

An das
Bundesministerium für Justiz

An das
Bundesministerium für Inneres

Betrifft: Bericht der Informellen Hochrangigen Beratenden Gruppe zur Zukunft der europäischen Innenpolitik ("Zukunftsgruppe") vom Juni 2008 (sog. „Stockholmer Programm“)

Der Datenschutzrat hat in seiner 186. Sitzung am 6. März 2009 die im Betreff genannte Thematik **diskutiert** und sich dabei insbesondere auf folgende **Erwägungen** gestützt:

Standardisierte Datenschutzformeln:

In den letzten Jahren hat sich auf europäischer Ebene die Praxis entwickelt, sowohl in politischen Dokumenten als auch in Rechtsakte im Rahmen der, bzw. mit Bezug auf die sog. Dritte Säule „standardmäßig“ Datenschutzformeln aufzunehmen. So wird routinemäßig von einem „Gleichgewicht zwischen Sicherheit und Schutz der Privatsphäre“, „ergänzenden geeigneten Datenschutzinstrumenten“, „Technologien zur Verbesserung des Datenschutzes“, einem „soliden Datenschutzregime als Grundvoraussetzung“ oder der „Verarbeitung von Informationen im Einklang mit den Grundsätzen der Verhältnismäßigkeit und Notwendigkeit“ gesprochen. Diese an sich erfreulichen, allgemein gehaltenen Bekenntnisse, wie sie sich auch im Stockholmer Programm wiederfinden, stehen allerdings in einem unverkennbaren Widerspruch zum konkreten Inhalt zahlreicher einschlägiger Maßnahmen mit Eingriffscharakter, wie sie sich gerade auch in den nachstehend skizzierten Zielvorgaben des Programms widerspiegeln.

Weiterverfolgung bzw. –entwicklung des „Verfügbarkeitsgrundsatzes“

Der sog. „Verfügbarkeitsgrundsatz“ stellt keinen Rechtsgrundsatz dar. Vielmehr handelt es sich um eine rechtspolitische Forderung der Sicherheitsbehörden, die vordergründig auf eine Effizienzsteigerung durch „Entbürokratisierung“ abzielt.

Die Kernproblematik liegt im gegebenen Kontext darin, dass erstens der (in Österreich im höchsten Verfassungsrang stehende) Rechtsgrundsatz der Rechtsstaatlichkeit wirksame Kontrollen der das Gewaltmonopol des Staates verkörpernden Sicherheitsbehörden bzw. –organe durch unabhängige Organe erfordert und zweitens der allgemeine Rechtsgrundsatz der Verhältnismäßigkeit sowie der spezifisch datenschutzrechtliche Grundsatz der Erheblichkeit/ Erforderlichkeit im Auge behalten werden müssen.

Der Verfügbarkeitsgrundsatz ist – wenn überhaupt - nur sehr eingeschränkt mit den vorher genannten Rechtsprinzipien in Einklang zu bringen.

Die Bindung an richterliche Genehmigungen /-Anträge als Voraussetzung der grenzüberschreitenden Informationsbeschaffung ist rechtsstaatlich v.a. dort unverzichtbar, wo unmittelbare staatliche Zwangsgewalt in Spiel kommt (Beschlagnahme von Dokumenten, Dateien, Hausdurchsuchung etc).

Darüber hinaus erscheint sie auch dann bedeutsam, wenn ein Austausch sensibler Informationen (bspw. Strafregisterauszüge) mit Drittstaaten erfolgen muss/soll, in welchen rechtsstaatliche Mindeststandards nicht existieren. In diesem Kontext problematisch sind im Übrigen direkte Zugriffsmöglichkeiten von Einrichtungen wie Europol oder Eurojust auf Informationen aus nationalen Datensammlungen, da die genannten Einrichtungen inzwischen einen regen, kaum kontrollierbaren Datenaustausch mit Drittstaaten pflegen, welche in Ermangelung eines entsprechenden Datenschutz- bzw. Rechtsstaatsstandards mit unkalkulierbaren Datenschutzrisiken einher gehen. Auch der heute bereits praktizierte rege Austausch von Daten zwischen EU-Staaten und Drittstaaten über Interpol wirft viele ungelöste Fragen auf. Interpol selbst unterliegt nämlich keiner unabhängigen Datenschutzkontrolle.

