Einrichtung von Online-Verbindungen im Bereich des Polizeiwesens

Bericht der Geschäftsprüfungskommission des Ständerates vom 19. November 1998

Bericht

1 Einleitung

11 Problematik

Die zunehmende Ausrüstung der Bundesbehörden mit EDV-Mitteln zur Erfüllung ihrer gesetzlichen Aufgaben hat namentlich im Bereich des Polizeiwesens dazu geführt, dass immer mehr Online-Verbindungen eingerichtet werden. Diese ermöglichen den vielen Amtsstellen den direkten Zugriff («Online») auf verschiedene Datenbanken.

Ein Schema ausgewählter polizeilicher Informatiksysteme soll diese Problematik verdeutlichen und verständlicher machen (*Quelle:* 1. Tätigkeitsbericht 93/94 des Eidgenössischen Datenschutzbeauftragten, aktualisiert durch die PVK, Januar 1998). Aus dem Schema wird ersichtlich, wie viele Online-Verbindungen zu Gunsten verschiedener Behörden bestehen oder geplant sind. Das Schema erfasst nur einen Teil aller Systeme der Bundesverwaltung.

Nicht alle in diesem Schema erfassten Online-Verbindungen erlauben den Zugriff auf die gesamten Daten eines Systems. Je nach Zugriffsmatrix kann nur auf einen Teil der Daten zugegriffen werden. Alle dargestellten Verbindungen bestehen bereits, können auf Grund von geltenden Gesetzes- oder Verordnungsbestimmungen eingerichtet werden oder sind im Rahmen von Gesetzesentwürfen geplant.

Das Bundesgesetz über den Datenschutz schreibt vor, dass Organe des Bundes Personendaten nur bearbeiten dürfen, wenn dafür eine gesetzliche Grundlage besteht. Weiter bestimmt das Gesetz, dass Bundesorgane Personendaten nur durch ein Abrufverfahren (Online) zugänglich machen dürfen, wenn dies ausdrücklich vorgesehen ist; diese Bedingung ist durch ein formelles Gesetz zu erfüllen, wenn die Online-Verbindung den Zugriff auf besonders schützenswerte Daten oder auf Persönlichkeitsprofile erlaubt.

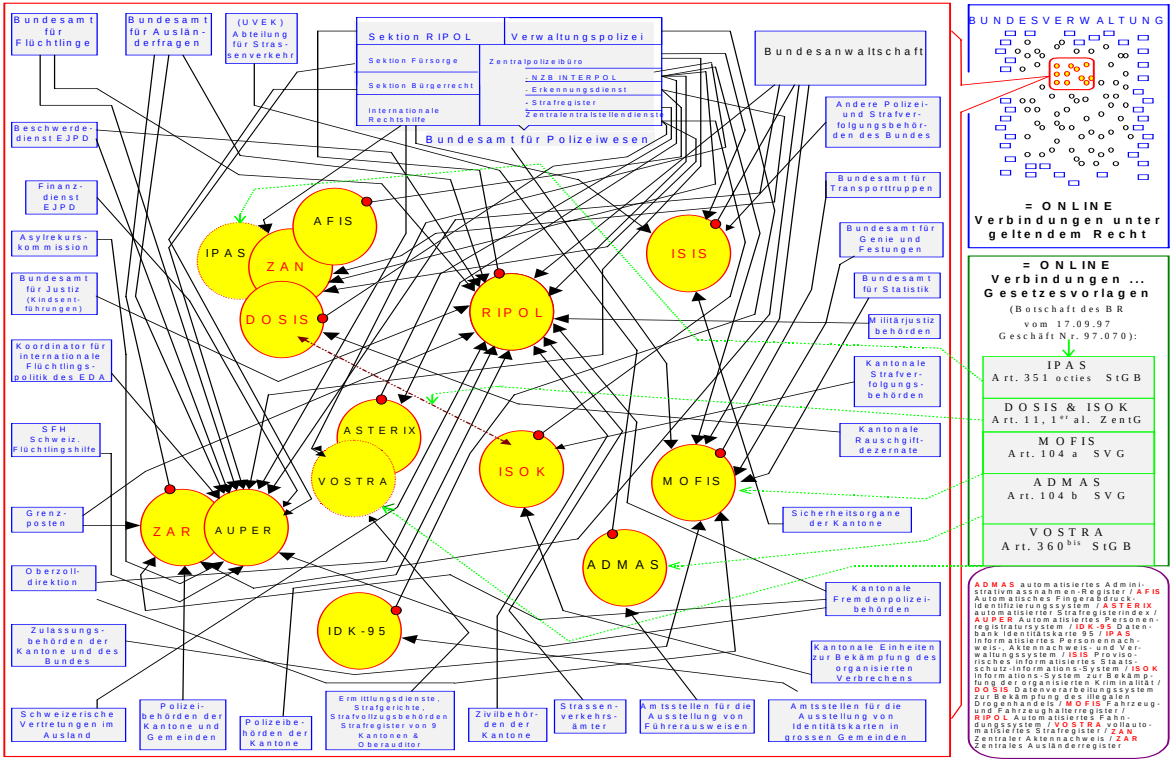
Das Bundesamt für Justiz und der Eidgenössische Datenschutzbeauftragte (EDSB) haben in Stellungnahmen bei Anhörungen, in Bekanntmachungen oder an Pressekonferenzen wiederholt darauf hingewiesen, dass diese Forderungen bei jeder Bearbeitung von Personendaten zu beachten seien. In den letzten Jahren nun drängten viele Bundesbehörden geradezu, Zugriff auf immer mehr Informationssysteme zu erhalten. Als Folge dieser Entwicklung wurden gesetzliche Grundlagen geschaffen, die alle möglichen Zugriffe erlauben, dies insbesondere im Bereich des Polizeiwesens.

Der Grundsatz der Gesetzmässigkeit soll in erster Linie Transparenz gewährleisten und ist allein nicht ausreichend als Begründung für einen Online-Zugriff. Der Einrichtung einer Online-Verbindung muss eine Prüfung ihrer Notwendigkeit, ihrer Kosten und ihrer Vereinbarkeit mit den Grundsätzen der Verhältnismässigkeit, der Zweckbindung und der Zweckmässigkeit vorangehen. Mit anderen Worten: Ein Abrufverfahren muss auch mit diesen Grundsätzen vereinbar sein und darf nicht einzig auf Grund einer gesetzlichen Grundlage geplant oder gerechtfertigt werden. Diese Problematik ist übrigens auch auf kantonaler Ebene erkannt worden[1].

[1] «Diese Anstrengung wird insbesondere im Bereich der Abrufverfahren deutlich: Angesichts der gegenwärtigen Tendenz, solche Verfahren in der ganzen Verwaltung einzuführen, wünscht die Kommission, dass eine grundsätzliche Reflexion stattfindet und sich die Regierung nicht einfach darauf beschränkt, dem Grossen Rat für jede neue Informatikverbindung eine einzelne gesetzliche Grundlage vorzuschlagen» (vgl. Rapport sur l'activité de l'Autorité cantonale fribourgeoise de surveillance en matière de protection des données, juillet 95–déc. 96, S. 7 (Französisch)

«ONLINE»-Inspektion (Einrichtung von «Online»-Verbindungen im Bereich des Polizeiwesens)

Inspektion der Geschäftsprüfungskommission des Ständerates und der Parlamentarischen Verwaltungskontrollstelle



Quellen: EDSB/Mai 1994, 1. Tätigkeitsbericht 1993/94, GPK/PVK Inspektion «ONLINE» Januar 1998, Projektleiter: Marc Buntschu

12 Auftrag der Geschäftsprüfungskommissionen

Die Geschäftsprüfungskommissionen haben im Rahmen ihres Jahresprogramms 1998 beschlossen, eine Inspektion über die «Einrichtung von Online-Verbindungen im Bereich des Polizeiwesens» durchzuführen.

Die Sektion Behörden der Geschäftsprüfungskommission des Ständerates, die mit der Inspektion beauftragt wurde, hat sich verschiedene Untersuchungsziele gesetzt. Dazu gehören insbesondere eine Untersuchung auf Konzeptstufe und eine Beurteilung der aktuellen Praxis (Expertenbericht, vgl. Anhang I[2]).

Die Untersuchung soll zuerst die geltenden rechtlichen und konzeptionellen Anforderungen für die Einrichtung von Online-Verbindungen herausarbeiten. Dieser Teil hat somit theoretischen Charakter und untersucht die konzeptionellen Anforderungen, Fragen des Datenschutzes und die Beachtung von Verhältnismässigkeit, Zweckbindung und Zweckmässigkeit bereits auf der Planungsebene aus allgemeiner Sicht.

Der Expertenbericht untersucht die Praxis der Bundesverwaltung bei der Einrichtung von Abrufverfahren von der Planung eines Systems an sowie die Zuteilung neuer Online-Zugriffsmöglichkeiten an die Bundes- und Kantonsbehörden.

13 Organisation und Vorgehen der Kommission

131 Personelle Organisation

Die Sektion ist wie folgt organisiert:

Präsident:	SR Pierre Aeby
Mitglieder:	SR Hans Danioth; SR Bruno Frick (bis Ende 1997); SR Hans Hess (ab Juni 1998); SR Andreas Iten; SR Franz Wicki; SR Kaspar Rhyner (bis Ende Mai 1998)
Sekretariat:	Mariangela Wallimann-Bornatico, Sekretärin der GPK

Parlamentarische Verwaltungskontrollstelle (PVK): Marc Buntschu

Beauftragter Experte: Lukas Fässler, Rechtsanwalt und Informatikexperte

132 Zeitliche Organisation

Die Sektion Behörden befasste sich an ihrer Sitzung vom 8. April 1997 mit dieser Problematik, wobei ein von der Parlamentarischen Verwaltungskontrollstelle (PVK) verfasstes Arbeitsdokument als Grundlage diente. Die Sektion bejahte die Notwendigkeit weitergehender Untersuchungen und setzte den Bundesrat in ihrem Schreiben vom 10. April 1997 davon in Kenntnis.

Am 27. Juni 1997 nahm die Sektion die Projektskizze der PVK zur Kenntnis. Sie bestimmte im Rahmen einer Machbarkeitsstudie den Bereich, den Zeitplan und die

[2] Dieser Bericht wird im Bundesblatt nicht veröffentlicht. Separatdrucke davon können bezogen werden beim Sekretariat der Geschäftsprüfungskommission, Parlamentsdienst, 3003 Bern

organisatorischen Aspekte der Untersuchung und legte fest, welche Fragen zu behandeln seien.

Ende März 1998 legte die PVK ein Arbeitsdokument vor. Am 6. Mai 1998 trug der beauftragte Experte der Sektion mündlich seine ersten Schlussfolgerungen vor. Die Sektion ihrerseits orientierte die Geschäftsprüfungskommission des Ständerates an ihrer Plenarsitzung vom 25. und 26. Mai 1998 über die ersten Erkenntnisse aus der Inspektion. Nach einer Konsultation der interessierten Ämter reichte der Experte seinen Schlussbericht am 31. Juli 1998 ein.

Die Sektion besprach am 2. September 1998 erstmals die Untersuchungsergebnisse. Nach einer zweiten Besprechung liess sie den Berichtsentwurf den Vorstehern des EJPD und des EFD zur Stellungnahme zukommen. Die Haltung dieser betroffenen Departemente besprach die Sektion mit Bundesrat Arnold Koller an der Sitzung vom 5. November 1998. Die Sektion hörte ebenfalls den Datenschutzbeauftragten an.

Die Sektion unterbreitete ihren Schlussbericht der Geschäftsprüfungskommission des Ständerates, die ihn am 19. November 1998 verabschiedete.

133 Zusammenarbeit mit der Bundesverwaltung

Sowohl die PVK wie auch der Experte betonen die interessierte und konstruktive Zusammenarbeit mit den betroffenen Ämtern des Justiz- und Polizeidepartements. Verbesserungsvorschläge, die der Experte in einem ersten Arbeitsdokument gemacht hatte, konnten teilweise bereits vor Abschluss der Untersuchung verwirklicht werden.

134 Unabhängigkeit der Mitglieder der Sektion

Die Mitglieder der Sektion bestätigen, dass sie keine Verbindungen privater oder beruflicher Natur haben, die mit den hier behandelten Fragen in Konflikt stehen könnten.

