

Bundesamt für Polizei fedpol  
Stab Rechtsdienst  
Nussbaumstrasse 29  
3003 Bern

Zürich, 5. Februar 2010

## **Vernehmlassung Bundesgesetz über die polizeilichen Aufgaben des Bundes (PoIAG)**

Sehr geehrte Damen und Herren

Die Vereinigung der schweizerischen Datenschutzbeauftragten bedankt sich für die Möglichkeit, zum Entwurf des neuen Bundesgesetzes über die polizeilichen Aufgaben des Bundes Stellung zu nehmen. Wir begrüssen die Stossrichtung hinsichtlich der Vereinfachung des Rechtszuganges durch Bündelung des geltenden Polizeirechts und erlauben uns die folgenden Anmerkungen.

### **1. Allgemeine Anmerkungen**

#### **a. Mangelnde Bestimmtheit des Gesetzes**

Das neue PoIAG regelt Mittel, die einen klaren Eingriff in die Grundrechte der Bürger darstellen. Im Hinblick auf die informationelle Selbstbestimmung sind dies insbesondere die Observation, der Einsatz von Informanten und Vertrauenspersonen, die polizeiliche Informationshilfe, die verdeckte Registrierung sowie die Führung und den Zugriff auf die zu verknüpfenden polizeilichen Informationssysteme des Bundes.

Im Bericht des Bundesrates wird darauf hingewiesen, wie wichtig die Schaffung einer klaren gesetzlichen Grundlage für diese Eingriffe sei. Ferner betont der Bundesrat mehrfach die Bedeutung des Bestimmtheitsgebots für den Grundrechtsschutz (siehe etwa S. 8). Dennoch sind die wichtigsten Bestimmungen des neuen Gesetzes entweder generalklauselhaft formuliert, enthalten ermessensbasierte Ausnahmen für die Anwendbarkeit von Voraussetzungen für Datenbearbeitungen oder delegieren weit gefasste Rechtssetzungsbefugnisse an den Bundesrat.

Dies ist aus datenschutzrechtlicher Sicht in verschiedener Hinsicht problematisch.

- **Zu unbestimmte Umschreibung der Polizeiaufgaben und erlaubten Mittel**

Das PolAG unterteilt die polizeilichen Aufgaben des Bundes in drei Bereiche: die Sicherheitspolizei, die Kriminalpolizei und die Verwaltungspolizei.

Die kriminalpolizeiliche Aufgaben, welche wegen des grossen Ermessenspielraumes aus datenschutzrechtlicher Sicht im Vordergrund stehen, umfassen einige wenig klar konturierte Bereiche, namentlich die Erkennung und Bekämpfung des organisierten Verbrechens, des unerlaubten Betäubungsmittelverkehrs, des Mädchenhandels, der Verbreitung unzuchtiger Veröffentlichungen und der Falschmünzerei.

Unklar ist, was unter dem Doppelbegriff des Erkennens und Bekämpfens zu verstehen ist. Dies kann sich auf die nachträgliche Ermittlung und Bestrafung, aber auch auf die Prävention der entsprechenden Straftaten beziehen. Dass letzteres gemeint sein soll, geht aus Wortlaut und Systematik des Gesetzes nicht deutlich hervor.

Der Bericht äussert sich dahingehend, dass bewusst auf eine Konkretisierung dieser Begriffe verzichtet worden sei. Eine Begründung hierfür fehlt, allerdings wird angedeutet, dass damit die Anwendung nachrichtendienstlicher Methoden zur Früherkennung von organisierten Verbrecherstrukturen ermöglicht werden soll. Hierzu passen auch die neu eingeführten Mittel der Observation sowie des Einsatzes von Privatpersonen, Informanten und Vertrauenspersonen ausserhalb eines Prozesses.

Den grossen Ermessenspielraum bei der Wahl und dem Einsatz der Mittel im Zusammenhang mit den kriminalpolizeilichen Aufgaben ist datenschutzrechtlich sehr problematisch. Gemäss Art. 12 PolAG umfassen die Mittel der Informationsbeschaffung im Vorfeld konkreter strafrechtlicher Untersuchungen, also ausserhalb des eigentlichen Strafprozesses, gegen Einzelpersonen u.a. die Auswertung öffentlich zugänglicher Quellen oder auch die Einholung und Entgegennahme von Auskünften von Behörden und Privatpersonen. Diese Daten können gemäss Abs. 3 ohne Wissen der betroffenen Personen gesammelt werden, sofern dies „zum Zweck der Erkennung und Bekämpfung des organisierten und international tätigen Verbrechens [im Sinne des Gesetzes] erforderlich“ ist.

