Humanistische Union

Datenschutz für die "nächste Gesellschaft"

Die Neuregulierung im Spannungsverhältnis von deutscher und europäischer Rechtssetzung

aus : Vorgänge Nr. 200 (Heft 4/2012), S.67-73

Fieberhaft wird von allen Seiten eine Neubestimmung und Anpassung des Datenschutzes gefordert. Die Europäische Kommission hat ein Konsultationsverfahren zur zentralen Datenschutzrichtlinie eingeleitet und setzt in diesen Prozess hohe Erwartungen. Doch beginnen wir mit einem Blick in die jüngere Geschichte: Es ist der 2.März 2010, der Tag, an dem die Entscheidung über die bis dato größte Verfassungsbeschwerde terminiert ist. Schätzungsweise wohl rund 20.000 Kläger schauen wie gebannt auf alles, was mit dem Hashtag #VDS über Twitter gepostet wird, gleichzeitig überträgt Phönix live aus dem Gerichtssaal. Der wiederum ist bis auf den letzten Platz gefüllt. Selten hat eine Urteilsverkündung des obersten deutschen Gerichts solch eine Aufmerksamkeit erfahren.

Die Quadratur des Kreises: Europäischer Grundrechtsschutz am Beispiel der Vorratsdatenspeicherung

Das Bundesverfassungsgericht steht vor dem, was viele für eine ausgesprochen schwierige Aufgabe halten. Es muss sich des Eindruckes erwehren, dass im Rahmen des europäischen Integrationsprozesses die Grundrechte auf dem Altar der europäischen Vereinigung geopfert wurden. 1983 schrieb das Bundesverfassungsgericht noch, dass mit dem Grundrecht auf informationelle Selbstbestimmung „die Sammlung nicht anonymisierter Daten auf Vorrat zu unbestimmten oder noch nicht bestimmbaren Zwecken nicht zu vereinbaren" sei (BVerfG Volkszählung, Rn. 181). Dies steht - zumindest scheinbar — im Widerspruch zur Richtlinie 2006/24/EG. Dort wird in Artikel 3 eine Einführung einer „Vorratsdatenspeicherungspflicht" von den Mitgliedsstaaten verlangt, bei der zumindest Zweifel berechtigt erscheinen, ob sie den Anforderungen des Volkszählungsurteils genügen kann. Zur Umsetzung dieser Vorratsdatenspeicherungspflicht ist Deutschland völkerrechtlich verpflichtet. Eine Nichtumsetzung berechtigt die Kommission, ein Vertragsverletzungsverfahren einzuleiten und anschließend empfindliche Strafen zuverhängen. Demgegenüber ist das Bundesverfassungsgericht selbst jedoch ausschließlich der Verfassung, also dem deutschen Grundgesetz, verpflichtet.

Hierin liegt ein Kern des Problems, und der geht über das Risiko von Vertragsstrafen hinaus: Was ist, wenn Deutschland sich nach außen zu etwas völkerrechtlich verpflichtet hat — in diesem Fall mit der Unterzeichnung der zahlreichen europäischen Integrationsverträge von den Römischen Verträgen bis zum Lissabonvertrag — was es innerstaatlich gar nicht umsetzen darf? Die Frage ist für die Europäische Union existentiell, denn wie kann, wie soll ein europäischer Einigungsprozess funktionieren, wenn man sich nicht auf die Zusagen, die die Mitgliedsstaaten im Rahmen ihrer Verträge gemacht haben, verlassen kann?

Diese Frage hat das Bundesverfassungsgericht bereits vorher in mehreren Entscheidungen zu beantworten gehabt, um schließlich nach anfänglichem Zögern eine Formel zu entwickeln, die alle Juristen auswendig lernen müssen: „Solange die Europäische Gemeinschaft [...] einen wirksamen Schutz der Grundrechte gegenüber der Hoheitsgewalt der Gemeinschaften generell gewährleistet, der dem vom Grundgesetz als unabdingbar gebotenen Grundrechtsschutz im Wesentlichen gleich zu achten ist, [...] wird das BVerfG seine Gerichtsbarkeit [...] nicht mehr ausüben und dieses (das Gemeinschaftsrecht, der Ver£) Recht mithin nicht

mehr am Maßstab der Grundrechte überprüfen” (sog. Solange-II Entscheidung).

