Deutscher Bundestag ■ Wissenschaftliche Dienste

Einzelfragen zu Datensicherheit und Datenschutz

- Ausarbeitung -

[redacted]

 WD 3 – 3000- 335/08

Wissenschaftliche Dienste des Deutschen Bundestages

Verfasser/in: [redacted]

Datensicherheit und Datenschutz

Ausarbeitung WD 3 – 3000 – 335/08

Abschluss der Arbeit: 12. September 2008

Fachbereich WD 3: Verfassung und Verwaltung

Telefon: [redacted]

W

1. Biometrische Daten und Selbstbestimmung

Frage:

Verstößt es gegen das Recht auf informationelle Selbstbestimmung, wenn der Bürger seine biometrischen Daten für den Reisepass preisgeben muss?

Antwort:

Nach § 6a **Paßgesetz**[1] müssen Bürger ihren **Fingerabdruck** der Passbehörde künftig zur Verfügung stellen. Der im Pass elektronisch gespeicherte Fingerabdruck soll helfen, Fälschungen auszuschließen. Dieser so genannte „**biometrische Pass**“ geht zurück auf eine **EG-Verordnung** aus dem Jahr 2004.[2] Die EG-Verordnung verpflichtet die Mitgliedstaaten, biometrische Daten in ihre Pässe einzuführen.[3]

Das Grundrecht auf **informationellen Selbstbestimmung**[4] dürfte solche „biometrischen Reisepässe“ zulassen. Die informationelle Selbstbestimmung gibt dem Bürger das Recht, selbst zu entscheiden, „wann und innerhalb welcher Grenzen [er] persönliche Lebenssachverhalte offenbart“.[5] Hierzu gehören auch **personenbezogene Daten**[6] wie der Fingerabdruck. Muss der Bürger solche Daten gegenüber einer Behörde offenbaren, ist sein Grundrecht auf informationelle Selbstbestimmung beeinträchtigt.

Das Grundrecht gilt jedoch nicht absolut. Besteht eine **sachliche Notwendigkeit**, kann der Staat das Grundrecht durch Gesetz einschränken. Dabei muss das Gesetz zu erkennen geben, unter welchen Voraussetzungen und mit welchem Umfang der Staat die Freiheit des Bürgers beschränken kann.[7] Die detaillierten Regelungen des Paßgesetzes dürften diese Anforderungen wohl erfüllen. Ferner muss der Eingriff in das Grundrecht des Bürgers **verhältnismäßig** sein. Das heißt: Der Eingriff muss seinen Zweck erfüllen können, der Eingriff muss das mildeste Mittel sein und Zweck und Beeinträchtigung dürfen nicht außer Verhältnis stehen. Der Einsatz biometrischer Merkmale dürfte die Sicherheit von Reisepässen erhöhen und damit seinen **Zweck** erfüllen. Hierbei hat der

---

1 Paßgesetz vom 19. April 1986 (BGBl. I S. 537), zuletzt geändert durch Artikel 11 des Gesetzes vom 26. Februar 2008 (BGBl. I S. 215).

2 Verordnung (EG) Nr. 2252/2004 des Rates vom 13. Dezember 2004 über Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten, Amtsblatt der Europäischen Union vom 29. Dezember 2004 L 385/1.

3 Gesetzentwurf zur Änderung des Passgesetzes BT-Drs. 16/4138, S. 14.

4 Art. 2 Abs. 1 i. V. m Art. 1 Abs. 1 Grundgesetz (GG).

5 BVerfGE 65, Seite 1 (41 f.).

6 BVerfGE 65, Seite 1 (42); vgl. BVerfGE 78, Seite 77 (84): „[…] Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person (personenbezogene Daten) […].“

