

Terrorismusbekämpfung darf nicht zur Datenschutzbekämpfung werden

Stellungnahme der Deutschen Vereinigung für Datenschutz

Kiel, den 25.09.2001

Mit dem Spruch "Datenschutz darf nicht zum Terroristenschutz werden" schaffte es der Sprecher von Bundesinnenminister Otto Schily am 16.09.2001 bis in die Tagesschau. Seit dem terroristischen Anschlag auf das World Trade Center und das Pentagon in den USA am 11.09.2001 findet ein Angriff auf unsere Freiheit und unseren demokratischen Rechtsstaat statt. Law-and-Order-Politiker fordern in der Bundesrepublik Deutschland Überwachungsmaßnahmen und Bürgerrechtseingriffe, die seit dem deutschen Herbst in den 70er Jahren nicht mehr vorstellbar waren. Datenschutz als eine besondere Form des Schutzes unserer Bürgerrechte wird als "**Tatenschutz**" diffamiert. Die Hilflosigkeit von Sicherheitsbehörden und Politik in der Folge des Terroranschlags schlug schon nach wenigen Tagen um in hektischen Aktionismus bei der Forderung von "Sicherheitsmaßnahmen", die regelmäßig nicht geeignet sind, mehr "Sicherheit" zu schaffen, mit Sicherheit aber unsere Freiheitsrechte unterminieren würden.

Die Deutsche Vereinigung für Datenschutz warnt davor, mit symbolischer Politik die Fundamente unserer offenen freiheitlichen Gesellschaft zu zerstören. Wir leben in einer Risikogesellschaft, in der es **keine 100%ige Sicherheit** vor derart furchtbaren Verbrechen gibt. Gegen "Schläfer", die unauffällig und legal in unserem Land leben, helfen auch die ausgeklügeltsten Überwachungsmaßnahmen nichts, solange diese verdächtige Verhaltensprofile vermeiden können. Dies muss offen gegenüber der Bevölkerung ausgesprochen werden. Risiken werden nicht durch flächendeckende Überwachung minimiert, sondern dadurch, dass Gefahrenquellen isoliert und entschärft werden. Insofern erhält die Feststellung von Robert Jungk aus den 70er Jahren des letzten Jahrhunderts Tagesaktualität, der vor der Tyrannei als Begleiterscheinung unserer Hochleistungstechnik mit Atom-, Chemie- und Bioindustrie warnte, vor der "atomaren Spaltung unserer Grundrechte".

Die anlasslose Überwachung unserer Gesellschaft bzw. von wesentlichen Teilen (z.B. der ausländischen Mitbürgerinnen, der islamischen Gruppen, der Telekommunikation) wird keine Aufklärung terroristischer Strukturen bringen, sondern insbesondere gesellschaftliche Minderheiten in **Angst und feindliche Stimmungen** versetzen. Und genau dies ist ein Nährboden für den Terrorismus.

Die pauschale sicherheitsbehördliche Überwachung produziert **Informations- und Datenberge**, deren sinnvolle Auswertung auch mit modernsten Mitteln unmöglich ist. Ungezielte Überwachung ist ein Stochern im Nebel, das keinen nachhaltigen Sicherheitsgewinn bringen kann.

Die Form der Überwachung mit weitgehenden unkontrollierten Befugnissen für die Sicherheitsorgane kann Angst und Abwehr in der Bevölkerung zur Folge haben. Dies sind die schlechtesten Rahmenbedingungen für Behörden, die nicht nur in, sondern auch mit der Bevölkerung Sicherheit schaffen wollen. **Vertrauen der Bevölkerung** in die Sicherheitsorgane bedingt deren Transparenz und Kontrollierbarkeit. Dieses Vertrauen ist Grundbedingung für den Kampf gegen terroristische Kriminalität.