Dem Gedanken nach hat diese Entscheidung dann nach der Wiedervereinigung Ein-gang in den novellierten Artikel 23 des Grundgesetzes gefunden — allerdings ohne das wichtige Wörtchen „unabdingbar”. Angewendet auf die zugrunde liegende Situation könnte man hier zumindest zweierlei Fragen aufwerfen: Meint das Bundesverfassungsgericht tatsächlich, dass der verfassungsgebende Gesetzgeber (also Bundestag und Bundesrat in Zweidrittelmehrheit) der Europäischen Gemeinschaft gestatten wollte, bei Bedarf alle Grundrechte bis auf ihren so genannten Wesenskern zu reduzieren? Es ist wohl unwahrscheinlich, dass alle zustimmenden Abgeordneten und Landesregierungen im Bewusstsein dieser Interpretation der Grundgesetzänderung zugestimmt haben. Das kann also nicht gemeint sein.

Oder wollte das Gericht damit sagen, dass im Rahmen des europäischen Integrationsprozesses ein insgesamt hoher Grundrechtsschutz erhalten bleiben muss, die konkrete Ausprägung im Einzelnen aber nicht unbedingt mehr dem Grundrechtsverständnis der Verfassung entsprechen muss. Letzteres wäre ein guter Weg, der sich mit dem Bild der Quadratur des Kreises — in seinem mathematischen Sinne — illustrieren ließe: Für jedes nationale Grundrechtssystem steht ein Quadrat, das, um die Unterschiede in den Ausprägungen zu verdeutlichen, eine unterschiedliche Schräglage einnimmt. Wenn wir diese Quadrate übereinander legen, wird ein Kreis erkennbar: der gemeinsame Grundrechtsbestand; die Kanten werden geschliffen. Aber das muss man wohl in Kauf nehmen, wenn man sich auf den Weg eines Einigungsprozesses begibt. Dafür hat jedes Quadrat ein kleines Kreissegment gewonnen. Die Fläche des Kreises bleibt dieselbe wie die des Ursprungsquadrates: ein gleichwertiger Grundrechtsschutz ist gewährleistet. Der Weg ist auch deswegen gut, weil er die Bundesregierung im Rahmen ihrer Mitgestaltungsmöglichkeiten im Europäischen Rat deutlich dazu anhalten würde, peinlichst eine Erosion des Grundrechtsschutzes zu vermeiden. Es bestünde ein vernünftiger Anreiz,das Auseinanderfallen verfassungsrechtlicher und europarechtlicher Anforderungen auszuschließen.

Aber dennoch gibt es selbst bei dieser Interpretation ein Problem: Auf beiden Ebenen, sowohl national wie auch europäisch, sind es nämlich die Regierungen, die das Heft in der Hand halten; oder mit den Worten des Bundesverfassungsgerichts: die Basis der demokratischen Legitimation. Was ist, wenn sich die Regierungen für jeden Grundrechtseingriff den Weg des geringeren Widerstandes aussuchen? Passt die Maßnahme nicht auf nationaler Ebene, wird sie durch das europäische System geschoben, und umgekehrt. Dann kommt insgesamt erkennbar ein reduzierter Grundrechtsschutz heraus.

In der Tat gibt es bei der Vorratsdatenspeicherung Anhaltspunkte dafür, dass ein solch — man möchte fast sagen — perfides Forumshopping stattgefunden hat. Dafür spricht die geradezu winkeladvokatische Gesamtkonstruktion der Richtlinie. Deutlich wird dies an der zweifelhafte Kompetenzgrundlage, die trotz ihres klaren Schwerpunkts in der Strafverfolgung, eine Regelung zur Förderung des gemeinsamen Marktes darstellen soll, wie der EuGH mit überraschend sparsamer Begründung bestätigt hat. Vor dem Hintergrund dieses Vorgehens muss man eine Aushöhlung des Grundrechtsschutzes befürchten, die mit dem deutschen Grundgesetz nicht vereinbar ist. Nun, das Bundesverfassungsgericht hat sich diesen Überlegungen — wie bekannt sein dürfte — nicht angeschlossen.

Bestimmungsschwierigkeiten bei der besonders hohen IT-Sicherheit und der Personenbeziehbarkeit der Daten

Man kann sich des Eindrucks nicht ganz erwehren: Ein bisschen sieht es aus wie bei Queen „Mum”, als schließlich der Präsident des Bundesverfassungsgerichts, Hans-Jürgen Papier, vor sein „Volk” tritt. Es hofft, dass er — quasi als guter König — in der Lage ist, die wildgewordene Regierung wieder zur Raison zu bringen.

