Eidgenössisches Justiz- und Polizeidepartement

Anhang

zu den Erläuterungen zur Änderung der
Verordnung über das automatisierte Strafregister
(VOSTRA II)

Bundesamt für Justiz
Januar 2006

Neuregelung der Online-Zugriffsrechte des Bundesamtes für Polizei (fedpol) auf Strafregisterdaten

---

Inhaltsverzeichnis

1. Worum geht es?

Eine departementsinterne Überprüfung der gesetzlichen Grundlagen für die Online-Zugriffe des fedpol auf das Strafregister hat ergeben, dass die bestehenden gesetzlichen Regelungen weder den praktischen Bedürfnissen des fedpol noch den heutigen datenschutzrechtlichen Standards genügen.[1]

Dies ist zum Teil auch eine Folge der *Reorganisation des fedpol im Rahmen des Projektes „Strupol“*. Damals wurde die Führung des Strafregisters neu dem BJ unterstellt. Im Zuge dieser Arbeiten wurden von der Bundeskanzlei auch die entsprechenden Bestimmungen des StGB über die Bearbeitung von Informationen aus dem Strafregister angepasst: An Stelle des fedpol wurde in Artikel 360bis Absatz 1 Buchstabe a StGB neu das BJ als registerführende Behörde aufgeführt. Ferner wurde die formell gesetzliche Grundlage für *Online-Zugriffe des fedpol auf die “gerichtspolizeilichen Ermittlungsverfahren“ nach Artikel 360bis Absatz 1 Buchstabe c StGB beschränkt*. Dabei wurde übersehen, dass verschiedene Spezialdienste des fedpol damit keine formell-gesetzliche Grundlage für den Zugriff auf VOSTRA-Daten haben: so etwa der Dienst Interpol oder die Meldestelle für Geldwäscherei (MROS).

Da von einem "gerichtspolizeilichen Ermittlungsverfahren" im Sinne von Artikel 360bis Absatz 1 Buchstabe c StGB erst bei einer formellen Eröffnung des Strafverfahrens gesprochen werden kann, dürfen heute im Stadium des *Vorverfahrens* oder gar im *präventiven Bereich* keine Strafregisterdaten eingesehen werden. Diese Differenzierung schliesst wiederum verschiedene Dienststellen des fedpol von einem Registerzugriff aus, obschon auch diese Dienststellen zum Teil gute Gründe anführen können, weshalb sie Informationen aus dem Strafregister für Ihre Aufgabenerfüllung benötigen. In Zukunft sollen die Zugriffsberechtigungen beim fedpol daher nicht mehr vom Stadium des Verfahrens abhängen, sondern davon, ob der jeweilige Zweck des Datenzugriffs unter Berücksichtigung des Verhältnismässigkeitsprinzips eine Informationsvermittlung rechtfertigt.

Damit es beim Ausbau der Online-Zugriffsrechte des fedpol zu keiner unverhältnismässigen Aufweichung des Datenschutzes kommt, wurde bei der Ausarbeitung der neuen Regelung ein besonderes Augenmerk auf die Vermeidung sogenannter Schattenregister gelegt. Heute besteht das Problem, dass die vom fedpol aus dem Strafregister abgerufenen Daten in einer der fedpol-Datenbanken neu gespeichert werden dürfen, sofern die entsprechende Datenbankregelung die Erfassung von Strafdaten vorsieht. Sobald die VOSTRA-Daten jedoch in die Schattendatenbank gewandert sind, gelten für sie andere Zugriffszwecke, Weitergaberegeln oder Entfernungsfristen als diejenigen, die in der VOSTRA-Regelung des StGB vorgesehen sind. Aus diesem Grunde wird vorgeschlagen, die Speicherung und die Weitergabe

[1] Im Inspektionsbericht vom 13. Juni 2002 wurde das BJ vom Inspektorat des GS-EJPD unter anderem beauftragt, eine detaillierte Erhebung über die bestehenden und gewünschten Online-Zugriffe des fedpol auf VOSTRA durchzuführen, die Philosophie der VOSTRA-Zugriffe (auch hinsichtlich Umfang der Datenbekanntgabe, Weitergabe und Aufbewahrung von VOSTRA-Daten) im Grundsatz zu überprüfen und Vorschläge für eine allfällige Änderung des Strafgesetzbuches und der VOSTRA-Vo auszuarbeiten (vgl. die Empfehlungen Nr. 6 – 8 des erwähnten Inspektionsberichts). Die Ergebnisse dieser Prüfung wurden im Bericht des BJ vom 15. April 2003 festgehalten und den involvierten Amtsstellen (fedpol, BA und GS-EJPD) zur Stellungnahme unterbreitet. Diese EJPD-interne Vernehmlassung ergab, dass eine Änderung des StGB und der VOSTRA-Vo dringend geboten ist. Dieser „Anhang“ stellt eine überarbeitete und gekürzte Fassung des vorstehend genannten Berichts des BJ vom 15. April 2003 dar.

von Strafregisterinformationen durch die Datenempfänger nur unter ganz bestimmten Voraussetzungen zuzulassen.

Die im Rahmen dieses Berichtes gemachten Vorschläge für eine gesetzliche Umsetzung des neuen Konzepts zur Regelung der Online-Zugriffsrechte des fedpol zielen nicht auf eine Änderung des aktuell geltenden Rechts (Art. 359 ff. StGB), sondern auf eine *Änderung der vom Parlament bereits beschlossenen Artikel 359 ff. des neuen Allgemeinen Teils des Strafgesetzbuches* in der Fassung vom 13. Dezember 2002 (nStGB).[2]

Da der Gesetzgebungsprozess für eine Änderung der einschlägigen Bestimmungen des Strafgesetzbuches relativ viel Zeit in Anspruch nimmt, soll die Neuregelung der Online-Zugriffe des fedpol *zuerst auf Verordnungsstufe* erfolgen. Dieses Vorgehen hat den Vorteil, dass möglichst schnell eine transparente Rechtslage in Sachen fedpol-Zugriffsrechte geschaffen wird. Falls die Umsetzung auf Verordnungsstufe lediglich als *Übergangslösung im Hinblick auf die Regelung auf Gesetzesstufe* angesehen wird, ist diese Lösung auch durchaus stufenkonform. Eine entsprechende Ermächtigung findet sich in *Artikel 367 Absatz 3 nStGB* (bzw. Artikel 360bis Absatz 3 StGB). Die Neuregelung der Online-Zugriffe auf Verordnungsebene soll im Rahmen der Anpassung der VOSTRA-Verordnung an den neuen AT-StGB erfolgen. In diesem Bericht wird immer dann, wenn konkrete Vorschläge für eine gesetzliche Umsetzung gemacht werden, auch auf die entsprechenden Bestimmungen des Verordnungsentwurfs verwiesen (Vorentwurf zur Änderung der Verordnung über das automatisierte Strafregister, VE-VOSTRA-Vo).

Die Neuregelung der Online-Zugriffe des fedpol *auf Stufe StGB* wird demnach *erst in einer zweiten Phase* erfolgen. Die entsprechenden Änderungsvorschläge sollen dem Parlament (zusammen mit anderen, datenschutzrechtlich motivierten Änderungen im Strafregisterrecht) nach Inkrafttreten des neuen AT-StGB – also erst im Verlaufe des Jahres 2007 - vorgelegt werden.

[2] Der Bundesrat hat den Zeitpunkt des Inkrafttretens des neuen AT-StGB noch nicht bestimmt; angestrebt wird jedoch eine Inkraftsetzung auf den 1.1.2007. Der Grund dafür, dass der Inkraftsetzungsbeschluss noch aussteht, liegt darin, dass das Parlament zurzeit noch über „dringliche Nachbesserungen“ am neuen AT-StGB zu beraten hat, die noch vor dessen Inkraftsetzung beschlossen werden sollen (Botschaft des Bundesrates vom 29. Juni 2005 zur dringlichen Nachbesserung des neuen AT-StGB vom 13. Dezember 2002). Um die Inkraftsetzung des revidierten AT-StGB nicht noch zusätzlich zu verzögern, wurde auch darauf verzichtet, die Neuregelung der Online-Zugriffsrechte des fedpol im Rahmen dieser dringlichen Nachbesserungen am neuen AT-StGB durchzuführen.

2. Leitlinien für die Neuregelung der Zugriffsrechte des fedpol

2.1 Zur Problematik einer Zugriffsgewährung nach Verfahrensstadien

Eine der zentralen Fragen bei der Neuregelung der Zugriffe des fedpol auf VOSTRA ist, ob bestimmte Stellen des fedpol[3] nicht nur im Rahmen von *eröffneten Strafverfahren* (gem. Art. 365 Abs. 2 nStGB, Art. 359 Abs. 2 StGB*)*, sondern bereits für die Vorermittlungen[4] und für präventive Aufgaben Strafregisterdaten erhalten sollen.

Die gebräuchliche Grenzziehung für die Zugriffsberechtigung *nach verschiedenen Verfahrensabschnitten (Prävention / Vorermittlungen / eröffnete Strafverfahren*) erweist sich bei näherer Prüfung als wenig sachgerecht und ist deshalb eine ungeeignete Richtschnur für die Gewährung von Zugriffsberechtigungen.

Für ein Abstellen auf den Zeitpunkt der Verfahrenseröffnung spricht, dass Strafregisterinformationen *unverzichtbar* sind, um im *Rahmen der Strafzumessung* Aussagen über das Vorleben des Beschuldigten zu machen, oder um über die Gewährung des bedingten Strafvollzuges entscheiden zu können.

Strafregisterinformationen werden im Rahmen von eröffneten Strafverfahren jedoch *auch für andere Zwecke angefordert*, wie etwa für die Erhärtung eines Tatverdachts und für die Glaubwürdigkeitsprüfung von Zeugen und Sachverständigen etc. Auch diese Zwecke lassen sich problemlos unter den allgemeinen Zweck der „Durchführung von Strafverfahren“ (gemäss Art. 365 Abs. 2 Bst. a nStGB, Art. 359 Abs. 2 Bst. a StGB) bzw. von „gerichtspolizeilichen Ermittlungsverfahren“ (im Sinne von Art. 367 Abs. 2 Bst. c nStGB, Art. 360^{bis} Abs. 2 Bst. c StGB) subsumieren.

Analysiert man diese Unterzwecke, für die Strafregisterinformationen bisher im Rahmen eines eröffneten Strafverfahrens eingefordert wurden, so stellt man fest, dass sie aus den gleichen Gründen *auch in anderen Verfahrensstadien (d.h. bei Vorermittlungen und sogar im Präventivbereich)* bedeutsam sein können.

Die Beschränkung von Strafregisterinformationen auf eröffnete Strafverfahren lässt sich auch mit dem *Argument des Persönlichkeitsschutzes nicht* rechtfertigen. Bisher wurde argumentiert, dass dann, wenn ein Strafverfahren erst einmal eröffnet ist, derjenige, der davon betroffen ist, erhöhte Eingriffe in seine Persönlichkeitsrechte zu dulden hat. Die Verfahrenseröffnung bei entsprechender Verdachtslage bilde die Grenze, ab der der Einzelne zunehmende staatliche Intervention hinnehmen müsse. Im Vorfeld sei deshalb eine grössere Zurückhaltung des Staates angezeigt. Dieses Argument mag zwar für den Beschuldigten seine Richtigkeit haben, es ist aber insgesamt fehl am Platze, da – wie bereits erwähnt - im Rahmen von eröffneten Strafverfahren bereits heute Strafregisterauszüge über nichttatverdächtige Verfahrensbeteiligte (Zeugen oder Auskunftspersonen) eingeholt werden, denen im Verfahren eine ganz andere Stellung zukommt.

