Schriften zum Öffentlichen Recht

Band 1387

Der Schutz personenbezogener Daten bei der Auslandsaufklärung durch Bundeswehrsoldaten

Von

Annelie Siemsen

Duncker & Humblot · Berlin

ANNELIE SIEMSEN

Der Schutz personenbezogener Daten bei der Auslandsaufklärung durch Bundeswehrsoldaten

Schriften zum Öffentlichen Recht

Band 1387

Der Schutz personenbezogener Daten bei der Auslandsaufklärung durch Bundeswehrsoldaten

Von

Annelie Siemsen

Duncker & Humblot · Berlin

Die Bucerius Law School – Hochschule für Rechtswissenschaft
hat diese Arbeit im Jahr 2018
als Dissertation angenommen.

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in
der Deutschen Nationalbibliografie; detaillierte bibliografische Daten
sind im Internet über http://dnb.d-nb.de abrufbar.

Fremddatenübernahme: 3w+p GmbH, Rimpar
Druck: CPI buchbücher.de gmbh, Birkach
Printed in Germany

ISSN 0582-0200
ISBN 978-3-428-15524-8 (Print)
ISBN 978-3-428-55524-6 (E-Book)
ISBN 978-3-428-85524-7 (Print & E-Book)

Gedruckt auf alterungsbeständigem (säurefreiem) Papier
entsprechend ISO 9706 ♾

Internet: http://www.duncker-humblot.de

Vorwort

Datenschutz wird allzu häufig als lästig und obsolet betrachtet oder als ineffektiv abgetan. Denn viele stellen ihre Daten ohnehin den sozialen Netzwerken freiwillig zur Verfügung und die rechtliche Umsetzung des Persönlichkeitsschutzes hinkt den technischen Möglichkeiten zu Eingriffen in eben jenes weit hinterher. Dabei wird übersehen, zu welchem Grad die Verarbeitung und Nutzung personenbezogener Daten unsere Gesellschaft und unser persönliches Leben durchziehen. Den entscheidenden Einfluss auf den Verbleib und die Nutzung dieser Daten haben wir längst verloren. Gleichzeitig ist das Recht auf informationelle Selbstbestimmung, aus dem der Datenschutz abgeleitet wird, nach wie vor ein wesentlicher Teil unseres Persönlichkeitsrechts.

Die genannten Bedenken und Vorwürfe gegenüber dem Datenschutzrecht einfach damit abzutun, dass das BVerfG den Schutz des informationellen Rechts als eine wichtige Aufgabe des Gesetzgebers und der Verwaltung einstuft, greift zu kurz. Die eingangs aufgezählten Einwendungen enthalten vielmehr entscheidende Anhaltspunkte dafür, wie der Schutz verbessert, umsetzbar und effektiv ausgestaltet werden kann. Wir befinden uns in einer Umbruchphase, in der die Bedeutung von Daten und deren Schutz neu definiert werden. Diese Definition wird zwar auch durch die gesetzgebende Gewalt vorgenommen, doch in entscheidendem Maße haben die Bürger, die Internetnutzer Einfluss darauf, wie weit sie gehen wollen. Nicht ohne Grund werben die größten Internetfirmen seit einiger Zeit damit, dass unsere Daten bei ihnen sicher seien, dass wir selbst bestimmen würden, was mit ihnen geschieht und wofür sie verwendet werden. Nichtsdestotrotz obliegt dem Gesetzgeber bislang auch weiterhin die Pflicht, das Recht auf informationelle Selbstbestimmung zu schützen. Soweit in dieser Umbruchphase nicht vorhergesehen werden kann, welches Ausmaß die Datenverarbeitung annehmen kann, hat der Gesetzgeber nach dem Vorsichtsprinzip zu handeln. Denn eines ist sicher: Technische Entwicklungen und deren rechtlicher Rahmen können kaum eingeschränkt, geschweige denn rückgängig gemacht werden. Sind Datenerhebungen und Datenverwendungen erst einmal ohne Einschränkungen erlaubt, wird es kaum möglich sein, diese Entwicklung zurückzudrehen und einen strikteren Datenschutz durchzusetzen. Mitunter mag der Eindruck entstehen, die Gesellschaft würde keinen Wert auf Rückzugsräume legen, weil sie ohnehin ununterbrochen online ist. Doch jeder braucht einen Raum für seine / ihre Privatsphäre. Genauso wie wir unsere Wohnungstür zumachen, wollen wir entscheiden können, wann wir sichtbar sind und wann wir uns zurückziehen, ohne dass andere unsere Handlungen beobachten. Nicht nur für unsere persönliche Entwicklung und unser Wohlergehen ist dies von Bedeutung, sondern auch für unsere de-

mokratische Gesellschaft. *Welzer* bringt die Bedeutung der Privatsphäre wie folgt auf den Punkt:

> „Demokratie setzt voraus, dass es Bürgerinnen und Bürger gibt, die für ihre Angelegenheiten und das Gemeinwesen eintreten und es gestalten. Das können sie aber nur, wenn es eine Trennung von öffentlich und privat gibt: (…) Als Sphäre, in der Menschen tun und lassen können, was sie wollen, ohne dass eine Öffentlichkeit davon auch nur Kenntnis gewinnen könnte, bildet Privatheit jenen Seinsbereich, in dem sich Sichtweisen bilden und entfalten, Persönlichkeiten entwickeln und Standpunkte ausprobieren lassen."[1]

Bei alledem muss sich unsere Demokratie gleichzeitig gegen Bedrohungen wehren. Datenschutz steht deshalb immer auch im Konflikt zwischen dem Freiheitsanspruch des Einzelnen und den Sicherheitsbestrebungen des Staates. Die Freiheit des Einzelnen meint dabei die Möglichkeit, über die Verwendung der eigenen Daten selbst bestimmen zu können. Die Sicherheitsbestrebungen des Staates umfassen die Bemühungen, Sicherheit für die Bürger und den Bestand des Staates zu schaffen, indem präventiv gegen feindliche Handlungen vorgegangen wird. Diese Konfliktlage wird mitunter auch als Schnittstelle betrachtet, innerhalb derer die Freiheit nicht ohne Sicherheit und die Sicherheit nicht ohne Freiheit bestehen kann. Dieser Betrachtungsweise als Schnittstelle wohnt der Anspruch inne, sowohl die Freiheit als auch die Sicherheit vergrößern zu können. Dementsprechend versteht auch die vorliegende Arbeit den Datenschutz als Möglichkeit, die freiheitsrechtlichen und die sicherheitsrechtlichen Bestrebungen unserer Gesellschaft in einen Ausgleich zu bringen. Unter Zugrundelegung dieses Verständnisses von Datenschutz greift die Arbeit eine Anwendungssituation der datenschutzrechtlichen Vorschriften heraus. Gegenstand der Betrachtung ist die bislang wenig untersuchte Konstellation, in der Bundeswehrsoldaten im Rahmen der Auslandsaufklärung tätig werden. Die hierbei getroffenen, grundlegenden Wertungen lassen sich auf weitere Konstellationen übertragen, bei denen Sicherheit und Freiheit ausgeglichen werden sollen.

Ich bedanke mich bei meinem Doktorvater Professor Dr. Jasper Finke für die hervorragende Betreuung und bei meinem Zweitgutachter Prof. Dr. Markus Kotzur. Ich bedanke mich außerdem bei meiner Familie für eure grenzenlose Unterstützung und Liebe. Mein größter Dank gebührt all den Frauen, die vor mir kamen.

Annelie Siemsen

[1] *Welzer*, Schluss mit der Euphorie!, Die Zeit, Ausgabe No. 18 v. 27.04.2017.

Inhaltsverzeichnis

Einleitung

Personenbezogene Daten durchziehen alle Bereiche unseres Handelns, weshalb sie auch verschiedene Rechtsbereiche betreffen.[1] Die vorliegende Arbeit beschäftigt sich mit dem Gebrauch personenbezogener Daten zur Identifizierung von Individuen durch deutsche Soldaten zum Zweck der Auslandsaufklärung. Die Auslandsaufklärung umfasst die Gewinnung und Auswertung von Erkenntnissen über das Ausland, die von außen- und sicherheitspolitischer Bedeutung sind.[2] Geläufig ist der Einsatz von Soldaten für Aufklärungsarbeiten durch den Militärischen Abschirmdienst (MAD), der das Ziel verfolgt, die Truppen im Ausland zu sichern.[3] Allerdings ist die Bedeutung des MAD in den letzten Jahren gesunken und ein anderer Akteur trat in diesem Zusammenhang auf die Bühne: Der Bundesnachrichtendienst (BND) hat faktisch die Aufgabe der Außensicherung der Truppen übernommen.[4] Er macht sich dabei das Potenzial der für Aufklärungsarbeit qualifizierten Soldaten zunutze. Auf Grundlage der sog. Rahmenvereinbarung zwischen dem Bundesministerium der Verteidigung und dem Bundeskanzleramt in der Fassung vom 13. 01. 1998 sowie der Richtlinie über die Verwendung von Truppenoffizieren beim BND vom 03. 08. 2001 werden Bundeswehrsoldaten an den BND überstellt. Die Angaben, wie viele Soldaten über diese Struktur beim BND beschäftigt sind, schwanken zwischen 10 % und 30 % der BND-Mitarbeiter.[5]

---

[1] Vgl. nur § 1 BDSG; § 10 BVerfSchG; § 3 BNDG; § 630 f BGB; §§ 67a-78 SGB X; § 203 StGB; *Bodenschatz*, Der europäische Datenschutzstandard (2010), S. 15, 135, 162; *Roßnagel*, Modernisierung des Datenschutzrechts für eine Welt allgegenwärtiger Datenverarbeitung, MMR 2005, 71 (71).