Zunächst scheint sich diese Hoffnung auch zu erfüllen, denn das Gericht tenoriert: „Die § 11 3a und 11 3b

des Telekommunikationsgesetzes [...] verstoßen gegen Artikel 10 Absatz 1 des Grundgesetzes und sind nichtig.” Die Vorratsdatenspeicherung ist gekippt. Nur die Würde des hohen Gerichtes verbietet es einem Großteil der anwesenden Öffentlichkeit, in Jubel auszubrechen oder wenigstens zu klatschen, als Papier diesen Satz verliest. Jubel wäre allerdings auch verfehlt gewesen. Denn aus der dann folgenden Begründung wird klar: Es gibt kein allgemeines, aus dem Grundgesetz abgeleitetes Prinzip, dass eine Speicherung auf Vorrat in der Form der Vorratsdatenspeicherung untersagt. Wir haben das Volkszählungsurteil wohl falsch verstanden: Das, von dem viele dachten, dass es eine klare und gute Begrenzung des Gesetzgebers sei, ist ihm doch gestattet. Der Staat darf Daten auf Vorrat speichern (lassen). Allerdings darf er das nur unter Einhaltung strenger IT-Sicherheitsvorgaben, und genau das hat der Gesetzgeber nicht hinreichend beachtet.

Damit hat sich das Gericht zweifelsohne auf einen wichtigen Aspekt konzentriert. Die der IT inhärente Unsicherheit, die mit ihr verbundenen (Rest-)risiken, machen sie insbesondere mit zunehmendem Einsatz in kritischen Bereichen zu einer Risikotechnologie. Das bedeutet, dass vor dem Einsatz Risikoabschätzungen durchgeführt werden müssen, die auch zu dem Ergebnis führen können, dass vom Einsatz der Technik abzusehen ist. Vor dem Hintergrund der „besonders hohen Anforderungen”, die das Gericht an die IT-Sicherheit bei der Vorratsdatenspeicherung gestellt hat, ist es durchaus zweifelhaft, ob es überhaupt möglich ist, die Vorratsdatenspeicherung technisch so zu gestalten, dass sie verfassungskonform umgesetzt werden kann. Dies kann und soll hier aber nicht im Detail erörtert werden.

Bei aller Wichtigkeit der IT- Sicherheit, den klassischen Datenschutz hat das Gericht nicht gestärkt. Mehr noch, schaut man sich die Abstimmung innerhalb des Bundesverfassungsgerichts selbst und die Minderheitenvoten an, so wird man feststellen, dass die Vorratsdatenspeicherung nur ganz knapp gekippt worden ist. Mit vier gegen vier Stimmen fiel die Entscheidung zugunsten der Nichtigkeit. Knapper geht es nicht. Nur weil die Nichtigkeit die grundgesetzliche Regelfolge der Verfassungswidrigkeit eines Gesetzes darstellt, reichte das Unentschieden aus.

Nun lässt die Nachbesetzung des Bundesverfassungsgerichts mit der Berliner Professorin, Susanne Baer, hoffen. Ihr Beitrag auf dem Netzpolitischen Kongress der Grünen Bundestagsfraktion Mitte November 2010 zeugte von einer angenehm aufgeklärten Unaufgeregtheit in Hinblick auf netzpolitische Fragestellungen. Wie auch insgesamt die Entscheidungen des Bundesverfassungsgerichts oft erschreckende Zeugnisse netzpolitischer Inkompetenz des Gesetzgebers darstellen. Zwar ist Baer netzpolitisch bisher nur insoweit konkret geworden, als sie sich wohl ein Grundrecht auf digitale Teilhabe vor-stellen kann. Ihre Einschätzungen zur Entwicklung des Datenschutzes blieben (zumindest im oben genannten Beitrag) im Dunklen. Einen weiteren Hinweis gab sie jedoch, denn sie stellte am Rande fest, dass die Dichotomie von „privat” und „öffentlich” problematisch sei. „Stating the obvious” mag man dem entgegen rufen. Schließlich zeigt sich doch im Netz tagtäglich, wie schwer die Grenzen zwischen diesen beiden Kategorien zu ziehen sind. Doch die Implikationen — gerade für den Datenschutz — sind immens, obschon sie im Datenschutzrecht schon stärker berücksichtigt werden, als es ihm oft nachgesagt wird. Dennoch: alte Formeln wie die bekannte Forderung, die der deutschen Version der Hackerethik entstammt: „Private Daten schützen — öffentliche Daten nützen!” sind nicht mehr so einfach anzuwenden.