14 Methodisches Vorgehen

141 Vorgehensweise

Die PVK und der Experte haben in einem ersten Schritt den Ist-Zustand erhoben und analysiert. Auf Wunsch der Experten lieferten die zuständigen Stellen folgende Unterlagen:

- alle geltenden Bestimmungen, die bei der Einrichtung von Online-Verbindungen zur Anwendung kommen (formelle Gesetze, Ausführungsverordnungen, technische Weisungen, Sicherheitsweisungen, Anwendungshandbücher, Bearbeitungsreglemente, Standard für die Führung und Abwicklung von Informatikprojekten, Controlling-Massnahmen usw.);

– alle Dokumente über die Entwicklung der untersuchten Informatiksysteme *(Unterlagen zu Initialisierung, Voranalyse, Konzepten, Realisierung, Inbetriebnahme, neuen Entwicklungen);*

– sowie die Rechtsgrundlagen, die für diese Systeme und Zugriffsmöglichkeiten geschaffen wurden *(Gesetze, Verordnungen, Weisungen, Reglemente, Zugriffsmatrizen).*

Die Ämter wurden auch gebeten, eine schriftliche Liste mit allen Online-Verbindungen ihres Informatiksystems einschliesslich der zugriffsberechtigten Behörden sowie eine chronologische Auflistung zur Systementwicklung und der Einrichtung der entsprechenden Online-Verbindungen zu liefern, sowie zu den Problemen Stellung zu nehmen, die bei der Einrichtung der verschiedenen Online-Verbindungen ihrer Informatiksysteme festgestellt oder aufgetreten sind.

Nach einer Prüfung dieser Dokumente wurden Vertreterinnen und Vertreter verschiedener Amtsstellen angehört und ergänzende schriftliche Stellungnahmen angefordert.

142 Gesprächspartner

Gesprächspartner im Rahmen dieser Untersuchung waren in erster Linie die Organe und Ämter, die an der Einrichtung von bestehenden oder geplanten Online-Verbindungen für die von der Sektion ausgewählten Informatiksysteme beteiligt waren oder sind, nämlich:

– das Bundesamt für Polizeiwesen
– die Bundesanwaltschaft
– das Bundesamt für Ausländerfragen
– Kantonsbehörden mit bestehendem oder geplantem Online-Anschluss an die ausgewählten Informatiksysteme
– das Bundesamt für Informatik
– die Generalsekretariate von EJPD und EFD
– das Rechenzentrum EJPD, der Datenschutzberater des EJPD
– der Eidgenössische Datenschutzbeauftragte.

Eine enge Zusammenarbeit erfolgte auch mit der Verwaltungskontrolle des Bundesrates (VKB), die den *«Online-Datenaustausch zwischen Bund und Kantonen»* untersuchte (VKB-Projekt Nr. 29)[3]. Ihr Bericht wurde am 16. März 1998 veröffentlicht.

143 Inhalt des Berichts

Dieser Bericht erhebt nicht den Anspruch, alle Probleme im Zusammenhang mit der Einrichtung von Online-Verbindungen erschöpfend zu behandeln, da dieses Gebiet

[3] Vgl. Bericht der Verwaltungskontrolle des Bundesrates vom 16. März 1998 «Online-Datenaustausch zwischen Bund und Kantonen».

äusserst weit und komplex ist. Er legt das Hauptgewicht auf die konzeptionellen und rechtlichen Aspekte und auf Datenschutzfragen.

Die Untersuchungsergebnisse und die darauf beruhenden Empfehlungen der Kommission sollen eine angemessenere Einrichtung von Online-Verbindungen im Allgemeinen, und im Bereich des Polizeiwesens im Besonderen, ermöglichen.

15 Auswahl der Informatiksysteme

Die Sektion prüfte mehrere Systeme als mögliche Untersuchungsobjekte [RIPOL, DOSIS, ISIS, ZAN, AFIS, ZAR, AUPER]. Sie arbeitete verschiedene Kriterien aus, die bei der Auswahl zu berücksichtigen waren, darunter insbesondere die folgenden: Welchen *Bedrohungen, Angriffen* und *potentiellen Missbräuchen* sind die Online-Verbindungen ausgesetzt? *Wie viele Behörden sind* per Abrufverfahren auf ein System *zugriffsberechtigt? Besteht bereits eine gesetzliche Grundlage* (de lege lata), oder wird sie erst *ausgearbeitet* (de lege ferenda)? Mit dieser Unterscheidung können Tendenzen in der Gesetzgebung abgeschätzt werden. Ebenfalls betont wurde, dass die Ergebnisse der von der *Delegation* der GPK durchgeführten Untersuchungen über die «Vorkommnisse im EMD (EBG 95)» zu berücksichtigen seien.

Auf Grund dieser Kriterien legte die Sektion das Hauptgewicht auf die folgenden Informatiksysteme:

- **RIPOL** (Automatisiertes Fahndungssystem)
- **DOSIS** (Datenverarbeitungssystem zur Bekämpfung des illegalen Drogenhandels)
- **ISIS-[**Plus] (Provisorisches informatisiertes Staatsschutz-Informations-System)
- **ZAR** (Zentrales Ausländerregister)

Die Sektion berücksichtigte bei ihrer Prüfung aber auch das System ZAN (Zentraler Aktennachweis), da damit Daten aus DOSIS importiert werden können, sowie das System ISOK (Informations-System zur Bekämpfung der organisierten Kriminalität), da seine Ausarbeitung mit den aktuellen Weiterentwicklungen von DOSIS in direktem Zusammenhang steht.

16 Abgrenzung des Untersuchungsgebiets

Die Diskussionen in der Sektion und in der Kommission zeigten, dass die Untersuchung der Einrichtung von Online-Verbindungen im Bereich des Polizeiwesens angebracht und notwendig ist. Neben den zahlreichen Verbindungen, die bereits in den letzten Jahren eingerichtet wurden, kann zudem eine stetige Zunahme festgestellt werden, und es kommt regelmässig zu neuen Projekten oder Weiterentwicklungen.

Die Kommission bejaht grundsätzlich die Notwendigkeit von Online-Verbindungen. Sie anerkennt, wie wichtig Effizienz und Koordination im Bereich des Polizeiwesens und Kompatibilität der Systeme sind.

Die Kommission weist jedoch auf die Gefahren solcher Online-Verbindungen hin und wünscht sich insbesondere mehr Transparenz. Sie ist der Auffassung, dass die genauen Bedingungen für die Einrichtung solcher Verbindungen unbedingt zu un-

tersuchen und dabei ihre stetig zunehmende Zahl und die Gefahr von Angriffen oder Missbräuchen zu berücksichtigen sind.

Die Sektion legte das Hauptgewicht nicht auf die technischen Aspekte der Inspektion. Dennoch wurden auch diese Aspekte behandelt, insbesondere im Rahmen der Untersuchung der Informatikkonzepte, der Sicherheitsmassnahmen oder der Kontrollmechanismen. Bei letzteren wurde das Schwergewicht auf Fragen des Datenschutzes gelegt.

Auf diese Weise konnten die von der GPK des Nationalrates im Rahmen der *Inspektion zur Einführung der Informatik in der Bundesverwaltung* durchgeführten Untersuchungen (BBl *88* II 665) weitergeführt werden. Denn obwohl im Bereich des Datenschutzes damals zahlreiche Lücken[4] festgestellt wurden, wurde die *Überwachung der Projekte zur automatisierten Bearbeitung* nie einer genaueren Überprüfung unterzogen. Die GPK des Nationalrates hatte diese Inspektion mit Hinweis auf die vorliegende Prüfung durch die ständerätliche GPK im Mai 1997 abgeschlossen.

2 Untersuchung auf Konzeptstufe

21 Untersuchungsbereich

Die zentrale Frage dieser Inspektion lautet: *Welche Regeln gelten bei Planung und Einrichtung von Online-Verbindungen im Bereich des Polizeiwesens?*

Mit dieser zentralen Frage stellten sich der Kommission folgende zusätzliche Fragen:

- Gibt es in der Bundesverwaltung und insbesondere im EJPD *Bestimmungen* über die Einrichtung von Online-Verbindungen?
- Sind die zahlreichen *Weisungen des BFI* auf diese Problematik anwendbar?
- Welche *Anforderungen* sind im Bereich des Datenschutzes zu erfüllen?
- Welche *Rechtsgrundlagen* gelten im Bereich des Datenschutzes?
- Werden die Grundsätze der *Verhältnismässigkeit, Zweckbindung, Zweckmässigkeit* und *Notwendigkeit* bei der Ausarbeitung der Informatikkonzepte berücksichtigt?
- Ist bei der Einrichtung von Online-Verbindungen im Rahmen der Ausarbeitung der Informatikkonzepte auch die Untersuchung der Kosten vorgesehen?
- Sind bei der Einrichtung von Online-Verbindungen die *Überwachung* und die *Kontrolle* geregelt?
- Welche Rolle spielt *das Verfahren HERMES* als Instrument und Standard für die Führung und Abwicklung von Informatikprojekten in der Bundesverwaltung?

4 Entwicklung von sogenannten verbundenen Systemen; Verflechtung der Informationssysteme (BBl **1988** II 683, 704); Rolle und Mittel des Eidgenössischen Datenschutzbeauftragten im Bereich der Überwachung (vgl. Schreiben der GPK-N vom 23. Mai 1995 an den BR).

– *Wer bewilligt* nach den geltenden Bestimmungen Online-Verbindungen?
– Welche Rollen und Kompetenzen haben die *Projekt-* oder *Fachgruppen*, die mit der Einrichtung der Online-Verbindungen beauftragt sind?

22 Einführung

Die Kommission konnte sich davon überzeugen, dass die Datenbanken und die Verbindungen, die den Zugriff auf diese Datenbanken ermöglichen, wie folgt geregelt sind:

RIPOL
– Artikel 251bis Schweizerisches Strafgesetzbuch
– RIPOL-Verordnung vom 19. Juni 1995
– Änderung der RIPOL-Verordnung vom 11. September 1996

DOSIS
– Bundesgesetz vom 7. Oktober 1994 über kriminalpolizeiliche Zentralstellen des Bundes
– DOSIS-Verordnung vom 26. Juni 1996

ISOK
– Bundesgesetz vom 7. Oktober 1994 über kriminalpolizeiliche Zentralstellen des Bundes
– ISOK-Verordnung vom 19. November 1997

ISIS
– Bundesgesetz vom 21. März 1997 über Massnahmen zur Wahrung der inneren Sicherheit (in Kraft getreten am 1. Juli 1998)
– ISIS-Verordnung vom 31. August 1992
– Änderung der ISIS-Verordnung vom 2. Dezember 1996
– ISIS-Weisungen vom 31. August 1992

ZAN
– Verordnung vom 1. Dezember 1986 über den Erkennungsdienst des Bundesamtes für Polizeiwesen
– Änderung der Verordnung vom 2. Dezember 1996

ZAR
– ZAR-Verordnung vom 23. November 1994
– Änderung der ZAR-Verordnung vom 4. Dezember 1995
– Bundesgesetz über Aufenthalt und Niederlassung der Ausländer (ANAG)

Der Grundsatz der Gesetzmässigkeit soll in erster Linie Transparenz gewährleisten. Er ist jedoch allein nicht ausreichend als Begründung für Online-Zugriffe. Der Einrichtung einer Online-Verbindung muss eine ganze Reihe von Etappen vorangehen (Initialisierung, Planung, Prüfung der Notwendigkeit, der Kosten und der Verhältnismässigkeit, Zweckbindung und Zweckmässigkeit, Prüfung der Sicherheitsmassnahmen, globale Risikobeurteilung usw.). Ein Abrufverfahren darf also nicht ausschliesslich auf Grund einer Rechtsgrundlage geplant oder gerechtfertigt werden, sondern muss bestimmte Vorverfahren durchlaufen, und seine Planung hat bestimmte Regeln oder Grundsätze zu befolgen.

Durch die Untersuchung der zentralen Frage und des damit zusammenhängenden Untersuchungsgebietes soll deutlich werden, welche Etappen jeder Einrichtung einer Online-Verbindung vorangehen sollen und ob in diesem Bereich Lücken bestehen, mit anderen Worten welche Regeln bei der Planung von Online-Verbindungen anzuwenden sind, bevor diese Verbindungen und die entsprechenden Rechtsgrundlagen geschaffen werden.

23 Untersuchung der zusätzlichen Fragen

231 Die Weisungen des BFI

Regeln die zahlreichen Weisungen des BFI diese Problematik?