7 BVerfGE 65, Seite 1 (44).

Gesetzgeber einen Einschätzungsspielraum.[8] Ein **milderes Mittel** dürfte nicht zur Verfügung stehen, zumal jede Identitätsprüfung eine Datenerhebung erforderlich macht. Auch hierbei hat der Gesetzgeber einen Einschätzungsspielraum.[9] Die allgemeine Sicherheit als angestrebter Zweck und die Beeinträchtigung des Bürgers durch den erforderlichen Fingerabdruck dürften **nicht außer Verhältnis** stehen. Hiergegen könnte zwar Folgendes sprechen: Im Zeitraum zwischen 2001 und 2006, also zu Zeiten des Reisepasses ohne digital gespeicherte biometrische Daten, ließen sich nur **sechs Fälschungen** und 344 Verfälschungen von deutschen Reisepässen feststellen.[10] **Kein** ge- oder verfälschter deutscher Reisepass wurde in diesem Zeitraum bei **terroristischen Anschlägen** oder deren Vorbereitung genutzt.[11] Allerdings dürften die folgenden beiden Aspekte die Bedenken ausräumen: Das durch sichere Reisepässe geschützte Rechtsgut – Sicherheit und **Funktionieren des Staates** – hat einen hohen Wert. Ferner hat der Gesetzgeber im Paßgesetz **Vorkehrungen** getroffen, die einem Missbrauch der biometrischen Daten vorbeugen sollen (vgl. nur § 16a Paßgesetz: „Die im Chip des Passes gespeicherten Daten dürfen nur zum Zweck der Überprüfung der Echtheit des Dokumentes oder der Identität des Passinhabers […] ausgelesen und verwendet werden.“).

2. Missbrauch durch Nicht-EU-Staaten

Frage:

Gibt es eine Garantie, dass die biometrischen Daten bei der Einreise in ein Nicht-EU-Land von den dortigen Behörden nicht gesammelt und missbraucht werden können (z. B. für schwarze Listen mit Fingerabdruckdaten)?

---

8 Vgl. nur BVerfG, Urteil vom 27. Februar 2008, 1 BvR 370, 595/07 – Online-Durchsuchungen, WM 2008, 503 (507).

9 Vgl. nur BVerfG, Urteil vom 27. Februar 2008, 1 BvR 370, 595/07 – Online-Durchsuchungen, WM 2008, 503 (507).

10 BT-Drs. 16/5507 vom 29. Mai 2007, Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Jan Korte, Petra Pau, Ulla Jelpke, weiterer Abgeordneter und der Fraktion DIE LINKE. – Drucksache 16/5228 – Notwendigkeit neuer biometrischer Pässe aus Sicherheitsgründen, http://dip.bundestag.de/btd/16/055/1605507.pdf, S. 1.

11 BT-Drs. 16/5507 vom 29. Mai 2007, Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Jan Korte, Petra Pau, Ulla Jelpke, weiterer Abgeordneter und der Fraktion DIE LINKE. – Drucksache 16/5228 – Notwendigkeit neuer biometrischer Pässe aus Sicherheitsgründen, http://dip.bundestag.de/btd/16/055/1605507.pdf, S. 1.

Antwort:

Der Staat kann nie für alle Fälle einen Missbrauch persönlicher Daten ausschließen. Wenn ausländische Behörden in der Lage sind, die elektronischen Daten aus den Pässen auszulesen, können sie damit nach den Gesetzen ihres Landes verfahren. Dabei wird der Datenschutz nicht in allen Ländern das in Deutschland bzw. der EU garantierte Niveau erreichen. Die Bundesregierung hat die Möglichkeit, durch internationale Verträge oder Verwaltungsvereinbarungen einem Missbrauch der Daten entgegenzuwirken. Derartige Vereinbarungen könnten theoretisch auch Sanktionen vorsehen. Bei weltweit derzeit rund 165 Nicht-EU-Staaten wäre der Aufwand jedoch groß.

3. Zusammenführung von Daten

Frage:

Wie kann der Staat den Bürger davor schützen, dass gespeicherte Daten wie Kontodaten, Adresse und Biometrie illegal zusammengeführt werden?

Antwort:

Daten dürfen nur **innerhalb gesetzlicher** Bestimmungen erhoben, verwendet oder übermittelt werden. Das Paßgesetz schreibt in § 16a vor, dass die „im Chip des Passes gespeicherten Daten nur zum Zweck der Überprüfung der Echtheit des Dokumentes oder der Identität des Passinhabers […] ausgelesen und verwendet werden“ dürfen. Verstöße hiergegen können nach dem Bundesdatenschutzgesetz mit einem **Bußgeld** oder einer **Geld**- und **Freiheitsstrafe** geahndet werden (§§ 43, 44 BDSG). Aus der Praxis sind Fälle bekannt, in denen **Strafgerichte** Täter eines Datenmissbrauchs verurteilt haben.[12]

4. Videoüberwachung

Frage:

Digitale Spuren hinterlässt der Bürger auch im Alltag: Schafft die Videoüberwachung an öffentlichen Plätzen wie Bahnhöfen mehr Sicherheit oder verlagert sie die Probleme nur?

