



LANDTAG
NORDRHEIN-WESTFALEN
10. WAHLPERIODE

ZUSCHRIFT
10/ 3052

**Gewerkschaft
Öffentliche Dienste,
Transport
und Verkehr**

ÖTV-Bezirksverwaltung NW 1,
Postfach 37 40, 4000 Düsseldorf

An den
Präsidenten des Landtages NW
Postfach 1143

4000 Düsseldorf 1

Bezirksverwaltung
Nordrhein-Westfalen 1

Fachausschuß Richter und
Staatsanwälte

Postfach 3740
Willi-Becker-Allee 10
4000 Düsseldorf 1

Ihre Zeichen	Ihre Nachricht	Unser Zeichen	☎-Durchwahl	Tag
		ka/kü	(02 11) 3 87 92 25	06.11.1989

Gesetz zur Fortentwicklung des Datenschutzes im Bereich der Polizei und der Ordnungsbehörden (GFDPol)

Unser Schreiben vom 08.06.1989

Sehr geehrter Herr Präsident,

wir beziehen uns auf unser obiges Schreiben und nehmen zu dem geplanten Gesetzesvorhaben wie folgt Stellung:

Die Gewerkschaft ÖTV begrüßt den Ansatz, jede Form der Datenerhebung als Eingriffsmaßnahme zu qualifizieren und ihre Zulässigkeit deshalb von einer ausdrücklichen gesetzlichen Ermächtigung abhängig zu machen. Damit wird eine der Forderungen des Bundesverfassungsgerichts in seinem Urteil zum Volkszählungsgesetz beachtet. Allerdings wollte das Bundesverfassungsgericht dadurch eine Begrenzung, Einschränkung erreichen. Der GFDPol-Entwurf in seiner derzeitigen Fassung erklärt jedoch letztlich vornehmlich das ausdrücklich für zulässig, was bisher ohnehin schon praktiziert wurde. Er hat also lediglich die Funktion, die alte Praxis zu legalisieren. Das erfüllt die Forderungen des Bundesverfassungsgerichts nur formal, widerspricht jedoch weithin dem Geist der Entscheidung. Wir halten diese Legalisierungswirkung für äußerst bedenklich und zudem gefährlich für die rechtsstaatliche Kultur. Denn wenn nun ausdrücklich erlaubt ist, was man bislang nur in einer rechtlichen Grauzone und mit einem "schlechten Gewissen" machen konnte, ist zu erwarten, daß nunmehr viele Eingriffe um so häufiger und intensiver vorgenommen werden. Vorangestellt sei, daß wir nicht die Absicht haben, der Polizei die notwendige Arbeit zu erschweren. Im Rahmen des polizeilich Erforderlichen sollen ihr auch präzise Ermächtigungen zur Verfügung

stehen. Diese sollen im Rahmen des möglichen auch so einfach und klar formuliert sein, daß ihre Beachtung auch in polizeilichen Eilsituationen nicht unnötig erschwert ist. Jedoch geht der GFDPol-Entwurf an manchen Stellen weit über dieses Ziel hinaus und ist vielfach so unbestimmt gefaßt, daß ein Mißbrauch der eingeräumten Befugnisse nur schwerlich verhindert wird. Zudem muß insbesondere bei schweren und schwersten polizeilichen Eingriffen in die - im Rechtsstaat des Grundgesetzes auch dem Rechtsbrecher zustehende - informationelle Selbstbestimmung genau abgewogen werden, ob der Schaden für den Rechtsstaat nicht größer ist als der maximal mögliche Nutzen für die polizeiliche Arbeit. Rechtsstaat bedeutet auch, nicht alles technisch Mögliche zuzulassen, sondern sich im Interesse der Freiheit des Einzelnen teilweise selbst zu beschränken.

Im einzelnen:

1) Verwertungsverbot

Es muß ein generelles und umfassendes Verwertungsverbot für alle nicht rechtmäßig erlangten Daten eingefügt werden. Denn wenn die Polizei die Daten nachher gar nicht verwerten kann und darf, entfällt auf Dauer auch eine Motivation, sie sich unter Überschreitung rechtlicher Grenzen zu beschaffen. Dies Verwertungsverbot kann sich nicht auf die von der Polizei selbst rechtswidrig erhobenen Daten beschränken, sondern muß auch die der Polizei rechtswidrig übermittelten oder sonstwie rechtswidrig zur Kenntnis gelangten Daten erfassen.

