

nahme nun mit einem Bedarf zur Harmonisierung der Rechtslage in verschiedenen EU-Staaten. Doch dieser Harmonisierungsbedarf wurde überhaupt erst dadurch geschaffen, dass die EU-Kommission die Einführung der Fluggastdatenspeicherung in einzelnen EU-Ländern mit ins Leben gerufen und unterstützt hat.

Der aktuelle Entwurf nimmt zwar Rücksicht auf die Interessen der Fluggastdatenspeicherung aus, tut ansonsten aber wenig, um die Privatsphäre der Fluggäste zu sichern: Die Daten dürfen von Strafverfolgungsbehörden nicht nur zur Aufklärung von Ver-

brechen, sondern auch für Profiling und Data-Mining verwendet werden. „Dies stellt eine Abkehr von traditioneller Strafverfolgung hin zu einer digitalen Rasterfahndung dar“, wie Kai Nothdurft, Vorstandsmitglied des FfF, betont. Auch der Austausch von Daten mit Strafverfolgungsbehörden und der europäischen Behörden ist nicht geregelt und kaum reguliert.

Die „offenen Fluggastdatenspeicherung und -auswertung lehnen wir entschieden ab“, betont Sylvia Johnigk, Vorstandsmitglied des FfF.

erschienen in der FfF-Kommunikation,
herausgegeben von FfF e.V. - ISSN 0938-3476
www.fiff.de



FfF e.V.

Rote Linien für die EU-Datenschutz-Grundverordnung

Nachdem die Datenschutzstandards in der Praxis des globalen Datenverkehrs immer mehr aufgeweicht wurden, schafft die Datenschutzgrundverordnung die Möglichkeit, bei einem europäischen Grundrecht in die Offensive zu gehen. Das FfF hat sich in den Diskussionsprozess mehrfach eingebracht und Vorschläge für eine datenschutzfreundlichere Zukunft gemacht. Letzte Entwicklungen um den Entwurf des Ministerrates zeigen aber deutlich, dass der Wirtschaftslobbyismus funktioniert und nicht alle Interesse an einem starken europäischen Datenschutz haben. Es ist beschämend, dass gerade Deutschland mit allein 51 Forderungen den Parlamentsvorschlag beschädigt hat. Die gemeinsame Position des Rats der Europäischen Union vom 15. Juni 2015, 9565/15, überschreitet diverse rote Linien und fällt hinter die Standards der Datenschutz-Richtlinie von 1995 zurück.

Einwilligung

Bisher tun die Anbieter von Dienstleistungen im Internet häufig so, als bedeute schon die Nutzung eines Dienstes oder das Nichtthandeln eine stillschweigende Einwilligung. In Artikel 7 wollen Parlament und Kommission sicherstellen, dass der betroffenen Person im Sinne einer informierten Einwilligung bewusst ist, dass sie ihre Einwilligung gibt. Eine ausdrückliche Handlung möchte der Rat vermeiden und fügt im Erwägungsgrund 25 ein, dass die Einwilligung auf „beliebige“ geeignete Weise und nur „eindeutig“ statt „ausdrücklich“ erfolgen soll. Schon die Einstellungen des Browsers oder einer anderen Anwendung sollen eine Einwilligung signalisieren können.

Will eine Person eine Einwilligung widerrufen, soll das nach dem Wunsch des Europäischen Parlaments so einfach sein wie das Erteilen der Einwilligung, als die ja schon der Besuch einer Website gesehen werden kann. Diese Forderung im Artikel 7 hat der Rat gestrichen.

Bei diesem Grundpfeiler des Datenschutzes ist so viel Entgegenkommen gegenüber den Datenkraken mit uns nicht zu haben!