Auch innerhalb der EU gibt es aus rechtsstaatlicher Perspektive nach wie vor bedeutsame faktische Unterschiede. Weder ist es bis dato in der EU zu einer vollständigen Harmonisierung der nationalen Straftatbestände und des Strafprozessrechts („Mindestrechtsschutz“) bzw. der nationalen Polizeibefugnisse

und der Beschwerdemöglichkeiten gegen deren Missbrauch gekommen, noch besteht bspw. eine EU-weit annähernd gleichmäßige Verteilung der Risiken in punkto Korruption des öffentlichen Sektors. Auch sind die im Haager Programm angesprochenen Vorbedingungen (gemeinsame Normen für den Zugang zu den Daten und gemeinsame technische Zugangsnormen [Protokollierung u.a.m.]; tatsächliche Überwachung der Einhaltung der Datenschutzvorschriften; geeignete Kontrolle vor und nach dem Austausch; Schutz der Einzelpersonen vor Datenmissbrauch) nicht ausreichend geregelt bzw. harmonisiert.

Und schließlich hat der sog. Rahmenschluss über den Datenschutz in der sog.

3. Säule der EU (Polizei- und Justizkooperation) nicht zu einer Standardisierung des Datenaustausches mit Drittstaaten (Mindestbedingungen) geführt.

Gerade im Falle von Online-Zugriffen ist zu bedenken, dass es hier weder eine unabhängige externe (Vorab)Kontrolle des polizeilichen Datenaustausches gibt noch ein sog. „polizeiinternes“ 4-Augen-Prinzip (im Sinne einer Plausibilitäts- bzw. Rechtmäßigkeitskontrolle durch die angefragte Sicherheitsbehörde) zur Anwendung kommt.

Im Übrigen ist zu bemerken, dass sich aus praktischer Sicht nur sehr wenige Kerninformationen aus polizeilichen Dateien (DNA-Profile, Fingerabdrücke, Kfz-Kennzeichen) ohne näheres Hintergrundwissen überhaupt dafür eignen, grenzüberschreitend ohne Vorabkontrolle (insbesondere „online“) abgefragt zu werden.

Aus all den vorgenannten Gründen erscheint aus heutiger Sicht eine Umsetzung des „Verfügbarkeitsgrundsatzes“ über das im Prümer Vertrag bereits erreichte Ausmaß grundsätzlich –vor allem im Hinblick auf die Frage der Erforderlichkeit - datenschutzrechtlich problematisch.

Wesentlich im Kontext der grenzüberschreitenden Online-Zugriffe ist der Gesichtspunkt, dass aus Verhältnismäßigkeitsgründen die den ausländischen Behörden eingeräumten Zugriffsrechte typischerweise nicht ident mit jenen der Beamten des Betreiberstaates sein können. Vielmehr ist zwecks Missbrauchsvorbeugung eine Beschränkung auf unbedingt erforderliche Referenzdaten vorzunehmen bzw. eine Beschränkung der Abfragekriterien vorzunehmen, wie dies etwa im Prümer Vertrag vorexerziert wurde („asymmetrischer“ Zugriff; Bsp.: Abfragemöglichkeit des Kfz-Registers aus dem

Ausland nur anhand vollständigem Kennzeichen oder Fahrgestellnummer; hingegen keine Suche etwa „nach allen Besitzern von weißen Mercedes samt Adresse“).

Dieser Grundgedanke müsste auch bei einer punktuellen Ergänzung der bestehenden Möglichkeiten beibehalten werden. Eine solche Ergänzung wäre aus heutiger Sicht bestenfalls in Form der Eröffnung eines strikt beschränkten Onlinezugriffs auf nationale Waffenregister denkbar (etwa: nur Suche anhand vollständiger Waffenregisternummer) oder Melderegister im strikt beschränkten Ausmaß, wie sie etwa in Österreich für Private offenstehen (Suche nur nach einer anhand Namens- und Adressdaten oder Namens- und Geburtsdaten genau bestimmten Person [„Verifikation“]; hingegen nicht zur „Identifizierung“ oder „Lokalisierung“ von Unbekannten).