Formulierungsvorschlag: *Personenbezogene Daten, die unter Verstoß gegen sich aus diesem oder anderen Gesetzen ergebende Vorschriften erhoben, übermittelt oder sonstwie erlangt worden sind, dürfen nicht gespeichert, verändert, übermittelt, abgeglichen oder sonstwie verarbeitet oder genutzt werden. Sie sind unverzüglich zu löschen.*

2) Altbestände

Das Gesetz erfaßt an keiner Stelle, was mit den bei seinem Inkrafttreten bei der Polizei schon vorhandenen Datenbeständen geschehen soll. Hierzu muß eine Regelung geschaffen werden, die die gesamten alten Bestände innerhalb einer kurz zu bemessenden Frist einer Prüfung daraufhin unterzieht, ob sie nach dem dann geltenden Recht rechtmäßig erlangt sind. Anderenfalls ist ihre sofortige Löschung anzuordnen und durchzuführen.

3) Unterrichtung des Datenschutzbeauftragten

Für die Mittel der Datenerhebung, die schwere und schwerste Eingriffe in die informationelle Selbstbestimmung enthalten (längerfristige Observation, verdeckter Einsatz technischer Mittel zur Anfertigung von Bild- oder Tonaufzeichnung, verdeckte Ermittler, Informanten) erscheint es sinnvoll, wenn neben den schon vorgesehenen Verfahrensvoraussetzungen (Behördenleiter/Richter) eine generelle Pflicht zur Unterrichtung des Landesdatenschutzbeauftragten eingeführt wird. Diese Unterrichtung

zwingt die Polizei, ihre Maßnahme gegenüber einer weiteren externen Stelle und damit auch gegenüber sich selbst zu legitimieren (rechtsstaatliche Warnfunktion). Eine Beeinträchtigung der rechtmäßigen Tätigkeit der Polizei kann dadurch nicht auftreten, denn der Datenschutzbeauftragte soll die polizeiliche Maßnahme nicht etwa genehmigen oder billigen müssen, sondern nur obligatorisch Kenntnis davon erhalten.

4) Auskunftsverweigerung/§136a StPO

Die Auskunftsverweigerungsrechte und der Ausschluß verbotener Vernehmungsmethode waren im Regierungsentwurf ursprünglich enthalten (vgl § 8b(3)). Ihre ersatzlose Streichung ist unerklärlich. Insbesondere auf eine entsprechende Anwendbarkeit des § 136a StPO kann nicht verzichtet werden, zumal die durch eine Befragung erlangten Daten nach dem derzeitigen Stand des Entwurfes ohne Einschränkung auch gespeichert und weiterverarbeitet werden dürfen, also selbst dann, wenn sie durch Drohung oder Täuschung erlangt worden sind.

5) Aufgabenerweiterung

Die Erweiterung des § 1(1) in S. 2 läßt sich keineswegs allein damit rechtfertigen, es sollte klar herausgestellt werden, daß die nordrhein-westfälischen Ordnungsbehörden keine Kriminalakten führen dürfen. Vielmehr wird damit der Aufgabenbereich der Polizei auch ins Vorfeld einer konkreten Gefahr ausgedehnt; damit wird ein ganzes Feld von Aufgaben im Bereich v o r der klassischen Gefahrenabwehr eröffnet. Es ist zweifelhaft, ob eine solche Vorverlegung der polizeilichen Prävention in dieser Weite sinnvoll ist.

Dabei liegt die Bedeutung vor allem darin, daß in zahlreichen Eingriffsbefugnissen zur Datenverarbeitung auf die Aufgabenzuweisung und damit auf die weite Aufgabenzuweisung in § 1(1)2 zurückgegriffen wird. Es werden dadurch die als Eingriffe zu qualifizierenden Maßnahmen trotzdem gleich wieder für zulässig erklärt, und zwar schon dann, wenn sie der Wahrnehmung der - erweitert gefassten - Aufgabe der Polizei dienen. Die rechtsstaatlich gebotene Trennung von Aufgaben-Normen und Befugnis-Normen wird damit zugleich letztlich unterlaufen. Das war nicht der Sinn des Bundesverfassungsgerichts-Urteils. Im Ergebnis ist man dann wieder da, wo man vor der Novelle stand: Damals wurde Datenverarbeitung als schlicht hoheitliches Handeln auf die Aufgabenzuweisung gestützt. Jetzt ist es als Eingriff anerkannt, aber trotzdem und sogar ausdrücklich zulässig, also ganz legal.