Eine Problematik, die sich leider auch bei „Open Government Data”, der systematische Veröffentlichung von Datenbeständen der Verwaltungen, stellen wird. Denn nicht nur die Abgrenzung zwischen Privatem und Öffentlichem wird feinsinniger; auch die Bestimmung dessen, was eigentlich personenbezogen ist und was nicht, ist oft kaum mehr zu treffen. Der Gesetzgeber hat im Bundesdatenschutzgesetz die Anwendbarkeit der Datenschutzregeln eben nicht nur für solche Daten vorgeschrieben, die offenkundig personenbezogen sind. Richtigerweise hat er das Datenschutzrecht auch auf solche Daten erstreckt, bei denen die bloße Möglichkeit besteht, den Personenbezug herzustellen (Personenbeziehbarkeit). Nur so können die Regelungen auch Fälle abdecken, in denen das Risiko der Zusammenführung besteht. Die Möglichkeiten effektiver Zusammenführung, der Verkettbarkeit oder De-Anonymisierung sind aber mit der zunehmenden Semantisierung (gemeint ist hier die Anreicherung mit durch den Computer interpretierba-ren Bedeutungen), den durch Moore's law stetig steigenden Rechenkapazitäten und der immensen Zunahme verfügbaren Datenmaterials ins Unüberschaubare angestiegen.

Längst taugen die überkommenen Verfahren des ehrwürdigen Statistischen Bundesamtes zur Absicherung der Anonymität der Statistiken nicht mehr. Ratlos scheint man dort vor der Aufgabe zu stehen, wie in Zukunft Daten anonymisiert veröffentlicht wer-den sollen. Bekannt ist diese Tatsache freilich schon lange. Es ist allerdings das Verdienst des US-amerikanischen Rechtsprofessors Paul Ohm, dass diese Erkenntnis auch auf der anderen Seite des Atlantiks zitierfähig geworden ist. Zu Recht hat er unlängst vor allem auch für seine Arbeit zu den Möglichkeiten der De-Anonymisierung den Dieter-Meurer Preis für Rechtsinformatik erhalten.

Kontextuelle Integrität auf dem Weg zur „nächsten Gesellschaft"

Doch was sind denn nun die Kriterien, mit denen wir zukünftig beurteilen können, ob eine staatliche Maßnahme oder eine private Datensammlung und -verarbeitung problematisch ist? Einen viel beachteten Ansatz stellt der von Helen Nissenbaum dar, die die Bedeutung der „kontextuellen Integrität" hervorhebt. Stark vereinfacht: Die Verwendung von Daten muss in ihrem Kontext verbleiben. Werden sie aus dem Kontext gerissen, sind sie potentiell gefährlich. Zurückführen kann man diese Überlegung auf Niklas Luhmann, der im Rahmen der Systemtheorie von der Notwendigkeit der funktionalen Differenzierung in einer modernen Gesellschaft sprach. Der Mensch verhält sich in unterschiedlichen Kontexten oder seinen unterschiedlichen Funktionen eben ... unterschiedlich. Er bewegt sich in Systemen mit jeweils unterschiedlichen Regeln.

Die neuere Forschung zur Datenschutztechnologie hat, diesem Gedanken folgend, Systeme modernen Identitätsmanagements entwickelt. Sie sollen es dem Individuum erleichtern, diese kontextspezifischen „Teilidentitäten" (oder Personae) seiner selbst zu managen. Zu Ende gedacht müssten wir uns also eine Vielzahl von „*Personae* mit beschränkter Haftung" zulegen, wie es eine internationale Unternehmensberatung vorschlägt.