Datensparsamkeit

In Artikel 5 Satz 1 (c) haben Parlament und Kommission in wünschenswerter Klarheit festgelegt, dass die zu erhebenden personenbezogenen Daten auf das für die Zwecke „notwendige“ Maß beschränkt sein müssen. Der Rat weicht den Zweckbezug zu „verhältnismäßig“ auf. An anderer Stelle (Erwägungsgrund 39) will der Rat die Verhältnismäßigkeit den Betreibern von elektronischen Kommunikationsnetzen und -diensten sowie Anbietern von Sicherheitstechnologien und -diensten erlassen. Dagegen verlangt das Europäische Parlament, dass die Verarbeitung „für die Gewährleistung der Netz- und Informationssicherheit unbedingt notwendig und verhältnismäßig“ sein muss.

An vielen Stellen hat der Rat die Vorgaben zur Datensparsamkeit gestrichen, die das Parlament eingeführt hat. In Erwägungsgründen 61 und 125 „kann“ sie eine Maßnahme sein, in Artikel 23 wird sie lediglich als ein Beispiel genannt, die Rechte der Betroffenen zu schützen. Lobby-Arbeit hat wohl auch dazu geführt, dass laut Erwägungsgrund 30 personenbezogene Daten verarbeitet werden dürfen, wenn sich der Zweck anders nicht „in zumutbarer Weise“ erreichen lässt. Schwammiger lässt sich die Datensparsamkeit kaum dem Ermessen der Unternehmen anheimstellen.

Bei der Verarbeitung personenbezogener Daten zu historischen, statistischen oder wissenschaftlichen Forschungszwecken (Erwägungsgrund 125) wünscht sich der Rat weitere Register mit den Daten großer Bevölkerungsanteile (auch Verstorbener, Erwägungsgrund 23). Das sind Sammlungen, die wachsende Begehrlichkeiten auf sich ziehen werden.

Datensparsamkeit als Anforderung endlich durchsetzbar zu machen, das wollen die Minister nicht. Wir bestehen auf den Formulierungen des Parlaments!

Zweckbindung

Der Entwurf des EU-Rats will es ins Ermessen der Unternehmen legen, den Zweck einer Verarbeitung nach Belieben neu zu definieren. Statt dass Daten gelöscht werden, wenn sie ihren

Zweck erfüllt haben, will der Rat in Erwägungsgrund 40 und Artikel 6 Satz 3a (a) eine Zweckänderung erlauben, wenn der neue Zweck mit dem ursprünglichen Zweck „vereinbar“ ist.

Im Erwägungsgrund 39 haben die Minister zudem die „*Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung*“ als berechtigtes Interesse definiert. – Wenn die Grundrechte und Grundfreiheiten der betroffenen Person überwiegen, soll das zwar ausgeschlossen sein, informationelle Selbstbestimmung sieht aber anders aus. Betroffene können nicht sicher wissen, ob bei der Verarbeitung „für nicht konforme Zwecke aufgrund der berechtigten Interessen dieses [...] Verantwortlichen oder eines Dritten“ dessen Interessen überwiegen, was die Verarbeitung rechtmäßig macht (Artikel 6 Satz 4).

Bei diesem Grundpfeiler des Datenschutzes ist so viel Entgegenkommen gegenüber den Datenkraken mit uns nicht zu haben!

Profile

Als Profiling sieht der Rat erst die Nutzung personenbezogener Daten an, die verarbeitet wurden, damit eine Person bewertet oder ihr Verhalten analysiert oder vorhergesagt werden kann (Artikel 4 (12a)). Das Parlament definiert Profiling bereits über den Zweck, wodurch die Rechte der Betroffenen, beispielsweise Auskunfts- und Widerspruchsrecht, besser und früher greifen können, nicht erst dann, wenn womöglich eine Entscheidung gefallen ist. Der Rat hat das Profiling sogar aus dem Titel von Abschnitt IV und Artikel 20 gestrichen, um die automatisierte Entscheidungsfindung zum Ansatzpunkt für die Rechte der Betroffenen zu machen, nicht etwa schon das Profiling selbst. Es müssen rechtliche Folgen oder eine erhebliche Beeinträchtigung der Betroffenen vorliegen, bevor ihnen Möglichkeiten zum Widerspruch gegeben werden. Wo die Kommission noch von „auf Profiling basierenden Maßnahmen“ spricht und das Parlament vom Profiling selbst, macht der Rat die Entscheidungsfindung zur Überschrift und das Profiling zur Nebensache.

