschaften in Kriminalfällen haben. Sie können auch von Bedeutung dafür sein, Straftaten zu verhindern. Daher kommt die Idee, Daten „auf Vorrat zu speichern."

Vorratsdatenspeicherung bedeutet die allgemeine und anlasslose Speicherung von Bürgerdaten. „Allgemein" heißt, dass die Daten aller Personen, die grob gesprochen im Internet surfen oder telefonieren, gespeichert werden. „Anlasslos" heißt, dass kein bestimmter Grund (z. B. eine Straftat) zur Speicherung von Daten vorliegt. Denn die Vorratsdatenspeicherung ist grundsätzlich als „präventive" („vorbeugende) Speicherung von Daten gedacht. Sie erfolgt ohne, dass es einen konkreten „Anfangsverdacht" in Bezug auf Straftaten gibt.

Wenn über Vorratsdaten gesprochen wird, sind in der Regel Verkehrs-, Zugangs- und Standortdaten gemeint. Unter „Verkehrsdaten" versteht man ganz allgemein, wer wo mit wem telefoniert hat. Telekommunikationsanbieter speichern Telefonnummern, Gesprächsdauer und Ort von dem das Telefonat aus geführt wurde. Allerdings werden nur die Zeiten und Nummern gespeichert, der Inhalt der Gespräche wird nicht aufgezeichnet. Unter Zugangsdaten sind man hingegen die Daten gemeint, die man bei Vertragsschluss angibt. Also Name, Adresse, aber auch IP-Adressen, die für einen Anschluss vergeben werden, um so die Identität einer Person nachvollziehen zu können, die eine bestimmte Seite im Internet besucht hat.

Standortdaten hingegen sind Ortsangaben, die mittels Zeitangabe eine Ortung der Person ermöglichen, um so möglicherweise auch Bewegungsprofile anlegen zu können oder zu bestimmen, wann sich eine Person wo befand.

Die Idee der Vorratsdatenspeicherung ist im Grunde genommen leicht zu erklären: Die Telekommunikationsanbieter, die ihren Kunden die Infrastruktur zum Surfen im Internet bereitstellen, sollen alle Daten ihrer Kunden speichern. Die Behörden sollen diese dann mittels Auskunftsanspruch anfragen können. Dabei erfolgt

die Speicherung nicht anonymisiert, sondern wird auf jederzeitigen Abruf durch die Ermittlungsbehörden zur Verfügung gestellt. Dadurch dass das Konzept der Vorratsdatenspeicherung gegenüber jeder Art von Daten und Personen gerichtet ist, kommt auch ein massives Paket an Daten zusammen.

Die anlasslose und generelle Speicherung erfolgt auch nicht systematisiert, jedenfalls nicht von Seiten des Telekommunikationsanbieters. Die Provider stellen nur „Rohdaten" aber keine „Profile" zur Verfügung. Die Behörden müssen die Daten selbst analysieren, um so auf einen Tatverdacht systematisch zu reagieren und den oder die Tatverdächtigen ausfindig machen können. Provider können sich nicht dagegen wehren und ebenso auch nicht die Betroffenen, da sie zu Beginn der Ermittlungen nicht einmal wissen, dass auf ihre Daten zugergriffen wird. Erst wenn sich der Tatverdacht nicht erhärtet, sollen die Betroffenen informiert werden.

Was sagt unsere Verfassung zu Vorratsdaten?

Angesichts der großen Menge an Daten, die es mittlerweile über jede/n von uns gibt, fragen viele, ob es faktisch überhaupt möglich ist, all diese Daten auszuwerten und zu sammeln. Aber ganz grundsätzlich stellt sich die Frage, ob all das rechtlich überhaupt zulässig ist.

Weil Datenschutz eine grenzüberschreitende Angelegenheit (siehe http://bit.ly/2v8IH4w) ist, haben sich die EU-Mitglieder schon länger darauf geeinigt, Datenschutz grundsätzlich EU-weit zu regeln. 2006 haben sie auch eine Richtlinie beschlossen, nach der jeder Mitgliedsstaat Vorratsdatenspeicherung einführen sollte. Das sollte aber in den Gesetzen jedes Mitgliedsstaats passieren.

