PRESSEMITTEILUNG

28. März 2014

Unsere Daten sicherer machen - wir selbst haben es in der Hand!

Forderungen der 87. Konferenz der Datenschutzbeauftragten des Bundes und der Länder

Die bisherigen rechtlichen und politischen Reaktionen auf das massenhafte Ausspähen der Kommunikation durch Nachrichtendienste sind enttäuschend. Das zeigt exemplarisch die Diskussion um das No-Spy-Abkommen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, die am 27. und 28. März 2014 in Hamburg stattfindet, fordert deshalb alle staatlichen und gesellschaftlichen Akteure dazu auf, die Grundrechte der Bürgerinnen und Bürger durch technische und organisatorische Maßnahmen wirksam zu schützen. Die Unversehrtheit der freien und geheimen Kommunikation muss wieder hergestellt werden. Dies erfordert vor allem die Bereitstellung einer von jeder Person einfach nutzbaren Verschlüsselungsinfrastruktur. Sie gilt es insbesondere bei der Kommunikation zwischen Bürger und Verwaltung vorzuhalten. Neben der standardisierten Verschlüsselung beim Transport von Daten muss auch der Einsatz von Mechanismen der Ende-zu-Ende-Verschlüsselung angeboten werden. Außerdem sollten die Angebote zur anonymen Kommunikation sowie die Vertrauenswürdigkeit von Hard- und Software durch Einsatz von Zertifizierungsverfahren ausgebaut werden. Diese Maßnahmen erfordern nicht nur eine Sensibilisierung und Aufklärung der Nutzerinnen und Nutzer durch eine Bildungsoffensive, sondern müssen auch durch eine ausreichende Finanzierung ermöglicht werden.

Hierzu Johannes Caspar, der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit und amtierender Vorsitzender der Datenschutzkonferenz: „Wir haben es selbst in der Hand, durch die Schaffung einer sicheren IT-Infrastruktur die Hürden für eine massenhafte anlasslose Überwachung unserer Kommunikation durch die Nachrichtendienste wesentlich zu erhöhen. Gerade wenn die politische Kraft nicht ausreicht, den Schutz der Grundrechte auf internationaler Ebene wiederherzustellen, ist die Errichtung technisch organisatorischer Schutzmaßnahmen alternativlos.“

Mit einer Entschließung zur biometrischen Gesichtserkennung durch Internetdienste fordern die Datenschutzbeauftragten zudem, dass die Verarbeitung biometrischer Merkmale der Gesichter der Nutzer in sozialen Medien nur mit der ausdrücklichen und informierten Einwilligung der Betroffenen erfolgen darf. Die individuellen Gesichtsabdrücke der Nutzerinnen und Nutzer werden bei diesen Verfahren dauerhaft und reproduzierbar millionenfach gespeichert. Das Missbrauchspotential derartiger Gesichtsdatenbanken ist

immens. Das informationelle Selbstbestimmungsrecht der Betroffenen muss daher bei der Erhebung und Verarbeitung dieser unveränderbaren biometrischen Daten in jedem Fall gewahrt werden.

Die polizeiliche Öffentlichkeitsfahndung mit Hilfe sozialer Netzwerke darf künftig nur unter Beachtung strenger Vorgaben erfolgen. Diese Art der Veröffentlichung von Fahndungsdaten greift nicht zuletzt wegen der größeren Reichweite deutlich intensiver in die Grundrechte ein als die herkömmliche Öffentlichkeitsfahndung. Davon sind unter Umständen nicht nur die mutmaßlichen Täter betroffen, sondern auch Zeugen. Die Datenschutzbeauftragten fordern daher unter anderem, dass eine Speicherung der Fahndungsdaten nur auf den Servern der Polizei erfolgen darf. Entscheidend ist zudem, dass die Fahndung nicht als Aufruf zu Hetzjagden und Selbstjustiz im Internet führt. Dazu muss die Kommentierungsfunktion zwingend deaktiviert sein.

Dazu Imke Sommer, die Landesbeauftragte für Datenschutz und Informationsfreiheit der Freien Hansestadt Bremen: „Das letzte Jahr hat uns allen die Augen dafür geöffnet, in welch hohem Maße unser Grundrecht auf informationelle Selbstbestimmung von den großen Datensammlern und allen, die die von ihnen angehäuften Datenberge nutzen, verletzt wird. Wir dürfen jetzt nicht darin nachlassen, alle, die zum Schutz unserer Rechte handeln können, dazu zu bringen, dies auch tatsächlich zu tun."

Die Datenschutzkonferenz hat die langjährige Forderung zur Schaffung eines nationalen Beschäftigtendatenschutzgesetzes erneut erhoben. Gesetzgeber und Regierung sind aufgefordert, angesichts des Einsatzes mannigfaltiger digitaler Technologien am Arbeitsplatz für einen hinreichenden Datenschutz der Arbeitnehmer und Arbeitnehmerinnen zu sorgen. Die immer stärkere Vermischung von Arbeit und Privatem durch die Nutzung von Handy, Laptop und Dienstwagen mit GPS, aber auch die immer weiter um sich greifende Videoüberwachung am Arbeitsplatz müssen künftig rechtssicher geregelt werden.

Schließlich begrüßt die Datenschutzkonferenz den Entwurf einer Europäischen Datenschutzgrundverordnung, fordert aber in der „Entschließung zur künftigen Struktur der Aufsichtsbehörden in Europa" Nachbesserungen. Hierbei bekräftigt sie insbesondere den Grundsatz, dass jede Aufsichtsbehörde zur Kontrolle von datenschutzrechtlichen Verstößen befugt ist, wenn Bürgerinnen und Bürger des jeweiligen Mitgliedstaats betroffen sind. Bei grenzüberschreitender Datenverarbeitung soll die Aufsichtsbehörde am Ort der Hauptniederlassung nur federführend tätig werden und eng mit den anderen Aufsichtsbehörden kooperieren. In Streitfällen sollte der Europäische Datenschutzausschuss verbindlich entscheiden.

Andrea Voßhoff, die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, unterstreicht: „Eine effiziente Datenschutzaufsicht nahe an den Bürgerinnen und Bürgern muss auch in Zukunft gesichert sein."

Pressekontakt/ Rückfragen:
Arne Gerhards
Tel.: 040/42854-4153
E-Mail: presse@datenschutz.hamburg.de

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder ist ein freiwilliger Zusammenschluss der Datenschutzbeauftragten. Mitglieder sind die Datenschutzbeauftragten des Bundes und der Länder. Sie tagen zweimal jährlich unter turnusmäßig wechselndem Vorsitz. Die Konferenz verabschiedet Entschließungen, in denen die Datenschützer Stellung zu aktuellen, datenschutzrelevanten Fragen aus Technik, Wirtschaft und Recht nehmen. Sie wird durch fachlich spezialisierte Arbeitskreise vorbereitet.