Automatisierte Entscheidungsfindung und Profiling sogar auf der Grundlage besonderer Kategorien von personenbezogenen Daten sollen erlaubt sein, wenn eine Datenschutz-Folgenabschätzung stattgefunden hat (Erwägungsgrund 58), hier wird Diskriminierung zur Abwägungsfrage.

Wir im FfF e.V. hatten eine Verschärfung der Profiling-Bestimmungen gefordert, der Rat schwächt sie noch weiter ab. So viel Entgegenkommen gegenüber den Datenkraken ist mit uns nicht zu haben!

Datenschutz durch Technik und Datenschutzfreundliche Voreinstellungen

Diese Prinzipien hatte die Kommission eingeführt und das Parlament zur Freude von Datenschützern zur Pflicht gemacht, der Rat hat sie abgeschwächt. Er will die Hersteller der Produkte, Dienste und Anwendungen lediglich „ermutigen“, Datenschutz bei der Entwicklung der Produkte, Dienste und Anwendungen zu berücksichtigen. Neben den Verantwortlichen

für die Datenverarbeitung will das Parlament die Hersteller für solche datenschutzfreundlichen Produkte verantwortlich machen (Erwägungsgrund 61). Der Rat hat diese Vorgabe des Parlaments aufgeweicht. Das Parlament weist in Artikel 23 ausdrücklich darauf hin, dass sich Datenschutz durch Technik in der Technikfolgen-Abschätzung auf das gesamte Lebenszyklus-Management der Verarbeitung bezieht. Diesen Hinweis hat der Rat ebenso gestrichen wie in Artikel 33 die Forderung des Parlaments, zu dokumentieren, welche Maßnahmen getroffen wurden (Satz 3 g).

Wir haben die Neuerungen durch Parlament und Kommission begrüßt und hätten sie uns stärker gewünscht. Eine Abschwächung als Entgegenkommen gegenüber den Datenkraken ist mit uns nicht zu haben!

Unabhängige Kontrollen und Sanktionen

Entgegen dem Parlamentsbeschluss (Artikel 32a und 35) sieht der Rat keine *Pflicht* zur Einführung von Datenschutzbeauftragten vor, sie soll nur bestehen, wenn das nationale Recht dies vorsieht. Andernfalls „*kann*“ oder „*darf*“ der Verantwortliche einen Datenschutzbeauftragten benennen. Es muss nicht mehr sichergestellt sein, dass bei einer Gruppe von Unternehmen der Datenschutzbeauftragte von jedem Standort leicht zugänglich ist. Auch zur Vertraulichkeit über die Identität der betroffenen Person sollen Datenschutzbeauftragte nicht mehr verpflichtet sein (Artikel 36 Satz 4). Die vom Parlament geforderte Bereitstellung aller benötigten Mittel, darunter Personal, will der Rat nicht. In Artikel 35 Satz 10 wurde der Rechtsanspruch der Betroffenen, den Datenschutzbeauftragten zu Rate zu ziehen, abgeschwächt zu: „*Betroffene Personen können den Datenschutzbeauftragten [...] zu Rate ziehen.*“