Dies bedeutet, dass fedpol die Berechtigung eingeräumt werden soll, Personen ausserhalb konkreter Strafverfahren ohne ihr Wissen zu überwachen, unter Einsatz beliebiger Observationsmethoden, wie etwa durch Befragung ihrer Freunde und Bekannten, sowie durch Infiltration der Umgebung dieser Personen durch Vertrauensleute und Informanten.

Im Ergebnis sind sowohl die Aufgaben wie die zulässigen Mittel bestimmter zu regeln. Aus der Forderung, das Gesetz solle die zulässigen Mittel sowie die Indizienliste, ab der ein solches zulässig wäre, regeln, folgt indessen in keiner Weise zwingend die Forderung, der Bund müsse die technischen Einzelheiten und Möglichkeiten dieser Mittel veröffentlichen. Vielmehr geht es darum, dass das Gesetz einen Massstab enthalten muss, an dem die Ermessensausübung der Behörde durch ein Gericht überprüft werden kann. Dies ist im vorliegenden Entwurf kaum der Fall.

- **Relativierende Ausnahmen von Bearbeitungsvoraussetzungen**

Soweit der Entwurf Verfahrensvorschriften festlegt, werden diese regelmässig durch Ausnahmen und Notklauseln ausgehebelt.

Beispiele hierzu finden sich in Art. 12 Abs. 4, welche eine Ausnahme von der Informationspflicht einer betroffenen Person vorsieht oder auch bei der Verlängerung der Observation nach Art. 13 Abs. 2.

Sodann gibt es Ausnahmeregelungen beim Ersuchen um Informationshilfe (Art. 42 ff). Art. 42 und 43 regeln das Verfahren des Ersuchens, während Art. 44 bestimmt, dass diese Verfahrensbestimmungen nicht angewendet werden müssen, soweit konkrete Gründe für die Annahme bestehen, dass die zu übermittelnde Information zur Abwehr einer unmittelbar drohenden ernsthaften Gefahr für die öffentliche Sicherheit oder zur Aufklärung oder Verhütung einer Straftat dienen könnte.

Da die Datenübermittlung nur an Behörden mit sicherheits- oder kriminalpolizeilichen Kompetenzen erfolgen darf, wird insbesondere letztere Voraussetzung sehr oft erfüllt sein.

Ein weiteres solches Beispiel findet sich in Art. 46 PolAG, welcher die Bearbeitung und Weitergabe von Daten an ausländische und internationale Behörden mit sicherheits- oder kriminalpolizeilichen Befugnissen durch fedpol regelt und einen Datenaustausch im Bereich der sicherheits- und kriminalpolizeilichen Aufgaben zwischen fedpol und ausländischen Polizeibehörden auch ohne gesetzliche Grundlage erlaubt.

Auch Art. 49 Abs. 5 PolAG stellt eine solche Ausnahmeregelung dar, wenn er bestimmt, dass bei der Datenweitergabe von erhaltenen Daten ans Ausland auf das Erfordernis eines adäquaten Datenschutzniveaus verzichtet werden könne, wenn die Übermittlung der fraglichen Personendaten im Einzelfall zur Wahrung schutzwürdiger privater oder eines überwiegenden öffentlichen Interesses erforderlich ist.

Folglich liegt es im Ermessen von fedpol, ob Personendaten ohne Schutzgarantie ins Ausland übermittelt werden dürfen.

Im Ergebnis sind diese weiten Ermessensspielräume von fedpol wesentlich einzugrenzen. Die Polizeibehörden der Schweiz dürfen bereits aufgrund der Verfassung im Rahmen der polizeilichen Generalklausel in Notfällen ausserhalb des Gesetzes handeln. Die Wiederholung dieser Selbstverständlichkeit auf Gesetzesstufe birgt die Gefahr, dass das Vorliegen einer Notsituation zu schnell angenommen wird und ist überdies unnötig.