Die Beschränkung der Zugriffsberechtigung auf eröffnete Strafverfahren lässt sich auch nicht mit dem Akteneinsichtsrecht begründen. Es wird argumentiert, dass eine

---

[3] Insbesondere die Stellen der BKP, welche sich mit der Verfolgung von Straftaten befassen und der Dienst Operationen des DAP, der präventiv tätig ist.

[4] Der Begriff "Vorermittlungen" basiert auf Artikel 2 der Verordnung über die Wahrnehmung kriminalpolizeilichen Aufgaben im Bundesamt für Polizei (SR 360.1). Gemäss dieser Bestimmung führt die Bundeskriminalpolizei als gerichtliche Polizei des Bundes unter der Leitung der Bundesanwaltschaft Vorermittlungs- und Ermittlungsverfahren im Zuständigkeitsbereich des Bundes durch, wenn tatverdachtsbegründende Hinweise und Informationen vorliegen.

Person, der die Beschuldigtenrolle im Strafprozess zugewiesen wird, ihr Akteneinsichtsrecht wahrnehmen und verifizieren kann, ob über sie ein Strafregisterauszug beschafft worden ist. Da das Akteneinsichtsrecht grundsätzlich nur den Parteien im Strafverfahren zusteht (vgl. etwa Art. 174 StPO-SG), vermag diese Theorie nicht zu erklären, weshalb dann das Einholen eines Strafregisterauszuges über Zeugen möglich sein soll, denn diese haben bekanntlich kein Akteneinsichtsrecht.

Aus all diesen Gründen ist für die Frage der Zugriffsberechtigung der Zweck der Datenerhebungen viel aussagekräftiger als das Stadium, in welchem sich das Verfahren gerade befindet[5].

2.2 Zur Bedeutung des Zweckgedankens für die Zugriffsgewährung

Die Zweck-Norm des Artikels 365 Absatz 2 nStGB (Art. 359 Abs. 2 StGB) bildet den programmatischen Auftakt der Strafregisterregelung im nStGB. Entscheidend für die Frage, ob ein Zugriff auf Strafregisterdaten gewährt werden darf oder nicht, ist also primär, zu welchem Zweck dieser Datenaustausch erfolgt.

Die Zwecke, für die ein Zugriff auf Strafregisterinformationen zu gewähren ist, sind nicht beliebig erweiterbar. Bereits aus dem Verhältnismässigkeitsprinzip lässt sich ableiten, dass nur *Zwecke von Bedeutung sein können, die sich ohne Strafregisterinformationen nicht oder nur sehr schwer verwirklichen lassen*. Mit anderen Worten: Der Zugriff auf Strafregisterdaten ist nur dann legitim, wenn er zur Erfüllung einer spezifischen gesetzlichen Aufgabe *erforderlich bzw. notwendig* ist - nicht aber, wenn der Zugriff bloss angenehm wäre.

Es steht ausser Zweifel, dass Strafregisterinformationen grundsätzlich für alle Behörden interessant sind, welche eine Person einschätzen müssen. So gesehen hätte auch die SUVA ein Interesse an einem Einblick in Strafregisterdaten, wenn es darum geht abzuklären, ob sie den Angaben des Leistungsempfängers trauen kann oder nicht. Nach der hier vertretenen Auffassung sollten Behörden jedoch nur dann Zugriff auf Strafregisterinformationen erhalten, wenn die Information *für eine effiziente Aufgabenerfüllung der betroffenen Behörde von wesentlicher Bedeutung* ist. Da Strafregisterdaten besonders schützenswerte Daten sind, ist der *Zugriff auf Strafregisterinformationen im Zweifel eher zu verneinen*.

Welches sind nun aber die Zwecke, die für das fedpol von Bedeutung sein könnten? Das fedpol ist kein einheitliches Gebilde. Es besteht aus einer Vielzahl von Diensten, welche z.T. sehr *unterschiedliche Aufgaben* erfüllen. Insofern ist auch der Zweck, weshalb Strafregisterinformationen vom fedpol angefordert werden, *nicht* auf einen *einheitlichen, hinreichend präzisen Nenner* zu bringen.

[5] Dies heisst nun aber nicht, dass eine Grenzziehung nach Verfahrensstadien immer falsch wäre, wie das Beispiel der Auskünfte im Bereich Interpol zeigt (vgl. dazu die Ausführungen unten in Ziff. 2.4.3). Da sich die Schattenregisterproblematik (Weitergabe, Speicherung, Missbrauchskontrolle etc.) bei einer Übermittlung der Daten ins Ausland meist nicht regeln lässt, kann es trotzdem angezeigt sein, die Zugriffe auf bestimmte Verfahrensstadien zu begrenzen. Mit einer Begrenzung der Zahl der Gesuche (z.B. im Rahmen eröffneter Strafverfahren) wird auch das Missbrauchspotential verringert.

Hinsichtlich der Zweckbestimmung von Strafregisterdaten lassen sich die fedpol-Stellen in zwei Gruppen aufteilen: die Ermittlungsdienste sowie die Spezialdienste:

- **Gruppe: Ermittlungsdienste:**

  Es gibt fedpol-Dienste, welche in erster Linie polizeiliche Ermittlungen zur Verhütung und Verfolgung von Straftaten durchführen. Bei diesen Stellen hängt die Zugriffsberechtigung heute vom Verfahrensstadium (eröffnetes Strafverfahren) ab. Diese Dienste benötigen Strafregisterdaten letztlich vor allem zu vier Hauptzwecken, welche nachfolgend genauer umschrieben werden. Teilt man die Auffassung, dass der Zugriff auf Strafregisterdaten zur Erreichung dieser Zwecke Sinn macht, so darf man den Datenzugriff nicht mehr vom Stand des Verfahrens abhängig machen, da diese Zwecke unter Umständen bereits im Stadium der Vorermittlungen oder gar im präventiven Bereich zum Tragen kommen:

  Strafregisterdaten werden von den fedpol-Ermittlungsdiensten vor allem für folgende vier Hauptzwecke benötigt:

  Zweck 1: Erhärtung oder Entkräftung eines Anfangsverdachts
  (Eingrenzung des Täterkreises)

  Die Tatsache, dass eine verdächtige Person im Strafregister wegen einschlägiger Delikte verzeichnet ist, liefert *erste Anhaltspunkte* für die Konkretisierung eines vagen Anfangsverdachts. Strafregisterinformationen über abgeurteilte Taten können jedoch *nicht als beweistaugliche Indizien* für die neu zur Last gelegten Delikte gewertet werden. Diese Informationen werden vom fedpol vielmehr als *Hinweis* gewertet*, dass sich zusätzliche Abklärungen lohnen könnten*. Somit besteht zwar die Gefahr, dass die frühzeitige Gewährung von Strafregisterinformationen zu einer Konzentration der Ermittlungstätigkeit auf wenige Wiederholungstäter führen könnte - obschon die Zahl der Ersttäter bedeutend grösser ist. Da Strafregisterdaten jedoch *nie die einzigen Verdachtsindikatoren* sind, wird dies nur in Einzelfällen falsche Ermittlungsentscheide provozieren. Da diese Daten wichtige Querverbindungen aufzeigen, um die Ermittlungen in eine Erfolg versprechende Richtung zu lenken, sollte dem fedpol die Zugriffsberechtigung auf Strafregisterdaten zum Zwecke der Erhärtung eines Anfangsverdachts nicht verwehrt werden.

  Zweck 2: Verhinderung von „Parallelermittlungen“

  Zur Verhinderung von Parallelermittlungen bedarf es eines Zugriffs auf den Datensatz betreffend hängige Strafverfahren.

  Dabei geht es darum zu erkennen, ob von verschiedenen Strafbehörden gleichzeitige Ermittlungen gegen eine bestimmte Person geführt werden. Dies kann in folgenden Konstellationen der Fall sein:

  - Wenn jemand *eine strafbare Handlung* an mehreren Orten ausgeführt hat oder der Erfolg an mehreren Orten eingetreten ist (Art. 346 Abs. 2 StGB). Allein deshalb ist jedoch noch kein Zuständigkeitskonflikt *zwischen dem fedpol und den Kantonen* zu befürchten, denn entscheidend ist, ob das in Frage stehende Delikt in die Bundeszuständigkeit fällt.
  - Wenn jemand *mehrere strafbare Handlungen an verschiedenen Orten verübt* hat (Art. 350 Ziff. 1 StGB). Zu Parallelermittlungen zwischen fedpol und Kanto-

nen kommt es jedoch nur dort, wo diesfalls mindestens ein Delikt – aufgrund von Art. 340 StGB - in die Zuständigkeit des fedpol fällt[6].

- Wenn eine *fakultative Bundeskompetenz* im Sinne von Artikel 340bis StGB besteht und nicht ausgeschlossen werden kann, ob ein Kanton nicht bereits eine Untersuchung angehoben oder gar ein rechtskräftiges Urteil[7] gefällt hat. Dies betrifft die in den Artikel 260ter, 260^{quinquies}, 305bis, 305ter und 322ter - 322^{septies} StGB erfassten Delikte sowie Verbrechen, die von einer kriminellen Organisation i.S.v. Artikel 260ter StGB ausgehen.

Informationen über hängige Strafverfahren werden im Strafregister immer bezogen auf den Beschuldigten vermerkt. Durch Einblick ins Strafregister lassen sich daher „Parallelermittlungen“ im Dunstkreis eines Tatverdächtigen nicht verhindern, da nirgends registriert wird, gegen wen sich die Ermittlungen sonst noch richten.

Vor allem diejenigen Stellen des fedpol, welche auch Koordinationsaufgaben wahrnehmen, können diesen Zugriffszweck für sich in Anspruch nehmen.

Zweck 3: Informationsvorsprung für Befragungen
(Glaubwürdigkeitsüberprüfung)

Befragungen können effizienter gestaltet werden, wenn der Befragende bereits zu Beginn der Befragung möglichst viele Kenntnisse über die einvernommene Person besitzt. Gerade Vorkenntnisse über die Deliktsvergangenheit sind dabei von besonderem Interesse, da sie ein wirksames Mittel sind, die Glaubwürdigkeit der betroffenen Person zu überprüfen. Bei Befragungen von Personen, über die sonst keine Informationen vorhanden sind, ist der Zugriff auf Strafregisterinformationen unumgänglich.

Zweck 4: Schutz von verdeckten Ermittlern
(Abklärung des Täterumfeldes)

Auch hier handelt es sich um einen Zweck, der sich nicht auf alle fedpol-Dienste bezieht, sondern vornehmlich auf das Gesuch der Organisationseinheit Spezialeinsätze/Kommissariat verdeckte Ermittlungen der Bundeskriminalpolizei (BKP).

Für die Planung eines V-Mann-Einsatzes ist es äusserst wichtig zu wissen, in welchem Umfeld der verdeckte Ermittler tätig ist. Um das Risiko eines Einsatzes besser abschätzen zu können, sind Informationen über das Vorleben der in dem betreffenden Milieu sich bewegenden Personen unerlässlich. Der Zugriff auf Strafregisterinformationen stellt ein wirksames Mittel dar, V-Männer besser auf ihren Einsatz vorzubereiten.

[6] Nach Artikel 340bis Absatz 1 StGB besteht eine ausschliessliche und nach Absatz 2 eine fakultative Zuständigkeit des Bundes.
[7] Diesfalls wäre auch ein Zugriff auf Urteilsdaten nötig, um abzuklären, ob die Aufnahme von Vorermittlungen überhaupt nötig ist.