Erfolge in der Terrorismusbekämpfung in der Vergangenheit und in der Gegenwart wurden vor allem dadurch erreicht, dass **konkreten Spuren und Hinweisen** nachgegangen wurde. Dies wird für die Zukunft noch mehr gelten als bisher, wo unter Nutzung von Angriffsmitteln niedriger Technologie gewaltige Schäden verursacht werden können und Terroristen sich zugleich im Besitz von High-Tech befinden, mit der die eigene Kommunikation und Organisation abgeschirmt werden kann. Der intelligente

Einsatz "intelligenter" technischer Ermittlungsmethoden (signal intelligence - sigint) durch die Sicherheitsbehörden muss immer flankiert bleiben durch gezielte menschliche Ermittlung (human intelligence - humint).

Die **gesetzlichen Möglichkeiten** zur Aufklärung terroristischer Verbrechen wurden seit den 70er Jahren in der Bundesrepublik geschaffen, ohne dass sie mit dem Abebben des Terrorismus in der 90er Jahren wieder beseitigt worden wären. Dieses gesetzliche Instrumentarium erlaubt auch die Nutzung modernster Informationstechnik. Entgegen unsubstanziierter Behauptungen von vielen Law-and-Order-Politikern stehen Datenschutzregelungen der Aufklärung solcher Verbrechen nicht entgegen. Die DatenschützerInnen haben sich noch nie vernünftigen Methoden der Verbrechensaufklärung verschlossen. Sie legen aber Wert darauf, dass alle Sicherheitsmaßnahmen demokratisch (per Gesetz) legitimiert und rechtsstaatlich kontrolliert werden. Waffengleichheit zwischen Strafverfolgern und Terroristen kann nicht bedeuten, dass sich Strafverfolger kontrollfrei und voraussetzungslos der gleichen Mittel bedienen dürfen wie die Terroristen. Informationsdefizite bei den Sicherheitsbehörden im Zusammenhang mit terroristischen oder sonstigen schweren Straftaten, die zunächst "dem Datenschutz" in die Schuhe geschoben werden, erweisen sich bei genauerem Hinsehen oft als organisatorische oder sonstige behördliche Defizite oder haben ihren Grund in einer unzutreffenden Lageanalyse.

Vor diesem Hintergrund werden im Folgenden die von Politikern vorgeschlagenen politischen Maßnahmen erörtert, die durch die Erhebung und Nutzung personenbezogener Daten Eingriffe in den Datenschutz darstellen.

In einem ersten Maßnahmenbündel wurde im Eilverfahren am 19.09. vom Bundeskabinett Folgendes beschlossen:

- Kredit- und Finanzinstitute sollen verpflichtet werden, auch unterhalb der bisherigen Schwelle von 20.000 DM verdächtige Geldtransaktionen anzuzeigen. Auf Anfrage soll im Verdachtsfall eine Auskunftspflicht der Finanzinstitute und eine damit verbundene Durchbrechung des Bankgeheimnisses vorgesehen werden. Die bisherige Regelung des **Geldwäschegesetzes** hat wenig Erfolge gezeigt. Eine unreflektierte Ausweitung macht daher wenig Sinn. Soweit die Übermittlungspflicht sich aber auf größere Summen beschränkt und ein förmliches Verfahren beachtet wird, ist gegen Änderungen wenig einzuwenden. Wichtiger als eine Überwachung der konventionellen Geldströme dürfte für eine Rekonstruktion von Geldwäsche die Auswertung des elektronischen Geldverkehrs sein. Die derzeitige Privilegierung der Banken durch das Bankgeheimnis nach § 30a Abgabenordnung gegenüber sonstigen Geschäftsbereichen ist ohnehin ein Verstoß gegen den Gleichheitsgrundsatz. Bei höheren Summen nimmt mit der Höhe deren Bezug zur Verwirklichung des allgemeinen Persönlichkeitsrechtes ab.
- Die **Abschaffung des Religionsprivileg** im Vereinsrecht erleichtert die Überwachung in diesen Vereinen, bewirkt aber gegenüber den sonstigen Vereinen lediglich die Herstellung von Gleichberechtigung und ist aus Datenschutzsicht neutral.
- Mit der Schaffung eines neuen § 129b im Strafgesetzbuch (StGB) wird der Anwendungsbereich der Strafbarkeit **terroristischer Vereinigungen** (§ 129a StGB) auf Auslandsvereinigungen ausgeweitet. Der bisherige § 129a StGB war wegen seiner unbestimmten Tatbestandsvoraussetzungen ("Werben", "Unterstützen") in der Vergangenheit vor allem ein Ermittlungstatbestand, der bei banalen Anlässen massive informationelle Ermittlungseingriffe ermöglichte. Gegen eine Ausweitung auf internationale Organisationen ist nur dann nichts einzuwenden, wenn zugleich eine rechtsstaatliche Eingrenzung der