12 Vgl. nur AG Düsseldorf, RDV 1986, 285.

Antwort:

Einheitliches und verlässliches **Datenmaterial** über die Wirksamkeit von Videoüberwachungsmaßnahmen[13] **liegt** nach wie vor **nicht vor**. Eine amerikanische Analyse von insgesamt 19 internationalen Einzelstudien kam zu dem Ergebnis, dass in Arealen mit Videoüberwachung im Vergleich zu Kontrollgebieten ohne Überwachung die Kriminalität um durchschnittlich 21 % verringert werden konnte. In Stadtzentren, Wohngebieten oder im öffentlichen Nahverkehr hatte die Videoüberwachung allerdings nur geringen oder keinen signifikanten Effekt.[14] Eine in Großbritannien durchgeführte Studie von insgesamt 14 Überwachungsbereichen konnte insgesamt nur eine geringe Auswirkung auf die Kriminalitätsentwicklung feststellen.[15]

Insgesamt besteht die Gefahr, **statistisch nicht erfasste** oder nicht erfassbare **Verdrängungseffekte** mit dem tatsächlichen Erfolg der Maßnahme zu verwechseln. Seriöse Untersuchungen in diesem Bereich müssen für die Annahme valider Ergebnisse eine Reihe – praktisch kaum zu leistender – **Bedingungen** erfüllen[16]:

- Die Überwachungszeiträume müssen lange genug gewählt werden, um die Gefahr kurzfristiger Ausschläge in der Statistik zu minimieren.

- Neben der überwachten Zone müssen auch angrenzende und übergreifende Gebiete mit untersucht werden, da sich Verlagerungen nicht notwendig nur auf angrenzende Straßenzüge oder Stadtteile beschränken werden.

- In die Betrachtung sind auch sonstige Veränderungen im überwachten Bereich (z. B. verkehrstechnische oder bauliche Maßnahmen in Bezug auf so genannte „Angsträume“) mit einzubeziehen.

---

13 Zur „Videoüberwachung an Verkehrsknotenpunkten in Europa“ und zur Einschätzungen des Erfolgs siehe auch die Ausarbeitung WD3 – 26/04; Zur Rechtslage bei der Videoüberwachung im öffentlichen und privaten Bereich siehe die Ausarbeitung WD 3 – 143/07.

14 Welsh/Farrington, Annals of the American Academy of Political and Social Science 587 (2003), 110ff.; dies., Crime Prevention and Community Safety: An International Journal 6 (2004), 21ff; zitiert nach Thomas Fetzer/Mark A. Zöller, Verfassungswidrige Videoüberwachung – Der Beschluss des BVerfG zur geplanten Überwachung des Regensburger Karavan-Denkmals durch Videotechnik, in: NVwZ 2007, S. 775ff.

15 Gill, Spriggs et al., The impact of CCTV: fourteen case studies, 2005 (abrufbar unter www.homeoffice.gov.uk/rds/pdfs05/hors292.pdf); zitiert nach Thomas Fetzer/Mark A. Zöller, Verfassungswidrige Videoüberwachung – Der Beschluss des BVerfG zur geplanten Überwachung des Regensburger Karavan-Denkmals durch Videotechnik, in: NVwZ 2007, S. 775ff.

16 Thomas Fetzer/Mark A. Zöller, Verfassungswidrige Videoüberwachung – Der Beschluss des BVerfG zur geplanten Überwachung des Regensburger Karavan-Denkmals durch Videotechnik, in: NVwZ 2007, S. 775ff.

- Zudem ist eine Aufgliederung nach Deliktsarten vorzunehmen, da das Aufstellen von Kamerasystemen auch dazu führen kann, dass bestimmte Straftaten erst mit den Überwachungsmaßnahmen überhaupt statistisch erfasst werden.

5. Kommunikation von Terroristen im Netz

Frage:

Terroristen organisieren sich heute über moderne Kommunikationswege wie das Internet. Können Behörden diese jederzeit nachvollziehen und unterbrechen, oder sind ihnen durch Datenschutzgesetze die Hände gebunden?