- **2. Gruppe: Spezialdienste**

  Diese fedpol-Stellen sind mit ganz besonderen Aufgaben betraut. Entsprechend benötigen diese Funktionen Zugriff auf Strafregisterdaten auch für ganz spezifische Zwecke, welche sich nicht mehr auf den allgemeinen Nenner „Durchführung von Strafverfahren“ bringen lassen (vgl. etwa die Ausführungen zu den Spezialdiensten MROS, Kontrolldienst-JANUS oder zum Ausländerdienst).

2.3 Zu weiteren Gesichtspunkten, die zu berücksichtigen sind

Wie erwähnt, ist der Zugriff auf Strafregisterinformationen generell nur dann zu gewähren, wenn dies notwendig ist, um eine bestimmte Aufgabe erfüllen zu können, nicht aber, wenn der Zugriff bloss angenehm wäre. Eine Aufweichung dieses Prinzips scheint auch aus folgenden Gründen nicht angezeigt.

- Bereits heute haben zahlreiche „Polizeistellen“ Zugriff auf Strafregisterdaten. So die kantonale Fremdenpolizei und die Strassenverkehrsämter. Der Zugriff ist aber bei diesen Stellen allein dadurch motiviert, dass sie ihre *Aufgaben ohne Strafregisterinformationen nicht erfüllen* könnten.
- Durch eine möglichst umfassende Verfügbarkeit von (Strafregister-)Informationen können *Effizienzsteigerungen bei der Verhütung und Verfolgung von Straftaten* erreicht werden. Im Zuge der Ereignisse des 11. Septembers 2001 wurde eine Verbesserung der polizeilichen Schlagkraft namentlich im Bereich der Terrorismusbekämpfung auch vermehrt gefordert (vgl. die entsprechenden parlamentarischen Vorstösse). Generell wird jedoch auch im Parlament die Meinung vertreten, dass solche Effizienzsteigerungen möglichst *nicht auf Kosten einer Aufweichung des Datenschutzes* gehen sollten. Dies zeigen auch die Reaktionen auf den Änderungsentwurf zum Datenschutzgesetz.
- Auch das rechtspolitische Konzept des Strafregisters, wonach eine Person, die einmal einen Fehler begangen hat, diesen „Rucksack“ nicht ihr ganzes Leben lang mit sich herumtragen soll, spricht gegen eine allzu extensive Ausgestaltung der Zugriffsrechte.
- Aus rechtsvergleichender Sicht sind keine klare Tendenzen auszumachen. In Österreich hat die Bundesgendarmerie allgemein Zugriff. Auch in Deutschland dient das Strafregister sowohl der Verhütung als auch der Verfolgung von Straftaten. In Frankreich wird zwischen verschiedenen Formen von Auszügen (sog. Bulletins) unterschieden.[8]

[8] Ein Vollauszug ist nur für Justizbehörden erhältlich; Administrativbehörden werden zu genau definierten Zwecken nur Teilauszüge ausgehändigt; auch Private erhalten lediglich einen Teilauszug.

2.4 Zur Problematik der Schattenregister

2.4.1 Erster Teilaspekt: Speicherung von Strafregisterdaten ausserhalb der VOSTRA-Datenbank (neuer Art. 17 Abs. 2 VE-VOSTRA-Vo; Änderung von Art. 367 nStGB)

So genannte Schattenregister sind personenbezogene Datenbanken, in denen – wenigstens teilweise - die gleichen Informationen wie im Ursprungsregister gespeichert bzw. aufbewahrt werden und dort unmittelbar abrufbar sind.

Das Problem der Schattenregister liegt v.a. darin, dass Daten in der „Schattendatenbank" oft *zu einem anderen Zweck gespeichert und abgerufen* werden, als dies nach den Bestimmungen der Ursprungsdatenbank möglich wäre[9]. Auch gelten für die betroffenen Datensammlungen *meist andere Löschungsfristen*. Die Daten führen daher in den Schattendatenbanken - aus Sicht des Ursprungsregisters - ein Eigenleben und werden gewissermassen zweckentfremdet. Die Transparenz des Datenbearbeitens geht so zu einem guten Stück verloren. Schattenregister sind daher nach Möglichkeit zu vermeiden.

Ein Konzept zur Vermeidung von Schattenregistern bestünde darin, dass Daten nur noch abgefragt, nicht aber gespeichert werden dürfen. Dies hätte den Vorteil, dass mangels Speicherung *keine Zweckentfremdung* mehr möglich wäre und dass *keine unterschiedlichen Löschungsfristen* mehr bestünden[10].

Das fedpol könnte damit leben, dass keine Strafregisterdaten in den Datenbanken des fedpol gespeichert werden, wenn die Daten permanent abgefragt werden könnten; allenfalls würde die *Speicherung eines Bearbeitungsvermerkes* (d.h. ob Abfrage erfolgt ist, oder ob eine Interpol-Anfrage bearbeitet worden ist)[11] genügen. Es bestehen jedoch Zweifel, ob sich dieses Idealkonzept so einfach verwirklichen lässt. Denn es stösst insbesondere auf folgende Hindernisse:

- Die *elektronische Speicherung* oder das *Aufbewahren in Papierform* von Strafregisterinformationen ausserhalb von VOSTRA lässt sich nicht verhindern. Soweit Strafregisterdaten herangezogen werden, um Verfügungen, Entscheide oder weitere Verfahrensschritte zu *begründen*, müssen diese Informationen zwangsläufig – nämlich *als Teil der Begründung* – auch elektronisch erfasst oder in Papierform

[9] In den einschlägigen Gesetzesgrundlagen für die jeweilige Datenbanken das fedpol (Janus, IPAS, ISIS etc.) wird zwar bestimmt, zu welchem Zweck und unter welchen Voraussetzungen Informationen aufbewahrt werden dürfen. Diese Zwecke sind indessen mit den Zwecken des Strafregisters nicht deckungsgleich, so dass es zu einer Zweckentfremdung der Strafregisterdaten kommt. Zudem funktionieren fedpol-Datenbanken nach dem „Prinzip der Verlängerung der Löschungsfristen"; somit können Strafregisterdaten in fedpol-Datenbanken vorhanden sein, die gemäss VOSTRA schon längst hätten entfernt oder gelöscht werden müssen.

[10] Unterschiedliche Löschungsfristen lassen sich kaum vermeiden. Eine *elektronische Koppelung* der Löschungsfristen wäre technisch nur mit unverhältnismässigem Aufwand durchführbar und eine materielle *Vereinheitlichung der Löschungsfristen* in den betreffenden Datenbankgesetzen hätte ebenfalls nicht die erhoffte Wirkung, da die Entfernung eines Eintrages u.a. vom Vollzug der Sanktion abhängt und das fedpol heute nicht über die entsprechenden Meldungen verfügt. Das Problem liesse sich nur dadurch beheben, dass das Strafregister alle Empfängerdatenbanken informiert und Ihnen die erfolgten Entfernung mitteilt, was praktisch ebenfalls kaum technisch durchführbar wäre.

[11] Schlimmer als die Speicherung der Daten selbst wäre jedoch die Speicherung eines *Vermerks, dass Daten vorhanden, bzw. weitergegeben worden sind*, denn diese Information kann an sich verfänglicher sein, als die eigentliche Registerinformation selbst.

abgelegt werden können. Es muss jedoch verhindert werden, dass VOSTRA-Daten gespeichert werden, wenn mit diesen Daten erst später ein Entscheid begründet werden soll. Dieses Speicherungsverbot soll durch ein permanentes Einsichtsrecht kompensiert werden.

- Ferner würde ein generelles Verbot (elektronischer) Speicherung von Informationen aus dem Strafregister auch verhindern, dass Aktendossiers zwecks Archivierung *elektronisch gescannt* werden können.
- Ein allfälliges Speicherungsverbot dürfte zudem nur auf *deliktsspezifische Informationen* im Sinne von Artikel 366 Absatz 2 - 4 nStGB beschränkt werden. Gegen eine elektronische Speicherung des *Personaliensatzes* – wie dies etwa für den Kontrolldienst der Datenbank "JANUS" von Bedeutung sein kann – wäre nichts einzuwenden. Denn hierbei handelt es sich nicht um besonders schützenswerte Daten.

Vorgeschlagene Änderung

Um den vorstehend umschriebenen Problemen Rechnung zu tragen, wird vorgeschlagen, Artikel 367 nStGB durch einen neuen Absatz zu ergänzen, wonach Strafregisterdaten nach Artikel 366 Absatz 2 - 4 nStGB nicht isoliert in einer neuen Personendatenbank gespeichert oder aufbewahrt werden, sondern nur dann, wenn dies zur Begründung eines getroffenen Entscheides, einer erlassenen Verfügung oder eines eingeleiteten Verfahrensschritts notwendig ist.

Für die Zeit bis zur Umsetzung dieses Vorschlags auf Gesetzesstufe wird vorgeschlagen, die Verordnung zum automatisierten Strafregister mit einer entsprechenden Bestimmung zu ergänzen (Art. 17 Abs. 2 VE-VOSTRA-Vo).

Diese Regel wurde zwar im Hinblick auf den Ausbau der fedpol-Online-Zugriffsrechte entwickelt; sie *soll jedoch für alle Behörden gelten, welche Informationen aus dem Strafregister erhalten*.

2.4.2 Zweiter Teilaspekt: Weitergabe der Daten an Dritte (neuer Art. 17 Abs. 3 VE-VOSTRA-Vo; Änderung von Art. 367 nStGB)

Auch die Weitergabe der Information durch den Informationsempfänger ist ein Teilproblem der Schattenregisterproblematik, denn wenn die Informationen an Dritte weitergegeben werden, sind sie der Bewirtschaftung durch den Herrn der Ursprungsdatenbank entzogen; sie führen dann wieder ein Eigenleben, was zu den vorstehend erwähnten Problemen führen kann. Zudem könnte die Weitergabe zu ganz anderen Zwecken erfolgen, als dies in der VOSTRA-Regelung vorgesehen ist.

Um das Problem der Weitergabe gesetzlich zu lösen, ist im StGB (das die Hauptregelung für das Strafregister enthält) zu definieren, wer Strafregisterdaten erhalten soll und an wen und unter welchen Voraussetzungen diese Stellen die Daten allenfalls weitergeben dürfen.

Die einfachste Lösung wäre zweifelsohne auch hier ein *generelles Verbot der Weitergabe* von Strafregisterinformationen. Doch wäre eine solche Regelung kaum praktikabel:

- Bei einem Weitergabeverbot müsste allen Stellen, welche Strafregisterdaten benötigen und diese bisher aus anderen Datenbanken erhalten haben, ein Zugriff auf VOSTRA erteilt werden. Diese Empfänger zu ermitteln, stellt allerdings ein kaum zu bewältigendes Unterfangen dar.
- Ein generelles Weitergabeverbot von Strafregisterdaten würde auch verhindern, dass Entscheide oder Verfügungen, die Strafregisterinformationen enthalten, weitergegeben werden können. In Fällen, in denen VOSTRA-Daten an einem anderen Ort gespeichert und mit anderen Daten verknüpft werden dürfen (vgl. die Ausführungen oben in Ziff. 2.4.1.) sollte daher grundsätzlich auch eine Weitergabe möglich sein.

Ein pauschales gesetzliches Verbot der Weitergabe von Strafregisterinformationen schiesst auch deshalb über das Ziel hinaus, weil man nur die *Zweckentfremdung* der Strafregisterdaten verhindern will.

Vorgeschlagene Änderung

Aus all diesen Gründen ist in Artikel 367 nStGB ein neuer Absatz vorzusehen, wonach die Weitergabe von Strafregisterdaten zu anderen Zwecken - als diejenigen, die im VOSTRA definiert sind – verboten ist, selbst wenn für die Weitergabe der Daten in der einschlägigen Schattendatenbankregelung eine gesetzliche Grundlage vorhanden wäre.