- **Zu weit gefasste Delegation an den Bundesrat**

Der Entwurf überträgt in Art. 74 dem Bundesrat eine weit gefasste Rechtsetzungsbefugnis.

Diese Delegation ist aus datenschutzrechtlicher Sicht problematisch.

Die Frage des Zugriffs auf die in den polizeilichen Informationssystemen des Bundes gespeicherten Daten sollte im Gesetz geregelt sein. Dies deshalb, weil Personendaten durch die Speicherung in einem polizeilichen Informationssystem grundsätzlich als besonders schützenswert zu gelten haben. Entsprechend wäre gemäss Art. 17 DSG eine Rechtsgrundlage auf Stufe eines formellen Gesetzes erforderlich.

Auch die Regelung der Aufbewahrungsfrist sowie die Weitergabe an Private zu anderen als polizeilichen Zwecken muss formell-gesetzlich verankert werden.

Damit stehen die Delegationsbestimmungen des Entwurfs PolAG in Widerspruch zu Art. 17 Abs. 2 DSGVO, der für die Bearbeitung von besonders schützenswerten Personendaten und Persönlichkeitsprofilen grundsätzlich eine gesetzliche Grundlage im formellen Sinn verlangt. Eine Generalklausel, welche sämtlichen durch den Bundesrat zu bezeichnenden Behörden einen umfassenden Zugriff im Rahmen der Erfüllung ihrer Aufgaben gewährt, erfüllt diese Anforderung nicht.

Eine Grundlage in einer Verordnung wäre nur möglich, wenn entweder die Information für eine formell-gesetzlich klar umschriebene Aufgabe unentbehrlich wäre (Art. 17 lit. a DSGVO) oder der Bundesrat eine Bearbeitung im Einzelfall bewilligte und die Rechte der Betroffenen dadurch nicht gefährdet würden (Art. 17 lit. b DSGVO) oder aber die betroffene Person einwilligte.

Die sehr weit gefasste Delegation ist zudem schwer mit den diesbezüglichen von Lehre und Rechtsprechung entwickelten verfassungsrechtlichen Grundsätzen vereinbar.

## **b. Wirksamkeit bisheriger Massnahmen**

Als generelle Anmerkung erlauben wir uns festzustellen, dass aus den Erläuterungen zum PolAG nicht hervor geht, ob die bisher in anderen Gesetzen geregelten Massnahmen der polizeilichen Arbeit auch tatsächlich wirksam angewendet wurden.

Wir sind der Auffassung, dass vor einer generellen Übernahme der entsprechenden Massnahmen in ein neues Gesetz, deren Wirksamkeit evaluiert werden muss und allfällig nicht wirksame Massnahmen keinen Eingang in das neue Regelwerk finden sollten.

## **2. Anmerkungen zu einzelnen Artikeln**

### **a. Art. 7 Einsatz von optischen Überwachungsgeräten**

Art. 7 Abs. 1 PolAG erlaubt optische Überwachung an allgemein zugänglichen Orten, soweit dies für den Schutz der Gebäude und Personen nach diesem Kapitel erforderlich ist.

Generell gilt festzustellen, dass die erwähnte Bestimmung im Hinblick auf den zeitlichen und sachlichen Geltungsbereich zu weitgehend ist. Unklar bleibt dementsprechend wann welche Gebäude oder Personen auf Grund welcher Indizien geschützt werden müssen.

Selbst wenn die Bestimmung klarer formuliert wäre, stellt sie keine gesetzliche Grundlage für den Einsatz optischer Überwachungsgeräte dar. Dies deshalb, weil die allgemein zugänglichen Orte häufig auf Gemeinde- oder Kantonsgrund liegen und daher nicht der

Bund, sondern die Kantone und Gemeinden für die Erlaubnis einer Überwachungsinstallation zuständig sind. Sollen Geräte zur optischen Überwachung an allgemein zugänglichen Orten installiert werden, so braucht es entsprechende Grundlagen in den kantonalen bzw. kommunalen Erlassen.

Weiter gilt es im Hinblick auf Abs. 2 festzustellen, dass sich die Bearbeitung der dadurch erfassten Personendaten nach dem jeweiligen kantonalen Datenschutzrecht richtet.