Zum spezifischen Thema der Umsetzung des Verfügbarkeitsprinzips im Verhältnis zwischen den Nachrichtendiensten ist anzumerken, dass hier erschwerend der Umstand hinzu kommt, dass es sich bei den bezüglichen Informationen in der Regel weniger um Tatsachen als um Vermutungen und Behauptungen handelt (sog. „weiche Daten“). Sowohl die Quellen als auch Information weisen hier sehr unterschiedliche Qualitäten auf. Ohne Zusatzinformation über die „Zuverlässigkeit“ der Quelle bzw. die Information, ob eine Überprüfung der Information erfolgt ist und zutreffendenfalls wie (Auswertung weiterer Quellen) sind nachrichtendienstliche Informationen daher kaum von Nutzen. Eine einheitliche europäische Methode der Klassifizierung solcher Informationen existiert jedoch nicht. Oft ist der Inhalt einer Information auch geeignet, Hinweise auf die Quelle zu geben (Quellenschutz!). Führen derartige Informationen zu ungerechtfertigten Grundrechtseingriffen (Bsp.: heimliche Observation, Entführungen nach Guantanamo Bay) besteht i.d.R. kein effektiver Rechtsschutz. Aus all den genannten Gründen ist schon ein ungefilterter Informationsaustausch zwischen nationalen Sicherheitsbehörden und Nachrichtendiensten mit dem Rechtsstaatsprinzip praktisch nicht vereinbar.

In Ermangelung europaweit einheitlichen nationalen Regeln für den Umgang mit dieser Grundproblematik potenzieren sich die angesprochenen Probleme im Falle des grenzüberschreitenden Austausches nach der Idee des „Verfügbarkeitsgrundsatzes“. Diesen Bedenken trägt das Stockholmer Programm ebenso wenig Rechnung wie der Tatsache, dass es aktuell an jeglicher transparenter Regelung zum grenzüberschreitenden Austausch zwischen Nachrichtendiensten fehlt.

Im Lichte der obigen Erwägungen sollte im Stockholmer Programm der Verfügbarkeitsgrundsatz neu formuliert werden. Uzw. im Sinne der dargelegten differenzierten Sichtweise, die insbesondere auf die Nachrangigkeit dieser politischen Forderung gegenüber Rechtsstaatsprinzip und Erforderlichkeitsgrundsatz verweist. Schon aus letzterem Grundsatz ergibt sich die Notwendigkeit, jede einzelne in der Praxis auftauchende Informationsfrage gesondert zu betrachten.

Der im Stockholmer Programm an einzelnen Stellen formulierte Ansatz der Erleichterung des Datenaustausches durch einen nicht näher spezifizierten „allgemeinen, kohärenten Ansatz“, der sich ausschließlich an vermeintlichen „operativen Bedürfnissen“ der Praxis und technischen Machbarkeiten ausrichtet und keine inhaltlichen Grenzen zu kennen scheint („Interoperabilität“, „beliebige Erweiterbarkeit“), ist damit freilich nicht vereinbar und in dieser Form abzulehnen.

Im Übrigen fällt auf, dass das Stockholmer Programm eine ausreichend klare inhaltliche Umschreibung bzw. Abgrenzung verschiedener, wenngleich zusammenhängender, teils überschneidender Themenkreise vermissen lässt. So werden die Themen „Verfügbarkeitsprinzip“, „kohärenter Ansatz bei der Entwicklung von Informationstechnologien“, „ganzheitlicher Ansatz für den Informationsaustausch“, „Interoperabilität“ oder „europäischen Strategie der Verwaltung strafverfolgungsrelevanter Informationen“ quasi in loser Folge verwendet und teilweise ohne nähere Erläuterungen miteinander in Beziehung gesetzt. Angemerkt sei an dieser Stelle, dass bereits der Aktionsplan des Rates und der Kommission zur Umsetzung des Haager Programms aus 2005 die „Festlegung einer Strategie für einen kohärenten Ansatz bei der Entwicklung von Informationstechnologien zur Unterstützung der Sammlung, der Speicherung, der Verarbeitung, der Analyse und des Austauschs von Informationen“ für das Jahr 2005 angekündigt hatte. Bis heute ist es dabei geblieben.

In Bezug auf den konkreten Anwendungsfall der Einräumung von Onlinezugriffen wäre im Programm auf das Prinzip des asymmetrischen Zugriffs, dessen genaue normative Festlegung (Abfragekriterien) sowie Mindestbedingungen für die Ex-Post-Kontrolle (vollständige Protokollierung, Nachvollziehbarkeit der abfragenden Person, Pflicht zur stichprobenartigen Auswertung und Rechtmäßigkeitskontrolle der Protokolldaten durch interne und externe Kontrollstellen) hinzuweisen.

Zu den im Stockholmer Programm anvisierten weiteren IT-Großsystemen ist festzuhalten, dass schon die bestehenden gravierende datenschutzrechtliche

Probleme aufwerfen und z.T. unter weitgehender Außerachtlassung der Empfehlungen der nationalen Datenschutzbehörden sowie des Europäischen Datenschutzbeauftragten errichtet sind. Es stellt sich insofern weniger die Frage nach einem weiteren Ausbau, sondern eher die Frage nach einem durchdachten Rückbau der bezüglichen Systeme. Der im Stockholmer Programm skizzierte weitere Weg steht dieser Erkenntnis freilich diametral entgegen.