Für die Zeit bis zur Umsetzung dieses Vorschlags auf Gesetzesebene wird vorgeschlagen, die Verordnung zum automatisierten Strafregister mit einer entsprechenden Bestimmung zu ergänzen (Art. 17 Abs. 3 VE-VOSTRA-Vo).

Auch diese Klausel wurde zwar im Hinblick auf den Ausbau der fedpol-Online-Zugriffsrechte entwickelt; sie *soll jedoch für alle Behörden gelten, welche Informationen aus dem Strafregister erhalten*.

Es versteht sich von selbst, dass diese Regelung nicht als Grundlage für die Weitergabe von Strafregisterdaten schlechthin verstanden werden kann. Für diese braucht es – entsprechend den datenschutzrechtlichen Grundsätzen – eine selbständige gesetzliche Grundlage.

Den neuen Empfängern der Strafregisterdaten ist die Speicherung ebenfalls nur unter sehr eingeschränkten Voraussetzungen erlaubt. D.h. die neue Speicherungsregel gemäss Artikel 17 Abs. 2 VE-VOSTRA-Vo (welche später in Art. 367 nStGB integriert werden soll; vgl. die Ausführungen oben in Ziff. 2.4.1) gilt auch für Daten, die an Dritte weitergeben werden.

Abschliessend ist festzuhalten, dass zwar auch *das Datenschutzgesetz* (DSG, SR 235.1) Bestimmungen enthält, die sich an den Gedanken der Zweckbindung anlehnen, es löst jedoch die oben umschriebene Schattenregisterproblematik nicht. So genügt es nach Artikel 4 Absatz 3 DSG, dass der Zweck der Bearbeitung der Daten gesetzlich geregelt ist. Die oben dargestellte Weitergaberegel erweist sich daher als unverzichtbar.

2.4.3 Sonderfall: Datenweitergabe ins Ausland / Speicherung im Ausland

Das Schattenregisterproblem besteht auch bei der Datenweitergabe von Strafregisterdaten ins Ausland. Es stellt sich die Frage, ob den ausländischen Stellen dieselben Auflagen (betreffend Speicherung und Weitergabe) gemacht werden können, wie den schweizerischen Behörden.

- Was den Datenaustausch mit *Europol* betrifft, dürfte es in Zukunft ohne Probleme möglich sein, dem Ausland entsprechende Bearbeitungsbeschränkungen aufzuerlegen. Das Abkommen zwischen der Schweizerischen Eidgenossenschaft und dem Europäischen Polizeiamt (welches das Parlament am 7. Oktober 2005 genehmigt hat, aber bisher noch nicht in Kraft gesetzt worden ist; vgl. BBl 2005 5971) verpflichtet Europol, sich an allfällige Bearbeitungsbeschränkungen zu halten, welche ihm durch die schweizerischen Behörden auferlegt werden (vgl. Art. 7 Ziff. 4[12] und Art. 8 Ziff. 1[13] des Europol-Übereinkommens). Welche Bearbeitungsbeschränkungen dies sind, sagt das Übereinkommen jedoch nicht. Deshalb musste auch eine innerstaatliche Rechtsgrundlage für den Datenaustausch mit Europol geschaffen werden. Der neue Artikel 351^{novies} StGB[14] sieht vor, dass das fedpol Europol diejenigen Bearbeitungsbeschränkungen auferlegt, die gemäss innerstaatlichem Recht auch für die entsprechende Tätigkeit des fedpol gelten würden.[15]

- Anders liegt die Sachlage im Bereich *Interpol*.[16] An sich ist die ausländische Interpol-Stelle, wenn sie Daten vom fedpol erhält, *weder* an die neu vorgeschlagene Speicherungsregel gemäss Artikel 17 Absatz 2 VE-VOSTRA-Vo (vgl. oben Ziff. 2.4.1) *noch* an die Weitergabenorm gemäss Artikel 17 Absatz 3 VE-VOSTRA-Vo (vgl. oben Ziff. 2.4.2) *gebunden*, da sich diese Bestimmungen *nur an schweizerische Behörden* richten.

  Die Interpol-Verordnung (SR 351.21) sieht in Artikel 10 Absatz 2 zwar vor, dass die Empfängerinnen und Empfänger die Daten nur zu dem Zweck bearbeiten dürfen, für den sie ihnen weitergeben worden sind. Soweit es sich bei diesen Empfängern um ausländische Amtsstellen handelt, kann die Verordnungsbestimmung

---

[12] *Die Schweiz stellt Europol nur Informationen zur Verfügung, die in Übereinstimmung mit ihren innerstaatlichen Rechtsvorschriften eingeholt, gespeichert und übermittelt worden sind.*

[13] *Die Schweiz unterrichtet Europol zum Zeitpunkt der Informationsübermittlung oder vorher über den Zweck, zu dem die Informationen übermittelt werden, sowie über jegliche Beschränkung hinsichtlich ihrer Verwendung, Löschung oder Vernichtung einschliesslich etwaiger allgemeiner oder besonderer Zugriffsbeschränkungen.*

[14] Vgl. Bundesbeschluss vom 7. Oktober 2005; BBl 2005 5971. Diese Bestimmung wurde noch nicht in Kraft gesetzt. Mit dem Inkrafttreten der Änderung vom 13. Dez. 2002 des Allgemeinen Teils des Strafgesetzbuches wird Art. 351^{novies} zum neuen Art. 355a StGB (vgl. FN 5 in BBl 2005 5971).

[15] Art. 351^{novies} StGB hat folgenden Wortlaut:
[1] Das Bundesamt für Polizei kann dem Europäischen Polizeiamt (Europol) Personendaten, einschliesslich besonders schützenswerter Personendaten und Persönlichkeitsprofile, weitergeben.
[2] Für die Weitergabe dieser Daten gelten insbesondere die Voraussetzungen nach den Artikeln 3 und 10–13 des Abkommens vom 24. September 2004 zwischen der Schweizerischen Eidgenossenschaft und dem Europäischen Polizeiamt.
[3] Gleichzeitig mit der Weitergabe von Daten unterrichtet das Bundesamt für Polizei Europol über die Zweckbestimmung der Daten sowie über alle Beschränkungen hinsichtlich ihrer Bearbeitung, die ihm selbst nach Massgabe der eidgenössischen oder kantonalen Gesetzgebung auferlegt sind.

[16] Vgl. auch die Ausführungen in Ziff. 3.4.

aber *keine rechtliche Verbindlichkeit für die Datenbearbeitung im Ausland* bewirken.

Das Gleiche gilt für Artikel 10 Absatz 3 Buchstabe b der Interpol-Verordnung. Nach dieser Bestimmung unterrichtet das Nationale Zentralbüro (NZB)[17] die ausländischen NZB bei jeder Vermittlung von Daten über alle anderen Bearbeitungsbeschränkungen, welche dem NZB nach Massgabe der eidgenössischen oder kantonalen Gesetzgebung auferlegt sind. Diese Bestimmung hat *keine staatsvertragliche Absicherung* wie bei Europol.

Beim Datenaustausch mit Interpol besteht also die Gefahr, dass *Strafregisterdaten ins Ausland wandern, ohne dass sich Schattenregister vermeiden lassen.*

Die Schattenregisterproblematik liesse sich nur durch einen weitgehenden Verzicht auf Speicherung in anderen Datenbanken vermeiden. Ein solcher Verzicht scheint aber nur dort praktikabel, wo jederzeit problemlos auf die Ursprungsdatenbank zugegriffen werden kann. Da den ausländischen Polizeistellen – aus innenpolitischen Gründen und wegen der unübersehbar grossen Zahl der Anschlussbegehren - kein direkter Zugriff auf VOSTRA gewährt werden kann (zumal dies ebenfalls eine detaillierte Analyse der Aufgaben voraussetzen würde), muss die Speicherung übermittelter Informationen im Ausland wohl hingenommen werden.

Umgekehrt kann man dem fedpol aus aussenpolitischen Gründen die Weitergabe von Strafregisterdaten an Interpol nicht generell verbieten. Nach Auffassung des fedpol drohe die Gefahr einer internationalen Isolierung der Schweiz, wenn der Datenaustausch mit Interpol an allzu restriktive Voraussetzungen gebunden werde.

All diese Überlegungen zeigen, dass es notwendig ist, für den Austausch von Strafregisterinformationen mit dem Ausland eigene Regeln zu entwickeln. Beim Datenaustausch mit dem Ausland muss daher ein etwas einfacheres, standardisiertes Vorgehen angewandt werden. Zu berücksichtigen ist auch, dass die Informationsvermittlung ins Ausland letztlich auch ein Abbild des innerstaatlichen Informationsflusses sein sollte.

Obschon die Schweiz für ausländische Interpol-Empfänger die Speicherung und die Weitergabe nicht rechtlich verbindlich regeln und kontrollieren kann, stellt sich dennoch die Frage, unter welchen Voraussetzungen die Schweiz bereit ist, Strafregisterdaten ins Ausland zu transferieren – im Wissen darum, dass man keine Gewähr hat, dass sich die ausländischen Stellen an den zugesicherten Verwendungszweck halten werden und die Daten daher (wenn sie erst einmal herausgegeben worden sind) im Ausland ein Eigenleben führen werden. *Ein entsprechender Regelungsvorschlag wird in Ziff. 3.4 näher erläutert.*

In diesem Zusammenhang ist ferner zu bedenken, dass die Schweiz gestützt auf die Artikel 13 und 22 des Europäischen Übereinkommens über die Rechtshilfe in Strafsachen (SR 0.351.1) schon heute einen Austausch von Strafregisterinformationen mit gewissen Staaten praktiziert, ohne dass jeweils vorher abgeklärt würde, in welchen ausländischen Datenbanken diese Informationen schliesslich landen, bzw. welche Entfernungsfristen im Ausland für diese Informationen gelten.

Leider hält auch das *neue DSG* (welches zurzeit im Parlament beraten wird) in Bezug auf die Weitergabe von Daten ins Ausland *keine Patentrezepte* bereit:

[17] Vgl. Ziff. 3.4.

Gemäss neuem Artikel 6 E-DSG, darf eine Weitergabe ins Ausland grundsätzlich nur erfolgen, *wenn die Gesetzgebung im Ausland einen angemessenen Schutz dieser Daten gewährleistet*.[18] Dies dürfte bei Europol der Fall sein, ist bei Interpol – in Anbetracht der weltweit unterschiedlichen Datenschutzstandards - jedoch zumindest fraglich. In diesem Zusammenhang ist jedoch zu erwähnen, dass das DSG gemäss Artikel 351^{quinquies} StGB für den Informationsaustausch mit Interpol ohnehin nicht zur Anwendung kommt.

2.5 Zur Problematik des Datenumfangs

Ist für eine bestimmte Stelle ein Zugriff auf Strafregisterdaten aufgrund der erfolgten Zweckprüfung denkbar, so muss der Umfang der Daten bestimmt werden, auf die der Zugriff zu erteilen ist. Dieser ergibt sich ebenfalls aus dem Zweck der Datenerhebung. Für welche Datensätze der Zugriff zu erteilen ist, ist daher *individuell zu prüfen*, da nicht jeder Zweck auf die gleichen Datensätze abzielt. Um beispielsweise Parallelermittlungen zu vermeiden, sind nur Angaben über hängige Verfahren von Bedeutung.