#### **b. Art. 9 Aufgaben, insbesondere lit. d**

Art. 9 lit. d PolAG bestimmt, dass die Zentralstellen nach diesem Titel die nationale und internationale Informationshilfe sicherstellen.

Dies Bestimmung bildet lediglich die Grundlage des zur Verfügungstellens einer Austauschplattform. Die entsprechenden materiellen gesetzlichen Grundlagen für die effektive Informationshilfe der kantonalen Behörden sind jedoch im jeweiligen kantonalen Recht in detaillierter Form zu verankern.

#### **c. Art. 12 Mittel der Informationsbeschaffung, insbesondere Abs. 2 lit. b und Abs. 4**

Art. 12 PolAG regelt die Mittel der Informationsbeschaffung und bestimmt in Abs. 2 lit. b, dass neben den Behörden auch von Privatpersonen Auskünfte eingeholt oder entgegengenommen werden können.

Diese Bestimmung geht im Hinblick auf die Privatsphäre einer betroffenen Person sehr weit, besteht doch keine Eingrenzung auf einen bestimmten Personenkreis. So können auch Freunde, Familie oder der Arbeitgeber etc. ohne das Wissen der betroffenen Person befragt werden.

Zusätzlich ist anzumerken, dass Art. 12 Abs. 4 PolAG der Behörde einen sehr grossen Ermessensspielraum bei der Benachrichtigung der betroffenen Person über die Datenbeschaffung einräumt. Werden Personendaten ohne das Wissen der Betroffenen gesammelt, so ist sie zwar laut Gesetz im Nachhinein zu informieren, allerdings kann auf die Benachrichtigung verzichtet werden, wenn „diese Information mit einem unverhältnismässigen Aufwand verbunden wäre“.

Soweit jedoch der Aufwand nicht zu gross ist, ermöglicht Abs. 4 weiter den Verzicht auf die Benachrichtigung auch dann, wenn ein überwiegendes öffentliches Interesse dies erfordert.

Damit liegt es im dreifachen Ermessen der Behörde, ob informiert wird. Als erstes kann sie abwägen, ob der Grund der Geheimhaltung noch vorhanden ist, als zweites kann sie abwägen, ob der Aufwand der Benachrichtigung nicht zu gross sei und als drittes kann sie abwägen, ob nicht ein überwiegendes öffentliches Interesse der Benachrichtigung entgegenstehe.

Ein so weitgehendes Ermessen ist schwer zu überprüfen und dementsprechend grundrechtlich problematisch.

#### **d. Art. 13 Observation**

Art. 13 PolAG regelt das neue Instrument der Observation. Zur Erkennung und Bekämpfung des organisierten und international tätigen Verbrechens können die Zentralstellen ausserhalb von Strafverfahren Personen und Sachen an allgemein zugänglichen Orten verdeckt beobachten und dabei Bild- oder Tonaufzeichnungen machen, wenn andere Massnahmen zur Informationsbeschaffung aussichtslos wären oder unverhältnismässig erschwert würden. Zur Unterstützung der Observation können Ortungsgeräte eingesetzt werden, wenn ihre Durchführung sonst wesentlich erschwert wäre (Abs. 1).

Es handelt sich bei der Observation um eine Massnahme, welche ausserhalb des Strafverfahrens und vor Bestehen eines konkreten Verdachts – zur sog. Strukturermittlung - verwendet werden soll. Als Beispiel dient die Observation einer Tankstelle. Als hinreichender Grund für eine Observation würde gemäss den neuen Bestimmungen in Art. 13 PolAG die Vermutung der Zentralstelle, dass diese Tankstelle ein Treffpunkt für Angehörige einer kriminellen Organisation sein könnte, ausreichen (zum Ganzen s. S. 27 f. des Berichts). Eine solch technisch ausgestaltete Massnahme bedeutet einen schweren Eingriff in die Grundrechte der Betroffenen und ist deshalb mit hinreichender Bestimmtheit im Gesetz zu regeln, was vorliegend nicht der Fall ist. Zudem handelt es sich um ein präventives Mittel; dies bedeutet, dass der Eingriff dadurch zusätzlich verschärft wird.