231.1 Verzeichnis der Weisungen des BFI[5]

Die Rechtsgrundlagen der Bundesinformatik sind hauptsächlich:

- Die Verordnung vom 11. Dezember 1989 über das Bundesamt für Informatik und über die Koordination der Informatik in der Bundesverwaltung (SR *172.010.58*).
- Die Verordnung vom 10. Juni 1991 über den Schutz der Informatiksysteme und -anwendungen in der Bundesverwaltung (SR *172.010.59*).
- Das Informatikbild des Bundes vom 8. Juli 1994.

Gestützt auf diese Grundlagen gab das Bundesamt für Informatik verschiedene Technische Weisungen (TW), Weisungen zur Informatiksicherheit (WS) und Strategien heraus:

A Verzeichnis der Technischen Weisungen

(Artikel 3 der Verordnung des BR über das BFI und über die Koordination der Informatik in der Bundesverwaltung):

TW 01	Vergabe von Informatik-Dienstleistungsaufträgen an externe Firmen, vom 15. Januar 1997	
	Beilage 1	Einstufungsbedingungen, Ausgabe 1994
	Beilage 2	Ansatz pro Stunde für Informatikdienstleistungen, Ausgabe 1998
	Beilage 3	Vorlage für die Vertragsurkunde zur Beschaffung von Informatik-Gesamtsystemen sowie die Herstellung von Individualsoftware (Werkvertrag), Ausgabe vom 15. Januar 1997
	Beilage 4	Vorlage für die Vertragsurkunde für Informatikdienstleistungen (Auftrag), Ausgabe vom 15. Januar 1997
	Beilage 5	Allgemeine Geschäftsbedingungen für die Beschaffung von Informatik-Gesamtsystemen sowie die Herstellung von Individualsoftware (gelbes Papier), Ausgabe Juli 1997
	Beilage 6	Allgemeine Geschäftsbedingungen für Informatikdienstleistungen (grünes Papier), Ausgabe Juli 1994
	Beilage 7	Anwendungshandbuch, in Bearbeitung
TW 02	Finanz- und Beschaffungsablauf im Informatikbereich, vom 15. Januar 1997	
	Beilage 1	Checkliste für eine Beschaffung nach BoeB und VoeB, Januar 1997

5 Vgl. Publikation BFI «BFI-News 1997», S. 39–47 und vgl. Schreiben BFI vom 9. Jan. 1998, Punkt 4. Online-Verbindungen allgemein, S. 5–6.

TW 03 Meldung der Informatikprojekte an das BFI, vom 22. August 1990

TW 04 Konzeption der Registraturautomation, vom 11. Dezember 1990
- Beilage 1 Kriterienkatalog zur Bewertung von Registraturanwendungen

TW 05 Jährliche Meldungen der Dienststellen über Personalbestände, Ausgaben und Kosten im Informatikbereich, vom 16. September 1992

TW 06 PC-HANDBUCH, aufgehoben am 18. Oktober 1995

TW 07 Adressierung der elektronischen Post in der Bundesverwaltung, vom 17. Januar 1996
- Beilage 1 Übergang von der TW 07 von 1991 zur TW 07 von 1996, vom 17. Januar 1996

TW 08 Handbuch für LAN-Projektleiter, vom 16. Oktober 1996
Beilagen 1–15 (nur auf Deutsch erhältlich)

TW 09 SNA / SNI Namenskonventionen – 92, vom 16. September 1992

TW 10 Weiterverwendung von nicht mehr benötigtem Informatikmaterial, vom 15. Juni 1994

TW 11 Domain Name System (DNS), vom 13. November 1996

TW 12 Koordination und Standardisierung von Geschäftsverwaltungssystemen (GEVER), vom 18. Januar 1995
- Beilage 1 GEVER-Datenmodell (nur auf Deutsch erhältlich)
- Beilage 2 Einsatzprofile (nur auf Deutsch erhältlich)

TW 13 Einführung und Einsatz der Software SAP R/3, vom 17. September 1997
- Beilage 1 Architektur SAP R/3
- Beilage 2 SAP-Koordination

TW 14 Abgabeschnittstelle BAR, vom 21. August 1996

TW 15 EDV-basierende Systeme für die Zeiterfassung in der Bundesverwaltung, vom 17. Mai 1995
- Beilage 1 Erfassungsblatt: EDV-basierende Zeiterfassung in der Bundesverwaltung, vom 17. Mai 1995

TW 16 Projektführung und Systementwicklung in Informatikprojekten, vom 19. April 1995
- Anhang 1 Beigefügte Dokumente
- Anhang 2 Aufgaben und Dienstleistungen des Bundesamtes für Informatik
- Anhang 3 Koordinations- und Kontrollstellen
- Anhang 4 Standards

Sonderdruck: Richtlinien für Projektführung und Systementwicklung in Informatikprojekten (RPS), vom 19. April 1995

TW 17 Adressierung NSAP (Network Service Access Point), vom 18. Oktober 1995
- Beilage 1 Antragsformular für NSAP-Adressraum Administrativ-Domain
- Beilage 2 Antragsformular für NSAP-Adressraum Routing-Domain
- Beilage 3 Antragsformular für NSAP-Adressraum Routing-Area

TW 18 World Wide Web (WWW) in der Bundesverwaltung, vom 15. Januar 1997

Beilage 1 Antrag für einen eigenen http-Proxy
Beilage 2 Antrag für WWW-Zugriff auf Internet ab Proxy-Server
Beilage 3 Antrag für Public-WWW-Server am Internet

TW 19 Informatikcontrolling und Wirtschaftlichkeitsrechnung in der Bundesverwaltung, vom 14. Januar 1998

B Verzeichnis der Weisungen zur Informatiksicherheit (WS)

(Art. 8 der Verordnung vom 10. Juni 1991 über den Schutz der Informatiksysteme und -anwendungen in der Bundesverwaltung (SR 172.010.59):

WS S01 Handhabung der Benutzeridentifikationen und der Passwörter, vom 18. August 1993
Merkblatt zur Verwendung von Passwörtern in der Bundesverwaltung, vom Dezember 1993

WS S02 Grundschutz von Informatiksystemen und -anwendungen, vom 19. April 1995

Anhang 1 Anleitung zur Erhebung und Einstufung von Schutzobjekten
Anhang 2 Katalog der Grundschutzmassnahmen
Anhang 3 Erhebungsformulare (Farbige Formulare erhältlich beim BFI)

HANDBUCH Nr. 1 zur WS S02: Verfahren für die Checklistenbearbeitung und Gesamtmassnahmenkatalog, vom 1. Oktober 1996

WS S03 Umsetzung der Network Security Policy (NSP), vom 25. Juni 1997

C Verzeichnis der Strategien

Nach Ziffer 3 des Informatikleitbildes des Bundes (ILB) werden die bundesweit gültigen Umsetzungsstrategien durch das BFI im Einvernehmen mit der Informatikkonferenz Bund (IKB) ausgearbeitet und gemäss der Verordnung über das BFI und über die Koordination der Informatik in der Bundesverwaltung erlassen.

GEVER-Strategie Strategie zur Koordination und Standardisierung von Geschäftsverwaltungssystemen der allgemeinen Bundesverwaltung, vom 18. Januar 1995

Anhang A Glossar
Anhang B Literaturverzeichnis
Anhang C Abbildungen

Telekommunikations-Strategie Telekommunikationsstrategie der Allgemeinen Bundesverwaltung, vom 12. Juni 1996

Anhang Verwendete Abkürzungen

Network Security Policy (NSP), vom 25. Juni 1997

231.2 Sehen diese Weisungen für die Einrichtung von Online-Verbindungen bestimmte Bestimmungen vor?

Dem Bundesamt für Informatik kommt bei der Einrichtung von Online-Verbindungen die Aufgabe zu, die *Kommunikationsinfrastrukturen* im Bereich der gesamten Bundesverwaltung zu planen und zu betreiben. Die Online-Verbindungen im Polizeibereich erfolgen auf der physischen Ebene, wo vorhanden, über die Datenkommunikationsinfrastruktur des Bundes. Auf der logischen Ebene sind die Netze jedoch aus Sicherheitsgründen getrennt.

Das Bundesamt für Informatik hat, wie erwähnt, zahlreiche Weisungen ausgearbeitet und herausgegeben. Anwendungen wie RIPOL, DOSIS, ISOK, ZAN, ZAR und ISIS gehören zu Organisationseinheiten, die den Sicherheitsweisungen des BFI unterstehen. Daher gelten für diese Systeme die Sicherheitsgrundsätze und -bestimmungen der Bundesverwaltung, insbesondere:

- das Bundesgesetz und die Verordnung über den Datenschutz (SR *235.1* und *235.11*);
- die Verordnung über den Schutz der Informatiksysteme und -anwendungen in der Bundesverwaltung (SR *172.010.59*);
- die Sicherheitsweisung WS S01: Handhabung der Benutzeridentifikationen und der Passwörter;
- die Sicherheitsweisung WS S02: Grundschutz von Informatiksystemen und -anwendungen;
- die Sicherheitsweisung WS S03: Umsetzung der Network Security Policy (NSP).

Das bedeutet insbesondere Folgendes:

- Diese Anwendungen sind gemäss der Sicherheitsweisung WS S02 über den Grundschutz von Informatiksystemen und -anwendungen als Schutzobjekte zu erheben und einzustufen und in jedem Fall einer Risikobeurteilung zu unterziehen.
- Für diese Applikationen sind gemäss den Sicherheitsweisungen WS S01 und WS S02 Sicherheitsmassnahmen zu ergreifen.
- Gemäss der Sicherheitsweisung WS S02 sind organisatorische Massnahmen zu treffen (Anwendungsverantwortliche, Sicherheitsbeauftragte, Kontrollorgane usw.).
- Neu gewährte Zugriffe auf diese Anwendungen haben seit 1997 den Anforderungen der *Network Security Policy (NSP)* und der *Sicherheitsweisung WS S03: Umsetzung der Network Security Policy* zu genügen.

Die Bedeutung dieser Sicherheitsmassnahmen wurde übrigens auch im Bericht des Finanzdepartements «*Bericht EFD (BFI) an den Bundesrat vom 14. April 1997 bzw. vom 13. Juni 1997 betreffend: a) Stand der Umsetzung der Verordnung über den Schutz der Informatiksysteme und -anwendungen in der Bundesverwaltung; b) Sicherheit im Umfeld Büroautomation und Auditmöglichkeiten von Zugriffen auf sen-*

sible Datenbanken»[6] hervorgehoben (z. B. Risikobeurteilung, Ernennung von Informatiksicherheitsbeauftragten, Datenchiffrierung, Authentifikation, tägliche Aufzeichnung der Zugriffe usw.).

Doch trotz der zahlreichen, oben erwähnten Weisungen und Bestimmungen, die für die von der Sektion Behörden ausgewählten Systeme gelten, ist festzuhalten, dass diese Weisungen keine Bestimmungen enthalten, die spezifisch für die Einrichtung von Online-Verbindungen gelten, insbesondere was die Prüfung der Grundsätze der Zweckmässigkeit, Zweckbindung und Verhältnismässigkeit betrifft. Aus den Unterlagen und Stellungnahmen des BFI und den Erklärungen des Datenschutzberaters des EJPD geht denn auch hervor, dass die oben aufgeführten Weisungen vielmehr Fragen zu Sicherheitsmassnahmen, Authentifikations- und Zugriffsverfahren, Chiffriermassnahmen, organisatorischen Massnahmen, Risikobeurteilungen, unterschiedlichen Schutzstufen (1–3) und Schutz der Systeme und angeschlossenen Applikationen (Network Security Policy/NSP) regeln.

Anhang 2 der WS S02 über die Informatiksicherheit, der einen «Katalog der Grundschutzmassnahmen» enthält, sieht zwar in Kapitel 8 «Vertraulichkeit und Integrität» für Zugriffe auf Informatiksysteme zahlreiche genauere Bestimmungen vor. Diese Bestimmungen gelten jedoch hauptsächlich für *individuelle Zugriffe*. So beschreibt Anhang 2 die Massnahmen für Benutzeridentifikation und Passwörter und legt bestimmte Kriterien fest, so beispielsweise die Unterbrechung inaktiver Verbindungen, die Sperrung nicht beanspruchter Zugriffsrechte, die Kontrolle der Subjekte, Objekte, Häufigkeit und Dauer der Zugriffsrechte, die Vergabe der Zugriffsrechte von Fall zu Fall in Abhängigkeit von individuellen Aufgaben und Funktionen der betreffenden Personen oder die Vergabe oder Veränderung von Privilegien.