Im Artikel 79 haben sich nationale Interessen besonders deutlich niedergeschlagen, im vorauseilenden Gehorsam gegenüber den IT-Konzernen. Wo das Parlament Klartext redet und eine unabhängige Aufsichtsbehörde ermächtigt, Geldbußen bis zu 5 % (im EP-Beschluss) ihres (Konzern-)Umsatzes oder einer Milliarde Euro zu verhängen, da erteilt der Rat den *Mitgliedstaaten* die Befugnis, Gerichtsverfahren anzustrengen. Geldbußen dürfen die Aufsichtsbehörden selbst nur verhängen, wenn dies im nationalen Recht vorgesehen ist (Erwägungsgründe 100, 118 b, 120, 120 a und viele andere). Die Aufsichtsbehörde schrumpft zur rein nationalen Angelegenheit und ein Staat „*kann*“ (Artikel 79 Satz 3 b und 5) entscheiden, ob überhaupt Geldbußen verhängt werden sollen. Wenn ja, kann die Aufsichtsbehörde nur noch maximal 2 % des Umsatzes festlegen. Die Mitgliedstaaten setzen damit einen der größten Vorteile einer europaweiten und durchsetzbaren Verordnung außer Kraft. Wir müssen davon ausgehen, dass sich große Konzerne nun weiterhin ihren Hauptsitz danach auswählen werden, wo die geringsten Kontrollen und Sanktionen zu befürchten sind.

Statt einheitliche Kontroll- und Sanktionsstandards zu schaffen, wollen die Minister nationale Standortvorteile behalten. Diese Egoismen zu Lasten des Datenschutzes sind mit uns nicht zu haben!

Drittstaaten-Regelung

Weil Datenschutz in Europa ein verbindliches Grundrecht mit Verfassungsrang in der EU-Grundrechtecharta ist, dürfen personenbezogene Daten grundsätzlich nur innerhalb Europas verarbeitet werden. Das scheint nicht zu den Interessen von Konzernen zu passen, die immer mehr Daten benötigen für ihre Geschäfte mit Big Data oder Scoring. Es ist ganz im Sinne der IT-Monopolisten, als „Big Data“ alles zu speichern, was irgendwie verarbeitet werden kann. Regelungen aus der Parlamentsvorlage für die Übertragung von Daten in Drittstaaten (Nicht-EU-Staaten) hat der EU-Rat durchlöchert. Zu Recht sieht er vermutlich die Freihandelsabkommen TTIP und TISA dadurch

gefährdet. Insbesondere die regulatorische Zusammenarbeit wird fatale Folgen für die informationelle Selbstbestimmung und den Grundrechtsschutz in der EU haben.

Eine Aufweichung der Drittstaaten-Regelung als Entgegenkommen gegenüber den Datenkraken ist mit uns nicht zu haben!

Der Text ist eine Stellungnahme des FfF zur EU-Datenschutz-Grundverordnung, die für die DANA – Datenschutz-Nachrichten, Ausgabe 3/2015, der Deutschen Vereinigung für Datenschutz erarbeitet wurde. Autorin ist Dagmar Boedicker mit Unterstützung von Martin Degeling.

FfF e.V.

„Wir haben einen Abgrund von Landesverrat im Lande“

Kommentar zum Ermittlungsverfahren gegen netzpolitik.org

3. August 2015 – Am 30. Juli 2015 wurde bekannt, dass der Generalbundesanwalt ein Ermittlungsverfahren wegen Landesverrats gegen die Journalisten und Blogger Markus Beckedahl und André Meister sowie gegen Unbekannt eröffnet hat – aufgrund einer Strafanzeige des Präsidenten des deutschen Inlandsgeheimdienstes (Bundesamt für Verfassungsschutz). Dieses Vorgehen hatte in der Geschichte der Bundesrepublik Deutschland zuvor nur zwei Beispiele: die Spiegel-Affäre (1962) – die mit dem Rücktritt des damaligen Verteidigungsministers Franz Josef Strauß endete – und die Affäre um die Zeitschrift Cicero (2005).