Antwort:

Zur **Strafverfolgung** dürfen die Behörden die **Telekommunikation** von Strafverdächtigen nach § 100a Strafprozessordnung **überwachen** und aufzeichnen. Hierzu gehört auch die Telekommunikation über vernetzte Rechner. Die Überwachung ist zulässig, wenn der Verdacht einer schweren Straftat vorliegt. Hierzu gehören nach § 100a Abs. 2 Nr. 1 lit. d StPO auch terroristische Straftaten. Die Befugnis der Behörden bezieht sich jedoch nur auf Telekommunikation, nicht auf Daten, die sich auf Computern des Betroffenen befinden. Der Bundesgerichtshof hat es daher für **unzulässig** erklärt, wenn Behörden einen Computer von Verdächtigen über das Netz elektronisch durchsuchen („**Online-Durchsuchung**“).[17]

Zur **Gefahrenabwehr** steht der Bundespolizei im Bereich der **Telekommunikation** derzeit nur die Möglichkeit zur Verfügung, das „nicht öffentlich **gesprochene Wort**“ abzuhören, § 28 BPolG. Die gleiche Befugnis steht auch dem Bundesamt für Verfassungsschutz[18] und dem Bundesnachrichtendienst[19] zu. Ferner können Bundesbehörden auch **Verbindungsdaten** zur Internetnutzung abfragen.[20] Den Bundesbehörden stehen aber **keine Rechtsgrundlagen** zur Verfügung, die es erlauben, die Telekommunikation von Verdächtigen über das **Netz** direkt („live“) zu **überwachen**. Als erstes Bundesland hat **Nordrhein-Westfalen** im Jahr 2006 eine Vorschrift[21] geschaffen, die der Verfassungsschutzbehörde des Landes die Befugnis zum „heimliche(n) Zugriff auf informati-

17 BGH, Beschluss vom 31. Januar 2007 - StB 18/06, NJW 2007, 930; zur „Online-Durchsuchung“ siehe auch die Ausarbeitung WD3 – 161/07 (im Intranet des Bundestages abrufbar).

18 § 8 f. Bundesverfassungsschutzgesetz vom 20. Dezember 1990 (BGBl. I S. 2954, 2970), zuletzt geändert durch § 32 des Gesetzes vom 23. November 2007 (BGBl. I S. 2590).

19 § 2a BND-Gesetz vom 20. Dezember 1990 (BGBl. I S. 2954, 2979), zuletzt geändert durch Artikel 4 u. 10 Abs. 3 des Gesetzes vom 5. Januar 2007 (BGBl. I S. 2).

20 Vgl. nur § 8a Abs. 2 Nr. 5 Bundesverfassungsschutzgesetz: Daten zu „Telediensten“.

21 § 5 Abs. 2 Gesetz über den Verfassungsschutz in Nordrhein-Westfalen, GVBl 2006, 620.

onstechnische Systeme auch mit Einsatz technischer Mittel“ gewährt.[22] Daneben erlaubt das Landesgesetz „heimliches Beobachten und sonstiges Aufklären des Internets, wie insbesondere die verdeckte Teilnahme an seinen Kommunikationseinrichtungen bzw. die Suche nach ihnen“. Das **Bundesverfassungsgericht** hat die Vorschriften des Verfassungsschutzgesetzes Nordrhein-Westfalen zur Online-Durchsuchung für **verfassungswidrig** und **nichtig** erklärt.[23] Der Erste Senat des Gerichts stellte klar, dass Online-Durchsuchungen nur vorgenommen werden dürfen, wenn tatsächliche Anhaltspunkte für eine konkrete Gefahr für ein **überragend wichtiges Rechtsgut** vorliegen. Zudem seien sie unter den Vorbehalt **richterlicher** Anordnung zu stellen. Diesen Anforderungen genüge die im nordrhein-westfälischen Verfassungsschutzgesetz getroffene Regelung nicht. Auch die in diesem Gesetz vorgesehene Ermächtigung zum heimlichen **Aufklären** des **Internet** erachtete das BVerfG für **verfassungswidrig** und nichtig. Denn sie enthalte unter anderem keine Vorkehrungen zum Schutz des **Kernbereichs privater Lebensgestaltung**.

In jedem Fall kann die Polizei eine **Kommunikation unterbrechen**, um eine Gefahr, z. B. für die Gesundheit einer Person, abzuwehren; unerheblich ist, ob sie die Telekommunikation zu Zwecken der Strafverfolgung oder zu Zwecken der Gefahrenabwehr überwacht. Für die Bundespolizei dürfte sich die Befugnis zur Unterbrechung aus § 14 Abs. 1 Bundespolizeigesetz ergeben.