6) Katalog der erheblichen Straftaten

Der in § 8(3) aufgenommene Katalog von erheblichen Straftaten darf nicht dadurch aufgeweicht werden, daß einleitend ein "insbesondere" eingefügt wird.

Wichtig ist auch, daß die Definition der erheblichen Straftaten auf das Merkmal der "gewohnheitsmäßigen" Begehung verzichtet, wie es der derzeitige Entwurf durchweg neben den Merkmalen "gewerbs- und bandenmäßig" verwendet. Denn während letztere wirklich - wenn auch sehr weite - Merkmale von organisierter Kriminalität enthalten, die doch mit den schwereren Eingriffsmitteln bekämpft werden soll, erfaßt das

Merkmal "gewöhnheitsmäßig" auch den völlig isoliert handelnden Einzeltäter. Das ermöglicht in letzter Konsequenz die Ausspähung jedes (strafbaren) sozial abweichenden Verhaltens und kann in besonderem Maße politisch mißbraucht werden. Eine Rechtfertigung für derart massive Eingriffe vermögen wir nur bei echter organisierter Kriminalität zu sehen.

7) Sach-/personenbezogene Daten

Es bedarf der gesetzlichen Klarstellung, daß personenbezogene Daten diese Eigenschaft auch dann (noch) haben, wenn sie in einer vornehmlich nach Sachkriterien sortierten Datei wie z.B. dem System SPUDOK gespeichert sind.

8) Auskunftspflicht, § 9(2)2

Die Auskunftspflicht ist in § 9(2)2 sehr unklar geregelt. Es ist nicht erkennbar, ob etwa der Störer zur Auskunft hinsichtlich der diese seine Eigenschaft begründenden Tatsachen verpflichtet ist oder ob nur sich aus anderen Gesetzen ergebende "Handlungspflichten" gemeint sein sollen. Wenn spezialgesetzliche Auskunftspflichten gemeint sein sollten, ist ihre Bezeichnung als *Handlungspflichten* mißverständlich. Wenn eine Auskunftspflicht gemeint ist, die aus der Störereigenschaft resultiert, sind Auskunftsverweigerungsrechte einzuführen.

9) Belehrung über Auskunftspflicht, § 9(4)

Die Einschränkung der Pflicht zur Belehrung über die Auskunftspflicht und ihre Grenzen im letzten Halbsatz des § 9(4) ist zu weit gefaßt. Die Belehrung muß stets erfolgen; die Ausnahmen können allenfalls für Personen in Betracht kommen, die nach § 9(2)2 einer spezialgesetzlichen Auskunftspflicht unterliegen.

10) Versammlungs-Kontrollstelle

Die Möglichkeit, eine Kontrollstelle auf dem Weg zu einer öffentlichen Versammlung einzurichten (§ 9(1) Nr. 4, letzter Fall), ist zu streichen. Denn abgesehen davon, ob man eine solche Maßnahme überhaupt für zulässig halten kann, kann sie aus kompetenzrechtlichen Gründen nicht in dieser Weise geregelt werden. Denn der Weg zur Versammlung gehört nach der Rechtsprechung des Bundesverfassungsgerichts schon in den Schutzbereich des Art. 8 GG. Damit ist in erster Linie der Bund zuständig (Versammlungsrecht).

11) Speicherung von Razzia-Daten

Die Identitätsfeststellung nach § 12(1) Nr. 3 ermöglicht die sog. Fischzug-Razzia weit im Vorfeld jeder konkreten Gefahr oder der Aufklärung einer Straftat. Dies ist allenfalls dann hinnehmbar, wenn ausdrücklich geregelt wird, daß die dabei gewonnenen Daten nur dann gespeichert (und weiter verarbeitet) werden dürfen, soweit sich bei der Razzia Anhaltspunkte für eine individuell zuzuordnende Straftat oder eine anhaltende Gefahr ergeben haben. Soweit dies nicht der Fall ist, ist die Speicherung zu verbieten bzw die unverzügliche Löschung vorzusehen.

12) Andere Personen in § 15

In § 15(1) ist die Befugnis, auch völlig Unbeteiligte zu filmen, tatbestandlich nicht näher eingegrenzt. Zur Klarstellung sollte aufgenommen werden, daß schon ihre Erfassung auf Bild- oder Tonträgern nur in dem technisch unvermeidbaren Umfange zulässig ist.