Verfassungsschutzpräsident Maaßen begründet sein Vorgehen Zeitungsberichten zufolge damit, „die weitere Arbeitsfähigkeit meines Hauses im Kampf gegen Extremismus und Terrorismus sicherzustellen“. Um die Arbeitsfähigkeit des Verfassungsschutzes muss er sich in der Tat Sorgen machen – weder leistete die dem Bundesinnenministerium unterstehende Behörde einen erkennbaren Beitrag zur Verhinderung der rechtsgerichteten, terroristischen Morde des *Nationalsozialistischen Untergrunds (NSU)*, noch konnte sie bei der Spionageabwehr reüssieren, die ebenfalls zu ihren Aufgaben zählt. Die Ausspähung durch den US-Geheimdienst NSA – der dabei offenbar auch noch mit dem anderen deutschen Geheimdienst, dem Bundesnachrichtendienst (BND) zusammenarbeitet – konnte und kann sie offensichtlich nicht verhindern. Von Bundesregierung und Bundesbehörden wird nach wie vor behauptet, es gebe keine gerichtsverwertbaren Beweise für eine solche Ausspähung – angesichts der seit nun zwei Jahren beinahe wöchentlich neu an die Öffentlichkeit kommenden Indizien ist das nicht nachvollziehbar.

Gerade angesichts der offenkundigen Zurückhaltung bei der Aufklärung des NSA- und BND-Skandals ist das schnelle Handeln des Generalbundesanwalts nun besonders auffällig.

Zunehmend unklar wird inzwischen, wer die Strafanzeige und das Vorgehen der beiden Behörden – Verfassungsschutz und Generalbundesanwaltschaft – initiiert und getragen hat. Aussagen von Maaßen zufolge wurde lediglich Anzeige gegen Unbekannt erstattet, der Generalbundesanwalt bestreitet dies. Unklar auch die Rolle der beiden Ministerien, die die Fachaufsicht über die Behörden führen. Bundesjustizminister Maas distanziert sich vom Vorgehen des Generalbundesanwalts – dass aber, bei der zu erwartenden Öffentlichkeitswirkung, der zuständige Minister vom Ermittlungsverfahren nicht vorab informiert wurde, ist nur

schwer vorstellbar und war, anderen Presseberichten zufolge, auch nicht der Fall. Damit muss Maas wohl eine Mitverantwortung zugeschrieben werden. Gleiches gilt für Bundesinnenminister de Maizière, dessen Fachaufsicht der Verfassungsschutz untersteht. Inzwischen ließ selbst Bundeskanzlerin Merkel durch eine Sprecherin erklären, sie hätte Zweifel am Vorwurf des Landesverrats. Bundesjustizminister Maas hatte nach seiner Kehrtwende bei der Vorratsdatenspeicherung – die er selbst freilich immer noch bestreitet – ohnehin bereits einiges an Vertrauen in der netz- und bürgerrechtspolitischen Öffentlichkeit verspielt.

Über die Motive kann nun munter spekuliert werden:

- Ist das Ganze ein Versuchsballon, um die Reaktion der Öffentlichkeit zu testen? Gut vorstellbar. In diesem Fall könnten wir zunächst beruhigt sein – die heftige Reaktion in großen Teilen der Presse zeigt, dass solch ein Versuch, die Pressefreiheit einzuschränken, (noch) nicht hingenommen wird.
- Es kann auch der erste Schritt einer Gewöhnungsstrategie sein. So heftig die Reaktionen dieses Mal ausfielen – es ist abzusehen, dass im nächsten derartigen Fall die Empörung bereits deutlich geringer sein wird. Ebenso wie Überwachungsmaßnahmen Schritt für Schritt zum Normalzustand werden, lässt sich so auch Schritt für Schritt die Pressefreiheit – und weitere Grundrechte – abbauen.
- 2014 wurden im Bundeskanzleramt Referenten mit verhaltensökonomischem Hintergrund eingestellt, von denen angenommen wird, dass sie sogenannte *Nudging*-Techniken in die Regierungsarbeit einführen werden. Ist also die Strafanzeige ein „Stups“, um kritische Presse im eigenen Sinn zu beeinflussen?