[2] § 1 Abs. 2 S. 1 BNDG.

[3] Vgl. § 62 Abs. 1 SG; § 14 Abs. 1 S. 3, Abs. 2 S. 3, Abs. 6 S. 2 und 3 MADG.

[4] http://www.sueddeutsche.de/politik/bilanz-des-bundesnachrichtendiensts-knapp-anschlaege-auf-bundeswehrsoldaten-verhindert-1.2203724 (zuletzt abgerufen am 21. 05. 2017); deshalb werden auch immer wieder Stimmen nach der Abschaffung des MAD laut, wogegen sich regelmäßig der / die Bundesminister/in der Verteidigung wendet, http://www.welt.de/politik/deutschland/article13396754/MAD-der-geheimste-aller-Geheimdienste.html (zuletzt abgerufen am 21. 05. 2017).

Der MAD ist deshalb kein eigenständiges Untersuchungsobjekt dieser Arbeit.

[5] http://www.berliner-zeitung.de/archiv/bnd-beamte-im-irak-waren-auch-angehoerige-der-bundeswehr-untersuchungsausschuss-rueckt-naeher-uniform-unter-der-agentenkluft,10810590,10353496.html (zuletzt abgerufen am 21. 05. 2017); zum Amt für Militärkunde siehe https://de.wikipedia.org/wiki/Amt_f%C3%BCr_Milit%C3%A4rkunde (zuletzt abgerufen am 21. 05. 2017). Bundeswehrsoldaten unterstützen den BND außerdem bei der Datenauswertungen und Übersetzungsarbeiten, http://www.zeit.de/politik/deutschland/2015-03/bnd-bundeswehr-daten-ueberwachung (zuletzt abgerufen am 21. 05. 2017); https://netzpolitik.org/2015/bundesnachrichtendienst-gibt-massenhaft-inhaltsdaten-an-die-bundeswehr-juristen-halten-das-fuer-

Doch nicht nur in diesem Bereich werden die Soldaten mit der Bearbeitung personenbezogener Daten betraut. Auch innerhalb bundeswehreigener Strukturen ist der verstärkte Gebrauch solcher Daten zu beobachten, was maßgeblich durch den veränderten Aufgabenbereich der Bundeswehr bedingt ist. Die ursprüngliche Aufgabe der Bundeswehr – die Landesverteidigung[6] – wurde in großen Teilen durch friedenserhaltende und friedenserzwingende Einsätze in anderen Staaten abgelöst.[7] Neben Kampfmaßnahmen werden die Soldaten dort zu einem wesentlichen Teil für die Aufrechterhaltung der öffentlichen Ordnung eingesetzt. Für letztere Tätigkeit sind personenbezogene Daten des verbündeten Personals und der Arbeitskräfte im jeweiligen Land, der gegnerischen Partei und auch der Zivilbevölkerung von entscheidender Bedeutung. Die Identifizierung von Personen anhand solcher Daten ist essentiell, da eine Zuordnung nicht wie früher durch eine sichtbare Zugehörigkeit zu einer Gruppe von Soldaten oder durch Informanten erfolgen kann. So tritt der „Gegner" heute weniger als einheitliche Streitmacht auf, als vielmehr in kleinen Gruppen oder als Einzelpersonen, die häufig in der Zivilbevölkerung untertauchen und unerkannt bleiben, bis sie die sicherheitsgefährdende Handlung ausführen. Eine erfolgreiche Identifizierung solcher Personen wird durch die Verwendung personenbezogener Daten erheblich vereinfacht. Als Aufgabe der deutschen Soldaten im Ausland kommen zahlreiche Grenzschutzeinsätze und Pirateriebekämpfungen hinzu, bei denen Daten der Betroffenen erhoben werden. Auch diese Tätigkeiten zielen auf die Identifizierung der Personen und die Qualifikation ihres Gefahrenpotenzials ab.

Die Rechtsfragen, die sich stellen, wenn deutsche Soldaten innerhalb der Streitkräfte oder beim BND mit Datenerhebung, -speicherung, -verwendung und -übermittlung betraut werden, sind bislang kaum untersucht worden. Jene nach Umfang und Qualität des Datenschutzes greift die vorliegende Arbeit auf.