13) Kurzfristige Observation

Nach dem derzeitigen Stand des Entwurfes soll die weniger als 24 Stunden dauernde, sog. kurzfristige Observation in § 16(4) ausdrücklich geregelt werden. Das ist an sich zu begrüßen, weil auch darin eindeutig ein Eingriff liegt. Jedoch soll sie schon zulässig sein, wenn sie nur für die Erfüllung der - erweiterten - polizeilichen Aufgabe erforderlich ist. Damit wird die Observation schon weit vor der Schwelle der konkreten Gefahr für zulässig erklärt. Dies erscheint in dieser Weite nicht gerechtfertigt, zumal Behördenleitervorbehalt und Unterrichtungspflicht hier nicht gelten sollen.

14) Richtervorbehalte

Die Richtervorbehalte in den §§ 17(3) und 18(3) sind jetzt so formuliert, daß es einer richterlichen Entscheidung nicht mehr bedarf, wenn die Polizei annehmen kann, daß sie ihren Einsatz schneller beendet hat, als ein Richter entscheiden könnte. Das prämiert den "schnellen Einsatz", der einer richterlichen Entscheidung zuvorkommt. Dies kann auch nicht mit einer ähnlichen Regelung im Bereich der Freiheitsentziehung gerechtfertigt werden. Dort hat diese Regelung den Grund, den Betroffenen nicht etwa deshalb weiter in Gewahrsam zu halten, weil der Richter noch nicht entschieden hat. Der Eingriff in die Rechte des Einzelnen würde sonst durch die Notwendigkeit einer richterlichen Entscheidung noch verschärft. Das ist auf die richterliche Entscheidung über den Einsatz verdeckter Kameras und Mikrophone nicht übertragbar.

Das Argument, das Fehlen einer amtsrichterlichen Entscheidung eröffne die Möglichkeit verwaltungsgerichtlicher Kontrolle, ist zwar richtig. Jedoch scheint der generelle Richtervorbehalt rechtsstaatlich sicherer, zumal sich jeder Betroffene auch vor dem Verwaltungsgericht nur gegen Eingriffe wehren kann, die ihm bekannt geworden sind.

15) Kontakt- und Begleitpersonen

Die Ausdehnung der Erhebungsbefugnis auf die Kontakt- und Begleitpersonen (in jeweils Abs.1 S.1 Nr. 2 der §§ 16, 17, 18 und 19) ist unverhältnismäßig weit.

Jedenfalls sollte die ganze Nr. 2 auf Straftaten mit mindestens erheblicher Bedeutung i.S.v. § 8(3) beschränkt werden. In jedem Fall muß die Befugnis, die Daten auch der Kontakt- und Begleitpersonen zu speichern und weiter zu verarbeiten, ausdrücklich und zweifelsfrei geregelt und dabei wirksam begrenzt werden.

16) Verdeckte Ermittler

Der Einsatz verdeckter Ermittler zur vorbeugenden Verbrechensbekämpfung ist besonders problematisch. Denn von diesen kann eine er-

hebliche Anheizung der Szene ausgehen, die neue Straftaten erst provoziert (agent provocateur). Auch der verdeckte polizeiliche Scheinkäufer initiiert zunächst einmal ein Geschäft.

Dem steht ein sehr kleiner Nutzen gegenüber. Denn die Aufklärung gerade der organisierten Kriminalität im Bereich der Rauschgiftszene ist trotz des Einsatzes verdeckter Ermittler sehr gering. Dem rechtsstaatlichen Schaden steht also ein sehr geringer Nutzen gegenüber. Deshalb ist der verdeckte Ermittler im Bereich der Gefahrenabwehr (Polizeirecht) an sich entbehrlich.

Damit ist nicht gesagt, daß es ihn nicht als Mittel der repressiven Straftataufklärung auf der Grundlage des Strafprozeßrechtes und ab der Schwelle eines konkreten Tatverdacht es geben soll!

Wenn man ihn den schon als polizeiliches Mittel zuläßt, muß aber sein Einsatzbereich sehr viel stärker eingeschränkt werden. Nach dem Entwurf soll der Einsatz zur vorbeugenden Bekämpfung jedes gewerbs-, bandenmäßigen und auch gewohnheitsmäßigen Vergehens zulässig sein. Das deckt beispielsweise auch die Einschleusung eines verdeckten Ermittlers in nach polizeilicher Sicht verdächtige Szenen ab, um etwa die weitere Begehung von Schwarzfahrten mit der Straßenbahn oder das Besprühen von Gebäuden zu verhindern (§ 20(2) Nr. 2).

