Schleswig-Holsteinischer Landtag

Schleswig-Holsteinischer Landtag
Umdruck 16/640

Schleswig-Holsteinischer Landtag

Innen- und Rechtsausschuss
Der Vorsitzende

Schleswig-Holsteinischer Landtag ▪ Postfach 7121 ▪ 24171 Kiel

An die Mitglieder
des Innen- und Rechtsausschusses und
des Europaausschusses
Abg. Spoorendonk (SSW)
im H a u s e

Ihr Zeichen:
Ihre Nachricht vom:

Mein Zeichen:
Meine Nachricht vom:

Bearbeiter/in: Dörte Schönfelder

Telefon (0431) 988-1141
Telefax (0431) 988-1156
Innenausschuss@landtag.ltsh.de

3. März 2006

Unterlagen zur Vorratsdatenspeicherung von Internet- und Telefonverbindungen

Sehr geehrte Damen und Herren,

anliegend erhalten Sie zur Vorbereitung der Beratung zum Thema Vorratsdatenspeicherung die vom Ministerium für Justiz, Arbeit und Europa und dem ULD zugeleiteten Unterlagen der Europäischen Union sowie ein Gutachten des Bundeskriminalamtes zu diesem Thema.

Mit freundlichem Gruß
Im Auftrag

gez. Dörte Schönfelder
Ausschussgeschäftsführerin

EUROPÄISCHE UNION

DAS EUROPÄISCHE PARLAMENT **DER RAT**

Brüssel, den 3. Februar 2006

2005/0182 (COD) **PE-CONS 3677/05**

COPEN 200
TELECOM 151
CODEC 1206
OC 981

GESETZGEBUNGSAKTE UND ANDERE RECHTSINSTRUMENTE

Betr.:	RICHTLINIE DES EUROPÄISCHEN PARLAMENTS UND DES RATES über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG **GEMEINSAME LEITLINIEN** **Konsultationsfrist für Bulgarien und Rumänien: 14.2.2006**

RICHTLINIE 2006/.../EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom

über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION -

gestützt auf den Vertrag zur Gründung der Europäischen Gemeinschaft, insbesondere auf Artikel 95,

auf Vorschlag der Kommission,

nach Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses[1],

gemäß dem Verfahren des Artikels 251 des Vertrags[2],

---

1 ABl. C

2 Stellungnahme des Europäischen Parlaments vom 14. Dezember 2005 (noch nicht im Amtsblatt veröffentlicht) und Beschluss des Rates vom … (noch nicht im Amtsblatt veröffentlicht).

in Erwägung nachstehender Gründe:

(1) Die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr[1] verpflichtet die Mitgliedstaaten zum Schutz der Grundrechte und Grundfreiheiten und insbesondere der Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten, um den freien Verkehr personenbezogener Daten in der Gemeinschaft sicherzustellen.

(2) Die Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation)[2] transponiert die Grundsätze der Richtlinie 95/46/EG in besondere Vorschriften für den Bereich der elektronischen Kommunikation.

(3) Die Artikel 5, 6 und 9 der Richtlinie 2002/58/EG enthalten Vorschriften für die Verarbeitung von Verkehrs- und Standortdaten, die im Zuge der Nutzung elektronischer Kommunikationsdienste erzeugt wurden, durch Netzbetreiber und Diensteanbieter. Daten dieser Art müssen gelöscht oder anonymisiert werden, sobald sie zur Übermittlung einer Nachricht nicht mehr benötigt werden, außer wenn es sich um Daten handelt, die für die Abrechnung von Gebühren oder Bezahlung von Zusammenschaltungen erforderlich sind. Mit Einwilligung des Betroffenen dürfen bestimmte Daten auch für Vermarktungszwecke oder die Bereitstellung von Diensten mit einem Zusatznutzen verarbeitet werden.