Tatbestandsvoraussetzungen erfolgt. Anderenfalls kann mit diesem Paragrafen fast beliebig politisches internationales Engagement strafprozessual ausgeforscht und verfolgt werden.

- Die Anwendung von **Sicherheitsüberprüfungen** nach dem Sicherheitsüberprüfungsgesetz auf Angestellte deutscher Flughäfen dürfte angesichts der neuen Gefährdungslage angemessen sein.

Von allen Seiten wird der Einsatz der **Rasterfahndung** mit dem Ziel der Erkennung weiterer "Schläfer" gefordert. Baden-Württemberg, Berlin, Brandenburg und Hamburg ordneten diese Fahndungsmethode an, Niedersachsen will baldmöglichst nachziehen. Es soll mit Hilfe von Daten aus Meldeämtern, Krankenkassen, der Polizei und Hochschulen von Studierenden und anderen Personen aus 14 arabischen Ländern ein vom amerikanischen FBI geliefertes Verdächtigen-Profil abgeglichen werden. Die rechtlichen Voraussetzungen für derartige Rastermaßnahmen bestehen in den meisten Landespolizeigesetzen sowie in der Strafprozessordnung (StPO, §§ 98a ff.). Ob diese Gesetze beachtet werden, kann derzeit von Außen nicht beurteilt werden.

Die Forderung z.B. des niedersächsischen Innenministers Heiner Bartling (SPD) nach **Einblick in Passagierlisten** von Fluggesellschaften zum Zweck der Erstellung von Bewegungsbildern wäre als Maßnahme der Rasterfahndung (s.o.) oder bei einem konkreten Tatverdacht gegen einen Passagier (§ 161a StPO) zulässig. Der verdachtslose Datenabgleich würde dagegen zu einer Erstellung von Bewegungsprofilen aller Flugreisenden führen und wäre für Aufklärungszwecke unergiebig und unverhältnismäßig.

Immer wieder wurde beklagt, die Daten aus dem Bestand des **Ausländerzentralregisters** (AZR) stünden nicht umfassend zur Verfügung. Diese Behauptung ist falsch. Nach den §§ 15-17 AZRG haben Justiz- und Polizeibehörden, nach § 20 AZRG haben die deutschen Geheimdienste inhaltlich ungehinderten Zugang zu den AZR-Daten, nach § 22 AZRG auch im Wege der Online-Übermittlung. Außerdem sieht § 12 AZRG ausdrücklich die Rasterfahndung (Gruppenauskunft) mit AZR-Daten vor.

Von Innenminister Schily wurde Zugriff von Polizei und Verfassungsschutz auf die **Visadateien** der Botschaften gefordert. Diese Forderung macht keinen Sinn, da nach den §§ 32, 33 AZRG den genannten Behörden - auch der automatisierte - Zugriff auf die Visadatei beim Bundesverwaltungsamt zugelassen ist und dadurch ein zentraler und nicht nur viele kleine dezentrale Datenbestände zur Verfügung stehen. Auf Einzelanfrage bei den Botschaften ist den Sicherheitsbehörden nach dem jeweiligen Recht (StPO, Geheimdienstgesetze) Auskunft zu erteilen.