6. IT-Angriffe auf Unternehmen

Frage:

Die IT wird nicht nur von Terroristen, sondern auch von Hackern genutzt. Gibt es Erkenntnisse, inwieweit Unternehmen die Attacken von Computerkriminellen, Malware und Wirtschaftsspionen fürchten müssen?

Antwort:

Der Verfassungsschutzbericht 2007 des Bundesministeriums des Innern[24] weist auf die Gefährdung durch die **Wirtschaftsspionage** hin: „In Deutschland befinden sich Wirtschaft, Wissenschaft und Spitzentechnologien im Mittelpunkt der Ausspähungs- und Beschaffungsbemühungen fremder Nachrichtendienste, aber auch von konkurrierenden

22 Sachs, Krings, Das neue „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“, JuS 2008, 481.

23 Urteil vom 27. Februar 2008, 1 BvR 370/07, 1 BvR 595/07, DÖV 2008, 459.

24 www.bmi.bund.de/Internet/Content/Common/Anlagen/Broschueren/2008/VSB__Vorabfassung, templateId=raw,property=publicationFile.pdf/VSB_Vorabfassung.pdf.

ausländischen Unternehmen.“ Presseberichten zu Folge sind auf **Rechnern** gespeicherte Daten ein typisches Ziel der Wirtschaftspionage.[25]

Die Gefahr, die von Computerkriminellen auch für die Wirtschaft ausgeht, beschäftigt den Gesetzgeber schon seit längerem: In § 202a Strafgesetzbuch hat der Gesetzgeber z. B. das **Ausspähen von Daten** unter Strafe gestellt, die **Computersabotage** in § 303b, das **Abfangen von Daten** in § 202b, **Vorbereitungshandlungen** zu Computerstraftaten in § 202c und in § 263a Strafgesetzbuch den **Computerbetrug**. Auf die Gefahr, die **Systemeindringlinge** („Hacker“) bedeuten, hat auch der **Bundesnachrichtendienst** hingewiesen, der bereits im Jahr 2000 zu diesem Thema ein Symposium veranstaltet hat.[26] Computerspione setzen dabei auch verdeckte schädigende Programme, sogenannte „Malware“, ein.[27]

Für alle **Mitgliedstaaten** der **EU** gilt der **Rahmenbeschluss** 2002/222/JI des Rates vom 24. Februar 2005 über **Angriffe auf Informationssysteme**.[28] Ziel ist die Angleichung der einzelstaatlichen Strafrechtsvorschriften über die Strafbarkeit des vorsätzlichen und unbefugten Verschaffens von Zugang zu einem Informationssystem sowie des rechtswidrigen Systemeingriffs („Hacking“). Jeder Mitgliedstaat muss seine Gerichtsbarkeit für die im Rahmenbeschluss genannten Delikte begründen und wirksame Sanktionen vorsehen, wobei bestimmte Mindesthöchststrafen bei Vorliegen bestimmter erschwerender Umstände vorgeschrieben sind. Die Kooperation der Polizeibehörden soll gewährleistet sein, wozu ein Netz operativer Kontaktstellen dient. Der deutsche Gesetzgeber hat den Rahmenbeschluss durch eine **Ergänzung** des **Strafgesetzbuches** umgesetzt und dabei zum Teil neue Straftatbestände geschaffen.[29]

[redacted]

25 www.faz.net/s/RubEC1ACFE1EE274C81BCD3621EF555C83C/Doc~E4816CA3D291049369EA4FBA4B4C40A56~ATpl~Ecommon~Scontent.html?rss_aktuell.

26 www.bnd.de/cln_099/nn_736416/DE/Unser__Auftrag/Schwerpunkte/Information__Warfare/Information__Warfare__node.html?__nnn=true.

27 Ernst, Hacker und Computerviren im Strafrecht, DS 2004, 14.

28 ABl. Nr. L 69 vom 16. März 2005, S. 67.

29 Pressemitteilung des BMJ vom 20. September 2006, Besserer Schutz vor Hackern, Datenklau und Computersabotage, www.bmj.bund.de/enid/42dea3031ea0518f5b9e7ea7f0f66c63,7b4816707265737365617274696b656c5f6964092d0932353638093a096d795f79656172092d0932303036093a096d795f6d6f6e7468092d093039093a095f7472636964092d09333630/Presse/Pressemitteilungen_58.htm.