In der Richtlinie wurde die Heranziehung der Daten für "schwere Straftaten" für zulässig erachtet. In Österreich wurden dabei alle Taten, mit einem Strafausmaß über einem Jahr bedroht waren, zu schweren Straftaten erklärt. Das hat einen sehr breiten Zugriff der Behörden ermöglicht. Und es führte dazu, dass die Vorratsdaten mehrheitlich nicht zur Terrorismusbekämpfung oder dem Kampf gegen die organisierte Kriminalität genutzt wurden, sondern um Vergehen im Bereich der Vermögensdelikte oder bei "Stalking" aufzuklären.
Seit 2006 haben sich viele Gerichte in den EU-Mitgliedstaaten mit der Vorratsdatenspeicherung befasst. In Österreich hat der Verfassungsgerichtshof (VfGH) 2014 eine Entscheidung (http://bit.ly/2sttiLh) getroffen: Die Vorratsdatenspeicherung, die durch Änderungen des Telekommunikationsgesetzes, des Sicherheitspolizeigesetzes und der Strafprozessordnung eingeführt worden war, stellt für den Verfassungsgerichtshof einen gravierenden Eingriff in das Grundrecht auf Privat- und Familienlebens (Artikel 8 Europäische Menschenrechtskonvention) sowie in das Grundrecht auf Datenschutz dar. Die Bestimmungen wurden daher als verfassungswidrig aufgehoben.

Die Eingriffe in Grundrechte müssen im öffentlichen Interesse erfolgen, zur Zielerreichung geeignet und die Mittel hierfür notwendig und verhältnismäßig sein. Diese Voraussetzungen waren bei einer allgemeinen und anlasslosen Vorratenspeicherung aus Sicht des Verfassungsgerichtshofs nicht gegeben.

Begründet hat er dies mit der Vorgehensweise gegen alle Bürger, die eine anlasslose Speicherung ohne jeglichen Tatverdacht ermöglichte . Dies sei keine notwendige Maßnahme, um das gewünschte Ziel der Bekämpfung "schwerer Straftaten", entgegenzutreten, da dies auch mit weniger schweren Eingriffen erreicht werden könnte. In Bezug auf den Kreis der Delikte, die eine Vorratsdatenspeicherung ermöglichen, sah der VfGH keine Rechtfertigung für den Eingriff in die Grundrechte der Betroffenen, da diese Delikte zu undifferenziert und aus diesem Grund zu weit gefasst waren.

Weiters seien die Bedingungen für die Speicherung solcher Daten, die Anforderungen an deren Löschung sowie die Sicherungen beim Zugriff auf diese Daten, die in den Gesetzen vorgesehen waren, nicht mit der Verfassung vereinbar. Nach Ansicht des VfGH fehlte es an präzisen gesetzlich verankerten Sicherheitsvorkehrungen, wie etwa die Bedingungen für den Zugriff auf diese Daten oder eine Löschverpflichtung. Der Verfassungsgerichtshof erklärte die Vorratsdatenspeicherung aber nicht generell für unzulässig, solange die Bestimmungen im Einklang mit der Verfassung stehen.

Kann man jetzt aber doch Vorratsdaten sammeln?

Der Verfassungsgerichtshof (http://bit.ly/2vLCWt4) hat Bedingungen aufgestellt, unter denen Vorratsdaten gesammelt werden können. Diese sind nicht leicht zu erfüllen, aber es gibt immer wieder Versuche dazu.