Als zusätzliche Sicherung zur präziser auszugestaltenden gesetzlichen Grundlage ist zudem eine Genehmigungspflicht durch eine unabhängige richterliche Behörde (z. B. analog der Regelungen in den Art. 6 und Art. 7 des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF; SR 780.1) notwendig.

Sodann bestimmt Art. 13 Abs. 2 PolAG, die Observation dürfe längstens einen Monat dauern, ohne ihren Zweck zu erreichen. Nach Ablauf dieser Frist darf sie jedoch durch den Direktor von fedpol beliebig lange um jeweils einen weiteren Monat verlängert werden.

Das Gesetz nennt keine Kriterien, wann eine Observation gerechtfertigt ist. Insbesondere in Zusammenhang mit dem sehr weit gefassten Zweck der Erkennung der organisierten und international tätigen Kriminalität liegt hier ein extrem weites Ermessen vor. Zudem ist festzuhalten, dass eine Verlängerung durch den Direktor des fedpol der Eingriffsschwere nicht entspricht. Mit anderen Worten muss auch hier eine unabhängige richterliche Behörde die Verlängerung bewilligen.

#### **e. Art. 14 bis 17 Einsatz von Privatpersonen**

Die Bestimmungen 14 bis 17 PolAG regeln den Einsatz von Privatpersonen als InformantInnen und Vertrauenspersonen zwecks Erkennung und Bekämpfung des organisierten und international tätigen Verbrechens. Art. 14 PolAG dient als Generalklausel für den Einsatz solcher Personen. In den darauf folgenden Art. 15, Art. 16 und Art. 17 werden die Einsätze und eine allfällige Entschädigung bzw. Prämie für diese Personen rudimentär geregelt.

Allerdings werden keine genaueren Voraussetzungen genannt, wann diese Personen eingesetzt werden. Weder regelt das PolAG Voraussetzungen zur Ausbildung oder den persönlichen Anforderungen dieser Personen, noch sind die Befugnisse klar festgehalten.

Der Einsatz solcher Privatpersonen bedeutet eine mindestens gleich grosse Gefährdung von Einzelpersonen in ihren Grundrechten wie der Einsatz von verdeckten Ermittlern (gemäss dem Bundesgesetz über die verdeckte Ermittlung [BVE; SR 312.8]). Da es sich um Privatpersonen handelt, die auch nur für einen einmaligen Einsatz rekrutiert werden können und keinerlei polizeiliche Kenntnisse haben müssen, geht die Gefährdung von Einzelpersonen wohl noch über diejenige bei einer verdeckten Ermittlung hinaus. Im Bundesgesetz über die verdeckte Ermittlung gibt es jedoch immerhin klarere Bestimmungen zu den Voraussetzungen, wann eine solche Ermittlung angesetzt werden darf (Art. 4 BVE), zudem ist der Personenkreis, der zu einer Ermittlung eingesetzt werden kann eingegrenzt (Art. 5 BVE) und es ist für die Ernennung einer Ermittlerin oder eines Ermittlers die Genehmigung einer richterlichen Behörde notwendig (Art. 7 BVE).

Angesichts der Schwere des Eingriffs in die Grundrechte möglicher Betroffener, sind beim Einsatz von Privatpersonen als Informantinnen und Vertrauenspersonen mindestens analoge formell-gesetzliche Regelungen wie im BVE zu erlassen.

Schliesslich sei noch angemerkt, dass Art. 16 Abs. 3 eine Dokumentationspflicht dieser Personen verlangt. Allerdings bestehen keine genaueren Regelungen darüber, welche Daten zu erfassen sind, wie diese bearbeitet werden dürfen und wie sie aufzubewahren und zu löschen sind. Da mit den erwähnten Bestimmungen Privatpersonen angesprochen sind, müssen genaue Regelungen hinsichtlich der durch diese wahrzunehmenden Datenbearbeitungen verankert werden, ansonsten können in der praktischen Umsetzung gravierende Probleme entstehen.