17) Speicherungsbefugnis

Der Tatbestand des § 24 (1) schränkt die Befugnis der Polizei zur Speicherung erhobener oder sonstwie erlangter Daten entgegen seinem Wortlaut tatsächlich nicht ein. Denn er bindet die Befugnis ausschließlich an die Erfüllung der - erweiterten - Aufgabe der Polizei (§1(1)). Damit besagt er etwas juristisch selbstverständliches, nämlich daß auch die Polizei grundsätzlich nicht außerhalb ihres Zuständigkeitsbereiches handeln darf. Eine inhaltliche Begrenzung der Speicherung wird damit jedoch nicht normiert.

Diese müßte - nach dem Grad des Eingriffs bei der Erhebung gestaffelt - entweder im § 24 zusammenhängend oder bei der jeweiligen Erhebungsermächtigung aufgenommen werden.

18) Datenübermittlung

Die Datenübermittlung durch (§§ 27 - 29) und an (§ 30) die Polizei ist in den jeweiligen Vorschriften wiederum inhaltlich entgegen dem Anschein nicht beschränkt, weil stets nur auf die Aufgabenerfüllung (und damit auf die Zuständigkeitsregelung) Bezug genommen wird.

Die Regelung über die Übermittlung von Daten an die Polizei darf sich inhaltlich nicht darauf beschränken, daß die Daten - gleich wie sie erhoben wurden! - von der Polizei zur Aufgabenerfüllung benötigt werden. Das erlaubt z.B. die Übernahme mit nachrichtendienstlichen - der Polizei also nur eingeschränkt zustehenden - Mitteln erlangter oder etwa von Privatdetektiven mit möglicherweise strafbaren Methoden erwirkter Daten, die die Polizei selbst so nicht erheben dürfte. Um die Motivation für eine Umgehung der eigenen Erhebungsermächtigungen zu senken, sollte die Speicherung und Weiterverarbeitung übermittelter Daten darauf beschränkt werden, daß die Polizei sie nach ihren Rechtsgrundlagen auch selbst hätte erheben dürfen.

Besonders bedenklich ist die Übermittlung an Private, deren Aufgaben nicht gesetzlich definiert sind. Ein Bedürfnis für die Übermittlung personenbezogener Daten an Private kann allenfalls im Rahmen der Verfolgung konkreter Ansprüche (Schädiger, Zeugen) von Bedeutung sein und sollte auf diese Fälle beschränkt werden. Nur insoweit dürfte die Übermittlung von der Aufgabenstellung der Polizei gedeckt sein.

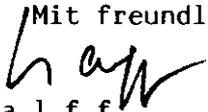
19) Automatisierter Abruf

Die Regelung, hinsichtlich der Verantwortung für den automatisierten Abruf (§ 26(3) letzter Satz) ist gefährlich, weil sie praktisch zu einer unkontrollierten Selbstbedienung führt. Gefahren lauern hier insbesondere bei einem datentechnischen Zusammenschluß (direkt oder über Dritte) von Nachrichtendiensten und Polizei. Es ist nämlich praktisch nicht kontrollierbar, wer wann welche Daten automatisiert abgerufen hat, zumal dies bei der abgefragten Stelle nicht aufgezeichnet oder sonstwie vermerkt wird. Eine wirksame Begrenzung ist nur möglich, wenn man gleichzeitig die Befugnis zum automatisierten Abruf ausdrücklich regelt und eine ausnahmslose Dokumentationspflicht normiert.

20) Haftungsregelung

Für einen wirksamen Schutz der Bürger gegenüber rechtswidrigen polizeilichen Maßnahmen im Bereich von Eingriffen in das Recht auf informationelle Selbstbestimmung sind Auskunfts-, Berichtigungs- und Löschungsrechte nicht ausreichend. Unverzichtbar ist eine Haftungsregelung, die dem (rechtswidrig) geschädigten Bürger Ersatzansprüche für erlittene materielle und immaterielle Schäden zuerkennt. Dabei ist an entsprechende Überlegungen im Datenschutzrecht anzuknüpfen. Die Haftungsregelung ist klarstellend dahin auszuformulieren, daß haftungsauslösende "Maßnahme" (z.Zt. i.S.v. § 39 OBG) auch jede Form von Datenerhebung, -speicherung, -veränderung, -übermittlung oder sonstiger -nutzung ist.

Mit freundlichen Grüßen


K a l f f

Abt.-Geschäfts-
führer


S t ö t z e l

Sprecher des
Fachausschusses

PS

Die beigegeführten Mehrexemplare bitten wir an den Innenausschuß weiterzuleiten.