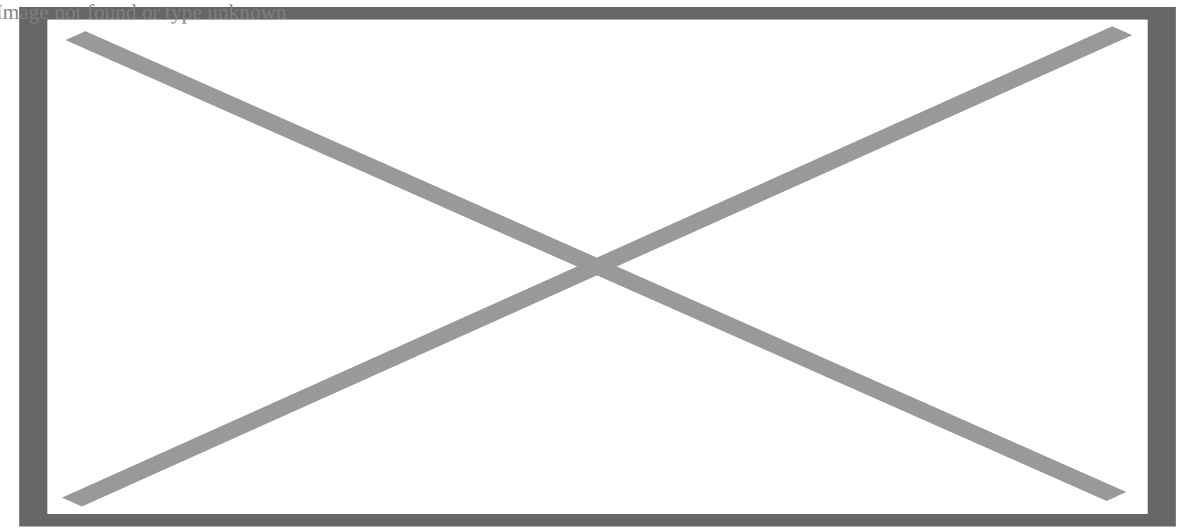
Humanistische Union

"Handys sind wie Elektronische Fußfesseln"

Burckhard Nedden referierte in Marburg über Datenschutz. Bericht von einer Informationsveranstaltung am 28. Oktober in Marburg

Image not found or type unknown



"Handys sind wie Elektronische Fußfesseln." Seinen überspitzt erscheinenden Vergleich begründete Burckhard Nedden am Dienstag (28. Oktober) im Hörsaalgebäude der Philipps-Universität. Eingeladen zu seinem Vortrag unter dem Titel "Ich habe doch nichts zu verbergen, oder?" hatten den ehemaligen niedersächsischen Landesbeauftragten für Datenschutz die Humanistische Union (HU) und das Zentrum für Konfliktforschung (ZfK) der Philipps-Universität.

Anhand alltäglicher Verrichtungen skizzierte Nedden die vielfältigen Vorgänge, bei denen Daten über die Bürgerinnen und Bürger erhoben werden. Wer beispielsweise telefoniert, der hinterlässt damit eine Datenspur, die die Ermittlungsbehörden mindestens sechs Monate lang nachvollziehen können. Denn durch die gesetzlich vorgeschriebene Vorratsdatenspeicherung ist jeder Telefon-Anbieter verpflichtet, alle Verbindungsdaten mindestens sechs Monate lang aufzuheben.

Zwar hat das Bundesverfassungsgericht (BVerfG) mit einer Einstweiligen Anordnung den Zugriff auf diese Daten stark eingeschränkt, doch steht das endgültige Urteil dazu noch aus. Aufgehoben werden müssen die Daten so lange jedenfalls. "Wir Datenschützer haben ernste Bedenken bei jeder großen Datensammlung, die irgendwo besteht", erklärte Nedden. Denn nach allgemeiner Erfahrung sei es nur eine Frage der Zeit, bis sie gehackt wird oder Informationen daraus anderswo auftauchen.