Es wäre auf jeden Fall falsch, nur einen Zugriff auf die *Information* zu erlauben, *ob ein Eintrag vorhanden ist oder nicht*, denn dies würde nur Tür und Tor für Spekulationen öffnen. Dazu ein Beispiel: Um im Rahmen eines V-Mann Einsatzes die Gewaltbereitschaft gewisser Personen besser einschätzen zu können, nützt es nichts, wenn das fedpol bloss weiss, dass jemand im Strafregister registriert ist. Viel wichtiger ist es zu wissen, wegen welcher Taten jemand verurteilt worden ist. Denn hinter dem Vermerk „Eintrag vorhanden“ könnte sich auch eine Verurteilung wegen Fahrens in angetrunkenem Zustand verbergen.

Es lohnt sich nicht, in dieser Frage um jeden einzelnen Datensatz zu feilschen. Durch die Verweigerung des Einblicks in gewisse Randdaten wird der Schutz für die Betroffenen nicht wesentlich erhöht. Entscheidend ist vielmehr die Frage, ob neben dem Zugriff auf Daten über Urteile auch ein Zugriff auf Daten über *hängige Verfahren* erforderlich ist. Gegebenenfalls sind Artikel 367 Absatz 4 nStGB und der Anhang zur VOSTRA-Vo (der die Zugriffsberechtigung in Bezug auf den einzelnen Datensatz im Rahmen von Online-Abrufverfahren festgelegt) entsprechend zu ergänzen.

Gemäss dem Regelungsvorschlag von Artikel 20 Absatz 2 VE-VOSTRA-Vo wird allen fedpol-Stellen, welche Strafregisterdaten erhalten, auch ein Zugriff auf Daten über hängige Strafverfahren erteilt.

2.6 Zur Problematik des Online-Zugriffs

Der Umstand, dass im Rahmen dieser Vorlage ein Online-Anschluss für einen Dienst des fedpol bejaht wird, heisst nicht automatisch, dass diese Stelle auch zwingend einen Online-Anschluss erhalten wird. Im StGB wird nur die grundsätzliche Berechtigung für einen solchen Anschluss geregelt.

[18] Für den Fall, wo *im Ausland eine entsprechende Gesetzgebung fehlt*, gilt der Ausnahmekatalog gemäss Artikel 6 Absatz 2 E-DSG.

Die Einrichtung einer Online-Verbindung und die Erteilung von individuellen Zugriffsbewilligungen erfolgt nach den Bestimmungen der Weisung des EJPD über die Einrichtung von Online-Verbindungen und die Erteilung von Zugriffsbewilligungen auf Informatikanwendungen vom 30. September 2004 (Online-Weisung EJPD). Demnach ist es grundsätzlich Sache des für das *Strafregister zuständigen Datenschutzbeauftragten des BJ* zu entscheiden, ob die betreffende Behörde online ans Strafregister angeschlossen werden soll oder nicht (vgl. Art. 17 der Online-Weisung EJPD). Der Datenschutzbeauftragte des BJ entscheidet in Zusammenarbeit mit dem Chef des Strafregisters auch darüber, wie viele und welche Mitglieder dieser Behörde eine individuelle Zugriffsberechtigung auf VOSTRA erhalten sollen (vgl. die Bestimmungen des 4. Abschnitts sowie Art. 13 – 15 und 18 – 20 der Online-Weisung EJPD).[19]

[19] Dabei sind u.a. folgende Faktoren zu berücksichtigen: Benutzungsintensität, Anzahl der bereits zugriffsberechtigten Mitarbeitenden des betreffenden Organs, Notwendigkeit des unabhängigen und raschen Handelns (z.B. ausserhalb der ordentlichen Geschäftszeiten), Umfang der abgefragten Daten, beantragte Funktionen (Abfragen, Schreiben, Mutieren, Löschen).

3. Zugriffsberechtigungen für die einzelnen Dienste des fedpol

3.1 Dienst für Analyse und Prävention: Operationen

Status quo

Diese Dienststelle erhält heute keine Auskünfte aus VOSTRA.

Aufgaben

Der Dienst DAP-Operationen trifft vorbeugende Massnahmen in den Bereichen Terrorismus, verbotener Nachrichtendienst, gewalttätiger Extremismus, Handel mit Waffen und radioaktiven Materialien, Technologietransfer, organisierte Kriminalität (Art. 2 Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit, BWIS, SR 120).

Er führt konzentrierte Aktionen als präventive Operationen durch, die über den normalen Nachrichtendienst hinausgehen. Er führt ferner längerfristige polizeiliche Aktionen als präventive Fahndungsprogramme durch (Art. 14 Verordnung über Massnahmen zur Wahrung der inneren Sicherheit, VWIS, 120.2).

Zweck der Datenerhebung

- *Erhärtung eines Verdachts:* Im präventivpolizeilichen Bereich ist es unumgänglich, sich über die verdächtigen Personen ausreichend informieren zu können, insbesondere auch ausserhalb der Bürozeiten.
- *Verhinderung von parallelen Ermittlungen*: Mit der Information über ein eröffnetes Verfahren lassen sich parallele Ermittlungen vermeiden.
- *Informationsvorsprung / Glaubwürdigkeitsprüfung bei Befragungen*: Es werden Befragungen durchgeführt, jedoch nicht wie in einem Ermittlungsverfahren, sondern auf „freiwilliger“ Basis. Der Befragte ist nicht verpflichtet, zu antworten oder sonstwie mitzuwirken.
- *Schutz von verdeckten Ermittlern / Überprüfung des Täterumfeldes*: Die Dienststelle Operationen arbeitet nicht mit eigentlichen V-Männern, sondern mit so genannten „Quellen“, d.h. Personen im Umfeld der Zielperson, die dem fedpol Informationen zukommen lassen. Die Prüfung der Glaubwürdigkeit dieser Personen ist sehr wichtig. Sie dürfen ferner nicht in ein Strafverfahren verwickelt sein (damit sie sich nicht mit ihrer Tätigkeit als Quelle im Prozess zu rechtfertigen suchen).

Anzahl Erhebungen

Voraussichtlich werden 80 Zugriffe pro Monat auf VOSTRA erfolgen.

Aufbewahrung der Daten

Die Daten dieser Dienststelle werden im Staatsschutz-Informationssystem (ISIS) gespeichert. Es werden keine isolierten Strafregisterdaten gesammelt. Registriert wird, was in amtlicher Funktion unternommen wird. Zum Teil erhält die Dienststelle DAP

Operationen auch direkt Urteile von den Kantonen, die dann in ISIS registriert werden.

Weitergabe der Daten

Die Weitergabe erfolgt in begründeten Fällen, soweit es zur Wahrung der inneren Sicherheit notwendig ist (Art. 17 BWIS und Art. 18 VWIS und Art. 13 ISIS-Verordnung, SR 120.3).

Fazit

Die Dienststelle Operationen des DAP erfüllt Aufgaben, für die ein Zugriff auf VOSTRA-Daten sinnvoll ist.

Angesichts der Anzahl Anfragen ist ein Online-Zugriff angezeigt.

Der Zugriff soll alle Datensätze umfassen (der Datensatz betreffend Ersuchen an ausländische Strafregister wird nicht gewünscht).

Rechtliche Anpassungen

- *Die Zweckbestimmung nach Artikel 365 Absatz 2 nStGB ist um folgenden Zweck zu ergänzen: „Verhütung von Straftaten nach Artikel 2 Absatz 1 und 2 des Bundesgesetzes vom 21. März 1997 über Massnahmen zur Wahrung der inneren Sicherheit“.*
- *In Artikel 367 Absatz 2 nStGB soll festgehalten werden, dass das fedpol für die vorstehend definierte Aufgaben durch ein Abrufverfahren auf VOSTRA zugreifen kann.*

Für die Zeit bis zur Umsetzung der Vorschläge auf Gesetzesstufe wird gestützt auf Artikel 367 Absatz 3 nStGB vorgeschlagen, die Verordnung zum automatisierten Strafregister entsprechend zu ergänzen (Art. 20 Abs. 2 Bst. a VE-VOSTRA-Vo).

3.2 Dienst Analyse und Prävention: Ausländerdienst

Status quo

Es besteht bereits ein Online-Zugriff auf die Strafregisterdaten.

Aufgaben

Der Ausländerdienst prüft Personen im Zusammenhang mit der Verhängung oder Aufhebung von Fernhaltemassnahmen. Er verfügt Einreisesperren gegenüber Personen aus dem Ausland, namentlich aufgrund von Informationen aus dem Ausland.

Zweck der Datenerhebung

Erhärtung eines Verdachts: Der Auszug aus dem Strafregister dient der Erhärtung der eingegangenen Meldung. Es werden keine Befragungen oder Verfahren durchgeführt. Allenfalls nimmt der Dienst mit dem Eidgenössischen Departement für auswärtige Angelegenheiten Rücksprache.

Anzahl Erhebungen

Es werden über 100 Zugriffe pro Monat vorgenommen.

Aufbewahrung der Daten

- In ISIS wird die konkrete Verfügung über die Einreisesperre aufgenommen (eingescannt).
- Im automatisierten Fahndungssystem (RIPOL) wird die Information aufgenommen, dass gegen eine bestimmte Person eine Einreisesperre erlassen wurde. Diese Information geht auch an die Zollbehörde.

Weitergabe der Daten

Die Daten werden an andere Dienststellen des fedpol und an kantonale Staatsschützer weitergegeben.

Fazit

Der Zweck der „Erhärtung eines Tatverdachts“ kann einen Zugriff auf Strafregisterdaten rechtfertigen.

Es erscheint sinnvoll, wenn der Dienst online auf alle Strafregisterdaten zugreifen kann.

Rechtliche Anpassungen

- *Bezüglich des Zugriffszwecks braucht es keine Anpassungen (dieser wird bereits in Artikel 365 Absatz 2 Buchstabe e nStGB genannt).*
- *In Artikel 367 Absatz 2 Buchstabe c nStGB ist zu präzisieren, dass das fedpol für Aufgaben nach Artikel 365 Absatz 2 Buchstabe e nStGB auf das Strafregister zugreifen kann.*

Für die Zeit bis zur Umsetzung der Vorschläge auf Gesetzesebene kann die entsprechende Kompetenz auf Verordnungsstufe beibehalten werden (heute Art. 3 Abs. 3 Bst. c VOSTRA-Vo; neu Art. 20 Abs. 2 Bst. f VE-VOSTRA-Vo).

3.3 Bundeskriminalpolizei I

Ermittlungsoffiziere
Ermittlungen I **(Abteilungen Ermittlungen Lausanne, Ermittlungen Zürich, Ermittlungen Lugano)**
Ermittlungen II **(Abteilungen Ermittlungen Mitte, Ermittlungen Staatsschutz/Besondere Tatbestände, Ermittlungen Terrorismusfinanzierung)**
Ermittlungen III **(Abteilungen Ermittlungen Forensik/Informatik, Spezialeinsätze, Observation)**

Die oben aufgeführten Dienststellen der Bundeskriminalpolizei (BKP) werden gemeinsam beurteilt, weil sich alle mit der *Verfolgung* von Straftaten befassen.

Status quo

Rechtlich wäre ein Online-Zugriff für Ermittlungen im Rahmen eines *eröffneten Strafverfahrens* möglich. Der Zugriff auf VOSTRA erfolgt heute jedoch über die bestehenden Anschlüsse der BA (der BA ist ein schriftliches Gesuch einzureichen). Der Zugriff umfasst alle Informationen (eröffnete Strafverfahren sowie offene und gelöschte Eintragungen).