Nach langen Diskussionen haben das Innenministerium und das Justizministerium im Sommer 2017 ein sogenanntes “Sicherheitspaket” präsentiert, mit denen mehrere Gesetze geändert werden sollen (http://bit.ly/2ue0Z7s; http://bit.ly/2uec74f). Zu diesen Gesetzentwürfen wurden im Rahmen des Begutachtungsverfahrens mehrere tausend Stellungnahmen abgegeben. Die damalige SPÖ-ÖVP-Regierung konnte aber keine Einigung mehr finden. Im Februar 2018 wurde dieser Vorschlag von der ÖVP-FPÖ-Regierung in leicht veränderter Form wieder vorgelegt (http://bit.ly/2ETez5F).

Der wesentliche Unterschied zum alten Modell der Vorratsdatenspeicherung ist, dass für die Speicherung der Daten nun in jedem Fall ein Anfangsverdacht notwendig soll. Weiters soll nicht jede Person betroffen sein, sondern konkrete Tatverdächtige, bei denen ein bereits ein Tatverdacht besteht. Das soll schon bei Straftaten möglich sein, die mit einer Strafe von einem Jahr bedroht sind. Zudem sollen die Sicherheitsbehörden nur nach gerichtlicher Bewilligung auf Grundlage staatsanwaltlicher Anordnung ermitteln dürfen.

Statt Vorratsdatenspeicherung soll das Verfahren “Quick-Freeze” heißen. Die Daten sollen für die Dauer von maximal 12 Monaten “eingefroren” werden. Erhärtet sich ein Tatverdacht nicht, soll die betroffene Person über das Ermittlungsverfahren informiert werden. Neu ist eine Art Vorratsdatenspeicherung für den gesamten Auto- und Motorradverkehr, bei der Kennzeichen gespeichert werden. Außerdem sollen die Sicherheitsbehörden mehr Zugriffs- und Überwachungsmöglichkeiten auf Mobiltelefone, Computer und Kommunikationsanwendungen bekommen. Ob das im Sinne der Verfassung ausreicht, wird wohl erst eine neue Entscheidung des Verfassungsgerichtshofes klären können.

Wer kontrolliert eine Überwachung?

Bei einer Hausdurchsuchung müssen sich Polizei und Staatsanwaltschaft Zutritt zu einer Wohnung oder einem Büro verschaffen. Bei einer Vernehmung wird man persönlich befragt. Aber wenn Daten überwacht und gesammelt werden, kann es für die allermeisten schwierig bis unmöglich sein, das festzustellen. Aber wie wir gesehen haben (http://bit.ly/2vLCWt4) ist es ganz wichtig, dass die Rechte der Betroffenen gewahrt werden. Wenn diese aber (zunächst) nichts davon erfahren sollen, braucht es jemanden, der gewissermaßen „für sie“ ein Auge darauf wirft. Das sollen die sogenannten „Rechtsschutzbeauftragten“ tun.

Es gibt in Österreich vier Arten von Rechtschutzbeauftragten, deren Aufgaben in der Prüfung und Kontrolle von Rechtsgutbeeinträchtigungen betroffener Personen besteht und ihnen besonderen Rechtschutz gewährt. Jeder Rechtsschutzbeauftragte ist für ein besonderes Gesetz zuständig. Es gibt sie für den Bereich der Strafprozessordnung (StPO), des Sicherheitspolizeigesetz (SPG), des polizeilichen Staatsschutzgesetzes (PStSG), des Finanzstrafgesetzes (FinStrG) sowie des Militärbefugnisgesetzes (MBG).

Rechtsschutzbeauftragte sind unabhängig und dürfen von niemanden Weisungen annehmen. Sie unterliegen der Amtsverschwiegenheit und dürfen also niemanden ihr Wissen über Ermittlungen weitergeben. Ihre Bestellung ist auf die Dauer von drei bis fünf Jahren beschränkt.

Die Institution des Rechtsschutzbeauftragten gibt es bereits seit 1997, wobei ihre Aufgaben seither laufend weiter ausgebaut wurden. Ihr Aufgabengebiet umfasst die Prüfung und Kontrolle von Anordnung, Genehmigung, Bewilligung und Durchführung von Ermittlungsmaßnahmen, die zu Eingriffen in Grundrechte führen. Dazu gehören optische oder akustische Überwachungsmaßnahmen, verdeckte Ermittlungen und Abschluss von Scheingeschäften, der automationsunterstützten Datenabgleich und weitere Maßnahmen.