Das *Vorgehen* bei der Einrichtung von Informatiksystemen und den entsprechenden Online-Verbindungen wird hingegen nicht durch diese Weisungen geregelt, sondern durch ein besonderes Projektführungssystem, das Verfahren HERMES.

232 Vorgehen und Kompetenzen

Gibt es in der Bundesverwaltung und insbesondere im EJPD Bestimmungen über die Einrichtung von Online-Verbindungen?

Welche Rolle spielt das Verfahren HERMES als Instrument und Standard für die Führung und Abwicklung von Informatikprojekten in der Bundesverwaltung?

Wer bewilligt nach den geltenden Bestimmungen Online-Zugriffe?

Welche Rolle und Kompetenzen haben die Projekt- oder Fachgruppen, die mit der Einrichtung der Online-Verbindungen beauftragt sind?

Der Datenschutzberater des EJPD, der von der Sektion Behörden zu diesem Problemkreis ausführlich befragt wurde, gab detailliert Auskunft über die rechtlichen Bestimmungen, die im EJPD bei der Einrichtung von Online-Verbindungen ange-

6 Vgl. Bericht EFD (BFI) an den Bundesrat vom 4. Jan. 1997, bzw. vom 13. Juni 1997 und Bundesratbeschluss vom 16. Juni 1997 betr. a) Stand der Umsetzung der Verordnung über den Schutz der Informatiksysteme und -anwendungen in der Bundesverwaltung, b) Sicherheit im Umfeld Büroautomation und Auditmöglichkeiten von Zugriffen auf sensible Datenbanken.

wendet werden, und über den Einsatz von HERMES als Instrument und Standard für die Führung und Abwicklung von Informatikprojekten im EJPD.

232.1 Die gesetzlichen Bestimmungen

Das EJPD wendet in diesem Zusammenhang folgende gesetzlichen Bestimmungen an:

– die *Verordnung* vom 14. Juni 1993 *zum Bundesgesetz über den Datenschutz* (SR *235.11*)

  Artikel 20 Absatz 2 dieser Verordnung bestimmt, dass die verantwortlichen Bundesorgane dem Eidgenössischen Datenschutzbeauftragten unverzüglich alle Projekte zur automatisierten Bearbeitung von Personendaten melden. In der Regel erfolgt diese Meldung an den Datenschutzbeauftragten über das Bundesamt für Informatik.

– die *Verordnung* vom 10. Juni 1991 *über den Schutz der Informatiksysteme und -anwendungen in der Bundesverwaltung* (SR *172.010.59*)

  Artikel 7 dieser Verordnung legt fest, dass die verantwortlichen Organisationseinheiten für Informatiksysteme dem BFI die Planung von Systemen gemäss technischer Weisung der Informatik-Konferenz Bund (IKB) melden. Die Meldung erfolgt ans BFI, während gleichzeitig dem Eidgenössischen Datenschutzbeauftragten eine Kopie zugestellt wird.

– *die Technische Weisung TW 03* vom 22. August 1990: *Meldung der Informatikprojekte an das BFI*

  Artikel 1 dieser Technischen Weisung legt fest, dass jedes neue Informatikprojekt in Form eines Projektantrags nach HERMES zu melden ist.

232.2 Das Verfahren HERMES im Allgemeinen

HERMES ist eine Methode zur Führung und Abwicklung von Informatikprojekten in Form eines Instruments zur Organisierung, Planung, Ausführung, Steuerung und Kontrolle von Informatikprojekten[7].

Dieses Projektführungssystem wird in der Bundesverwaltung seit 1975 eingesetzt. 1986 erfolgte eine grössere Revision von HERMES, und seine Anwendung wurde für alle Informatikprojekte verbindlich.

232.3 Das Verfahren HERMES im EJPD

Laut dem Datenschutzberater des EJPD wird im Justiz- und Polizeidepartement das Verfahren HERMES als Instrument und Standard für die Führung und Abwicklung von Informatikprojekten eingesetzt. HERMES unterscheidet verschiedene Phasen,

[7] Vgl. Handbuch «HERMES», Führung und Abwicklung von Informatikprojekten, BFI, Ausgabe 1995

die alle einzeln zu genehmigen sind, bevor die nächste Phase freigegeben werden kann. Die Hauptphasen sind:

a. Initialisierung des Projekts (Projektantrag): Dokument von ungefähr zehn Seiten; gibt Aufschluss über das geplante Projekt, die dafür erforderlichen Mittel usw.

b. Voranalyse: Festlegung und Überprüfung der grundsätzlichen Aspekte des Projekts, Prüfung und Vorbereitung allfälliger Rechtsgrundlagen

c. Konzept: Verfeinerung des gewählten Lösungsvorschlags

d. Realisierung: Programmierung und Tests

e. Einführung: Ausbildung der Benutzer, Betrieb des Systems

HERMES nennt des Weiteren die Punkte, die in jeder Phase zu überprüfen sind. Bevor ein Entscheid getroffen werden kann, sind somit verschiedene Fragen zu klären, die die grundsätzliche Organisation eines Projektes festlegen.

Die Rollen und Kompetenzen der Projektgruppen oder anderer Fachorgane sind im Handbuch HERMES genau definiert[8]:

– Genehmigungsinstanz
– Projektauftraggeber
– Projektausschuss
– Projektleitung
– u. a.

Laut dem Datenschutzberater des EJPD begleiten verschiedene Instanzen die Informatikprojekte im EJPD auf Departementsebene, wie dies nach HERMES vorgesehen ist:

a. Die Genehmigungsinstanz

Sie gibt die verschiedenen Phasen frei.

Im EJPD entscheidet bei Grossprojekten der Generalsekretär oder sein Stellvertreter, ob eine Phase beendet ist und zur nächsten übergegangen werden kann.

b. Der Projektausschuss

Er besteht je nach Projekt aus einer unterschiedlichen Anzahl Mitglieder, darunter der Projektleiter, der Chef Informatik des Departements, ein Datenschutzberater (je nachdem derjenige des Amtes oder des Departementes; bei manchen Projekten nehmen auch beide teil), Vertreter der Benutzer (Ämter und Kantone). Manchmal nimmt auch der Eidgenössische Datenschutzbeauftragte teil, doch im Normalfall greift er nicht in die Projektausschüsse ein. Der Projektausschuss versammelt sich zwei- bis viermal pro Jahr und betreut jedes Informatikprojekt während seiner gesamten Lebensdauer. Zum Projektausschuss gehören ein Vertreter der Benutzer und bei Grossprojekten im Normalfall ein Kantonsvertreter.

An dieser Stelle ist darauf hinzuweisen, dass Informatikprojekte nie abgeschlossen sind: Bei den meisten Projekten wird, sobald eine Version läuft, gleich mit der Ausarbeitung der nächsten Version begonnen (RIPOL-4, ZAR-3, AUPER-2 usw.). Der

8 Vgl. Handbuch HERMES, BFI, Ausgabe 1995, S. 6–3 bis 6–13

Projektausschuss betreut daher ein Projekt während seiner ganzen Lebensdauer. Jede Änderung eines Informatiksystems ist vom Projektausschuss zu genehmigen, und bei jeder grösseren Änderung sind erneut die fünf Phasen (Initialisierung, Voranalyse, Konzept, Realisierung, Einführung) zu durchlaufen. Bei jeder grösseren Änderung beginnt somit der Prozess wieder von vorn.

c. Die Projektleitung

Darunter werden die Aufgaben der operativen Projektleitung zusammengefasst, also die Planung, Koordinierung, Überwachung und Steuerung der Projektarbeit innerhalb des gesetzten Kosten- und Terminrahmens. Der Projektleiter übernimmt die Verantwortung für die operative Leitung des Projekts.

Für die Freigabe der Projektphasen wird ein Formular verwendet. Im EJPD muss dieses Formular insbesondere von der Direktion des betreffenden Amtes, dem Chef des Rechenzentrums, dem Datenschutzberater des Departements und dem Chef Informatik des Departements unterschrieben werden. Der Datenschutzberater des EJPD erhält für jede Phase ein Formular zur Unterschrift. Dabei kann er Vorbehalte anbringen, die dann in der nächsten Phase zu behandeln sind.

Der Erwerb von Informatikmaterial ist nicht möglich, wenn er nicht in einer der Projektphasen genehmigt wurde. Ohne Projekt nach der Methode HERMES darf weder Software noch Hardware erworben werden.

232.4 Von wem geht der Anstoss für die Einrichtung von Online-Verbindungen oder für die Entwicklung eines Informationssystems im Bereich des Polizeiwesens aus?

Die Kommission hat festgestellt, dass der Anstoss für die Einrichtung einer Online-Verbindung hauptsächlich von der Schweizerischen Polizeitechnischen Kommission oder von anderen polizeilichen Fachstellen, namentlich innerhalb der INTERPOL, ausgeht. Das *Bundesamt für Polizeiwesen* und das *Rechenzentrum des EJPD* sind in diesen Arbeitsgruppen vertreten, und ihre Mitarbeiter bringen aus den Sitzungen neue Ideen zur Effizienzsteigerung der Informatikinstrumente mit. Diese Vorschläge werden von der Projektleitung geprüft und dem Projektausschuss vorgelegt.

232.5 Einsatz des Verfahrens HERMES im EJPD für Online-Verbindungen

Genehmigt der oben erwähnte Projektausschuss den Vorschlag, eine Online-Verbindung einzurichten, so werden die Rechtsgrundlagen geprüft und, falls erforderlich, eine Gesetzesänderung durchgeführt. Gleichzeitig entsteht im Hinblick auf eine allfällige Verwirklichung dieser Online-Verbindung ein neues Projekt nach HERMES (d. h. die fünf Phasen von HERMES sind zu durchlaufen).

Die Abklärungen beim Datenschutzberater des EJPD ergeben somit, dass bei der Einrichtung einer Online-Verbindung die fünf Phasen nach HERMES erneut durchlaufen werden, wenn die Einrichtung der Verbindung eine Änderung der Anwendung (neue Funktionalitäten) bedeutet. Da der Grundsatzentscheid zur Verwirklichung und Einrichtung von Online-Verbindungen eine wesentliche Änderung des Projekts darstellt, sind die verschiedenen Projektphasen zwingend erneut zu durch-

laufen. Der Entscheid zur Einrichtung der Online-Verbindung wird unabhängig von diesen Phasen vom Projektausschuss mit Genehmigung des Generalsekretärs des Departements getroffen.

Dasselbe gilt, wenn der Projektausschuss den Entscheid für den Anschluss eines bestimmten Kantons trifft. In diesem Fall kommt es allerdings häufig vor, dass die für den Anschluss der Kantone erforderlichen Rechtsgrundlagen bereits bestehen und ein Pilotprojekt mit 4 oder 5 Kantonen durchgeführt wurde. Wird danach beschlossen, alle Kantone anzuschliessen, so muss nicht der ganze Phasenzyklus neu aktiviert werden. Der Anschluss eines neuen Kantons erfordert weder eine neue Rechtsgrundlage noch neue Software, da bereits beim Anschluss des ersten Kantons alles Notwendige verwirklicht wurde. Auf Betriebsebene hingegen hat sich das EJPD vor dem Anschluss neuer Kantone davon zu überzeugen, dass die erforderlichen Leitungen und peripheren Geräte vorhanden sind.

232.6 Die Grenzen des Verfahrens HERMES

Wie bereits dargelegt ist das *Vorgehen* bei der Einrichtung von Informatiksystemen und den entsprechenden Online-Verbindungen nicht durch Weisungen geregelt, sondern durch ein besonderes Projektführungssystem, das Verfahren HERMES. Dieses Verfahren wird vom EJPD durchaus sinnvoll eingesetzt, doch bleibt HERMES in erster Linie eine «Methode» zur Führung von Informatikprojekten, die verschiedene obligatorische Phasen vorsieht.