Aufgaben

- *BKP Ermittlungsoffiziere*
  Die Ermittlungsoffiziere sind für die abteilungsübergreifende Koordination und Steuerung von Verfahren zuständig. Sie sind Ansprechpartner für die Bundesanwaltschaft und können dort die Eröffnung von Ermittlungsverfahren beantragen. Sie stellen zudem den Informationsaustausch mit dem DAP und anderen Bundesstellen sicher.
- *BKP Ermittlungen I, II und III*
  Die Bundeskriminalpolizei (BKP) führt polizeiliche Vorabklärungen und gerichtspolizeiliche Ermittlungen in den Bereichen, welche in der Kompetenz des Bundes liegen (Art. 340 und 340^{bis} StGB) sowie in zugewiesenen Bereichen gemäss Nebenstrafgesetzgebung (Betäubungsmittelgesetz; SR 812.121). Dies umfasst insbesondere die Bekämpfung der grenzüberschreitenden Schwerstkriminalität in den Bereichen der organisierten Kriminalität, der Terrorismusfinanzierung, der Geldwäscherei sowie der Wirtschaftskriminalität, aber auch Verfahren in den Bereichen des Staatsschutzes (Beispiele: Sprengstoffdelikte, Korruption, Falschgelddelikte, Genozid). Zu diesem Zweck können die polizeiüblichen Instrumente wie z.B. Observation, verdeckte Ermittlung und Zielfahndung eingesetzt werden. Sie gewährleistet zudem den Vollzug von Rechtshilfeersuchen aus dem Ausland, die in die Bundeskompetenzen fallen.

Zweck der Datenerhebung

Der Zweck der Datenerhebung ist im weitesten Sinne die *Verfolgung von Straftaten*. Die Daten aus VOSTRA dienen (1) der Erhärtung eines Tatverdachts, (2) der Verhinderung von parallelen Ermittlungen, (3) dem Informationsvorsprung und der Glaubwürdigkeitsprüfung bei Befragungen sowie (4) dem Schutz von verdeckten Ermittlern (Überprüfung des Täterumfeldes).

Anzahl Erhebungen

Von Seiten des fedpol wird pro Abteilung mit 5 - 20, nach den neuesten Annahmen sogar bis zu 100 Erhebungen pro Monat gerechnet.

Aufbewahrung der Daten

Die Daten der in Frage stehenden Dienststellen werden im Informationssystem der Bundeskriminalpolizei (JANUS) gespeichert. Grundsätzlich dürfen heute alle aus VOSTRA gewonnenen Daten in JANUS aufgenommen werden.

Weitergabe der Daten

Alle aus VOSTRA gewonnenen Daten können weitergegeben werden. Die Weitergabe richtet sich nach Artikel 16 - 18 JANUS-Verordnung (SR 360.2) in Verbindung mit Artikel 13 Zentralstellengesetz (ZentG, SR 360) und Artikel 4 Absatz 2 - 4 der Verordnung über die Wahrnehmung kriminalpolizeilicher Aufgaben im Bundesamt für Polizei (SR 360.1).

Nach Eröffnung eines Ermittlungsverfahrens werden die Dossiers an die entsprechenden Abteilungen der BKP weitergeleitet. Aus organisatorischer Sicht werden auch im Vorermittlungsbereich andere Abteilungen der BKP über Erkenntnisse der Dienststelle informiert (Art. 100 ff. Bundesgesetz über die Bundesstrafrechtspflege, BStP, SR 312.0; Art. 2 der Verordnung über die Wahrnehmung kriminalpolizeilicher Aufgaben im Bundesamt für Polizei; Art. 13 Abs. 1 ZentG im Einzelfall).

Fazit

Die in diesem Kapitel erwähnten Stellen der BKP sollen grundsätzlich zu den oben erwähnten Zwecken Daten aus dem Strafregister erhalten.

Von den einzelnen Stellen wird mit höchstens 20, nach anderen Annahmen mit bis zu 100 Zugriffen pro Monat gerechnet. Der Datenschutzbeauftragte wird gestützt auf die Online-Weisungen des EJPD entscheiden müssen, welche Stelle einen eigenen Online-Zugriff erhält oder ob allenfalls nur ein oder einzelne zentrale Zugriffe für diese Stellen der BKP angezeigt sind.

Die in diesem Kapitel erwähnten Stellen der BKP sollen Einblick in alle Datensätze erhalten (Daten über hängige Verfahren und Daten über Urteile).

Rechtliche Anpassungen

- *Artikel 365 nStGB muss zwar nicht unbedingt geändert werden, weil alle hier zusammengefassten Stellen der BKP den Zweck der „Durchführung von Strafverfahren“ verfolgen (Art. 365 Abs. 2 Bst. a nStGB). Weil dieser Zweck neu auch die Vorermittlungen erfasst, wird vorgeschlagen, ihn in einem neuen Buchstaben als „Verfolgung von Straftaten“ zu umschreiben (im Gegensatz zur „Verhütung von Straftaten“; vgl. dazu Ziff. 3.1 dieses Berichtes). Damit soll überdies zum Ausdruck kommen, dass künftig nicht nur eröffnete Strafverfahren, sondern auch Vorermittlungen einen Strafregisterzugriff rechtfertigen können.*
- *In Artikel 367 nStGB soll neu erwähnt sein, dass das Bundesamt für Polizei für die vorstehend erwähnten Aufgaben Daten aus VOSTRA beziehen kann.*
- *Der Datenschutzbeauftragte wird entscheiden, welche Stellen der BKP einen Online-Zugriff erhalten (in Anbetracht der Abfrageintensität ist eine Zentralisierung des Zugriffsrechts denkbar).*

Für die Zeit bis zur Umsetzung dieser Vorschläge auf Gesetzesebene wird gestützt auf Artikel 367 Absatz 3 nStGB vorgeschlagen, die bestehende Kompetenz in ihrer neuen Umschreibung in der Verordnung zum automatisierten Strafregister anzuführen (Art. 20 Abs. 2 Bst. b VE-VOSTRA-Vo).

3.4. Bundeskriminalpolizei II (Interpol)

Ermittlungen IV (Abteilungen Einsatzzentrale, Internationale Polizeikooperation, Koordination)

Status quo

Ein Online-Zugriff der BKP auf VOSTRA besteht heute ausschliesslich für die Beantwortung von Interpol-Anfragen. Diese Zugriffsrechte sind heute bei der Einsatzzentrale (EZ) zentralisiert. Bei Interpol-Anfragen, aus denen klar ersichtlich ist, dass es sich um ein im Ausland eröffnetes Strafverfahren handelt, werden alle Informationen, d.h. (offene und gelöschte) Daten über Urteile sowie hängige Strafuntersuchungen zur Verfügung gestellt.

Geht aus einer Anfrage nicht klar hervor, ob im Ausland ein Verfahren eröffnet worden ist (also bei rein polizeilichen ausländischen Ermittlungen) werden heute nur offene Urteile angegeben (diese Differenzierung fällt mit dem neuen AT-StGB weg, weil es die so genannte Löschung nicht mehr gibt).

Verstösse gegen Militärbestimmungen werden nicht ins Ausland bekannt geben[20].

Aufgaben

- *Abteilung Einsatzzentrale und Abteilung Koordination*
  Sie sind Drehscheiben für den kriminalpolizeilichen Informationsaustausch mit in- und ausländischen Strafverfolgungsbehörden. Sie führen die Aufgaben des Nationalen Zentralbüros Interpol aus und tätigen erste polizeiliche Vorabklärungen. Sie koordinieren interkantonale und internationale Ermittlungen.
- *Abteilung Internationale Polizeikooperation*
  Sowohl die Polizeiattachés im Ausland als auch die Mitarbeiter der Kooperationszentren in Genf und Chiasso gewährleisten einen reibungslosen Informationsaustausch mit dem Ausland. Sie leisten Unterstützung bei Ermittlungsverfahren und stellen erste Kontakte mit ausländischen Behörden her.

Zweck der Datenerhebung

Die Einsicht in das Strafregister dient der Informationsbeschaffung im Rahmen des kriminalpolizeilichen Informationsaustausches mit Interpol-Stellen und ausländischen Polizeidienststellen bei der Beantwortung und der Stellung von Auskunftsersuchen.

Anzahl Erhebungen

Die Anzahl der Meldungen und Anfragen wird auf 3'000 pro Monat geschätzt. Nach Angaben des fedpol ist daher mit 1'000 Zugriffen pro Monat zu rechnen.

---

[20] Die generelle Nichtmeldung von militärischen Verurteilungen ist indessen rechtlich nicht haltbar. Artikel 1 Ziffer 2 des Europäischen Übereinkommens über die Rechtshilfe in Strafsachen (SR 0.351.1), schliesst lediglich die Rechtshilfe bezüglich *militärischen strafbaren Handlungen aus, die nicht nach gemeinem Recht strafbar sind*. Demnach dürfen nur diejenigen Delikte nicht gemeldet werden, die ausschliesslich nach MStG (SR 321.0) strafbar sind.

Aufbewahrung der Daten

- Strafregisterdaten werden in der Datenbank JANUS erfasst, sofern sie Straftaten betreffen, welche in die Zuständigkeit des Bundes oder der Zentralstellen fallen. Es werden nicht die gesamten erhobenen und im Rahmen von Interpol weitergegebenen Strafregisterdaten gespeichert, sondern nur die Tatsache, dass ein Informationsaustausch stattgefunden hat, einzelne Schlüsselangaben (z.B. "wegen Drogenhandels verurteil am 1.11.1999") sowie der Verweis auf eine Dossiernummer. Das fedpol stützt sich dabei auf Art. 2, 3, 4, 8 Abs. 1, 10, 11 ZentG; Art. 3, 4 Bst. a und b, 6, 7 Bst. a, b, e JANUS-Vo.
- Analoge Daten werden zudem im "informatisierten Personennachweis-, Aktennachweis- und Verwaltungssystem im Bundesamt für Polizei" (IPAS) erfasst (gemäss Artikel 351^{octies} Absatz 1 Buchstabe b und Absatz 3 Buchstabe e StGB i.V.m. Artikel 2 Buchstabe b und Artikel 5 Absatz 1 Buchstabe b IPAS-Vo, SR 361.2).
- Es ist nicht einsichtig, weshalb die gesamten Personendaten, die im Rahmen von Interpol-Anfragen an ausländische Stellen weitergegeben werden, in JANUS und IPAS gespeichert werden sollen. Diese Speicherungen stehen in Widerspruch zum ursprünglichen Zweck, zu dem der Zugriff auf die Daten von VOSTRA gewährt wurde. Hier werden so genannte Schattenregister geführt (vgl. Kapitel 2.4). Die neu vorgesehene Speicherungsverbotsregel gemäss Artikel 17 Absatz 2 VE-VOSTRA-Vo (welche in einem späteren Zeitpunkt ins StGB zu überführen ist) schiebt dieser Tätigkeit künftig einen Riegel.

Weitergabe der Daten

Die Weitergabe der Daten ist der Kern der Aufgabe des Interpol-Dienstes (Art. 1 ff. Interpol-Vo, SR 351.21)und insoweit unbestritten.

Die in JANUS gespeicherten Daten werden gestützt auf die Artikel 16 - 18 JANUS-Vo i.V. mit Artikel 13 ZentG und Artikel 4 Abs. 2 - 4 der Vo über die Wahrnehmung kriminalpolizeilicher Aufgaben im Bundesamt für Polizei an Dritte weitergegeben. Dasselbe gilt für die in IPAS gespeicherten Daten nach Artikel 11 IPAS-Verordnung. Diese Weitergabe diene der Unterstützung von Behörden des Bundes und der Kantone bei der Durchführung von Strafverfahren.

Fazit

Die Dienststellen der BKP sollen zur Erfüllung ihrer Aufgaben im Rahmen von Interpol Zugriff auf die Daten des Strafregisters haben.