---

1 ABl. L 281 vom 23.11.1995, S. 31. Geändert durch die Verordnung (EG) Nr. 1882/2003 (ABl. L 284 vom 31.10.2003, S. 1).

2 ABl. L 201 vom 31.7.2002, S. 37.

(4) In Artikel 15 Absatz 1 der Richtlinie 2002/58/EG ist festgelegt, unter welchen Bedingungen die Mitgliedstaaten die Rechte und Pflichten gemäß Artikel 5, Artikel 6, Artikel 8 Absätze 1, 2, 3 und 4 sowie Artikel 9 der genannten Richtlinie beschränken dürfen. Etwaige Beschränkungen müssen zu besonderen Zwecken der Aufrechterhaltung der öffentlichen Ordnung, d. h. für die nationale Sicherheit (d. h. die Sicherheit des Staates), die Landesverteidigung, die öffentliche Sicherheit oder die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen, in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig sein.

(5) Einige Mitgliedstaaten haben Rechtsvorschriften über eine Vorratsspeicherung von Daten durch Diensteanbieter zum Zwecke der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten erlassen. Diese nationalen Vorschriften weichen stark voneinander ab.

(6) Die rechtlichen und technischen Unterschiede zwischen den nationalen Vorschriften zur Vorratsdatenspeicherung zum Zwecke der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten beeinträchtigt den Binnenmarkt für elektronische Kommunikation, da Diensteanbieter mit unterschiedlichen Anforderungen in Bezug auf die zu speichernden Arten von Verkehrs- und Standortdaten, die für die Vorratsspeicherung geltenden Bedingungen und die Dauer der Vorratsspeicherung konfrontiert sind.

(7) In seinen Schlussfolgerungen vom 19. Dezember 2002 betont der Rat „Justiz und Inneres“, dass die beträchtliche Zunahme der Möglichkeiten bei der elektronischen Kommunikation dazu geführt hat, dass Daten über die Nutzung elektronischer Kommunikation besonders wichtig sind und daher ein wertvolles Mittel bei der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten und insbesondere der organisierten Kriminalität darstellen.

(8) In der vom Europäischen Rat am 25. März 2004 angenommenen Erklärung zum Kampf gegen den Terrorismus wurde der Rat aufgefordert, Vorschläge für Rechtsvorschriften über die Aufbewahrung von Verkehrsdaten durch Diensteanbieter zu prüfen.

(9) Gemäß Artikel 8 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK) hat jede Person das Recht auf Achtung ihres Privatlebens und ihrer Korrespondenz. Eine Behörde darf in die Ausübung dieses Rechts nur eingreifen, soweit der Eingriff gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig ist, unter anderem für die nationale oder öffentliche Sicherheit, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten oder zum Schutz der Rechte und Freiheiten anderer. Da sich die Vorratsspeicherung von Daten in mehreren Mitgliedstaaten als derart notwendiges und wirksames Ermittlungswerkzeug für die Strafverfolgung, insbesondere in schweren Fällen wie organisierter Kriminalität und Terrorismus erwiesen hat, muss gewährleistet werden, dass die auf Vorrat gespeicherten Daten den Strafverfolgungsbehörden für einen bestimmten Zeitraum unter den in dieser Richtlinie festgelegten Bedingungen zur Verfügung stehen. Die Annahme eines Instruments zur Vorratsspeicherung von Daten gemäß den Anforderungen des Artikels 8 der EMRK ist daher eine notwendige Maßnahme.

(10) Am 13. Juli 2005 hat der Rat in seiner Erklärung, in der die Terroranschläge von London verurteilt wurden, nochmals auf die Notwendigkeit hingewiesen, so rasch wie möglich gemeinsame Maßnahmen zur Vorratsspeicherung von Telekommunikationsdaten zu erlassen.

(11) Da sowohl wissenschaftliche Untersuchungen als auch praktische Erfahrungen in mehreren Mitgliedstaaten gezeigt haben, dass Verkehrs- und Standortdaten für die Ermittlung, Feststellung und Verfolgung von Straftaten von großer Bedeutung sind, muss auf europäischer Ebene sichergestellt werden, dass Daten, die bei der Bereitstellung von Kommunikationsdiensten von den Anbietern öffentlich zugänglicher elektronischer Kommunikationsdienste oder den Betreibern eines öffentlichen Kommunikationsnetzes erzeugt oder verarbeitet werden, für einen bestimmten Zeitraum unter den in dieser Richtlinie festgelegten Bedingungen auf Vorrat gespeichert werden.