#### **f. Art. 29 Ausschreibung von Personen und Sachen zwecks verdeckter Registrierung**

Bei der verdeckten Registrierung handelt es sich um einen Sonderfall der Observation und damit um ein neues Instrument der schweizerischen polizeilichen Arbeit. Zur verdeckten Registrierung ausgeschrieben werden, können dabei auch Personen, nicht nur Fahrzeuge etc. Das Schengener Durchführungsübereinkommen (SDÜ) sieht diese Art der Observation vor und weist dieselben Voraussetzungen auf, wie sie jetzt das Bundesrecht aufführt. Zudem gab es bereits im früheren Bundesgesetz über die polizeilichen Informationssysteme des Bundes (BPI; SR 361) eine vergleichbare Regelung, allerdings war diese – laut den jetzigen Erläuterungen – nicht ausreichend.

Die Voraussetzungen für eine verdeckte Registrierung, wie sie auch das SDÜ vorgibt, erscheinen jedoch nicht hinreichend bestimmt. Insbesondere weist die zweite Voraussetzung unter Abs. 2 lit. b im Hinblick auf die Bestimmtheit grosse Lücken auf. Diese Bestimmung erlaubt eine Ausschreibung, wenn die Gesamtbeurteilung einer Person insbesondere aufgrund der bisher von ihr begangenen Straftaten, erwarten lässt, dass sie auch künftig aussergewöhnlich schwere Straftaten planen könnte. Zwar orientiert sich der Katalog der schweren Straftaten am Katalog, der im Bundesgesetz über die verdeckte Ermittlung festgehalten ist, dennoch fragt es sich, ob ein solcher Eingriff in die Privatsphäre im ausserprozessualen Bereich (nach einem Strafverfahren) mit der Verfassung zu vereinbaren ist. Ist eine Person aus dem Strafvollzug entlassen, gilt die Unschuldsvermutung und

kein Generalverdacht, dass sie wieder ähnliche Straftaten begehen wird.

#### **g. Art. 39 Informationshilfe, insbesondere Abs. 2**

Art. 39 Abs. 2 bestimmt, dass für die Bearbeitungen der Informationen im Zusammenhang mit der Informationshilfe das Datenschutzrecht des Bundes und der Kantone zur Anwendung kommt.

Damit bringt diese Bestimmung richtigerweise zum Ausdruck, dass die Datenschutzgesetze des Bundes und der Kantone zur Anwendung kommen, je nachdem welche Behörde Daten bearbeitet. In Art. 104 wird demgegenüber nur das eidgenössische DSG als anwendbar erklärt, soweit es um die Bearbeitung von Personendaten nach diesem Gesetz geht. Im Sinne der Kompetenzregelungen zwischen Bund und Kantonen muss allerdings was in Art. 39 Abs. 2 steht, auch für alle anderen Bearbeitungen von Personendaten gelten, nicht nur für das Kapitel der Informationshilfe. Es gilt dementsprechend für sämtliche Bearbeitungen von Personendaten im Geltungsbereich des PolAG für die Bundesorgane das eidgenössische, für die kantonalen Behörden das jeweilige kantonale Datenschutzrecht.

#### **h. Art. 69 Grundsätze (der polizeilichen Informationssysteme des Bundes), insbesondere Abs. 2 und 3**

Art. 69 Abs. 2 PolAG bestimmt, dass in den Informationssystemen nach Abs. 1 besonders schützenswerte Daten und Persönlichkeitsprofile bearbeitet werden dürfen, soweit dies zur Erfüllung der gesetzlichen Aufgaben erforderlich ist. Diese Bestimmung steht im Widerspruch zu Art. 17 Abs. 2 DSG. Nach dieser Bestimmung ist für die Bearbeitung von besonders schützenswerten Personendaten und Persönlichkeitsprofilen, wie sie in den diversen, untereinander zu verknüpfenden polizeilichen Informationssystemen enthalten sein werden, grundsätzlich eine gesetzliche Grundlage im formellen Sinn erforderlich. Eine Generalklausel, welche sämtlichen durch den Bundesrat zu bezeichnenden Behörden einen umfassenden Zugriff im Rahmen der Erfüllung ihrer Aufgaben gewährt, erfüllt diese Anforderung nicht. Vielmehr ist für jedes einzelne System eine entsprechende, hinreichend bestimmte gesetzliche Grundlage erforderlich (mindestens analog Art. 76 Abs. 2 PolAG zum Informations- und Dokumentationssystem über Bedrohungen).