Mit anderen Worten: HERMES sieht zwar die Phasen vor, die bei Entscheiden zur Einrichtung von neuen Online-Verbindungen zu durchlaufen sind, enthält aber keine spezifischen Vorschriften oder Bestimmungen zu diesen Verbindungen, namentlich was die Prüfung der Grundsätze der Zweckmässigkeit, Verhältnismässigkeit oder Zweckbindung anbelangt. Es werden bloss einige Checkfragen angeführt und allgemeine Hinweise gegeben, beispielsweise für die Phase der Voranalyse: «Wurde die Sicherheit und der Datenschutz situationsgerecht analysiert und bewertet?»[9]; für die Phase des Konzepts: «Sind insbesondere die Sicherheits- und Datenschutzanforderungen erfüllt?»[10] oder in Bezug auf die Systemtypen, die HERMES unterscheidet: «...Informatikinfrastruktur. (...) Beispiele sind die Beschaffung und Installation von Kommunikationsnetzen.»[11]

Das Verfahren HERMES im EJPD ist also ein grundlegendes Instrument für die Einrichtung von Online-Verbindungen im Bereich des Polizeiwesens. HERMES ist allerdings auch hier nur die «Methode» für die Führung und Abwicklung von Informatikprojekten und sieht keine spezifischen Bestimmungen für Online-Verbindungen vor.

Die Erläuterungen des Datenschutzberaters des EJPD und des Eidgenössischen Datenschutzbeauftragten machten ebenfalls deutlich, dass das Fehlen spezifischer Vorschriften für Online-Verbindungen im Verfahren HERMES zu Problemen führen kann, was die Ermittlung der Bedürfnisse der Benutzer und die Effizienz der Kontrolle und Überwachung der Entwicklungen im Informatikbereich durch die zuständigen Stellen betrifft.

9 Vgl. Handbuch HERMES, BFI, Ausgabe 1995, S. 2–7
10 Vgl. Handbuch HERMES, BFI, Ausgabe 1995, S. 3–9
11 Vgl. Handbuch HERMES, BFI, Ausgabe 1995, S. 11–4

233 Fragen des Datenschutzes und Kontrolle der Einrichtung von Online-Verbindungen

Welche Rechtsgrundlagen gelten im Bereich des Datenschutzes?

Welche Anforderungen sind im Bereich des Datenschutzes zu erfüllen?

Werden die Grundsätze der Verhältnismässigkeit, der Zweckbindung, der Zweckmässigkeit und der Notwendigkeit bei der Ausarbeitung von Informatikkonzepten berücksichtigt?

Sind bei der Einrichtung von Online-Verbindungen die Überwachung und die Kontrolle geregelt?

233.1 Rechtsgrundlagen und Anforderungen im Bereich des Datenschutzes betreffend die Einrichtung von Online-Verbindungen

Die Rechtsgrundlagen im Bereich des Datenschutzes sind das Bundesgesetz vom 19. Juni 1992 über den Datenschutz (DSG; SR *235.1*) und die Verordnung des Bundesrates vom 14. Juni 1993 zum Bundesgesetz über den Datenschutz (VDSG; SR *235.11*).

Diese Rechtsgrundlagen regeln nicht nur Fragen betreffend die Einhaltung der Grundsätze der Verhältnismässigkeit und der Zweckbindung beispielsweise (Art. 4 DSG), sondern auch Sicherheitsmassnahmen (Art. 7 DSG) und technische und organisatorische Massnahmen (Art. 20 ff. VDSG), die bei der Bearbeitung von Personendaten zu treffen sind.

Es ist zu betonen, dass die Anforderungen im Bereich des Datenschutzes bei der Einrichtung von Online-Verbindungen im Bericht des Eidgenössischen Finanzdepartements[12] genau und ausführlich beschrieben und in Kapitel 4.2 «Büroautomation und Datenbankzugriffe; Anforderungen des EDSB» eingehend behandelt wurden. Hier die wichtigsten Punkte:

A Datenschutzgrundsätze

Gesetzmässigkeit

Organe des Bundes dürfen Personendaten nur bearbeiten, wenn dafür eine gesetzliche Grundlage besteht (Art. 4 Abs. 1, Art. 17 Abs. 1 DSG).

Bundesorgane dürfen Personendaten nur bekanntgeben, wenn dafür Rechtsgrundlagen bestehen (Art. 17 und 19 DSG). Sie dürfen Personendaten durch ein Abrufverfahren zugänglich machen, wenn dies ausdrücklich vorgesehen ist. Besonders schützenswerte Personendaten sowie Persönlichkeitsprofile dürfen nur durch ein Abruf-

12 Vgl. Bericht EFD (BFI) an den Bundesrat vom 14. April 1997 bzw. vom 13. Juni 1997 und Bundesratbeschluss vom 16. Juni 1997 betr. a) Stand der Umsetzung der Verordnung über den Schutz der Informatiksysteme und -anwendungen in der Bundesverwaltung, b) Sicherheit im Umfeld Büroautomation und Auditmöglichkeiten von Zugriffen auf sensible Datenbanken.

verfahren zugänglich gemacht werden, wenn ein formelles Gesetz es ausdrücklich vorsieht (Art. 19 Abs. 3 DSG).

Verhältnismässigkeit

Die Bearbeitung muss verhältnismässig sein (Art. 4 Abs. 2 DSG).

Zweckbindung

Personendaten dürfen nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist (Art. 4 Abs. 3 DSG).

Eine abfragende Behörde verfolgt häufig verschiedene Zwecke, und es besteht insofern ein faktisches Interesse an der Verwendung der abgefragten Daten auch zu anderen Zwecken. Bestimmte Daten dürfen jedoch von einer Behörde nur zu dem für die konkrete Aufgabenerfüllung erforderlichen bzw. dem in den Rechtsgrundlagen festgehaltenen Zweck abgefragt werden. Daten unbeteiligter Dritter dürfen in der Regel nicht abgefragt und in keinem Fall weiterbearbeitet werden (vgl. z. B. Art. 7 Abs. 3 ZAR-Verordnung, SR *142.215*; AS *1994* 2859).

Richtigkeit

Wer Personendaten bearbeitet, hat sich über deren Richtigkeit zu vergewissern (Art. 5 Abs. 1 DSG). Die Veränderung der Daten muss Kontrollmechanismen (insb. org. Massnahmen) umfassen, die gewährleisten, dass die Daten richtig sind (in Bezug zum vorgesehenen Zweck).

Datensicherheit

Personendaten müssen durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden (Art. 7 Abs. 1 DSG).

B Umsetzung/Massnahmen

Nachvollziehbarkeit

Die Nachvollziehbarkeit des Erstellers und der Bearbeitung von Daten (insbesondere die Beschaffung, Umarbeitung, Bekanntgabe und Vernichtung) muss gewährleistet sein (vgl. Kriterien für die Protokollierung gemäss Art. 10 VDSG).

Berechtigung zur Veränderung

Durch Speicherkontrolle ist zu gewährleisten, dass keine unerlaubte Eingabe in den Speicher und keine unbefugte Einsichtnahme, Veränderung oder Löschung stattfinden kann.

Zugriff nur für Berechtigte

Durch Zugriffskontrollen ist sicherzustellen, dass via Büroautomation-Systeme Personen nur auf diejenigen Daten Zugriff haben, die sie für ihre Aufgabenerfüllung benötigen.

Kontrolle über Verknüpfbarkeit von Daten

Es ist abzuklären, ob in Büroautomation-Systemen Daten aus verschiedenen Quellen verknüpft werden können, so dass z.B. Persönlichkeitsprofile entstehen können (fehlende Rechtsgrundlage, unverhältnismässige Datenbearbeitung, ungenügende Sicherheit und ungenügende Kontrolle der Richtigkeit). Ist die Zusammenführung der Daten nicht für die Aufgabenerfüllung erforderlich (gesetzliche Grundlage), ist eine technische Trennung vorzunehmen, die ein automatisiertes Verknüpfen unterbindet.

C Stand der Sicherheit

Es sollte unterschieden werden zwischen der Korrektheit (Gesetzmässigkeit, Verhältnismässigkeit, Zweckbindung und Richtigkeit) von Daten und der Datensicherheit (Schutz von Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität) von Daten.

Beispiele von technischen Massnahmen im Sinne des Datenschutzes: Protokollierung (Kontrolle Zweckbindung); Beispiele von technischen Massnahmen im Sinne der Datensicherheit: Netzwerkchiffrierung, Speicherchiffrierung.

233.2 Prüfung der Grundsätze der Verhältnismässigkeit, Zweckbindung und Zweckmässigkeit (Notwendigkeit) auf der Ebene der Ausarbeitung der Informatikkonzepte

Der Datenschutzberater des EJPD hat bei seiner Anhörung darauf hingewiesen, dass im EJPD die Bedürfnisse der Benutzer im Rahmen des Verfahrens HERMES ermittelt werden, da sich die Notwendigkeit einer Online-Verbindung aus solchen geäusserten Bedürfnissen ergibt.

Wie bereits erwähnt, enthalten allerdings weder die Weisungen des BFI noch das Verfahren HERMES, wenn man von einigen allgemeinen Hinweisen absieht, spezifische Bestimmungen für die Einrichtung von Online-Verbindungen, insbesondere was die Prüfung der Grundsätze der Zweckmässigkeit, Verhältnismässigkeit oder Zweckbindung betrifft.

Wenn im Rahmen eines Informatikprojekts des EJPD diese Grundsätze innerhalb der Phasen des Verfahrens HERMES geprüft werden, kann es vorkommen, dass Aspekte, die die Entwicklung neuer Online-Verbindungen betreffen, noch nicht klar umrissen sind. Manchmal ist daher sogar unklar, welche Zugriffsmöglichkeiten vorgesehen sind, weil das Projekt noch nicht genügend weit fortgeschritten ist. Dadurch wird einerseits die Beurteilung der Notwendigkeit, Verhältnismässigkeit und Zweckbindung einer zukünftigen Online-Verbindung, andererseits die Ausübung der Kontrollaufgaben, für die insbesondere der Eidgenössische Datenschutzbeauftragte zuständig ist, erschwert.

233.3 Überwachung und Kontrolle bei der Einrichtung von Online-Verbindungen

Nach Artikel 20 VDSG melden die Bundesorgane dem Eidgenössischen Datenschutzbeauftragten unverzüglich alle Projekte zur automatisierten Bearbeitung von Personendaten, damit die Erfordernisse des Datenschutzes sogleich berücksichtigt werden. Die Meldung an den Datenschutzbeauftragten erfolgt über das Bundesamt für Informatik, wenn das Projekt auch bei diesem angemeldet werden muss. Der Datenschutzbeauftragte und das BFI arbeiten im Rahmen ihrer Aktivitäten betreffend die technischen Massnahmen zusammen.

Dem Bundesamt für Informatik kommt bei der Einrichtung von Online-Verbindungen die Aufgabe zu, die *Kommunikationsinfrastrukturen* im Bereich der gesamten Bundesverwaltung zu planen und zu betreiben. Die Online-Verbindungen im Polizeibereich erfolgen auf der physischen Ebene, wo vorhanden, über die Datenkommunikationsinfrastruktur des Bundes. Auf der logischen Ebene sind die Netze jedoch aus Sicherheitsgründen getrennt. Im Rahmen seiner Kompetenzen nimmt das Bundesamt Stellung zu den Informatikprojekten, die entwickelt und ausgearbeitet werden, und erlässt zahlreiche Weisungen.

Nach Artikel 27 DSG obliegt es dem Eidgenössischen Datenschutzbeauftragten, die Einhaltung des Datenschutzgesetzes durch die Bundesorgane zu überwachen. Bei der Einrichtung neuer Online-Verbindungen hat er somit dafür zu sorgen, dass die Grundsätze der Verhältnismässigkeit, Zweckbindung und Notwendigkeit eingehalten werden. Aus den Untersuchungen geht jedoch hervor, dass sich dem Datenschutzbeauftragten bei der Ausübung dieser Kontrolle zwei Hauptschwierigkeiten stellen:

a. Einerseits weist der Datenschutzbeauftragte darauf hin, dass ihm für die angemessene Erfüllung seiner gesetzlichen Kontrollaufgaben die Mittel und namentlich das Personal fehlen. Auf diese Problematik wurde bereits im Rahmen der Inspektion zur Einführung der Informatik in der Bundesverwaltung eingegangen (Untersuchung der Rolle und der Mittel des Eidgenössischen Datenschutzbeauftragten im Bereich der Überwachung; Feststellung des Fehlens konkreter Massnahmen; Feststellung, dass der Datenschutzbeauftragte eine systematische und ausführliche Überprüfung aller Projekte zur automatisierten Bearbeitung von Personendaten in der Bundesverwaltung noch immer nicht durchführen kann, weil die erforderlichen Mittel fehlen).

b. Andererseits sieht sich der Datenschutzbeauftragte im Rahmen seiner Kontrollaufgaben einem anderen Problem gegenüber: Obwohl er während der verschiedenen Phasen eines Projekts nach HERMES konsultiert wird, und selbst wenn die Bedürfnisse der Benutzer grob ermittelt wurden, kann er sich zu Aspekten, die die Entwicklung neuer Online-Verbindungen betreffen, kaum äussern, da diese im Stadium des ihm vorgelegten Konzepts oft noch nicht klar umrissen sind. Die genaue Festlegung erfolgt im Prinzip erst, wenn die Rechtsgrundlagen für den entsprechenden Zugriff geschaffen werden müssen.

