

Andreas Pfitzmann 1958-2010

Vordenker des technischen Datenschutzes in der Informationsgesellschaft

Hannes Federrath, Marit Hansen, Michael Waidner

Erschienen in: Informatik Spektrum Heft 34/1 (2011) 99-102

Am 23. September 2010 verstarb Prof. Dr. Andreas Pfitzmann im Alter von 52 Jahren nach kurzer schwerer Krankheit. Im Mittelpunkt seines Denkens als Informatiker stand der Mensch und mit ihm die Gesellschaft, in der er lebt. Andreas Pfitzmann hat in seinem Leben als Forscher entscheidende und wegweisende wissenschaftliche Beiträge zur technischen Umsetzung des Grundrechts auf informationelle Selbstbestimmung geleistet.

Die wissenschaftliche Karriere von Andreas Pfitzmann begann 1982 an der Universität Karlsruhe als wissenschaftlicher Mitarbeiter am Lehrstuhl von Prof. Winfried Görke. Von Anfang an stand für ihn fest, dass seine wissenschaftliche Arbeit einen zwar starken technischen Kern, aber wichtiger noch einen gesellschaftlichen Sinn und Nutzen haben muss. Im Jahr 1983 entwickelte das Bundesverfassungsgericht im Volkszählungsurteil den Begriff des informationellen Selbstbestimmungsrechts. Andreas Pfitzmann erkannte als einer der ersten, dass die Umsetzung dieses Rechts nur gelingen kann, wenn Recht und Technik zusammenspielen.

Das Bundesverfassungsgericht im Jahr 1983: „Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. [...] Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden. Mit dem Recht auf informationelle Selbstbestimmung wäre eine Gesellschaftsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß.“ (1. BvR 209/83 Abschnitt C II.1, S. 43)

Am auf Rechnerarchitektur und Fehlertoleranz spezialisierten Institut begann Andreas Pfitzmann 1983 sich mit Anonymität im Netz, Pseudonymen, Signaturen und elektronischen Rechtsgeschäften zu beschäftigen. Zusammen mit seinen damaligen Studenten und späteren Kollegen Birgit Pfitzmann und Michael Waidner gründete er eine Arbeitsgruppe und verwandelte sein Büro in das „Café Pfitzmann“ – die Gruppe arbeitete dort nahezu rund um die Uhr, mit einem ungeheuren Konsum an Kaffee, Pfefferminztee und Schokolade.

Innerhalb eines Jahres erarbeitete die Gruppe die Grundbegriffe dessen, was später „Datenschutz durch Technik“ und „Mehrseitige Sicherheit“ genannt werden sollte: Datenschutz muss durch Technik unterstützt, kontrolliert und letztlich durchgesetzt werden, Datenschutz allein durch gesetzliche Vorgaben kann nicht gelingen. Systeme, die von mehreren Parteien verwendet werden, müssen die Sicherheitsinteressen aller dieser Parteien unterstützen. Damals revolutionär und utopisch sind dies heute Gedanken, die in der Informatik als „Privacy Enhancing Technologies“ (PET; dt.: datenschutzfördernde Techniken) geläufig sind.

1984 lernte Andreas Pfitzmann den amerikanischen Kryptographen David Chaum kennen. Chaum arbeitete damals am CWI in Amsterdam und entwickelte dort die kryptographischen Grundlagen für

Pseudonymität und Anonymität im Netz. Rasch erkannte Andreas Pfitzmann das praktische Potenzial der theoretischen Arbeiten von David Chaum, und es entwickelte sich eine intensive Arbeitsbeziehung zwischen den beiden Gruppen, die über viele Jahre anhalten sollte.

Andreas Pfitzmann begann, die theoretischen Konzepte von David Chaum und anderen auf ihren praktischen Wert abzuklopfen. Damals wie heute wurden in der politischen Debatte Datenschutz und Sicherheit oft als Gegensatz wahrgenommen. Mit der Publikation „Rechtssicherheit trotz Anonymität“ versuchte die Gruppe um Andreas Pfitzmann, für Juristen und Techniker verständlich zu erklären, wie man Datenschutz und Sicherheit miteinander vereinbaren kann.

Etwa ab 1987 begann Andreas Pfitzmann, die entwickelten Konzepte und Verfahren für datenschutzfördernde Techniken in prototypischen Implementierungen und Systementwürfen zu untersuchen. Gemeinsam mit Studierenden in Karlsruhe und später dann in Hildesheim entwickelte er das vermutlich erste Datenschutzpraktikum Deutschlands.