Eine Grundlage in einer Verordnung wäre nur möglich, wenn entweder die Information für eine formell-gesetzlich klar umschriebene Aufgabe unentbehrlich wäre (Art. 17 lit. a DSG) oder der Bundesrat eine Bearbeitung im Einzelfall bewilligte und die Rechte der Betroffenen dadurch nicht gefährdet würden (Art. 17 lit. b DSG) oder aber die betroffene Person einwilligte.

Art. 69 Abs. 3 PolAG bestimmt, dass Informationen über die politische Betätigung und die Ausübung der Meinungs- Koalitions- und Versammlungsfreiheit nicht bearbeitet werden dürfen.

Dieses Verbot gilt dann nicht, wenn der begründete Verdacht besteht, eine Organisation oder ihr angehörende Personen würden die Ausübung politischer Rechte oder Grundrechte als Vorwand nehmen, um strafbare Tätigkeiten vorzubereiten oder durchzuführen.

Gemäss Bericht dürfen die Ausübung politischer Rechte und die politische Meinungsbildung als solche nicht als Risiko für die innere Sicherheit betrachtet werden. Das Einschreiten des Staates sei in diesem Bereich erst gerechtfertigt, wenn Gründe für eine Abklärung bestehen, ob ein strafbares Verhalten vorliege (S. 66).

Damit wird mehr oder weniger der Gesetzeswortlaut wiederholt. Weder das Gesetz noch der Bericht machen deutlich, in welchem Zusammenhang Informationen über die Art und Weise, wie jemand diese Rechte ausübt, mit der Vorbereitung oder Begehung einer Straftat stehen müssen, um einen entsprechenden Eintrag in ein Register zu rechtfertigen, oder welche Intensität das fragliche Verbrechen hierzu aufweisen muss.

Das Gesetz deutet in Art. 76 PolAG jedoch an, dass Informationen über religiöse, weltanschauliche, politische oder gar gewerkschaftliche Ansichten und Tätigkeiten im Rahmen von Art. 69 Abs. 3 PolAG regelmässig im Informations- und Dokumentationssystem über Bedrohungen bearbeitet werden dürfen. Offenbar soll Art. 69 Abs. 3 PolAG insbesondere die Erfassung von solchen Gruppierungen ermöglichen, die Anschläge auf Gebäude oder Personen planen und/oder durchführen.

Aus grundrechtlicher Sicht ist es notwendig, dass die gesetzliche Bestimmung klare Angaben darüber enthält, wie gravierend ein geplantes oder durchgeführtes Verbrechen sein muss, damit in Zusammenhang damit religiöse, politische, weltanschauliche oder gewerkschaftliche Informationen über Personen gespeichert werden dürfen.

#### **i. Art. 72 Aufbewahrungsdauer, Löschung, Archivierung und Vernichtung der Daten**

Zunächst muss festgehalten werden, dass das Gesetz keine ausdrückliche Löschrfrist enthält. Die Bestimmung der Löschrfristen ist Teil der weit gefassten Gesetzesdelegation an den Bundesrat in Art. 74 PolAG. Die Rahmenbedingungen für die Löschrfristen sind auf gesetzlicher Stufe festzulegen.

Art. 72 Abs. 2 PolAG regelt sodann die möglichen Löschrverfahren für Daten, die in den polizeilichen Informationssystemen des Bundes gespeichert sind. Dabei werden nach lit. a einzelne Einträge gelöscht, sobald die entsprechende Aufbewahrungsdauer abgelaufen ist.

Hingegen bestimmt lit. b, dass verknüpfte Daten erst gelöscht werden, sobald die Aufbewahrungsdauer sämtlicher mit ihnen verknüpfter Daten abgelaufen ist. Dies ermöglicht eine unendliche Aufbewahrungsdauer von allenfalls veralteten Daten, obwohl diese schon längst nicht mehr benötigt werden und dementsprechend gelöscht werden müssten.