In diesem Stadium stellt sich den befragten Behörden ein weiteres Problem, jenes der «prophylaktischen» Gesetzgebung: Es werden Gesetzesänderungen vorgeschlagen für Online-Verbindungen, die noch nicht genau umrissen und auch nicht auf ihre Notwendigkeit, Verhältnismässigkeit usw. geprüft wurden. Laut dem Datenschutzberater des EJPD trifft es in der Tat zu, dass auf Grund der Schwierigkeiten

und der Dauer des Gesetzgebungsprozesses Gesetze «prophylaktisch» erlassen werden. So soll sichergestellt werden, dass für eventuelle zukünftige Online-Verbindungen die gesetzlichen Grundlagen bestehen.

Der Eidgenössische Datenschutzbeauftragte sieht sich im Rahmen seiner Kontrollaufgaben bei der Einrichtung von Online-Verbindungen somit verschiedenen Schwierigkeiten gegenüber:

- Die fehlenden Mittel, insbesondere fehlendes Personal, verunmöglichen ihm die angemessenen Kontrollen, mit deren Ausführung er gesetzlich beauftragt ist.
- Der Entwicklungsstand eines Projekts im Rahmen von HERMES reicht für die Beurteilung der Notwendigkeit oder Verhältnismässigkeit eines Zugriffs nicht immer aus.
- Diese Prüfung kann daher während der Ausarbeitung der gesetzlichen Grundlagen erfolgen. Einige Ämter sind sich jedoch über ihre tatsächlichen Bedürfnisse im Unklaren und haben die Tendenz, «vorbeugend» Zugriffe vorzusehen, deren Notwendigkeit nicht überprüft wurde.
- Andere Ämter wiederum halten bestimmte Zugriffe für nicht notwendig und sehen sie daher in ihren Gesetzesentwürfen nicht vor. Ist das entsprechende Gesetz einmal erlassen und scheint ein Zugriff dann doch erforderlich, wenden sich die Ämter an den Datenschutzbeauftragten, damit er diese Zugriffe, die keine gesetzliche Grundlage haben, bewilligt.

233.4 Die Kontrolle der Zugriffe, die den Kantonen gewährt werden

Werden den Kantonen Online-Zugriffe auf Informatiksysteme der Polizei gewährt, führt dies zu gewissen Problemen, namentlich was die Entscheidungsbefugnis zur Zuteilung solcher Zugriffe und die Kontrolle der Einhaltung der Anforderungen des Datenschutzes oder der Sicherheitsmassnahmen betrifft.

Einerseits sind die Entscheidungsverfahren für die Beantragung eines Zugriffs von Kanton zu Kanton verschieden. Der Entscheidungsprozess reicht von einem bis in die kleinsten Einzelheiten geregelten Verfahren für die Einrichtung von Online-Zugriffen, wie es beispielsweise im Kanton Luzern angewendet wird, bis zu weniger transparenten Verfahren in anderen Kantonen, wo die Bundesbehörden dafür zu sorgen haben, dass die Behördenhierarchie und die Entscheidungsbefugnisse im Kanton tatsächlich eingehalten werden.

Ein anderes Problem stellt sich dadurch, dass die kantonalen Datenschutzgesetze auf Bundesebene nicht überprüft werden können. Das DSG gibt den Stellen der Bundesverwaltung auch keine Kompetenz, Untersuchungen durchzuführen. Der Eidgenössische Datenschutzbeauftragte hat gegenüber den Kantonen eine reine Beratungsfunktion. Da die Kantone über ein eigenes Kontrollorgan verfügen müssen, kann der Eidgenössische Datenschutzbeauftragte in den Kantonen keine Überwachung vornehmen, was insbesondere bei Online-Zugriffen zu Problemen führen kann. Der Datenschutzbeauftragte kann wohl zum Zeitpunkt der Zugriffsgewährung eingreifen, danach hat er jedoch keine Möglichkeit mehr, im Kanton zu überprüfen, ob die Zugriffe eingehalten und nicht auf andere Stellen ausgedehnt werden. Diese

Kontrolle liegt in der Zuständigkeit der Kantonsbehörden. Das Niveau dieser Kontrollen kann jedoch von Kanton zu Kanton stark variieren.

Hinzu kommt, dass die Prüfung der Notwendigkeit oder der Verhältnismässigkeit der den Kantonen gewährten Online-Zugriffe relativ ist. Ein von den Kantonsbehörden geäussertes allgemeines Bedürfnis wird vom EJPD berücksichtigt, sobald sich die kantonale Hierarchie dafür ausgesprochen hat. Danach werden Sicherheitsmassnahmen ergriffen, um insbesondere im Rechenzentrum des EJPD eine gewisse Globalkontrolle der Zugriffe der Kantone zu gewährleisten (Passwörter, Protokollierung der Benutzer usw.). Beantragt hingegen eine kantonale Polizeistelle für fünf Personen einen Anschluss, weil dieser notwendig sei, überprüft das EJPD nicht, ob diese Notwendigkeit tatsächlich besteht.

233.5 Der Sonderfall Rechenzentrum EJPD

Die Untersuchungen der Sektion Behörden im Rahmen dieser Online-Inspektion einerseits, der Delegation der GPK im Rahmen ihrer Überprüfung der Systeme ISIS und DOSIS andererseits, machten eine Problematik deutlich, die sich aus dem Fehlen einer Sicherheitsprüfung für Mitarbeiter des Rechenzentrums des EJPD ergibt.

Im Gegensatz zu den Mitarbeitern der Bundespolizei unterstehen die Informatiker im Rechenzentrum von Zollikofen keiner Sicherheitskontrolle, obwohl sie auf besonders schützenswerte Daten im Bereich des Polizeiwesens und des Staatsschutzes Zugriff haben.

Diese Situation kann zu Problemen im Bereich der Sicherheitsmassnahmen führen. Der im Bericht der Verwaltungskontrollstelle des Bundes «Online-Datenaustausch zwischen Bund und Kantonen» behandelte Fall, dass ehemalige Mitarbeiter des Rechnungszentrums des EJPD ein kantonales Pendant (ABI) zu den Systemen DOSIS und ISOK entwickelt haben, zeigt im Übrigen, wie aktuell diese Problematik ist.

234 Untersuchung der Kosten

Ist bei der Einrichtung von Online-Verbindungen im Rahmen der Ausarbeitung der Informatikkonzepte auch die Untersuchung der Kosten vorgesehen?

Laut den Erklärungen des Datenschutzberaters des EJPD werden bei der Einrichtung von Online-Verbindungen zwischen dem Bund und den Kantonen die Kosten vereinfacht gesehen folgendermassen aufgeteilt:

Für Einrichtung und Betrieb des Netzes bis zum Anschlusspunkt im Kanton ist der Bund zuständig. Den Kantonen obliegt die Betreibung des internen Netzes (LAN) und der Erwerb der peripheren Geräte (PC, Drucker usw.).

Neben dem Grundsatz der Kostenaufteilung zwischen Bund und Kantonen stellen sich bei der Einrichtung von Online-Verbindungen zahlreiche weitere Fragen, die die Kosten betreffen. Damit diese Fragen konkreter angegangen werden konnten, wurden sie in Block 2 im Rahmen der Überprüfung konkreter Fälle behandelt. In Anbetracht der zahlreichen Zugriffe der Kantone auf die Informatiksysteme der Polizeibehörden des Bundes wurde dabei namentlich der Aspekt der Kostenaufteilung zwischen Bund und Kantonen behandelt, und zwar für jedes der von der Sektion

Behörden ausgewählten Systeme (RIPOL, DOSIS, ISOK, ZAN, ZAR und ISIS). Behandelt wurden ebenfalls Fragen betreffend Budgetierung, Investitionskosten, Betriebskosten usw.

Die Kostenproblematik wird eingehend im Expertenbericht behandelt.

24 Untersuchung der zentralen Frage

Welche Regeln gelten bei der Planung und Einrichtung von Online-Verbindungen im Bereich des Polizeiwesens?

Mit den Antworten und Präzisierungen zu den Zusatzfragen kann die Hauptfrage zusammengefasst wie folgt beantwortet werden:

241 Technische Bestimmungen und Sicherheitsbestimmungen

Auf der Grundlage von Rahmenvorschriften wie der *Verordnung* vom 11. Dezember 1989 *über das Bundesamt für Informatik und über die Koordination der Informatik in der Bundesverwaltung* und der *Verordnung* vom 10. Juni 1991 *über den Schutz der Informatiksysteme und -anwendungen in der Bundesverwaltung* hat das Bundesamt für Informatik verschiedene Technische Weisungen (TW), Weisungen zur Informatiksicherheit (WS) und Strategien herausgegeben.

Die im Rahmen dieser Untersuchung ausgewählten Anwendungen wie RIPOL, DOSIS, ISOK, ZAN, ZAR und ISIS gehören zu Organisationseinheiten, auf welche die Sicherheitsweisungen des BFI anwendbar sind. Daher gelten für diese Systeme die Sicherheitsgrundsätze und -bestimmungen der Bundesverwaltung (siehe Aufzählung in Kapitel 231.2).

Die Einhaltung dieser Vorschriften setzt einerseits voraus, dass diese Informatiksysteme als Schutzobjekte zu erheben und einzustufen und in jedem Fall auch einer Risikobeurteilung zu unterziehen sind. Andererseits sind für diese Anwendungen Sicherheitsmassnahmen und organisatorische Massnahmen (Anwendungsverantwortliche, Sicherheitsbeauftragte, Kontrollorgane usw.) zu ergreifen, und neu gewährte Zugriffe auf diese Anwendungen haben den Anforderungen der *Network Security Policy (NSP)* und *der Sicherheitsweisung WS S03* zu genügen.

242 Verfahrensvorschriften (Methode)

Das Vorgehen bei der Einrichtung von Informatiksystemen und den entsprechenden Online-Verbindungen erfolgt nach einem besonderen Projektführungssystem, dem Verfahren HERMES. Dieses Verfahren kommt im EJPD als Führungsinstrument und Standard für die Abwicklung von Informatikprojekten zur Anwendung. HERMES unterscheidet verschiedene Phasen und legt die Rollen und Kompetenzen der verschiedenen Projektgruppen oder anderer Organe (*Genehmigungsinstanz, Projektauftraggeber, Projektausschuss, Projektleitung* usw.) fest.

Die Befragungen des Datenschutzberaters des EJPD ergaben, dass für die Einrichtung einer Online-Verbindung jedes Mal die fünf Phasen nach HERMES neu zu durchlaufen sind. Dies trifft jedoch nicht zu, wenn ein Kanton oder mehrere Kanto-

ne bereits an einem System angeschlossen sind, beispielsweise im Rahmen eines Pilotprojekts, und danach der Anschluss anderer Kantone beschlossen wird.

Das im EJPD eingesetzte Verfahren HERMES ist ein grundlegendes Instrument für die Einrichtung von Online-Verbindungen im Bereich des Polizeiwesens. Das Verfahren regelt die Führung und Abwicklung von Informatikprojekten, enthält aber für Online-Verbindungen keine spezifischen Bestimmungen, insbesondere was die Prüfung der Grundsätze der Zweckmässigkeit, Verhältnismässigkeit oder Zweckbindung betrifft.

243 Datenschutzvorschriften

Das Bundesgesetz vom 19. Juni 1992 über den Datenschutz und die diesbezügliche Verordnung des Bundesrates vom 14. Juni 1993 regeln nicht nur Fragen betreffend die Einhaltung der Grundsätze der Verhältnismässigkeit und der Zweckbindung (Art. 4 DSG), sondern auch Sicherheitsmassnahmen (Art. 7 DSG) und technische und organisatorische Massnahmen (Art. 20 ff. VDSG), die bei der Bearbeitung von Personendaten zu treffen sind, sowie die Modalitäten für die Meldung der Informatikprojekte.