Weniger einen soziologischen, sondern eher einen rechtsempirischen Zugang wählt demgegenüber Dan Solove. In seiner „Taxonomy of Privacy" entwickelt er aus zumeist kasuistischen Analysen, orientiert an Fällen des amerikanischen Supreme Courts, insgesamt sechzehn Angriffsdimensionen auf die Privatheit, die er grob vier Oberkategorien zuordnet. Er zeigt damit die Vielfalt dessen, was wir unter dem Begriff von Privatheit als schützenswert zusammenfassen. Er leistet aber auch gleichzeitig einen wichtigen Beitrag zu dessen Systematisierung. Nur wenn wir unterscheiden zwischen beispielsweise dem Problem der „Appropriation", also der Aneignung von Informationen anderer zur eigenen Verwertung, und dem der Exklusion, der Verweigerung, dem Betroffenen Auskunft über die von ihm gespeicherten Daten zu geben (und dem daraus folgenden Gefühl der Verunsicherung), dann können wir auch die Risiken einzelner Sammlungen und Verarbeitungen bestimmen.

Beiden vorgenannten Ansätzen ist jedoch gemein, dass sie die Privatheit ins Zentrum der Überlegungen und des Schutzes stellen. Das Konzept des „Datenschutzes" in der auch vom Verfassungsgericht vertretenen Form ist – bei aller Kritik am Begriff selbst – ein weitergehendes. Die Kläger gegen die Vorratsdatenspeicherung und gegen ELENA haben längst erkannt, dass wir keine Behörden brauchen, um uns vor Paparazzieingriffen unserer Nachbarn zu schützen. Das haben sie manchen, die sich in der Debatte um Google Streetview lautstark zu Wort gemeldet haben, voraus.

Die Frage des Datenschutzes ist eine nach den Macht(un)gleichgewichten in der Informationsgesellschaft. In der Diktion des Bundesverfassungsgerichts ist die informationelle Selbstbestimmung „Grundbedingung eines auf demokratische Mitbestimmung ausgerichteten Gemeinwesens". Mehr noch, es geht um die Frage: Wer hat die Macht über die Daten? Wer kann mit ihnen arbeiten, das heißt korrelieren, Prognosen treffen, Profile bilden, Einteilungen und Kategorisierungen vornehmen? Eine hochpolitische Angelegenheit. Die Brisanz wird deutlich, wenn wir uns den Gedanken des Systemtheoretikers Dirk Baecker zu eigen machen.

Baecker sieht uns in einem Transitionsprozess in eine „nächste Gesellschaft”, der Computergesellschaft. Diesen Prozess setzt er gleich mit den Umwälzungen, die jeweils die Einführung der Sprache, der Schrift und des Buchdrucks bewirkt haben. Auch wenn man eine gewisse Skepsis gegenüber Überhöhungen aktueller Phänomene an den Tag legen sollte, da diese oft leicht der Überhöhung der eigenen Existenz in der aktuellen Zeit dienen, ist der Gedanke verlockend. Der Ansatzpunkt, den Computer (sprich: Rechner) zum gesellschaftsprägenden Paradigma zu erklären („the difference that makes the difference") ist schlüssig. Denn durch ihn wird es möglich, in nahezu unbegrenztem Umfang Daten zu verarbeiten (sprich: zu berechnen). Daraus folgt nach Baecker, dass der Überschusssinn der „nächsten Gesellschaft” der der Kontrolle ist. Ultimativ geht es also auch um die Frage, wer wen kontrolliert.

John Gilmore schien in seiner Eröffnungsrede auf dem 25c3, dem jährlichen Gettogether des Chaos Computer Clubs, überraschenderweise David Brins „Transparent Society” etwas Visionäres abgewinnen zu wollen. Er machte dabei allerdings einen reichlich bekifften (sic!) Eindruck. Brins 1998 veröffentlichte Dystopie geht davon aus, dass der Überwachungsstaat in der „Computergesellschaft” unvermeidlich sei und dass diesem Sachverhalt mit einer neuen Form der Offenheit und Toleranz zu begegnen sei. So sehr der Ruf nach mehr Offenheit und Toleranz stets unterstützt werden sollte, so wenig ist es meines Erachtens zwingend, dass die „Computergesellschaft” in die Überwachungsgesellschaft führen (oder sie fortsetzen) muss. Will man die „nächste Gesellschaft” politisch gestalten und nicht jegliches politisches Handeln zugunsten einer fatalistischen Grundhaltung aufgeben, so muss man tatsächlich eine transparentere Gesellschaft fordern. Aber nicht eine völlige Transparenz aller Informationen über die Menschen, sondern eine weitgehende Transparenz über die Prozesse, mit denen diese Informationen verarbeitet werden, ist zu fordern.