#### **j. Art. 77 Informationssystem über Gewalttätigkeiten anlässlich von Sportveranstaltungen, insbesondere Abs. 5**

Art. 77 Abs. 5 bestimmt, dass die Vollzugsbehörden in diesem System auch besonders schützenswerte Personendaten bearbeiten können, soweit es die Durchführung ihrer Aufgaben erfordert. Für diese Bearbeitung von besonders schützenswerten Personendaten fehlt jedoch die formell-gesetzliche Grundlage, wird doch der Katalog von Personendaten, welche in diesem System bearbeitet werden dürfen, in abschliessender Weise in Abs. 3

desselben Artikels genannt. Besonders schützenswerte Personendaten sind jedoch laut diesem abschliessenden Katalog nicht im System enthalten.

#### **k. Art. 82 System zur Unterstützung der Ermittlungen der Kantone im Bereich ihrer Strafverfolgungskompetenzen, insbesondere Abs. 3 und Abs. 4**

Gemäss Art. 82 PoIAG betreibt fedpol ein System zur Unterstützung der Ermittlungen der Kantone im Bereich ihrer Strafverfolgungskompetenzen.

Abs. 3 bestimmt, dass jeder Kanton für seine eigenen Daten den Polizei- und Strafverfolgungsbehörden des Bundes und der Kantone, die im Rahmen ihrer Tätigkeiten mit dem betroffenen Kanton zusammenarbeiten, Zugang mittels Abrufverfahren gewähren kann. Gegen eine solche Regelung im Bundesrecht spricht nichts, allerdings kann diese keine hinreichend bestimmte formell-gesetzliche Grundlage bilden. Eine solche ist in jedem Kanton zu schaffen.

Aus datenschutzrechtlicher Sicht ist im Hinblick auf solche online-Zugriffe zu bedenken, dass diese mit besonderen Risiken für die Rechte und Freiheiten der betroffenen Person verbunden sind. Diese stellen einen erheblichen Eingriff in die Grundrechte auf persönliche Freiheit und Privatsphäre dar. Das Risiko für die betroffenen Personen besteht einerseits darin, dass der Empfänger künftig auf Personendaten zugreifen kann, ohne dass die bekannt gebende Behörde jeweils davon Kenntnis hat. Die Behörde kann somit nicht beurteilen, ob die bezogenen Personendaten tatsächlich erforderlich waren. Andererseits kann der Empfänger die bezogenen Personendaten für einen anderen Zweck, als zu dem sie ursprünglich von der Behörde beschafft wurden, verwenden. Das Risiko ist dabei umso grösser, wenn nicht nur Behörden, sondern auch Private online auf Personendaten zugreifen können. Der online-Zugriff auf Personendaten ist deshalb nur zulässig, wenn er in einem Erlass ausdrücklich vorgesehen ist (vgl. auch Art. 19 Abs. 3 DSG). Besondere Personendaten dürfen nur dann online zugänglich gemacht werden, wenn dies in einem hinreichend bestimmten formellen Gesetz geregelt ist. Der online-Zugriff muss nicht nur ausdrücklich im Gesetz erwähnt sein; zusätzlich müssen insbesondere die Kategorien der Personendaten und der Verwendungszweck umschrieben sein.

Art. 82 Abs. 4 PoIAG verpflichtet die Kantone, Bestimmungen zum Schutz dieser Daten zu erlassen und ein Organ zu bezeichnen, das die Einhaltung dieser Bestimmungen überwacht. Diese Bestimmung ist dahingehend zu ergänzen, dass das überwachende Organ eine unabhängige Stellung inne hat und zudem auch wirklich mit entsprechenden Kompetenzen ausgestattet ist.

#### **I. Art. 104 Datenschutz**

Wie bereits oben unter Bst. g. erwähnt, handelt es sich bei Art. 104 um eine Regelung, welche für das ganze vorliegende Gesetz das Datenschutzgesetz des Bundes als anwendbar erklärt, ausser es bestehen besondere Bestimmungen.

Dabei handelt es sich um eine kompetenzwidrige Regelung. Richtigerweise wird die Bestimmung dahingehend korrigiert, dass für sämtliche Bearbeitungen von Personendaten

im Geltungsbereich des PoIAG für die Bundesorgane das eidgenössische, für die kantonalen Behörden das jeweilige kantonale Datenschutzrecht zur Anwendung kommt.

Wir danken Ihnen für die Berücksichtigung unserer Anmerkungen.

Freundliche Grüsse

Bruno Baeriswyl  
Präsident privatim