Angesichts der grossen Anzahl von Erhebungen ist ein Online-Zugriff gerechtfertigt.

Sie erhalten Zugriff auf alle Daten.

Der Informationsaustausch soll allerdings nur im Rahmen eines eröffneten Strafverfahrens erfolgen dürfen. Die Weitergabe für Vorermittlungen und die Prävention wird aus folgenden Gründen nicht vorgesehen: Es gibt zwar Zwecke im Bereich der Vorermittlungen und im präventiven Bereich, die Auskünfte rechtfertigen würden. Doch die Schattenregister-Problematik kann bei Interpol nicht gelöst werden; denn die Schweiz kann ausländischen Behörden nicht vorschreiben, dass sie die bezogenen Daten nicht elektronisch speichern und unter welchen Voraussetzungen sie die Daten weitergeben dürfen (selbst wenn dies möglich wäre, könnten wir es nicht kontrol-

lieren). Es stellt sich daher die Frage, wie weit das Strafregister für ausländische Stellen geöffnet werden soll. Da es bei Interpol um die ganze Bandbreite der Kriminalität geht, muss die Lösung ein Abbild des innerstaatlichen Datenflusses sein, um nicht ein Ungleichgewicht zu schaffen. Das heisst:

Grundsätzlich sind für kantonale Polizeistellen heute Strafregisterdaten im Rahmen eines eröffneten Strafverfahrens indirekt verfügbar (nach bisheriger Praxis erhalten sie diese Informationen - wo nötig - vom betreffenden Untersuchungsrichter und Staatsanwalt). Also sollten diese Daten grundsätzlich auch für Interpol nur im Rahmen eines eröffneten Verfahrens Daten zur Verfügung stehen.

- Ausnahme 1: Die BKP erhält für die Verfolgung bestimmter Delikte bereits für das Vorverfahren Auskünfte. Eine Auskunftserteilung über Interpol ist daher im Rahmen eines identischen Deliktskatalogs (Art. 340 und 340bis StGB) denkbar.
- Ausnahme 2: der DAP erhält zur Verhütung von schwersten Delikten im Rahmen des BWIS Auskünfte aus dem Strafregister. Eine Auskunftserteilung über Interpol ist daher im Rahmen eines identischen Deliktskatalogs (Terrorismus, verbotener Nachrichtendienst, gewalttätiger Extremismus, Handel mit Waffen und radioaktiven Materialien und Technologietransfer nach Art. 2 Abs. 1 und 2 BWIS) denkbar.

Diese Ausnahmen können als Konkretisierung von Artikel 351^{quater} StGB angesehen werden.

Die Aufbewahrung und Weitergabe richtet sich nach den neuen allgemeinen Grundsätzen (vgl. Art. 17 Abs. 2 und 3 VE-VOSTRA-Vo; später Änderung von Art. 367 nStGB). Da Strafregisterdaten nicht isoliert, sondern nur im Rahmen eines Entscheids, einer Verfügung oder Massnahme gespeichert werden dürfen, ist für den Interpol-Dienst des fedpol nur ein Bearbeitungsvermerk zulässig.

Rechtliche Anpassungen

Die Grundlage für den Zugriff des Dienstes Interpol auf VOSTRA-Daten ist nur auf Verordnungsstufe vorhanden (Art. 3 Abs. 3 VOSTRA-Vo und Art. 8 Interpol-Vo).

- *In Artikel 365 Absatz 2 nStGB soll eine neue Zweckbestimmung aufgenommen werden: „Informationsvermittlung an Interpol im Rahmen von eröffneten Strafverfahren (und Vorermittlungen im Zusammenhang mit Delikten im Sinne der Artikel 340 und 340bis StGB sowie zur Verhütung von Delikten im Sinne von Artikel 2 Absatz 1 und 2 des Bundesgesetzes vom 21. März 1997 über die Massnahmen zur Wahrung der inneren Sicherheit)“.*
- *In Artikel 367 Absatz 2 Buchstabe c nStGB soll neu erwähnt werden, dass das fedpol für die vorstehend erwähnten Aufgaben Daten aus VOSTRA beziehen kann.*

Für die Zeit bis zur Umsetzung des Vorschlags auf Gesetzesebene soll gestützt auf Artikel 367 Absatz 3 nStGB die entsprechende Kompetenz des fedpol auf Verordnungsebene präziser formuliert werden (Art. 20 Abs. 2 Bst. c VE-VOSTRA-Vo; ersetzt Art. 3 Abs. 3 Bst. a VOSTRA-Vo).

3.5 Bundeskriminalpolizei: Kontrolle JANUS

Status quo

Diese Stelle hat heute keinen Zugriff auf Strafregisterdaten.

Aufgaben

Sie führt die gesetzmässige Kontrolle der von den zuständigen Stellen in der JANUS-Datenbank erfassten Daten durch (nach Artikel 11 ZentG und Artikel 13 Absatz 2 JANUS-Vo).

Zweck der Datenerhebungen

Es geht darum, die Daten in JANUS periodisch auf ihre Glaubwürdigkeit und Richtigkeit hin zu überprüfen.

Die Überprüfung von unsicheren Daten in JANUS kann bis zu einem gewissen Grad mit Strafregisterdaten durchgeführt werden. Sinnvoll kann es z.B. sein, wenn der Personaliensatz mit Daten aus dem Strafregister (z.B. Alias-Namen) berichtigt wird.

Anzahl Erhebungen

Ca. 200 pro Monat.

Aufbewahrung der Daten

Mit Daten aus dem Strafregister werden lediglich bestehende Einträge in JANUS berichtigt. Es werden somit keine zusätzlichen Einträge von Personen und Verurteilungen vorgenommen.

Weitergabe der Daten

Die abgerufenen Strafregisterdaten werden zwar nicht gezielt weitergegeben. Immerhin werden die Daten, welche für eine Berichtigung herangezogen wurden, allen Benützern von JANUS zugänglich gemacht.

Fazit

Der Kontrolldienst JANUS soll Daten aus dem Strafregister erhalten.

Angesichts der Anzahl Erhebungen ist es sinnvoll, wenn ein Online-Zugriff gewährt wird.

Der Kontrolldienst kann auf alle Datensätze zugreifen (gemäss Erhebungstabelle werden die Daten über Ersuchen an ausländische Register nicht benötigt).

Die Aufbewahrung und Weitergabe richtet sich nach den allgemeinen Grundsätzen (vgl. Art. 17 Abs. 2 und 3 VE-VOSTRA-Vo, der in einem späteren Zeitpunkt ins nStGB zu überführen ist). Die Speicherungsbeschränkung gemäss Artikel 17 Absatz 2 VE-VOSTRA-Vo betrifft den Personaliendatensatz nicht. Der Kontrolldienst JANUS

kann mithelfen, isolierte Strafregisterdaten, die nicht gespeichert werden dürfen, aus den fedpol-Registern zu löschen.

Rechtliche Anpassungen

- *In Artikel 365 Absatz 2 nStGB soll ein neuer Zweck definiert werden: „Gesetzliche Kontrolle des Informationssystems der Bundeskriminalpolizei (JANUS)“.*
- *In Artikel 367 Absatz 2 Buchstabe c nStGB ist zu präzisieren, dass das Bundesamt für Polizei für die vorstehend genannte Aufgabe auf das Strafregister zugreifen kann.*

Für die Zeit bis zur Umsetzung dieses Vorschlags auf Gesetzesebene wird gestützt auf Artikel 367 Absatz 3 nStGB vorgeschlagen, die neue Kompetenz des fedpol in der Verordnung zum automatisierten Strafregister vorzusehen (Art. 20 Abs. 2 Bst. d VE-VOSTRA-Vo).

3.6 Dienste MROS

(MROS = Money Laundering Reporting Office Switzerland)

Status quo

Der Dienst MROS hat einen Online-Zugriff auf VOSTRA.

Aufgaben

Nach Artikel 23 Geldwäschereigesetz (SR 955.0) führt das Bundesamt für Polizei die Meldestelle für Geldwäscherei. MROS ist keine Polizei- oder Justizbehörde. Ihre Aufgaben werden in Artikel 1 der Verordnung vom 25. August 2004 über die Meldestelle für Geldwäscherei (MGwV, SR 955.23) wie folgt umschrieben:

a. Sie unterstützt die Strafverfolgungsbehörden in der Bekämpfung der Geldwäscherei, des organisierten Verbrechens und der Terrorismusfinanzierung;
b. sie agiert bei der Bekämpfung der Geldwäscherei, des organisierten Verbrechens und der Terrorismusfinanzierung als nationale Meldestelle;
c. sie sensibilisiert die Finanzintermediäre für die Problematik der Geldwäscherei, des organisierten Verbrechens und der Terrorismusfinanzierung;
d. sie veröffentlicht einen anonymisierten statistischen Jahresbericht über die Entwicklung der Bekämpfung der Geldwäscherei, des organisierten Verbrechens und der Terrorismusfinanzierung in der Schweiz.

Zur Erfüllung ihrer Aufgaben:

a. nimmt sie Meldungen und Anzeigen der Finanzintermediäre, der Selbstregulierungsorganisationen, der Kontrollstelle für die Bekämpfung der Geldwäscherei und der spezialgesetzlichen Aufsichtsbehörden entgegen und wertet diese aus;
b. führt sie Abklärungen zu den gemeldeten Vorgängen durch;
c. entscheidet sie über die Weiterleitung von Meldungen, Anzeigen, Mitteilungen und sonstigen Informationen an die Strafverfolgungsbehörden des Bundes und der Kantone;
d. tauscht sie auf nationaler und internationaler Ebene Informationen über die Geldwäscherei, das organisierte Verbrechen und die Terrorismusfinanzierung aus;
e. betreibt sie ein eigenes Datenverarbeitungssystem zur Bekämpfung der Geldwäscherei, des organisierten Verbrechens und der Terrorismusfinanzierung (GEWA);
f. wertet sie die Daten über die Geldwäscherei, das organisierte Verbrechen und die Terrorismusfinanzierung aus und erstellt dazu eine anonymisierte Statistik.

Zweck der Datenerhebungen

MROS muss in kurzer Zeit (i.d.R. 3 Tage) aufgrund der eingegangenen Meldungen eine Analyse durchführen. Die Bearbeitungsfrist beträgt insgesamt bloss 5 Tage: 3 Tage für MROS (danach wird das Dossier an die zuständige Justizbehörde weitergeleitet) und 2 Tage für den Untersuchungsrichter, damit verdächtige Gelder blockiert werden können.

- Im Vordergrund der Arbeit steht die Erhärtung oder Entkräftung des *Anfangsverdachts*.
- Auch das Wissen um *Parallelermittlungen* (eröffnete Verfahren) ist für MROS wichtig, damit das Dossier an die richtige Stelle weitergeleitet werden kann.

Anzahl Erhebungen

MROS erhält ca. 800 Meldungen mit mehreren Namen pro Jahr.

Aus dem Ausland gehen zudem pro Jahr ca. 2000 Anfragen ein.

Aufbewahrung der Daten

MROS führt das Datenverarbeitungssystem zur Bekämpfung der Geldwäscherei (GEWA).

Erfasst werden die Meldungen in einer *Statistik* so, dass MROS jederzeit in der Lage ist, Angaben zu machen über die Anzahl der Meldungen, deren Inhalt, Art und Herkunft, die Verdachtsgründe, deren Häufigkeit sowie die einzelnen Deliktsarten und über die Art der Behandlung durch die Meldestelle. Diese Angaben müssen anonymisiert sein.