Neben dem Telefonieren im Festnetz, wo nur die Rufnummer des Anrufers, die Nummer des Angerufenen und die Zeit und Dauer des Gesprächs aufgezeichnet werden, komme beim Mobiltelefon auch noch der Standort hinzu. Da sich jeder Handy-Nutzer mit seinem eingeschalteten Gerät von einer Sende-Funkzelle zur nächsten bewege und dort automatisch angemeldet oder weitergereicht werde, entstehe so ein engmaschiges Bewegungsprofil der Nutzer von Mobiltelefonen. Schließlich umfasse die Vorratsdatenspeicherung auch alle Verbindungsdaten im Internet sowie Informationen über verschickte e-Mails. Hier werden die E-Mail-Adressen und die sogenannten IP-Adressen des Versenders und des Empfängers sowie die Zeit der

Verschickung aufgehoben. Für die Provider bringe die gesetzliche Verpflichtung zur Speicherung dieser Daten gewaltige technische und damit letztlich auch wirtschaftliche Probleme mit sich. Schließlich müssten diese Daten nicht nur sicher verwahrt und vor unberechtigtem Zugriff geschützt werden, sondern im Bedarfsfall auch umgehend verfügbar sein.

Auf eine Frage aus dem Publikum, wie sicher solche Daten bei kommerziellen Providern sind, äußerte Nedden nochmals die Furcht vor einem Daten-Diebstahl. Allerdings glaube er nicht, dass Provider selbst nachlässig mit diesen Daten umgingen, weil sie damit ihr Geschäft massiv gefährdeten. Schließlich sei es ihr wesentliches Geschäftsinteresse, einen sicheren Informationsaustausch zu gewährleisten.

Allerdings warnte Nedden vor der schier grenzenlosen Daten-Sammelwut der Privatwirtschaft. Preisausschreiben oder auch die meisten Kundenkarten dienten nur dazu, Informationen über mögliche Konsumenten zu gewinnen. Diese Informationen werden häufig auch an andere Interessenten weiterverkauft. "Für einen Weinhandel ist es von Interesse, dass Sie gerne Wein trinken", erläuterte der Datenschützer. Für eine solche Firma sei es viel erfolgversprechender, ihre Werbung nur an Leute zu richten, die sie schon als mögliche Käufer einschätzt. Eine solche Information werde deswegen durchaus mit bis zu fünf Euro bezahlt.

Problematisch sei vor Allem die Anhäufung solcher Kenntnisse. Sie ermögliche es der Wirtschaft, ein umfassendes Bild über einen Menschen und sein Kaufverhalten zu gewinnen. In diesem Zusammenhang nannte Nedden die Suchmaschine Google, die detaillierte Profile aller Such-Anfragen speichere. Man selbst könne Daten seiner vorherigen Anfragen einsehen und sogar löschen, doch vernichte man damit nicht zugleich auch die Speicherung bei Google.

Bei einem Einkauf hinterlässt der Kunde vor allem dann Datenspuren, wenn er mit Scheck-, Kredit- oder Kundenkarte bezahlt. Problematisch werde das in Verbindung mit dem Einsatz sogenannter RFID-Chips. Dabei handelt es sich um winzige Chips, die an die Ware geklebt sind. Mit Funksignalen übermitteln sie die auf ihnen abgespeicherten Informationen berührungslos an entsprechende Lesegeräte. War der Strichcode auf Waren früher nur einzelnen Warengruppen wie Tomatensuppe einer bestimmten Marke zugeordnet, so erhält jeder einzelne RFID-Chip eine eigene Nummer. Bezahle man Schuhe mit einer Kredit- oder Kundenkarte, so könne man mit Hilfe der RFID-Technik hinterher ein Bewegungsprofil des betreffenden Käufers erstellen.

Hinzu kommt die Video-Überwachung. Nicht nur auf öffentlichen Plätzen oder in U-Bahnstationen wird flächendeckend gefilmt, sondern häufig auch in Geschäften, Diskotheken oder Hotels. Mitunter werden derartige Bilder auch durch Webcams übertragen. Im Internet kann dann jeder sehen, wer sich gerade vor der Kamera vorbeibewegt. Nicht alle Bilder aus Überwachungskameras werden auch gespeichert. Doch wo das geschieht, da bestehe auch die Gefahr eines Missbrauchs, meinte Nedden. Ohnehin gaukelten die Kameras nur eine zweifelhafte Sicherheit vor. In Hannover hätten Fahrgäste schon tatenlos bei Vorkommnissen zugeschaut, weil sie wegen der Überwachungskameras eine umgehende Intervention der Zuständigen erwartet hätten. Dieses Eingreifen sei aber nicht erfolgt. In Großbritannien sei die mehrere Millionen starke Zahl der Überwachungskameras inzwischen schon so groß, dass nicht mehr genug Personal vorhanden sei, alle Bilder auszuwerten. Deswegen gebe es dort mittlerweile auch Privatpersonen, die Bilder der Überwachungskameras von zu Hause aus beobachten und besondere Vorkommnisse melden. Für jeden "Erfolg" bekämen sie Punkte. Dieses Vorgehen brandmarkte Nedden als Installierung des "Elektronischen Blockwarts".