Nach Artikel 27 DSG obliegt es dem Eidgenössischen Datenschutzbeauftragten, die Einhaltung des Datenschutzgesetzes durch die Bundesorgane zu überwachen. Bei der Einrichtung neuer Online-Verbindungen hat er somit dafür zu sorgen, dass die Grundsätze der Verhältnismässigkeit, Zweckbindung und Notwendigkeit eingehalten werden. Die Geschäftsprüfungskommission teilt allerdings die Einschätzung des Datenschutzbeauftragten, dass ihm für die Erfüllung seiner gesetzlichen Kontrollaufgaben die Mittel und namentlich das Personal fehlen. Auf diese Problematik wurde bereits im Rahmen der Inspektion zur Einführung der Informatik in der Bundesverwaltung eingegangen. Die Kommission stellt fest, dass diese Situation immer noch aktuell ist.

Eine wirksame Kontrolle wird ferner dadurch in Frage gestellt, dass sich der Datenschutzbeauftragte zu Aspekten, die die Entwicklung neuer Online-Verbindungen betreffen, kaum äussern kann. Die Online-Verbindungen sind im Stadium des ihm vorgelegten Konzepts oft noch nicht klar umrissen. Dieses Kontrolldefizit wirkt sich auf den Gesetzgebungsprozess aus, indem Gesetzesänderungen vorgeschlagen werden für Online-Verbindungen, die noch nicht genau umrissen und auch nicht auf ihre Notwendigkeit, Verhältnismässigkeit usw. überprüft wurden.

244 Kantonale Vorschriften und Praktiken

Bei der Einrichtung von Online-Verbindungen sind ebenfalls die je nach Kanton sehr unterschiedlichen kantonalen *Bestimmungen* und *Entscheidungsverfahren* zu berücksichtigen. Der Eidgenössische Datenschutzbeauftragte hat gegenüber den Kantonen eine reine Beratungsfunktion. Er kann wohl zum Zeitpunkt der Zugriffsgewährung eingreifen, danach hat er jedoch keine Möglichkeit mehr, im Kanton zu überprüfen, ob die Zugriffe eingehalten und nicht auf andere Stellen ausgedehnt werden. Diese Kontrolle liegt in der Zuständigkeit der Kantonsbehörden. Das Niveau dieser Kontrolle kann jedoch von Kanton zu Kanton stark variieren.

Hinzu kommt, dass die Prüfung der Notwendigkeit oder der Verhältnismässigkeit der den Kantonen gewährten Online-Zugriffe relativ ist. Äussert eine Kantonalbehörde das Bedürfnis nach einem Anschluss, werden Sicherheitsmassnahmen ergriffen, die insbesondere im Rechenzentrum des EJPD eine gewisse Globalkontrolle der Zugriffe der Kantone ermöglichen (Passwörter, Protokollierung der Benutzer usw.). Beantragt hingegen eine kantonale Polizeistelle für fünf Personen einen Anschluss, weil dieser notwendig sei, überprüft das EJPD nicht, ob diese Notwendigkeit tatsächlich besteht.

25 Schlussfolgerungen der Kommission

Untersuchung auf Konzeptstufe

Die Kommission stellt auf Grund ihrer Abklärungen, die sich schwergewichtig auf vorbereitende Arbeiten der Parlamentarischen Verwaltungskontrollstelle stützen, *positive Aspekte*, aber auch *gewisse Lücken* bei der Einrichtung von Online-Verbindungen fest:

251 Die Rechtsgrundlagen für die Einrichtung von Informatiksystemen (Bundesgesetz und Verordnung über den Datenschutz, Verordnung über das BFI, Technische Weisungen und Sicherheitsweisungen des BFI) und das Verfahren HERMES bilden als Instrument und Standard für die Führung und Abwicklung von Informatikprojekten in der Bundesverwaltung einen präzisen und umfassenden rechtlichen Rahmen.

252 Bei der Planung und Einrichtung von Online-Verbindungen gelten verschiedene Bestimmungen, die sich von den obenerwähnten Vorschriften ableiten, sei es auf der Ebene der verschiedenen Phasen nach HERMES, der Sicherheitsmassnahmen und organisatorischen Massnahmen, der Sicherheitsweisungen oder der Datenschutzgrundsätze. Hierzu sind allerdings zwei Bemerkungen erforderlich:

– Einerseits enthalten die verschiedenen Weisungen in erster Linie zahlreiche Bestimmungen zu Sicherheitsmassnahmen, Authentifikations- und Chiffriermassnahmen, Schutzstufen, organisatorischen Massnahmen, Risikobeurteilungen oder Schutz der Systeme und angeschlossenen Applikationen (Network Security Policy/NSP). Sie enthalten hingegen keine Bestimmungen, die spezifisch für die Einrichtung von Online-Verbindungen gelten, insbesondere was die im Voraus durchzuführende Prüfung der Grundsätze der Notwendigkeit, Zweckbindung und Verhältnismässigkeit einer neuen Verbindung betrifft. Anhang 2 der Weisung über die Informatiksicherheit WS S02 sieht zwar einige genauere Bestimmungen vor; die Weisung bezweckt allerdings nicht eigentlich die Prüfung der genannten Grundsätze bei Verbindungen, die für Bundes- oder Kantonsbehörden geplant sind, sondern regelt vielmehr diejenigen Aspekte, die den individuellen Zugriff eines Benutzers auf ein System betreffen (Benutzeridentifikation, Passwörter, Unterbrechung inaktiver Verbindungen, Sperrung nicht beanspruchter Zugriffsrechte, Kontrolle der Subjekte, Objekte, Häufigkeit und Dauer von Zugriffsrechten, Vergabe der Zugriffsrechte von Fall zu Fall oder Veränderung von Privilegien).

– Andererseits sieht das Verfahren HERMES als Methode zur Führung und Abwicklung von Informatikprojekten zwar die Phasen vor, die bei Entscheiden für die Einrichtung neuer Online-Verbindungen zu durchlaufen sind. Doch abgesehen von einigen allgemeinen Hinweisen (z. B. *«Sind insbesondere die Sicherheits- und Datenschutzanforderungen erfüllt?»*) enthält das Handbuch keine Vorschriften oder Bestimmungen, die spezifisch für Online-Verbindungen gelten, insbesondere was die Prüfung der Grundsätze der Zweckmässigkeit, Verhältnismässigkeit oder Zweckbindung betrifft. Das im EJPD eingesetzte Verfahren HERMES ist demnach ein grundlegendes Instrument für die Einrichtung von Online-Verbindungen im Bereich des Polizeiwesens; es ist allerdings nur die «Methode» für die Führung und Abwicklung von Informatikprojekten.

253 Die Prüfung dieser Grundsätze ist in den Datenschutzvorschriften vorgesehen. Diese Vorschriften verankern nicht nur die Grundsätze der Zweckmässigkeit, Verhältnismässigkeit und Zweckbindung, sondern regeln auch die Modalitäten für die Meldung von Projekten zur automatisierten Bearbeitung von Personendaten an den EDSB über das BFI sowie die entsprechenden Kontrollkompetenzen.

Die Prüfung und Kontrolle der Einhaltung der Datenschutzgrundsätze bei der Einrichtung von Online-Verbindungen wird jedoch, wie bereits erwähnt, erschwert durch fehlende Mittel, die Tatsache, dass oft «vorbeugend» Zugriffe vorgesehen werden, deren Notwendigkeit nicht überprüft wurde, sowie durch die Einreichung von Gesuchen um die Bewilligung von Zugriffen, die keine gesetzlichen Grundlagen haben.

254 Der Online-Anschluss von Kantonen an Informatiksysteme des Bundes führt zu zahlreichen Problemen, insbesondere was die vielen verschiedenen kantonalen Regelungen (z. B. im Bereich des Datenschutzes), die von Kanton zu Kanton sehr unterschiedlichen Entscheidungsverfahren, die Prüfung der Notwendigkeit oder Verhältnismässigkeit oder die Kontrolle der zugewiesenen Zugriffe betrifft.

255 Mit folgendem Schema soll dargestellt werden, welches die wichtigsten Grundsätze oder Phasen bei der Einrichtung von Online-Verbindungen aufführt und jeweils die zufriedenstellenden Aspekte (✓) oder noch bestehenden Lücken (✘) angibt:

a. Rahmenbestimmungen für die Planung von Online-Verbindungen in Form von Technischen Weisungen (TW) Weisungen zur Informatiksicherheit (WS) oder Strategien	✓
b. Standard und Methode für die Führung und Abwicklung von Informatikprojekten in Form eines Instruments für Organisation, Planung, Ausführung und Steuerung	✓
c. Modalitäten für die Meldung von Informatikprojekten	✓

d.	Risikobeurteilung	*zu prüfen auf Grund der Untersuchungsergebnisse des Experten*
e.	Planung der Sicherheitsmassnahmen	
f.	Prüfung vor der Einrichtung der Online-Verbindungen	
g.	Notwendigkeit	✘
h.	Verhältnismässigkeit	
i.	Zweckbindung	
j.	Gewährung von Online-Anschlüssen der Kantone (Entscheidungsverfahren, Bestimmungen, Kontrolle)	✘
	Kontrolle der Online-Verbindungen (nachträgliche Überprüfung, Kontrolle des Umfangs der Zugriffe usw.)	✘
k.	Rechtsgrundlagen der Informatiksysteme	✓
l.	Formellgesetzliche Bestimmungen, die Online-Zugriffe für besonders schützenswerte Daten ausdrücklich vorsehen	✓

Untersuchung der Praxis der Bundesverwaltung

Die im Expertenbericht (vgl. Anhang I) dargelegten Resultate der Untersuchung der Praxis der Bundesverwaltung bei der Einrichtung von Online-Verbindungen im Bereich des Polizeiwesens bestätigen mehrheitlich und ergänzen die Schlussfolgerungen der Kommission.

Der Experte zeigt sich vor allem überzeugt von der Notwendigkeit, den Gesetzgeber für die Fragen der Delegationsnorm zu sensibilisieren und ihm eine exakte Wahl der Begriffe nahezulegen. Die Kommission teilt die Auffassung des Experten, dass es eine übergeordnete und generelle Regelung der Bewilligung von Online-Anschlüssen braucht. Die heutige Praxis der Weiterdelegation an die untersten operativen Verwaltungseinheiten wird dem Stellenwert des Polizeiinformationsbereichs, der mit besonders schützenswerten Personendaten und Persönlichkeitsprofilen arbeitet, nicht gerecht. Eine übergeordnete Verwaltungseinheit ist als unabhängige Bewilligungsinstanz zur Erteilung von Online-Anschlussbewilligungen besser geeignet als eine an der Nutzung und Verbreitung sowie am umfassenden Einsatz eines Informationssystems direkt interessierte Verwaltungseinheit. Eine Prüfung der strengen gesetzlichen Voraussetzungen zur Nutzung von Polizeiinformationssystemen (Notwendigkeit, Verhältnismässigkeit und Zweckmässigkeit) muss durch ein klar definiertes Verfahren garantiert werden.

Der Experte empfiehlt u. a. in seinem Bericht insbesonde folgende Massnahmen:

– klare Vorgaben des EJPD für das Bewilligungsverfahren bei Online-Verbindungen. Damit werde Transparenz geschaffen und sichergestellt, dass die Verfahren einheitlich abgewickelt werden;

– die Schaffung von gesetzlichen Grundlagen auch für Pilotprojekte;

– die Schaffung von Mindeststandards für die Zusammenarbeit zwischen Bund und Kantonen im Rahmen der Gesuchstellung und Errichtung von Online-Anschlüssen an Bundesinformationssysteme;
– Einbindung der politischen Verantwortungsträger (Bund und Kantone) in den Entscheid über die Realisierung und Zulässigkeit von Online-Anschlüssen;
– die Suche eines geeigneteren Standortes des Rechenzentrums EJPD;
– die Einführung einer Sicherheitsüberprüfung für Mitarbeiterinnen und Mitarbeiter des Rechenzentrums EJPD;
– die rasche Zusammenlegung der parallelen Netze KOMBV-KTV und EJPD-WAN.