Die vom bayerischen Innenminister Günther Beckstein geforderte **Regelanfrage** beim Bundesamt für Verfassungsschutz (BfV) oder beim Bundesnachrichtendienst (BND) **bei der Einreise**, also bei der Erteilung von Sichtvermerken (Visa) ist schlicht Unsinn. Ein derartiges Massengeschäft würde die Dienste zwangsläufig absolut überfordern und hätte zur Folge, dass ein Effekt mangels hinreichend tiefer Prüfung nicht erzielt würde. Auch weil über die meisten Antragstellenden mangels Kontakt zu deutschen Behörden ohnehin keine Erkenntnisse vorliegen, liefe eine solche Regelung ins Leere. Die geforderte Regelanfrage hätte zudem zur Folge, sämtliche Antragsteller einem Terrorismus-Pauschalverdacht auszusetzen. Entsprechendes gälte für eine Regelanfrage in Fall einer längerfristigen Visaerteilung zum Zweck der Zuwanderung.

Die Regelanfrage beim behördlichen Verfassungsschutz bei Beantragung **der Einbürgerung** kann als von § 85 Abs. 1 Nr. 1 AuslG abgedeckt angesehen werden. Bisher hatte von dieser Möglichkeit nur Bayern Gebrauch gemacht. Alle anderen Länder starteten bisher nur eine Anfrage, wenn begründete Anhaltspunkte für verfassungsfeindliche Bestrebungen vorhanden waren. Hieran sollte festgehalten werden.

Abgesehen von dem mit der Regelanfrage verbundenen Pauschalverdacht: Es ist kaum begründbar, weshalb von einem Eingebürgerten eine größere Terrorismusgefahr ausgehen könnte als von einem Ausländer. Die auf Grund der Regelanfrage in Bayern seit 1998 abgewiesenen über 200 Einbürgerungsanträge sind angesichts der fragwürdigen Datenbasis bei diesen Entscheidungen kein Beleg für die Gefährlichkeit der Antragstellenden.

Erwogen wird weiterhin, bei der **Beantragung von Visa** einen **Fingerabdruck** zu erfassen und diesen mit Fahndungsdatenbeständen (Automatisiertes Fingerabdruckidentifikationssystem - AFIS) abzugleichen. Eine solche Praxis besteht schon bei sämtlichen Asylsuchenden und Bürgerkriegsflüchtlingen und wird von vielen wegen des Verstoßes gegen das Verhältnismäßigkeitsprinzip als verfassungswidrig angesehen. Eine Verhältnismäßigkeit könnte nur unter engen Rahmenbedingungen angenommen werden (zeitliche Begrenztheit und Bezug zu bestimmtem Anlass, nur einer/nicht zehn Finger, fristgemäße Löschung, keine zweckfremde Nutzung).

Innenminister Schily forderte die Einführung des **Fingerabdrucks auf Reisedokumenten**, also wohl auf dem Reisepass wie dem Personalausweis, um eine präzise Identifizierung des Ausweisbesitzenden vornehmen zu können. Zunächst muss darauf hingewiesen werden, dass Deutschland eigenständig nur die Ausstellung von deutschen Reisedokumenten, die i.d.R. nur an Deutsche ausgestellt werden, regeln kann. Terroristen mit ausländischen Dokumenten könnten nicht erfasst werden. Die Forderung ist aber unabhängig von diesem Umstand entweder unsinnig oder gefährlich: Würde der Fingerabdruck auf dem Ausweis optoelektronisch lesbar oder elektronisch gespeichert (nach Umstellung der Ausweise auf Chipkartenbasis), so ließe er sich zweifellos auch fälschen. Würde der Abdruck jedoch außerhalb der Karte zentral in einer bundesweiten Referenzdatei gespeichert, so würde damit eine bundesweite daktyloskopische Sammlung sämtlicher Bundesbürgerinnen und Bundesbürger geschaffen. Eine derartige Erfassung muss aber als unverhältnismäßig abgelehnt werden. Der damit zu erreichende Sicherheitsgewinn ist kaum erkennbar. Denkbar wäre auch die Einführung von selbstreferenziellen Chipkarten als Ausweisen, auf denen der Fingerabdruck sowie das Lesefeld für den Lifeabdruck gespeichert sind. Derartige - aus Datenschutzsicht akzeptierbare - Karten sind technisch machbar, würden aber Kosten verursachen, die in keinem Verhältnis zum erhofften Nutzen stehen.