„Interoperabilität“ bzw. Fusion von Datenanwendungen im Stockholmer Programm

Angesprochen ist mit dem Konzept der Interoperabilität primär der fundamentale datenschutzrechtliche Grundsatz der Zweckbindung. Der Grundsatz der Zweckbindung bedeutet im Wesentlichen, dass personenbezogene Daten nur für festgelegte, eindeutige und rechtmäßige Zwecke ermittelt und nicht in einer mit diesen Zwecken unvereinbaren Weise weiterverwendet werden dürfen. Hinter diesem Grundsatz steht zunächst der Gedanke, dass für Betroffene schon im Zeitpunkt der Datenerhebung Gewissheit über Anlass und Zweck dieser Datenerhebung bzw. die weitere Nutzung der Daten bestehen soll („Transparenz“). Dieses Wissen ist zugleich Voraussetzung zur Beurteilung der Rechtmäßigkeit der Datenerhebung durch den Betroffenen selbst und damit die Grundlage zur Erhebung allfälliger Rechtsmittel gegen eine allfällige unzulässige Datenerhebung.

Als Konsequenz darf eine Weiterverwendung von einmal rechtmäßig erhobenen Daten nur unter klar definierten und eingeschränkten Bedingungen zulässig sein. Im Übrigen soll der Zweckbindungsgrundsatz auch die Verknüpfung verschiedener bestehender personenbezogener Datenbestände unterbinden. Dies ist wichtig, um die Betroffenen vor willkürlichen Überwachungsmaßnahmen bzw. Ausspionierung ihrer Lebensumstände durch Unbefugte zu schützen, Diskriminierungen gegen Einzelne oder Gruppen anhand verschiedener Kriterien (Religion, Hautfarbe etc.) zu unterbinden oder etwa zu verhindern, dass „auf technischem Wege“ aus einer Summe unbescholtener Bürger anhand verschiedener, willkürlich festgelegter Kriterien quasi „Verdächtige“ generiert werden („Rasterfahndung“).

Das Stockholmer Programm forciert zusammenfassend einen Ansatz, der sich an reinem polizeilichem Effektivitätsdenken orientiert. Alle IT-Systeme, sei es auf nationaler, sei es auf europäischer Ebene, sollen interoperabel gestaltet, soll heißen leicht miteinander abgleichbar, oder gleich anhand eines zentralen Personenkennzeichens (biometrisches Merkmal „Fingerabdruck“ u.a.) fix verknüpft

werden. Bestehende europäische IT-Systeme (Eurodac, VIS, SIS etc.) sollen dezidiert „über ihren derzeitigen Zweck hinaus“ genutzt werden bzw. künftige bzw. in Entwicklung befindliche europäische IT-Systeme von vornherein so gestaltet werden, dass eine Nutzung durch möglichst viele Behörden für mehrfache Zwecke möglich ist.

Im Lichte der obigen grundsätzlichen Überlegungen wird klar, dass der skizzierte Ansatz des Stockholmer Programms dem datenschutzrechtlichen Grundsatz der Zweckbindung fundamental entgegensteht.

Forcierung heimlicher Überwachungsmaßnahmen

In Kapitel II („Wahrung der inneren Sicherheit und äußeren Stabilität“), Pkt. 2 („Bekämpfung des globalen Terrorismus“), empfehlen die Autoren des Stockholmer Programms u.a. „speziellen Ermittlungstechniken auf der Agenda der Europäischen Union ein höherer Stellenwert“ einzuräumen. Was die Video-Überwachung anbelangt, so sollten unter anhand noch durchzuführender Analysen „weitere Maßnahmen erörtert werden“ (Rz 64).

Im Kontext des Zieles der Verhinderung der Terrorismusfinanzierung wird im Stockholmer Programm u.a. vorgeschlagen, die Zusammenarbeit zwischen den Zentralstellen für Verdachtsanzeigen zu verstärken, „wobei eine künftige Maßnahme etwa in der systematischen Überwachung von Finanztransaktionen in der Union bestehen könnte“. „Den für die Bekämpfung der Terrorismusfinanzierung zuständigen Strafverfolgungsbehörden sollten effizientere Rechtsinstrumente an die Hand gegeben werden, die ihnen die Nutzung von Datenbanken wie etwa SWIFT ermöglichen“ (Rz 66).