26 Motion und Empfehlungen der Kommission

Auf Grund dieser Darlegungen unterbreitet die Kommission ihrem Rat eine Motion und dem Bundesrat eine Reihe von Empfehlungen: Sie bittet ihn, auch die übrigen Vorschläge des Experten zu prüfen und, falls sie sich als zweckmässig erweisen, so rasch wie möglich umzusetzen.

Motion der Geschäftsprüfungskommission des Ständerates

Erhöhter Schutz für Personendaten bei Online-Verbindungen

Der Bundesrat unterbreitet eine Revision des Bundesgesetzes vom 19. Juni 1992 über den Datenschutz. Die Revision verfolgt folgende Ziele:

a. Bei der Errichtung von Online-Verbindungen ist auch für Pilotprojekte eine gesetzliche Grundlage vorzusehen.
b. Bei Gesuchen und der Errichtung von Online-Anschlüssen an Informationssysteme des Bundes schafft dieser Mindeststandards für die Zusammenarbeit zwischen Bund und Kantonen. Er legt Zugriff, Nutzung, Schutz und Kontrolle seiner Datenbanken fest.

Empfehlungen der Kommission

261 Prüfung der Zweckmässigkeit, Verhältnismässigkeit und Zweckbindung

Die zunehmende Ausrüstung mit EDV-Mitteln führt dazu, dass immer mehr Online-Verbindungen eingerichtet werden, die zahlreichen Bundes- und Kantonsbehörden den direkten Zugriff auf verschiedene Datenbanken ermöglichen. Der Bundesrat prüft diese Verbindungen auf ihre Zweckmässigkeit (Notwendigkeit), Verhältnismässigkeit und Zweckbindung, bevor sie in formellen gesetzlichen Bestimmungen geregelt werden.

262 Kontrolle durch die zuständige Instanz

Der Bundesrat sorgt für eine angemessenere Kontrolle der Online-Verbindungen durch den Eidgenössischen Datenschutzbeauftragten. Die Kontrolle stellt sicher, dass nur notwendige Verbindungen eingerichtet werden, d. h. wenn ein Bedürfnis nachgewiesen wurde, der Zweck bekannt ist, die Kosten geplant sind und die Risiken eines Missbrauchs oder einer Persönlichkeitsverletzung in einer Risikobeurteilung geprüft wurden.

263 Transparenz über Online-Verbindungen in den bundesrätlichen Botschaften

Der Bundesrat sorgt dafür, dass in seinen Botschaften alle erforderlichen Angaben zu den geplanten Zugriffen enthalten sind, und zwar sowohl hinsichtlich ihrer Notwendigkeit, Zweckbindung, Verhältnismässigkeit und ihres Umfangs sowie in Bezug auf die Behörden, denen sie gewährt werden sollen.

264 Zusammenarbeit und Koordination zwischen Bund und Kantonen

Der Bundesrat sorgt für eine bessere Koordination und Zusammenarbeit zwischen Bund und Kantonen. Auf diese Weise sollen kantonale Entscheidungsverfahren eingeführt werden, die, wenn nicht identisch, so doch vereinheitlicht oder vergleichbar sind und gleichwohl den Föderalismus und die geltenden kantonalen Regelungen berücksichtigen.

265 Grundsätze für alle Online-Bewilligungsverfahren

Der Bundesrat legt Grundsätze für alle Bewilligungsverfahren bei der Einrichtung von Online-Verbindungen im Polizeibereich fest. Insbesondere regelt er die Aufgaben, Kompetenzen und Verantwortungen im Verfahren.

266 Überprüfung der Delegationsnormen

Der Bundesrat überprüft die Delegation von Bewilligungsentscheiden auf die untersten operativen Verwaltungseinheiten in allen betroffenen Bereichen. Er sorgt dafür, dass die Online-Anschlussbewilligung von einer der Wichtigkeit und Tragweite des Bewilligungsentscheides sowie der Sensibilität der Daten adäquaten, unabhängigen Bewilligungsinstanz vorgenommen werden.

267 Kontrolle der Einhaltung der Anschluss- und der Sicherheits-Grundsätze durch die kantonalen/kommunalen Benutzer

Der Bundesrat schafft Kontrollmöglichkeiten (Sicherheitsinspektionen) für die Systembetreiber des Bundes. Diese sollen eine Kontrolle darüber gewährleisten, ob die Anschluss- und Sicherheits-Grundsätze durch Benutzerinnen und Benutzer aus Kantonen und Gemeinden eingehalten wurden.

268 Standards für Gesuche

Der Bundesrat legt Standards fest für die Einreichung von Gesuchen um die Bewilligung von Online-Verbindungen im Polizeibereich.

269 Überprüfung der Nutzungsintensität von Online Verbindungen

Der Bundesrat sorgt für die regelmässige Überprüfungen der Nutzungsintensität von Online-Verbindungen im Polizeibereich.

2610 Sicherheitsprüfung der Mitarbeiterinnen und Mitarbeiter des Rechenzentrums des EJPD

Der Bundesrat führt für Mitarbeiterinnen und Mitarbeiter des Rechenzentrums des EJPD eine Sicherheitsüberprüfung ein. Im Gegensatz zu den Angestellten der Bundespolizei unterstehen diese heute keiner Sicherheitsprüfung, obwohl sie auf besonders schützenswerte Personendaten, auf Polizei- oder Staatsschutzdaten oder auf Informationen über die Sicherheitsmassnahmen oder Informatikentwicklungen der Bundesapplikationen Zugriff haben.

2611 Standort des Rechenzentrums EJPD

Der Bundesrat sorgt für eine angemessenere Unterbringung des Rechenzentrums EJPD.

2612 Entscheid betreffend die Zusammenlegung von KOMBV-KTV und EJPD-WAN

Der Bundesrat entscheidet so rasch wie möglich, ob eine Zusammenlegung von KOMBV-KTV und EJPD-WAN zu erfolgen hat.

27 Weiteres Vorgehen

Die Kommission bittet den Bundesrat, bis Ende Juni 1999 zu diesem Bericht und den Empfehlungen Stellung zu nehmen.

19. November 1998

Im Namen der Geschäftsprüfungskommission des Ständerates:

Peter Bieri, Präsident

Im Namen der Sektion Behörden:

Pierre Aeby, Präsident

Die Sekretärin der Geschäftsprüfungskommissionen:

Mariangela Wallimann-Bornatico

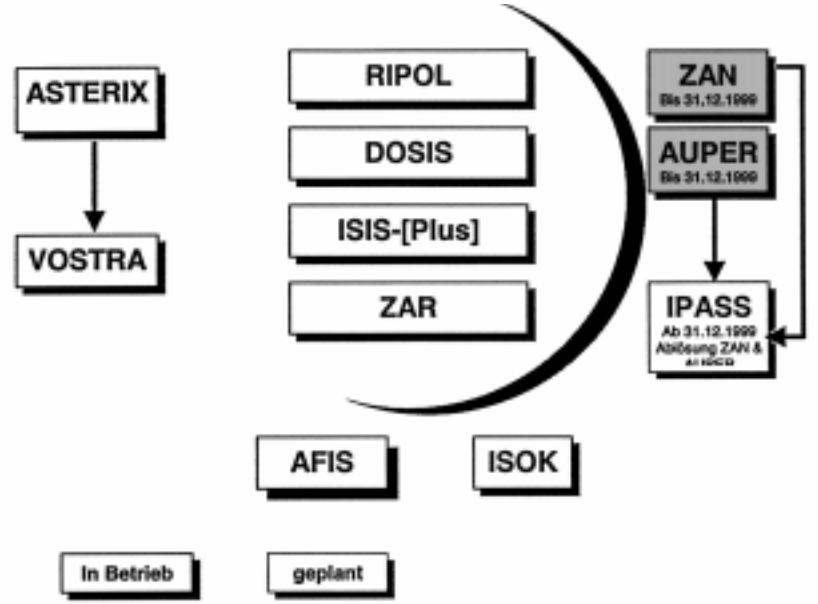
Beilage 1: Expertenbericht und Ergebnisse des Vernehmlassungsverfahrens (nicht veröffentlicht im Bundesblatt)
Beilage 2: Abkürzungsverzeichnis
Beilage 3: Systemübersicht

Abkürzungsverzeichnis

ABI	
AFIS	Automatisches Fingerabdruck-Identifizierungssystem (Automatic Fingerprints Identification System)
ANAG	Bundesgesetz über Aufenthalt und Niederlassung der Ausländer
AUPER	Automatisiertes Personenregistratursystem
BA	Bundesanwaltschaft
BAP	Bundesamt für Polizeiwesen
BFI	Bundesamt für Informatik
BR	Bundesrat
BWIS	Entwurf zum Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit
DOSIS	Datenverarbeitungssystem zur Bekämpfung des illegalen Drogenhandels
DSG	Bundesgesetz über den Datenschutz vom 19. Juni 1992 (SR *235.1*)
EDSB	Eidgenössischer Datenschutzbeauftragter
EFD	Eidgenössisches Finanzdepartement
EJPD	Eidgenössisches Justiz- und Polizeidepartement
EJPD-WAN	Eidgenössisches Justiz- und Polizeidepartement «Wide-Area-Network»
GPDel	Geschäftsprüfungsdelegation
GPK-S	Geschäftsprüfungskommission des Ständerates
GPK-N	Geschäftsprüfungskommission des Nationalrates
HERMES	(HERMES-Verfahren) Führung und Abwicklung von Informatikprojekten / Standard des Bundesamtes für Informatik
IKB	der Informatikkonferenz Bund
ISIS	Provisorisches informatisiertes Staatsschutz-Informations-System
ISIS-Plus	Entwurf eines provisorischen informatisierten Staatsschutz-Informations-Systemes mit «Online-Verbindungen» der kantonalen Behörden
ISOK	Informations-System zur Bekämpfung der organisierten Kriminalität
KOMBV-KTV	Kommunikation der Bundesverwaltung – Kantonalverbund
Online	«Online»-Verbindungen; Abrufverfahren; direkter Zugriff auf Informatiksysteme
PVK	Parlamentarische Verwaltungskontrollstelle

RIPOL	Automatisiertes Fahndungssystem
VDSG	Verordnung zum Bundesgesetz über den Datenschutz vom 14. Juni 1993
VKB	Verwaltungskontrolle des Bundesrates
ZAN	Zentraler Aktennachweis
ZAR	Zentrales Ausländerregister

Systemübersicht



System	Bezeichnung	Zuständigkeit und Verantwortung
RIPOL Art. 1 und 4 RIPOL-Verordnung	**Automatisiertes Fahndungssystem**	*Bundesamt für Polizeiwesen*
DOSIS Art. 19 DOSIS-Verordnung	**Datenverarbeitungssystem zur Bekämpfung des illegalen Drogenhandels**	*Bundesamt für Polizeiwesen*
ISIS-[Plus] Art. 1 und 23 Abs. 1 ISIS-Verordnung	**Provisorisches Staatsschutz-Informations-System**	*Bundesanwaltschaft* – Chef der Bundespolizei
ZAR Art. 1 ZAR-Verordnung	**Zentrales Ausländerregister**	*Bundesamt für Ausländerfragen*

System	Bezeichnung	Zuständigkeit und Verantwortung
ZAN	**Zentraler Aktennachweis**	*Bundesamt für Polizeiwesen* – Erkennungsdienst – Sektion Zentralstellendienst *Schweizerisches Zentralpolizeibüro* – Interpol
AUPER Art. 3 AUPER-Verordnung	**Automatisiertes Personenregistratursystem**	*Bundesamt für Flüchtlinge* *Bundesamt für Polizeiwesen* – Abteilung internationale Rechtshilfe und Polizeiwesen – Zentralpolizeibüro – Sektion Auslandschweizer-Fürsorge – Sektion Bürgerrecht *Bundesamt für Ausländerfragen* *Beschwerde- und Finanzdienst EJPD* *Asylrekurskommission*
IPASS Neu Art. 351^{octies} Abs. 1 StGB	**Informatisiertes Personennachweis-, Aktennachweis- und Verwaltungssystem**	*Bundesamt für Polizeiwesen*
AFIS Art. 6 Vo über den Erkennungsdienst	**Automatisches Fingerabdruck-Identifizierungssystem**	*Bundesamt für Polizeiwesen* – Erkennungsdienst
ISOK Art. 21 Abs. 1 ISOK-Vo	**Bekämpfung des organisierten Verbrechens**	*Bundesamt für Polizeiwesen*
VOSTRA Art.15 Abs.1bis, 1ter, 1^{quater} Vo über das Strafregister		

10338