Bayerns Innenminister forderte die **Erfassung des bloßen Aufenthalts in** Ländern, die als "**Schurkenstaaten**" bezeichnet werden. Abgesehen davon, dass es den deutschen Behörden praktisch unmöglich sein dürfte, derartige Feststellung zu machen und es mehr als ein praktisches bzw. politisches Problem geben dürfte, diese Staaten nach rechtsstaatlichen Gesichtspunkten zu definieren, hätte eine solche Erfassung einen kontraproduktiven Effekt. Gerade die Personen, die einen Dialog mit den Staaten suchen und sich für Ausgleich und Hilfe einsetzen, würden erfasst und von den deutschen Sicherheitsbehörden kontrolliert.

Insbesondere aus den USA kommend, wurde von der CDU/CSU die Forderung nach einer verstärkten **Überwachung der Telekommunikation** gestellt. Die Überwachungsmöglichkeiten bei jeder Form elektronischer Telekommunikation sind schon heute äußerst weitgehend (v.a. §§ 100a StPO). Der darüber hinausgehende Wunschkatalog reicht von einem Verschlüsselungsverbot bzw. einer Krypto-Regulierung, über die ungehinderte Emailüberwachung bis hin der Pflicht, vorsorglich sämtliche Kommunikationsverbindungsdaten für eine gewisse Zeit (von 6 Monaten bis zu 7 Jahren) für Strafverfolgungszwecke zwischenzuspeichern. Dabei wird ignoriert, dass professionell geschützte Kommunikation praktisch nicht erkennbar ist. Zwar lässt sich die Nutzung starker Verschlüsselung noch feststellen, nicht aber mehr, wenn geheime Botschaften in Bildern oder sonstigen Datenbeständen versteckt werden (Steganografie). Verschlüsselungsverbote würden nichts nützen gegen professionelle Verbrecher; sie

würden aber den Selbstschutz der unbescholtenen Bürgerinnen und Bürger sabotieren. Die langfristige Vorratsspeicherung sämtlicher Verbindungsdaten wäre zum einen eine selbst mit aufwändigen Mitteln kaum zu bewältigende technische Aufgabe, die wieder nur die Unbescholtenen treffen würde; Profis könnten evtl. im Ausland befindliche Anonymisierungsmöglichkeiten nutzen.

Sowohl der CSU-Politiker Norbert Geis wie auch FDP-Chef Guido Westerwelle forderten, **verdeckte Ermittler** (§ 110a StPO) sollten in einem gewissen Maß Straftaten begehen können. Wäre diese Forderung schon bei einfacher Kriminalität nicht hinnehmbar, so gilt dies erst Recht für den derzeit zur Diskussion stehenden Terrorismus. Abgesehen von diesen rechtsstaatlichen Bedenken stellt sich die praktische Frage, woher die Sicherheitsbehörden die Beamten nehmen sollen, die z.B. in das Milieu islamistischer Fundamentalisten eindringen können.