(12) Artikel 15 Absatz 1 der Richtlinie 2002/58/EG gilt weiterhin für Daten, einschließlich Daten im Zusammenhang mit erfolglosen Anrufversuchen, deren Vorratsspeicherung nach der vorliegenden Richtlinie nicht ausdrücklich vorgeschrieben ist und die daher nicht in den Anwendungsbereich der vorliegenden Richtlinie fallen, und für die Vorratsspeicherung zu anderen - einschließlich justiziellen - Zwecken als denjenigen, die durch die vorliegende Richtlinie abgedeckt werden.

(13) Diese Richtlinie bezieht sich nur auf Daten, die als Folge einer Kommunikation oder eines Kommunikationsdienstes erzeugt oder verarbeitet werden; sie bezieht sich nicht auf Daten, die Inhalt der übermittelten Information sind. Die Vorratsspeicherung von Daten sollte so erfolgen, dass vermieden wird, dass Daten mehr als einmal auf Vorrat gespeichert werden. Daten, die im Zuge der Bereitstellung der betreffenden Kommunikationsdienste erzeugt oder verarbeitet wurden, beziehen sich auf Daten, die zugänglich sind. Insbesondere bei der Vorratsspeicherung von Daten im Zusammenhang mit Internet-E-Mail und Internet-Telefonie kann die Verpflichtung zur Vorratsspeicherung nur für Daten aus den eigenen Diensten des Anbieters oder des Netzbetreibers gelten.

(14) Die technische Entwicklung in der elektronischen Kommunikation schreitet rasch voran und damit verändern sich möglicherweise auch die legitimen Anforderungen der zuständigen Behörden. Um sich beraten zu lassen und den Austausch von Erfahrungen mit bewährten Praktiken in diesen Fragen zu fördern, beabsichtigt die Kommission, eine Gruppe einzusetzen, die aus Strafverfolgungsbehörden der Mitgliedstaaten, Verbänden der Branche für elektronische Kommunikation, Vertretern des Europäischen Parlaments und europäischen Datenschutzbehörden, einschließlich des Europäischen Datenschutzbeauftragten, besteht.

(15) Die Richtlinie 95/46/EG sowie die Richtlinie 2002/58/EG sind auf die gemäß der vorliegenden Richtlinie auf Vorrat gespeicherten Daten uneingeschränkt anwendbar. Artikel 30 Absatz 1 Buchstabe c der Richtlinie 95/46/EG verlangt die Anhörung der durch Artikel 29 der letztgenannten Richtlinie eingesetzten Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten.

(16) Die Pflichten von Diensteanbietern hinsichtlich Maßnahmen zur Sicherstellung der Datenqualität, die sich aus Artikel 6 der Richtlinie 95/46/EG ergeben und ihre Pflichten hinsichtlich Maßnahmen zur Gewährleistung der Vertraulichkeit und der Sicherheit der Datenverarbeitung, die sich aus den Artikeln 16 und 17 der genannten Richtlinie ergeben, gelten uneingeschränkt für Daten, die im Sinne der vorliegenden Richtlinie auf Vorrat gespeichert werden.

(17) Die Mitgliedstaaten müssen gesetzgeberische Maßnahmen ergreifen um sicherzustellen, dass die gemäß dieser Richtlinie auf Vorrat gespeicherten Daten nur in Übereinstimmung mit den innerstaatlichen Rechtsvorschriften und unter vollständiger Achtung der Grundrechte der betroffenen Personen an die zuständigen nationalen Behörden weitergegeben werden.

(18) In diesem Zusammenhang sind die Mitgliedstaaten gemäß Artikel 24 der Richtlinie 95/46/EG verpflichtet, Sanktionen für Verstöße gegen die zur Umsetzung der Richtlinie 95/46/EG erlassenen Vorschriften festzulegen. Nach Artikel 15 Absatz 2 der Richtlinie 2002/58/EG besteht die gleiche Pflicht in Bezug auf die innerstaatlichen Vorschriften zur Umsetzung der Richtlinie 2002/58/EG. In dem Rahmenbeschluss 2005/222/JI des Rates vom 24. Februar 2005 über Angriffe auf Informationssysteme[1] ist vorgesehen, dass der vorsätzliche und rechtswidrige Zugang zu Informationssystemen, einschließlich der darin auf Vorrat gespeicherten Daten, unter Strafe gestellt werden muss.

