Ulla Jelpke
Mitglied des Deutschen Bundestages

Ulla Jelpke, MdB · Platz der Republik 1 · 11011 Berlin

Berlin
Ulla Jelpke, MdB
Platz der Republik 1
11011 Berlin
Büro: Unter den Linden 50
Telefon: +49 30 227- 71251
Fax: +49 30 227-76751
Email: ulla.jelpke@bundestag.de

Wahlkreis
Ulla Jelpke, MdB
Schwanenstr. 30
44135 Dortmund
Telefon: +49 231 8602747
Fax: +49 231 8602746
Email: ulla.jelpke@wk.bundestag.de

Berlin, 07.09.2017

Argumentationspapier: Sicherheitsgesetze vs. Datenschutz

Sogenannte Sicherheitsgesetze geben vor, Terroristen zu bekämpfen – obwohl sie häufig nichts weiter als gesetzliche Schnellschüsse sind. Was allerdings feststeht, ist: Häufig gehen sie auf Kosten von Datenschutz und Grundrecht auf informationelle Selbstbestimmung.

Beispiel polizeilicher Datenverbund:
Im neuen BKA-Gesetz wurde im Frühjahr 2017 festgeschrieben, die bisherige Datei-Struktur abzuschaffen. Bisher hat jede Polizeidatei einen ganz bestimmten Verwendungszweck, von dem abhängt, ob eine Person darin gespeichert werden darf. Wenn wegen Terrorverdachts ermittelt wird, dürfen die Erkenntnisse aus der Telefonüberwachung nicht einfach zur Aufklärung eines Bagatelldelikts verwendet werden.

In Zukunft soll es einen großen „Datenpool“ geben, in dem alle Daten gespeichert werden – damit entfällt jegliche Zweckbindung. Die Polizei gleicht dann z. B., an welchen Orten eine bestimmte Person sich häufiger aufhält. Dies wird dann kombiniert mit Autos, die an diesem Ort parken, und von denen wiederum werden die Halterdaten abgeglichen. Es gibt da kaum eine Begrenzung, und das Ergebnis muss mit der eigentlich verdächtigen Person nichts zu tun haben. Aber jeder „Treffer“ verlängert die Speicherfrist. Die Vielzahl von Verknüpfungsmöglichkeiten ermöglicht die verfassungswidrige Erstellung von Persönlichkeitsprofilen.

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) Andrea Voßhoff äußerte in einer Bundestagsanhörung „gravierende – verfassungsrechtliche – Bedenken“ und warnte, der Datenpool führe „zu unverhältnismäßig weitreichenden Speicherungen.“

Die Alternative dazu wäre, das bestehende Dateisystem anzupassen und zu modernisieren. Der Zweck einer Datenerhebung muss stets genau definiert sein, genauso wie die weitere Verwendung und der Personenkreis, über den Daten erhoben werden sollen. Speicherfristen dürfen nicht ins Unendliche verlängert werden.

Beispiel Staatstrojaner:
Das BKA-Gesetz ermöglicht die verdeckte Infiltration informationstechnischer Systeme, sprich: Das BKA darf Trojaner auf private Computer spielen, um die Daten auszulesen.

Unter Datenschutzgesichtspunkten sind dabei drei Punkte extrem heikel:
Erstens gibt es keinen ausreichenden Schutz für sogenannte Berufsgeheimnisträger. Das heißt, dass zum Beispiel Ärzte, Psychotherapeuten und Journalisten damit rechnen müssen, dass ihre Computer ausgespäht werden. Das untergräbt das Vertrauen von Patienten bzw. Klienten und auch die Pressefreiheit, weil Whistleblower bzw. Informanten sich nicht mehr darauf verlassen können, anonym zu bleiben.

Zweitens werden die technischen Anforderungen an den Trojaner in keiner Weise definiert. Es können somit auch Trojaner privater Anbieter genutzt werden, deren Funktionsweise nicht klar geregelt ist. Das ist eine eklatante Gefährdung: Es muss sichergestellt sein, dass der Trojaner nicht etwa die vorhandenen Dateisysteme verändert oder gar deren Inhalte.

Drittens sollen die Trojaner mittels Sicherheitslücken in der Nutzer-Software heimlich aufgespielt werden. Damit erhalten die Sicherheitsbehörden fatale Fehlanreize: Wenn sie eine Sicherheitslücke erkennen, werden sie versucht sein, diese nicht zu melden und zu beheben, sondern sie geheim zu halten, um sie selbst auszunutzen. Das gefährdet die Sicherheitsinteressen aller Computernutzer.

Beispiel Videoüberwachung:
Nach dem Anschlag auf den Berliner Weihnachtsmarkt wurde ein so genanntes „Videoüberwachungsverbesserungsgesetz“ auf den Weg gebracht, das privaten Betreibern den Betreib von Videokameras erleichtert und die Einsprache von Datenschutzbehörden einschränkt. Als Ziel nannte die Bundesregierung in der Gesetzesbegründung ausdrücklich, Anschläge wie in Berlin zu „verhindern“. Das ist pure Augenwischerei: Bislang hat noch keine Studie nachgewiesen, dass Videokameras präventiv gegen Kriminalität wirken. Allenfalls verlagert sich die Kriminalität an andere Orte. Gerade die Tat auf dem Weihnachtsmarkt hätte nicht durch mehr Kameras verhindert werden können. Die meisten Gewalttaten werden ohnehin spontan, meist unter Alkoholeinfluss, begangen – auch da hilft eine Videokamera nichts.

Die grundrechtsschonende Alternative dazu lautet, Kriminalitätsschwerpunkte mit Personal zu überwachen. Das ist dann auch wesentlich mobiler, um auf Verlagerungen zu reagieren.

Beispiel Gesichtserkennungs-Software:
Am Berliner Bahnhof Südkreuz testet die Bundespolizei derzeit den Einsatz von Videokameras mit einer Gesichtserkennungs-Software. Dies verschärft das Problem noch – vor allem, weil Polizei und Geheimdienste seit Frühjahr 2017 ohne jeden Anlass auf die Passfotos der Meldebehörden zugreifen dürfen. Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder verurteilte den Einsatz dieser Technik und wies darauf hin, dass dies „die Freiheit, sich in der Öffentlichkeit anonym zu bewegen, gänzlich zerstören“ könne.

Jede Überwachungstechnologie kann heutzutage mit anderen Technologien kombiniert werden. Der neue polizeiliche Datenverbund ermöglicht die Anlage von

Persönlichkeitsprofilen, die neue Videotechnik die Anlage von Bewegungsprofilen. Das wäre faktisch das Ende von Datenschutz und informationeller Selbstbestimmung.

Wir dürfen unsere Freiheiten nicht der Illusion einer falschen Sicherheit opfern!