Ein weiteres Problem sei das sogenannte "Scoring", erklärte Nedden. Bei Einkäufen im Internet, aber auch beim Eröffnen eines Bankkontos oder der Beantragung eines Kredits würden häufig Anfragen an sogenannte "Scoring-Agenturen" gestellt. Sie bewerten den jeweiligen Kunden anhand von durchaus zweifelhaften Daten wie beispielsweise der Zuordnung seiner Adresse zu einem eher gutbürgerlichen oder eher randständigen Wohngebiet. In aller Regel erfahre der Kunde von dieser Prüfung nichts. Zudem fehle jegliche Transparenz, welche Kriterien für die Zusage oder Ablehnung eines Kredits, eines Geschäfts oder für die Verweigerung der Bezahlung auf Rechnung ausschlaggebend waren. Agenturen wie die SchuFa

rühmten sich selbst mit der gigantischen Zahl von 440 Millionen Datensätzen über 65 Millionen Bürger. Die Firma "SchoWa" Schober beispielsweise werbe damit, dass sie über jedes Gebäude in Deutschland Aussagen treffen könne.

Ein weiteres Problem sieht Nedden in der sogenannten "Steuer-ID", die jedem Bundesbürger inzwischen zugeordnet wird. Eine Teilnehmerin berichtete, dass auch ihre Krankenkasse von ihr diese Nummer angefordert hatte und damit gedroht habe, dass sie ihre Beiträge sonst nicht steuerlich absetzen könne. Nedden nannte diese Nummer ein "Persönlichkeitskennzeichen", wie es bisher aus verfassungsrechtlichen Gründen abgelehnt wurde. Doch entfalte der Staat mit steigenden technischen Möglichkeiten einer Speicherung auch eine immer größere Sammelwut.

Ohnehin betrachtet der Datenschützer die Begründung staatlicher Datensammlungen mit der Gefahr terroristischer Anschläge als nicht stichhaltig. Viele der damit begründeten Maßnahmen könnten intelligente Täter relativ leicht umgehen. Aber auch der Bürger sollte sich nach Neddens Auffassung vor allzu freigebiger Übermittlung persönlicher Daten schützen. Man sollte in der Regel nicht an Preisausschreiben oder Umfragen teilnehmen, riet der Datenschützer. Wenn man überhaupt Kundenkarten akzeptieren wolle, sollte man sich vor einem Antrag die entsprechenden Geschäftsbedingungen genau durchlesen. Auch den Vorschlag aus dem Publikum, Handys untereinander auszutauschen, hielt Nedden für sinnvoll. Schließlich gebe es keine Bestimmung, die den Käufer zur Eigen-Nutzung des Mobiltelefons verpflichte. Besonders vorsichtig solle man mit sogenannten "Sozialen Netzwerken" im Internet wie Facebook oder studivz umgehen. Hier fänden Arbeitgeber häufig kompromittierende Fotos von Bewerbern, die sie dann als Grund gegen eine Anstellung des Betreffenden bewerteten. "Ins Internet sollte man nur Informationen einstellen, die auch der schlimmste Feind wissen darf", riet Nedden. Nur so sei man hinterher vor unangenehmen Überraschungen gefeit.

Eine kritische Bewertung der Situation stand am Ende der gut zweistündigen Veranstaltung. Einige Anwesende äußerten starke Zweifel, dass der Datenschutz überhaupt noch ernst genommen werde. Sie vermuteten, dass Firmen und Behörden die Gesetze nicht immer respektieren. Solche Vorkommnisse betrachtete Nedden aufgrund seiner beruflichen Erfahrung aber als Einzelfälle. Notwendig sei allerdings, dass die Bürgerinnen und Bürger den Schutz ihrer eigenen Daten ernst nehmen und auch einen entsprechenden Druck auf die Politik entfalten.

Sie können den Vortrag von Burckhard Nedden hier nachhören:

Video DirektTeil1

Video DirektTeil2

Video DirektTeil3