Im Jahr 1988 entwickelte und analysierte die Gruppe um Andreas Pfitzmann erstmals das Konzept der „ISDN-Mixe“ – das erste praktisch einsetzbare Verfahren zur anonymen Kommunikation in Realzeit. Wie sich später zeigte, war Andreas Pfitzmann mit diesem Verfahren und vielen anderen seiner Ideen aus dieser Zeit dem „Mainstream“ um 5 bis 10 Jahre voraus: Was im Zusammenhang mit ISDN oft als utopisch bezeichnet worden war, stellte sich mit dem Erfolg des Internets Mitte der 90er Jahre als visionär und wegweisend heraus.

Im Jahr 1989 promovierte Andreas Pfitzmann über „Diensteintegrierende Kommunikationsnetze mit teilnehmerüberprüfbarem Datenschutz“ und wechselte 1991 als Dozent an die Universität Hildesheim an den Lehrstuhl von Prof. Joachim Biskup. Gemeinsam mit David Chaum beantragte er hier erfolgreich das EU-Projekt CAFÉ, das das erste sichere und anonyme Smartcard-basierte Zahlungssystem implementierte und im praktischen Einsatz demonstrierte.

1993 erhielt Andreas Pfitzmann einen Ruf an die Technische Universität Dresden. Mit seiner Ernennung zum Professor begann sein wissenschaftliches Wirken an der TU Dresden. Sein 1993 in der Fachzeitschrift „Datenschutz und Datensicherheit“ erschienener Artikel zum Schutz mobiler Teilnehmer vor Beobachtung und Lokalisierung war für die ersten vier Jahre seiner Arbeit an der TU Dresden richtungweisend. Bei den Arbeiten ging es zunächst um die Anwendbarkeit und Adaption der „ISDN-Mixe“ auf GSM-Mobilfunknetze. Mit Forschungsgeldern der Deutschen Forschungsgemeinschaft und der Gottlieb-Daimler- und Karl-Benz-Stiftung entwickelte die neu gegründete Arbeitsgruppe um Andreas Pfitzmann Verfahren für Mobilfunknetze, die der weitverbreiteten Annahme, dass die Mobilfunkbetreiber ständig die Aufenthaltsorte ihrer Mobilfunkkunden kennen müssen, neue Lösungsansätze zum Vertraulichkeitsschutz entgegensetzten. Plötzlich gelang es, mit dem Handy erreichbar zu sein, ohne dass der Netzbetreiber ständig den aktuellen Aufenthaltsort kannte.

Im Rahmen des Daimler-Benz-Kollegs „Sicherheit in der Kommunikationstechnik“ wurden in den Jahren 1993 bis 1999 die Begriffe „Technischer Datenschutz“ und „Mehrseitige Sicherheit“ von ihm und anderen Wissenschaftlern, vor allem mit dem Leiter des Kollegs Prof. Günter Müller und dessen Koordinator Kai Rannenberg weiterentwickelt. Zur Einbeziehung der Schutzinteressen aller Beteiligten kam bei der mehrseitigen Sicherheit das Austragen daraus resultierender Schutzkonflikte beim Entstehen einer Kommunikationsverbindung.

Andreas Pfitzmann bekam aus Wissenschaft, Industrie und Politik große Anerkennung. Die Verleihung des Forschungspreises „Technische Kommunikation 1998“ der Alcatel SEL Stiftung war ein Meilenstein in der öffentlichen Wahrnehmung und breiten Akzeptanz seiner Arbeiten. Zu seinen größten politischen Erfolgen gehört sein Wirken während der Kryptodebatte der 90er Jahre. Als in den Jahren um 1997 die Ohnmachtserfahrung des Staates bei der Überwachung der Kommunikation im Internet groteske Züge annahm, wurde Andreas Pfitzmann nicht müde, als Wissenschaftler und Bürger für den freien und uneingeschränkten Einsatz von Kryptographie im Internet zu kämpfen. Eine seiner wesentlichen Botschaften war, dass bei einem Verbot von Verschlüsselung insbesondere

Kriminelle leicht auf unbeobachtbare technische Verschleierungsmöglichkeiten zurückgreifen können, während unbescholtene Bürger für den Staat zu gläsernen Menschen werden würden.

Ab dem Jahr 2000 konzentrierten sich wesentliche Arbeiten von Andreas Pfitzmann und seiner Gruppe auf den Bereich der anonymen Kommunikation im Internet. Gemeinsam mit Hannes Federrath und Marit Hansen beantragte er erfolgreich entsprechende Forschungsprojekte bei der Deutschen Forschungsgemeinschaft und dem Bundeswirtschaftsministerium. Mit dem Internet-Anonymisierungsdienst AN.ON wurde eines der ersten praktisch verwendbaren Selbstschutz-Werkzeuge für Bürger und Unternehmen geschaffen, das die frühen theoretischen Arbeiten für das Internet praktisch anwendbar machte.