MROS arbeitet mit einem Papierformular, auf dem u.a. eingetragen wird, ob jemand im Strafregister verzeichnet ist oder nicht. Dieses Formular geht in das Dossier. Im GEWA wird gespeichert, ob jemand im Strafregister verzeichnet ist und welches Delikt er begangen hat. Die Daten in GEWA ersetzen das Strafregister nicht: MROS fragt immer neu bei VOSTRA an, wenn nach einer bestimmten Zeit ein Dossier wieder aktuell wird.

Weitergabe der Daten

MROS tauscht mit der Bundesanwaltschaft (BA), den Kantonen und dem Ausland intensiv Daten aus.

Die Dossiers gehen an die BA oder den kantonalen UR, die in der Regel ein Verfahren eröffnen, um die in Frage stehenden Gelder sperren zu können.

Auf die spezifische Datenbank der Meldestelle (GEWA) hat zurzeit nur diese selbst Zugriff. Eine Revision ist jedoch im Gange, um die vielen Gesuche auf elektronischem Weg bearbeiten zu können. Vorgesehen ist, dass gestützt auf Artikel 35 Geldwäschereigesetz eine gesetzliche Grundlage für die Online-Zugriffe von schweizerischen Stellen auf GEWA geschaffen wird. Die zugängliche Information wäre: (1) dass jemand der Meldestelle gemeldet worden ist und (2) an welche Behörde die Meldestelle den Fall weitergeleitet hat. Ausländische Stellen müssten Informationen auf dem Amtshilfeweg einholen.

Fazit

Der Zweck der „Erhärtung eines Tatverdachts“ rechtfertigt einen Zugriff auf die Daten über Verurteilungen und der Zweck der „Vermeidung von Parallelermittlungen“ rechtfertigt den Zugriff auf die Daten über hängige Verfahren.

Der Zugriff soll angesichts der Zwecke und der Zugriffsintensität weiterhin online erfolgen.

MROS soll alle Datensätze aus VOSTRA erhalten.

Rechtliche Anpassungen

- *Die heutige Grundlage nach Artikel 35 Geldwäschereigesetz[21] (GwG), die auf das Zentralstellengesetz verweist, ist für einen Zugriff von MROS auf das Strafregister ungenügend. Im Rahmen einer Revision des Geldwäschereigesetzes[22] wird in Artikel 35bis Absatz 1 Buchstabe f GwG zwar die gesetzliche Grundlage für einen Zugriff auf VOSTRA vorgesehen. Der Zugriff umfasst indessen nur die Prüfung, ob jemand in VOSTRA verzeichnet ist oder nicht. Der Zugriff auf die eigentlichen Urteilsdaten und die Daten über hängige Strafverfahren wird indessen durch das revidierte GwG nicht gewährt. Im Rahmen des neuen Bundesgesetzes über die polizeilichen Informationssysteme des Bundes wird eine analoge Änderung von Artikel 35bis GWG vorgeschlagen. Auch hier umfasst der Zugriff indessen nur die Prüfung, ob jemand in VOSTRA verzeichnet ist oder nicht.*
- *Den in Artikel 6 und 7 der Verordnung über die Meldestelle für Geldwäscherei geregelten Kompetenzen fehlt in Bezug auf die Bearbeitung von Strafregisterdaten die notwendige Stufenkonformität. Für die Bearbeitung von sensiblen Personendaten ist eine Rechtsgrundlage in einem Gesetz im formellen Sinn notwendig (Art. 17 Abs. 2 Datenschutzgesetz).*
- *In Artikel 365 Absatz 2 nStGB könnte zwar MROS unter den neuen Oberbegriff „Verfolgung von Straftaten“ subsumiert werden. Im Sinne einer klaren gesetzlichen Grundlage soll indessen in einem neuen Buchstaben die Führung der Meldestelle Geldwäscherei als Zweck des Strafregisters erwähnt werden.*
- *In Artikel 367 Absatz 2 Buchstabe c nStGB ist zu präzisieren, dass das fedpol zur Führung der Meldestelle Geldwäscherei auf das Strafregister zugreifen kann.*

Für die Zeit bis zur Umsetzung dieses Vorschlags auf Gesetzesebene wird gestützt auf Artikel 367 Absatz 3 nStGB vorgeschlagen, die entsprechende Kompetenz in der Verordnung zum automatisierten Strafregister vorzusehen (Art. 20 Abs. 2 Bst. e VE-VOSTRA-Vo).

---

[21] *Art. 35 Bearbeitung durch die Meldestelle*

[1] *Die Bearbeitung von Personendaten durch die Meldestelle richtet sich nach dem Bundesgesetz vom 7. Oktober 1994 über kriminalpolizeiliche Zentralstellen des Bundes.*

[2] *Der Informationsaustausch zwischen der Meldestelle und den spezialgesetzlichen Aufsichtsbehörden, der Kontrollstelle und den Strafverfolgungsbehörden kann über ein Abrufverfahren (Online-Verbindung) erfolgen.*

[22] Gesetzesvorlage zur Umsetzung der revidierten Empfehlungen der "Groupe d'action financière sur le blanchiment des capiteaux" (Arbeitsgruppe zur Bekämpfung der Geldwäscherei).

4. Auswirkungen auf die Kantone

Die Gefahr des Missbrauchs eines Informationssystems ist umso grösser, je mehr Personen Zugriff auf dieses Informationssystem haben. Missbräuche lassen sich nur durch regelmässige Kontrollen vermeiden. In Anbetracht der beschränkten Kontrollkapazitäten des Datenschutzbeauftragten und der damit einhergehenden Gefahr einer exzessiven Nutzung der Strafregisterinformationen zu sachfremden Zwecken ist eine gewisse Zurückhaltung bei der Gewährung von Online-Zugriffen angebracht. Zumal es gerade im Polizeibereich recht häufig ist, dass eine einzelne Dienststelle viele verschiedene Aufgaben zu erfüllen hat.

Allerdings ist auch nicht einzusehen, weshalb den kantonalen Polizeistellen Strafregisterdaten zumindest dort, wo sie diese Informationen zu den gleichen Zwecken benötigen wie das fedpol, generell vorenthalten werden sollten.

Im Bericht über das Vernehmlassungsverfahren vom Februar 1997 zur Einführung von VOSTRA wurde festgehalten, dass die Kantone BE, FR, BS, AG, TG, die FDP, die KKJPD und die KKPKS für kantonale und städtische Kriminalpolizeien einen Anschluss forderten. Die Begründungen, weshalb es einen solchen Anschluss brauche, waren indessen eher rudimentär (Effizienzsteigerung; Notwendigkeit um Haftbefehl zu beantragen). In den Vernehmlassungen sprach sich niemand explizit *gegen* einen Anschluss aus, aber es wurde darauf hingewiesen, dass es sich eben um sehr sensible Daten handelt, die nur jenen Behörden zugänglich gemacht werden sollen, die diese Information zur Erfüllung ihrer gesetzlichen Aufgaben benötigen. Aus diesen Gründen wurden die Zugriffsrechte kantonaler Polizeistellen nicht weiter diskutiert, zumal man anlässlich der VOSTRA-Revision *keine materiellen Änderungen* einführen, sondern nur die rechtlichen Voraussetzungen für eine neue EDV-Lösung schaffen wollte.

Auch anlässlich der im März 2005 eröffneten Vernehmlassung zum neuen Bundesgesetz über die polizeilichen Informationssysteme (BPI) wurde von 6 Kantonen (FR, TI, VD, VS, GE, JU) ein Online-Anschluss für die kantonalen Polizeistellen gefordert. Dieses Anliegen wurde nicht weiterverfolgt, da die Zugriffsrechte auf VOSTRA von vornherein nicht Gegenstand dieses Gesetzgebungsprojektes waren.

Um eine gewisse *Gleichbehandlung* zwischen den polizeilichen Zugriffen des Bundes und der Kantone zu wahren, könnte eine mögliche Lösung für das Zugriffsrecht der Kantone sein, den Anschluss auf einen bestimmten Deliktskatalog zu beschränken, oder einen Zugriff nur für Delikte zu gewähren, für die „parallele“ Kompetenzen in Bund und Kantonen bestehen (z.B. im Rahmen von Art. 340^{bis} StGB).

Eine gewisse Zurückhaltung bei der Erteilung neuer Zugriffsrechte liesse sich auch mit dem Argument rechtfertigen, dass es sich bei der Neuregelung der Online-Zugriffe des fedpol jeweils um *Deliktsbereiche von einer gewissen Schwere* handelt, die genau deshalb in die Bundeszuständigkeit fallen. Innerhalb der (auch) *vom fedpol bearbeiteten Deliktsbereiche* wäre also eine Öffnung für die kantonalen Polizeibehörden (für Vorermittlungen oder gar im Präventivbereich) durchaus denkbar. Allerdings ist nur schwer einzusehen, weshalb man für Vorermittlungen bei einem möglichen Tötungsdelikt (kantonale Kompetenz) zurückhaltender sein sollte als beispielsweise bei Sprengstoffdelikten.

Um dennoch eine gewisse Parallelität zu den fedpol-Zugriffen zu wahren, liesse sich die Öffnung allenfalls auf *Verbrechen* beschränken. Zwar besteht die Gefahr, dass

bei der Verfolgung leichterer Delikte das schwerere Delikt jeweils als Vorwand gebraucht wird. Regelmässige Stichproben des Datenschutzbeauftragten oder der Strafregisterverantwortlichen könnten allfälligen Missbräuchen jedoch einen Riegel schieben. Den Zugriff kantonaler Polizeistellen von einem abstrakt formulierten Deliktskatalog („Verbrechen“) abhängig zu machen und nicht jedem Polizist wegen jedem erdenklichen Delikt Einsicht zu gewähren, scheint auch deshalb angezeigt, weil sonst die Gefahr besteht, dass sich die Strafverfolgung in erster Linie auf vorbestrafte Täter konzentriert.

Bei der Öffnung des Strafregisters für die Kantone gilt es zwei Zuständigkeitsbereiche zu unterscheiden:

1. Wo eine Zusammenarbeit zwischen Bund und Kanton besteht, dürften die Kantone bereits heute Strafregisterinfos vom fedpol erhalten. Eine solche Weitergabe liesse sich auch mit der vorgeschlagenen Weitergabenorm gemäss Artikel 17 Absatz 3 VE-VOSTRA-Vo (vgl. dazu die Ausführungen oben in Ziff. 2.4.2) vereinbaren, wonach Informationen des fedpol grundsätzlich an Dritte (kantonale Polizeibehörden) weitergeben werden dürfen, sofern die Zweckbindung der Daten gewahrt bleibt. Falls die Bearbeitung zu den gleichen Zwecken erfolgt, wie dies beim fedpol der Fall war, ist demnach gegen eine Weitergabe nichts einzuwenden.
2. Dort, wo die kantonalen Polizeibehörden selbständig (vor-)ermitteln oder präventiv tätig sind, könnte eine Öffnung für die Kantone sinnvoll sein. Sie sollte jedoch analog der Regelung beim fedpol – d.h. zu den gleichen Zwecken und im Rahmen der Verfolgung und Verhinderung von Schwerstkriminalität – getroffen werden.

Die Frage, inwieweit auch den Polizeistellen der Kantone ein Zugriffsrecht auf VOSTRA zu erteilen ist, sollte in einem ordentlichen Gesetzgebungsverfahren und nicht auf Verordnungsebene entschieden werden, da es sich um eine fundamental neue Fragestellung handelt. Diese Problematik ist daher anlässlich der angekündigten Revision der Strafregisterbestimmungen des nStGB nochmals aufzunehmen. Bis dann sollte sich abgezeichnet haben, welche Ausweitung der Zugriffsrechte für das fedpol (im Rahmen der Anpassung der VOSTRA-Vo) befürwortet wird.