---

illegal/ (zuletzt abgerufen am 21.05.2017). Der BND arbeitet wiederum den Streitkräften zu, indem er ihnen Informationen über Personenziele mitteilt, http://www.t-online.de/nachrichten/deutschland/militaer-verteidigung/id_72323542/bundeswehr-in-afghanistan-bnd-lieferte-daten-zu-personenzielen.html (zuletzt abgerufen am 21.05.2017).

[6] „Die Landesverteidigung prägt das Urbild des grundgesetzlichen Verteidigungsauftrags", *Depenheuer,* in: Maunz / Dürig, GG 78. EL (2016), Art. 87a Rn. 107. Zur Änderung der Aufgaben der Bundeswehr *Wieland*, Verfassungsrechtliche Grundlagen polizeiähnlicher Einsätze der Bundeswehr, in: Fleck, Rechtsfragen der Terrorismusbekämpfung durch Streitkräfte (2004), 167 (84); ausführlich zur Verwendung der deutschen Streitkräfte *Wiefelspütz*, Der Auslandseinsatz der Bundeswehr und das Parlamentsbeteiligungsgesetz (2008), S. 11 ff.

[7] Dabei wird die deutsche Sicherheit lediglich mittelbar verteidigt. „Die Sicherheit Deutschlands wird auch am Hindukusch verteidigt", betonte der damalige Verteidigungsminister Peter Struck (SPD) im Dezember 2002, http://www.heise.de/tp/artikel/13/13778/1.html (zuletzt abgerufen am 21.05.2017).

A. Thesen der Arbeit

Auch wenn der in Deutschland geltende Datenschutz weit davon entfernt ist, dem Persönlichkeitsrecht des Einzelnen umfassend Schutz zu vermitteln, so kann er doch im internationalen Vergleich als ausgereift bezeichnet werden; dies nicht zuletzt, weil er die menschenrechtlichen Standards umsetzt.[8] Er beruht jedoch maßgeblich auf einer bestimmten Anwendungsbedingung – dem Inlandssachverhalt: Dem Grundkonzept des Datenschutzes liegt die Konstellation zugrunde, dass eine deutsche öffentliche Stelle innerhalb der Bundesrepublik personenbezogene Daten von Personen erhebt und verarbeitet, die sich ebenfalls im Bundesgebiet aufhalten. Wendet man die datenschutzrechtlichen Regeln auf die Auslandaufklärung an, lassen sich folgende These aufstellen, die in dieser Arbeit untersucht werden.

Auslandssachverhalt. Die Auslandsaufklärung spielt sich auch innerhalb fremder Staatsgebiete ab und bezieht sich auf Tätigkeiten deutscher Stellen außerhalb der Bundesrepublik, bei denen Personen überwacht werden, die sich (auch) außerhalb des Bundesgebiets aufhalten. Daraus ergeben sich abweichende Anwendungsbedingungen, unter denen der Datenschutz gemäß den grund- und menschenrechtlichen Forderungen den Anspruch erhebt, Wirkung zu entfalten. Unter diesen Bedingungen können die Regeln zum Datenschutz nur eingeschränkt Schutz vermitteln. Dies ermöglicht den beteiligten Akteuren, bestimmte argumentative Strategien zu verwenden, um eine Anwendung der bestehenden Regeln zu vermeiden, was unten ausführlich dargestellt werden wird. So gibt es zwar datenschutzrechtliche Regeln, die sich auf die Auslandsaufklärung beziehen. Doch gleichen sie in ihrer rechtlichen Konstruktion denjenigen Regeln, die für Inlandssachverhalte konzipiert wurden. Aufgrund einer fehlenden Anpassung an die speziellen Umstände der Auslandskonstellationen ist ein effektiver Datenschutz bei der Auslandsaufklärung deshalb kaum gegeben. Diese abweichenden Anwendungsbedingungen sind die Grundlage der These 1:

These 1: Der Datenschutz kann Sachverhalte mit Auslandsbezug nur unzureichend aufgreifen.

Aus dieser ersten These lassen sich folgende Unterthesen ableiten:

Ideell geformtes Schutzobjekt. Im Zeitalter der Informationstechnologie hat das Schutzobjekt „personenbezogenes Datum“, als Teil des Persönlichkeitsrechts, eine herausgehobene Bedeutung. Die Beeinträchtigungen dieses Rechts gleichen den Eingriffen in ähnlich ideell gestaltete Schutzobjekte.[9] Statt jedoch diejenigen Wertungen auf Datenvorgänge zu übertragen, die hinsichtlich anderer ideell geformter Schutzobjekte bestehen, orientiert sich die Bewertung von Datenvorgängen zu

[8] Vgl. *Schaller*, Detaillierte Regeln für die Auslandsüberwachung, SWP-Aktuell 66 (Oktober 2016), S. 2.

[9] Vgl. *Milanovic*, Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age, Harv. Intl. Law J., Vol. 56 No. 1 (2015), 81 (120).