Die Lehre und die Studierenden waren ihm überaus wichtig. Der im Jahr 2001 erstmals vergebene Lehrpreis der Fachschaft Informatik der TU Dresden für die beste Lehrveranstaltung im Hauptstudium ging an ihn. Als langjähriger Studiendekan und späterer Dekan der Fakultät Informatik lebte und förderte er die Einheit – und Freiheit – von Forschung und Lehre.

Mit dem im Auftrag des Bundesinnenministeriums im Jahr 2001 in Auftrag gegebenen und gemeinsam mit Prof. Alexander Roßnagel und Prof. Hansjürgen Garstka verfassten Gutachten zur „Modernisierung des Datenschutzrechts“ verband sich für Andreas Pfitzmann die Hoffnung, dass sich seine Ideen eines technischen Datenschutzes auch in der Gesetzgebung niederschlagen werden. Mit der anstehenden Novellierung des Datenschutzrechts könnte dieser Wunsch nun gut 10 Jahre später in Erfüllung gehen. Auch hier wird deutlich, dass Andreas Pfitzmann seiner Zeit deutlich voraus war. Einen Einfluss auf die Gesetzgebung werden auf jeden Fall seine jüngsten Arbeiten zu einer Erweiterung des klassischen Schutzziel-Kanons (Vertraulichkeit, Integrität und Verfügbarkeit) um spezielle Privacy-Schutzziele wie Transparenz und Unverkettbarkeit nehmen, die in der Diskussion der Datenschutzbeauftragten des Bundes und der Länder aufgegriffen wurden.

Andreas Pfitzmann war als Sachverständiger in der politischen Debatte sowie vor verschiedenen Gerichten gefragt, u.a. zum Einsatz von Biometrie, zur Vorratsdatenspeicherung und zur Online-Durchsuchung. Insbesondere war Andreas Pfitzmann als Gutachter zur Online-Durchsuchung im Jahr 2007 für das Bundesverfassungsgericht ein viel beachteter Experte. So hat er mit dazu beigetragen, dass vom Bundesverfassungsgericht im Februar 2008 ein neues „Computer-Grundrecht“ auf „Gewährleistung von Vertraulichkeit und Integrität informationstechnischer Systeme“ formuliert wurde.

Das Thema „Anonymität“ in seinen verschiedenen Facetten prägte einen großen Teil der Forschungsarbeiten von Andreas Pfitzmann. Anlässlich des im Sommer 2000 organisierten „Workshops on Design Issues in Anonymity and Unobservability“, aus dem sich das jährlich stattfindende „Privacy Enhancing Technologies Symposium“ (PETS) entwickelte, startete er den Versuch, die Terminologie zu Anonymität und verwandten Begriffen systematisch aufzubereiten. Moderiert von Andreas Pfitzmann und Marit Hansen entwickelte sich das „Terminology-Paper“ mit Hilfe von Beiträgen aus der Community in den vergangenen 10 Jahren weiter. Noch im August 2010 stellte Andreas Pfitzmann die Version 0.34 des viel zitierten Papiers online zur Verfügung [http://dud.inf.tu-dresden.de/Anon_Terminology.shtml].

Andreas Pfitzmanns Sicht auf Datenschutz war zu Beginn von dem Prinzip der Datenminimierung dominiert: Wenn gar keine personenbezogenen Daten anfallen, besteht auch nicht das Risiko, dass sie missbräuchlich genutzt werden. Da eine absolute Datenvermeidung in vielen Fällen nicht möglich ist, erweiterte er seine Sicht auf Datenschutz um das Prinzip der Kontrolle durch den Betroffenen – ganz im Sinne des Rechts auf informationelle Selbstbestimmung und des Konzepts der mehrseitigen Sicherheit. Dies wird auch in seinen Forschungsarbeiten zum Thema Identitätsmanagement ab etwa 2000 deutlich. Ab dem Jahr 2004 wurden bis zuletzt von ihm und seiner Forschungsgruppe in den von der EU geförderten Projekten „PRIME – Privacy and Identity Management for Europe“ und „PrimeLife“ wesentliche Beiträge zum Thema „Datenschutzförderndes Identitätsmanagement“ in der Online-Welt geleistet. Zudem war Andreas Pfitzmann maßgeblich im europäischen Network of

Excellence „FIDIS – Future of Identity in the Information Society“ (2004-2009) beteiligt. Die jüngsten Vorschläge von Andreas Pfitzmann zu Datenschutzkonzepten, die einerseits einen lebenslangen Datenschutz ermöglichen sollen und andererseits eine Kontextbindung persönlicher Daten vorsehen, konnte er noch im August 2010 auf der IFIP/PrimeLife Summer School skizzieren und damit Impulse für das PrimeLife-Projekt geben.