Politisch besteht dann die Aufgabe darin, diese Verarbeitungen und Prozesse zu kontrollieren; zu entscheiden, welche Arten der Verarbeitung sinnvoll sind, und welche nicht. Dies zu ermöglichen, ohne sich dabei der Gefahr totaler oder gar totalitärer Medienkontrolle auszusetzen, wie es (der leider kürzlich verstorbene) Andreas Pfitzmann für den Einsatz von DRM-Verfahren in diesem Bereich prognostiziert hat, ist die große Herausforderung. Ein Teil der Antwort liegt auf der Hand: Es ist der Einsatz von quell-offener Software, die es ermöglicht, tief in die Verarbeitungsprozesse hineinzuschauen. Dieses „Recht auf Einsicht” (frei nach Jacques Derrida) gilt es neu gegen etwa den Schutz des Geschäftsgeheimnisses abzuwägen.

Verbot der Vorratsdatenspeicherung ins Grundgesetz?

Es führt kein Weg daran vorbei, das Politische im politischen Raum zu diskutieren und alle größeren neuen Prozesse und Verarbeitungsmöglichkeiten einer politischen Bewertung im Sinne der Frage nach Machtimplikationen zu unterziehen. Bei der Bewertung können klare Grenzziehungen helfen. Ein Verbot von Vorratsdatenspeicherungen, zum Beispiel. Man wundert sich allerdings, warum niemand die tatsächlich notwendige Konsequenz aus dem Urteil zur Vorratsdatenspeicherung gezogen hat: Wenn wir glauben, dass Yorratsdatenspeicherungen nicht erlaubt sein sollten, wenn wir glauben, dass Gesetze wie das eingangs erwähnte verfassungswidrig sein sollten, warum schreiben wir das nicht einfach in die Verfassung? Darüber nachzudenken, wie solche klaren Begrenzungen sinnvoll zu konstruieren sind, wäre möglicherweise endlich einmal ein konstruktiver Beitrag zum Thema „Datenschutz ins Grundgesetz”.

Es ist der Fluch und die Chance größerer gesellschaftlicher Transitionsprozesse, dass man neue Grundregeln und Grundprinzipien entwickeln muss. Die Entscheidung zur Vorratsdatenspeicherung spricht dafür, dass wir uns noch einmal grundsätzlicher auf die Suche begeben müssen. Dass die Novellierung der Datenschutzrichtlinie schon wird Antworten geben können ist bisher nicht zu erkennen.

Literatur

Dirk Baecker 2007: Studien zur nächsten Gesellschaft
Susanne Baer 2010: Braucht das Grundgesetz ein Update? Bürgerrechte für das Internetzeitalter, Rede auf dem Netzpolitischen Kongress der Bundestagsfraktion von Bündnis 90/Die Grünen am 13.11.2010, online unter http;//www.gruenesblog.de/netzpolitik/13461susanne-baer-brauchtdas-grundgesetz-ein-updateburgerrechte-fur-das-internetzeitalter
David Brin 1998, The transparent society, Auszug online unter httpa/www.wired.comlwired/archive/4,12/fftransparentpr.html
Chaos Computer Club (Hrsg.): hackerethics, online unter httpa/www.ccc.de/hackerethics.
John Gilmore 2009: „Nothing to hide?", Vortrag auf dem 25. Chaos Communication Congress, in Fragmenten verfügbar unter httpa/mirror.informatik.uni-mannheim.de/pub/ccclstreamdumplsaall/Tagl -Saal 1-SlotlO%3a00--Opening-INCOMPLETE.wmv
Helen Nissenbaum 2004: Privacy as Contextual Integrity, Washington Law Review Vo179, No. 1, Februar 2004, S.119—158, online unter httpa/www,nyu,edu/projectslnissenbaum/papers/washingtonlawreview.pdf
Paul Ohm 2009: Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, August 2009. University of Colorado Law Legal Studies; Research Paper Na. 09-12, online unter http://ssrn.com/abstract=1450006
Daniel J. Solove 2006: A Taxonomy of Privacy. University of Pennsylvania Law Review, Vol. 154, No. 3, S. 477ff. Januar 2006; GWU Law School Public Law; Research Paper No. 129, online unter httpa/ssrn.com/abstract=667622

---

https://www.humanistische-union.de/thema/datenschutz-fuer-die-naechste-gesellschaft/
Abgerufen am: 06.02.2023