Die Wiedereinführung der **Kronzeugenregelung** ist ein weiterer nun von der CDU/CSU mobilisierter Ladenhüter. Abgesehen von den bekannten Bedenken gegen dieses Instrument (z.B. Problem der Falschbeschuldigung), kann dieses Instrument bei dem in den USA aktiv gewordenen Täterkreis, dessen Fanatismus bis zur Todesbereitschaft geht, garantiert keinen Erfolg erbringen.

Am 20.09. haben die europäischen Innen- und Justizminister ein sicherheitspolitisches Sofortprogramm zur Bekämpfung des Terrorismus beschlossen, in dessen Zentrum die Aufwertung der europäischen Polizeibehörde **Europol** steht. U.a. ist vorgesehen, Europol mit den nationalen Nachrichtendiensten zu vernetzen, gemeinsame Ermittlungsteams aus europäischen Terrorspezialisten einzusetzen und die Zusammenarbeit mit sog. Drittstaaten zu intensivieren. Die nationalen Visa-Daten sollen europaweit verfügbar gemacht werden. Europäische Rasterfahndungen sind geplant. Gegen all diese Pläne wäre aus Datenschutzsicht nichts grundsätzlich einzuwenden, wenn sie in einen rechtsstaatlichen, demokratisch legitimierten und kontrollierten sowie mit subjektiven Rechten flankierten Rahmen eingebunden wären. Dies ist aber nicht der Fall. Europol arbeitet auf Grundlage einer Konvention, die in ihrer Unbestimmtheit der Befugnisnormen und wegen des Fehlens von Betroffenenrechten, dem Fehlen einer parlamentarischen wie auch einer richterlichen Kontrolle zu europäischen wie deutschen rechtsstaatlichen Prinzipien in diametralem Widerspruch steht. So wichtig eine Verbesserung der europaweiten Kooperation der Terrorismusbekämpfung ist, so wichtig ist es, diese rechtsstaatlich auszugestalten. Hierzu wurden noch nicht einmal ansatzweise die notwendigen Maßnahmen ergriffen.

Generell gilt: Jede Maßnahme, die zur Terrorismusbekämpfung genutzt wird und die dabei in die Freiheitsrechte der Bürgerinnen und Bürger eingreift, muss auf ihre Wirksamkeit hin überprüft werden. Erweist sich eine Maßnahme nach einer solchen **Evaluation** als nicht verhältnismäßig, so muss sie wieder abgeschafft bzw. eingestellt werden.

Die derzeit in der Diskussion befindlichen Vorschläge sind teilweise aus Datenschutzsicht akzeptabel, die Meisten aber sind hochgefährlich. Law-and-Order-Politiker betreiben wieder einmal das Geschäft mit der Angst. Sie präsentieren ungeniert ihre sicherheitspolitische Wunsch-Befugnisliste, während sich - angesichts der Ungeheuerlichkeit des erfolgten terroristischen Anschlags und aus Hilf- und Alternativlosigkeit - die bürgerrechtlich motivierten Menschen und PolitikerInnen kaum getrauen, dem etwas entgegen zu setzen. Die Abwehr gegen die Angriffe auf den Datenschutz durch die Datenschutzbeauftragten wie durch Bürgerrechtspolitiker ist äußerst defensiv, scheinbar mit dem Rücken an der Wand. Zu Unrecht: Denn viele der Law-and-Order-Vorschläge sind nicht nur untauglich zur Bekämpfung des Terrorismus, sie sind oft geeignet, ein politisches Klima des Terrorismus zu fördern. Nicht nur im Interesse der Verteidigung der Bürgerrechte, sondern auch im **Interesse der**



Deutsche Vereinigung
für Datenschutz e.V.

Sicherheit müssen daher - mit besten Gewissen - die Prinzipien des Datenschutzes verteidigt werden.

Dr. Thilo Weichert
Vorsitzender der Deutschen Vereinigung für Datenschutz
Bonner Talweg 33-35
53173 Bonn

E-Mail: weichert@datenschutzverein.de