Andreas Pfitzmann und die GI

Noch während seines Studiums kam Andreas Pfitzmann in Kontakt zu Rüdiger Dierstein, der 1980 Sprecher des neuen Fachbereichs 4 „Informationstechnik und technische Nutzung der Informatik“ der Gesellschaft für Informatik e.V. (GI) geworden war und sich von Anfang an sehr dafür einsetzte, dem Thema Datenschutz und Datensicherung in der GI deutlich mehr Geltung zu verschaffen als bisher. Rüdiger Diersteins Forderung, das Thema Sicherheit nicht nur technisch, sondern stets aus zwei einander ergänzenden Sichten zu betrachten – der technischen Verlässlichkeit und der auf die gesellschaftlichen Auswirkungen gerichteten Beherrschbarkeit (Duale Sicherheit) – war mit Andreas Pfitzmanns Vorstellung der datenschutzfördernden Techniken sehr nahe verwandt. Aus der ersten Begegnung wuchs im Laufe der Jahre eine enge Freundschaft und fruchtbare Zusammenarbeit. Später wurde das Thema Datenschutz und Datensicherheit innerhalb der GI insbesondere in der Fachgruppe VIS (Verlässliche Informationssysteme, später Verlässliche IT-Systeme) und im Präsidiumsarbeitskreis „Datenschutz und IT-Sicherheit“ durch Andreas Pfitzmann sehr aktiv mitgestaltet. Eine der ersten über den Präsidiumsarbeitskreis veröffentlichten Publikationen war die zusammen mit Kai Rannenberg kritisch-konstruktive Auseinandersetzung mit den seinerzeitigen ITSEC-Evaluationskriterien für Sicherheit in der Informationstechnik. Sie führte u.a. zur Prägung des Begriffs „Mehrseitige Sicherheit“.

Ab 1985 ergab sich eine enge interdisziplinäre Zusammenarbeit mit dem Netzinformatiker Dr. Eckart Raubold, dem damaligen Leiter der Gesellschaft für Mathematik und Datenverarbeitung (GMD), sowie mit dem Verfassungsjuristen Prof. Alexander Roßnagel, dem Gründer der Projektgruppe Verfassungsverträgliche Technikgestaltung e.V. (provet), in der die Basis zur interdisziplinären Sicherheitsentwicklung gelegt wurde, in dessen Mittelpunkt der Mensch mit seinen konfligierenden Interessen steht.

Andreas Pfitzmann und Eckart Raubold gründeten etwa 1990 die GI-Fachgruppe VIS. Nach einer Vorläufertagung 1985 in München waren sie Ko-Editoren des ersten Tagungsbandes der ersten „offiziellen“ VIS-Tagung in Darmstadt 1991. Andreas Pfitzmann war erster und langjähriger Sprecher der GI-Fachgruppe VIS bis 2001.

Auch bei der Gründung des GI-Fachbereichs „Sicherheit, Schutz und Zuverlässigkeit“, der aus mehreren GI-Gliederungen einschließlich der Fachgruppe VIS entstand, hat er tatkräftig mitgewirkt und seine gesamtheitliche Sicht auf das Thema deutlich gemacht. Die Dualität der Eigenschaften Schutz und Zuverlässigkeit bei der Betrachtung des Themas Sicherheit wurde erfolgreich im Fachbereich dargestellt und wird dort mit großem Elan weitergeführt. Die zweijährige Konferenzreihe „GI Sicherheit“ ist ein deutlicher Beweis der erfolgreichen Arbeit des Fachbereichs.

Visionär und Vordenker

Andreas Pfitzmann war Visionär und Vordenker. Mit seiner ausgeprägten Beobachtungsgabe, seinem tiefen Detailverständnis, seiner hohen Intelligenz und dem ausgeprägten Willen, Menschen mit gleichen – und insbesondere auch unterschiedlichen – Interessen zusammen zu bringen, hat er als Wissenschaftler und Mensch unschätzbar viel dazu beigetragen, unsere Welt zu verbessern.

Danksagung

Unser Dank für Hinweise, Ergänzungen und Verbesserungsvorschläge geht an Katrin Borcea-Pfitzmann, Rüdiger Dierstein, Rüdiger Grimm, Hermann Härtig, Steffen Hölldobler, Hartmut Pohl, Kai Rannenberg und Manfred Reitenspieß.