Im Kontext der Erhöhung der Transportsicherheit und zum besseren Schutz vor der illegalen Einfuhr gefährlicher Stoffe werden, Sicherheitsüberprüfungen der Mitarbeiter im Transportwesen in Verbindung mit Zugangsgenehmigungen zu kritischen Infrastrukturen“ vorgeschlagen (Rz 67).

Die obzitierten Aussagen im Stockholmer Programm deuten – wenngleich wenig konkret gehalten - auf einen verstärkten Trend hin zu heimlichen Überwachungsmaßnahmen hin, die die gesamte Bevölkerung treffen. Heimliche technische Überwachungsmaßnahmen sind v.a. deshalb problematisch, da die Betroffenen i.d.R. keinerlei Möglichkeiten haben, sich effektiv dagegen zur Wehr zu setzen bzw. unverhältnismäßige Eingriffe in ihre Privatsphäre einer rechtsstaatlichen

Kontrolle zu unterwerfen (Rechtsstaatsprinzip). Dies gilt insbesondere für die nicht näher ausgeführte „systematische Überwachung von Finanztransaktionen“ oder den Zugriff auf SWIFT, welcher in jüngerer Vergangenheit bekanntlich Ziel illegaler Überwachungsmaßnahmen durch US-Behörden war. Davon abgesehen widerspräche eine verdachtsunabhängige systematische Kontrolle auch dem Verhältnismäßigkeitsprinzip. An der tatsächlichen Wirksamkeit solcher, auf die Gesamtheit der Bevölkerung abzielender Maßnahmen müssen zudem massive Zweifel angemeldet werden.

Automatisierte Außengrenzkontrollen

Schon in der Mitteilung der Kommission vom November 2005 „über die Verbesserung der Effizienz der europäischen Datenbanken im Bereich Justiz und Inneres und die Steigerung ihrer Interoperabilität sowie der Synergien zwischen ihnen“ (siehe Dok. KOM [2005] 597 endg.) war die Rede von der „Einrichtung eines Einreise-/Ausreise-Erfassungssystems“ (siehe Pkt. 5.3.2). Ein solches würde die Registrierung Drittstaatsangehöriger unter Verwendung biometrischer Merkmale bei jeder Einreise in die Europäische Union und bei der Ausreise aus derselben bedeuten, so die Vorstellung der Kommission.

Das Stockholmer Programm knüpft an diese Überlegungen an und geht noch darüber hinaus. Während die Kommission noch 2005 meinte, „die Ausweitung eines derartigen Einreise-/Ausreise-Erfassungssystems auf EU-Bürger“ könne „nicht in Betracht gezogen werden, da dies dem Grundsatz des freien Personenverkehrs zuwiderlaufen würde“, ist jetzt auch von einem automatisierten Grenzkontrollsystem für EU-Bürger die Rede. Vordergründig mit dem Hinweis auf beschleunigte Abfertigung.

Hinsichtlich visapflichtiger Drittstaatsangehöriger ist zu sagen, dass diese sich ohnehin sehr weitgehenden Vorabkontrollen im Visumverfahren unterwerfen müssen. Eine zusätzliche „biometrische“, automatisiert ablaufende Kontrolle an der Grenze in Form einer „Selbstabfertigung“ wäre unverhältnismäßig 1. wegen der Erhebung biometrischer Daten ohne Notwendigkeit und 2. weil die lückenlose automatisierte Erfassung und Speicherung der Reisebewegungen die Erstellung und Auswertung von Bewegungsprofilen (Ein- und Ausreise, Ort, Zeit des Übertritts ergeben Frequenz, Hinweise auf örtliche bzw. persönliche/berufliche Beziehungen, Richtung der Reisetätigkeit [wo wird ein-, wo ausgereist], Wahl des Verkehrsmittels etc).

erlauben würde. Solche Profile würden mit Sicherheit über rein fremdenpolizeiliche Nutzungen hinaus herangezogen.

Für Unionsbürger, die einem analogen automatisierten System beim Überschreiten der Außengrenze unterworfen würden, stellt sich die Problematik gleichartig dar. Auch der insofern vom Stockholmer Programm weiterentwickelte Ansatz der automatisierten Grenzkontrollen erscheint daher mit fundamentalen Datenschutzgrundsätzen unvereinbar.

25. März 2009
Für den Datenschutzrat:
Der Vorsitzende:
WÖGERBAUER

Elektronisch gefertigt