Das Recht, wieder vergessen zu werden

Man gibt es zwar selten zu, aber die meisten haben schon einmal ihren eigenen Namen bei Google eingeben, um sich die Suchergebnisse anzusehen. Die Treffer interessieren nicht nur einen selbst, sondern auch künftige Arbeitgeber/innen oder andere Menschen, die in die virtuelle Visitenkarte eines Menschen Einblick erhalten wollen.

Doch nicht alle Ergebnisse, die man auf Google über sich oder andere findet, sind tatsächlich erfreulich. Manche Treffer, die in Zusammenhang mit seinem Namen in Suchmaschinen auftauchen, sind schon veraltet und daher möglicherweise nicht mehr zutreffend oder stellen einen falschen Kontext dar. Die Treffer in der Suchmaschine verlinken dann zu Zeitungsartikeln, Gästebüchern oder Bewertungsportalen, die eine Verbindung zu Vor- und Nachname erzeugt haben.

Im Jahr 2014 hat der Europäische Gerichtshof in Luxemburg entschieden, dass man als betroffene Person unter bestimmten Voraussetzungen ein Löschungsbegehren an den Suchmaschinenbetreiber stellen kann (http://bit.ly/1jeYXrK).

Man hat in solchen Fällen zwei Möglichkeiten, entweder man bittet Google die Verknüpfung des Namens mit dem Treffer auf der Website aus der Suchmaschine löschen zu lassen, also „vergessen zu werden" und/oder man wendet sich direkt an den Medieninhaber, der den Originalartikel bzw. Post veröffentlicht hat, um die Ergebnisse schwerer auffindbar zu machen bzw. löschen zu lassen.

Dabei sollte man jedoch wissen, dass das „Recht auf Vergessen werden" nicht automatisch bedeutet, dass man nie wieder mit Name und ungewünschtem Posting gefunden wird. Google ist nicht verpflichtet alle Treffer in seinem Suchmaschinen-Netzwerk zu löschen, sondern macht dies nur für das Land in dem das „Vergessen werden" beantragt wurde. So kann sein, dass ein Treffer nicht mehr über die österreichische Seite zu finden ist, sehr wohl aber über die französische. Jetzt (im Juni 2017) hat aber das Höchstgericht Kanadas entschieden, das Google auch die Pflicht hat, Suchergebnisse weltweit zu löschen. Diese Entscheidung wurde damit begründet, dass es „im Internet keine Grenzen gebe." (http://bit.ly/2tpOceH)

Zum anderen ist das „Original", also der ursprüngliche Ort, an dem die ungewünschte Veröffentlichung stattfand, noch immer vorhanden. Google listet den Treffer nur nicht mehr in seinen Suchergebnissen und macht ihn daher schwerer zu finden. Das Recht auf Vergessen werden ist also nicht gleichzusetzen mit einem Recht auf eine „digitale Tabula Rasa". Es steht allerdings jedem Betroffenen frei, sich bei den jeweiligen Websites zu melden und entweder eine Korrektur zu verlangen bzw. einen Widerspruch gegen die Verarbeitung zu erheben.

Es gibt kein generelles Recht auf Löschung. Vielmehr ist im Einzelfall zu prüfen, was mehr Gewicht hat: Das Recht auf Informations- und Meinungsfreiheit von potenziell am Zugang zu der Information interessierten Nutzer/innen oder das Grundrecht jedes einzelnen auf Achtung des Privatlebens und auf Datenschutz der betroffenen Person vorzunehmen. Diese Abwägung ist wichtig: Denn ansonsten könnte daraus auch ein Recht darauf werden, etwas vergessen zu lassen. So könnten Informationszugänge beschränkt und Zensur legalisiert werden.