(19) Das Recht jeder Person, der wegen einer rechtswidrigen Verarbeitung oder jeder anderen mit den einzelstaatlichen Vorschriften zur Umsetzung der Richtlinie 95/46/EG nicht zu vereinbarenden Handlung ein Schaden entsteht, Schadensersatz zu verlangen, das sich aus Artikel 23 der genannten Richtlinie ergibt, besteht auch im Zusammenhang mit einer rechtswidrigen Verarbeitung personenbezogener Daten gemäß der vorliegenden Richtlinie.

(20) Das Übereinkommen des Europarates über Datennetzkriminalität von 2001 und das Übereinkommen des Europarates zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten von 1981 gelten auch für Daten, die im Sinne dieser Richtlinie auf Vorrat gespeichert werden.

---

[1] ABl. L 69 vom 16.3.2005, S. 67.

(21) Da die Ziele dieser Richtlinie, nämlich die Harmonisierung der Pflichten für Diensteanbieter bzw. Netzbetreiber im Zusammenhang mit der Vorratsspeicherung bestimmter Daten und die Gewährleistung, dass diese Daten zum Zwecke der Ermittlung, Feststellung und Verfolgung von schweren Straftaten, wie sie von jedem Mitgliedstaat in seinem nationalen Recht bestimmt werden, zur Verfügung stehen, auf Ebene der Mitgliedstaaten nicht ausreichend erreicht werden können und daher wegen des Umfangs und der Wirkungen dieser Richtlinie besser auf Gemeinschaftsebene zu erreichen sind, kann die Gemeinschaft gemäß dem in Artikel 5 des Vertrags niedergelegten Subsidiaritätsprinzip tätig werden. Entsprechend dem in demselben Artikel genannten Grundsatz der Verhältnismäßigkeit geht diese Richtlinie nicht über das zur Erreichung dieser Ziele erforderliche Maß hinaus.

(22) Diese Richtlinie wahrt die vor allem mit der Charta der Grundrechte der Europäischen Union anerkannten Grundrechte und Grundsätze. In Verbindung mit der Richtlinie 2002/58/EG ist die vorliegende Richtlinie insbesondere bestrebt, die volle Wahrung der Grundrechte der Bürger auf Achtung des Privatlebens und ihrer Kommunikation sowie auf Schutz personenbezogener Daten gemäß Artikel 7 und 8 der Charta zu gewährleisten.

(23) Da die Pflichten von Anbietern elektronischer Kommunikationsdienste verhältnismäßig sein sollten, wird in dieser Richtlinie vorgeschrieben, dass sie nur solche Daten auf Vorrat speichern müssen, die im Zuge der Bereitstellung ihrer Kommunikationsdienste erzeugt oder verarbeitet werden. Soweit derartige Daten nicht von diesen Anbietern erzeugt oder verarbeitet werden, besteht auch keine Pflicht zur Vorratsspeicherung. Durch diese Richtlinie soll nicht die Technologie für die Vorratsspeicherung von Daten harmonisiert werden, deren Wahl eine Angelegenheit ist, die auf nationaler Ebene zu regeln ist.

(24) Nach Nummer 34 der Interinstitutionellen Vereinbarung über bessere Rechtsetzung[1] wirkt der Rat darauf hin, dass die Mitgliedstaaten für ihre eigenen Zwecke und im Interesse der Gemeinschaft eigene Tabellen aufstellen, aus denen im Rahmen des Möglichen die Entsprechungen zwischen dieser Richtlinie und den Umsetzungsmaßnahmen zu entnehmen sind, und diese veröffentlichen.

(25) Diese Richtlinie berührt nicht das Recht der Mitgliedstaaten, Rechtsvorschriften über den Zugang zu und die Nutzung von Daten durch von ihnen benannte nationale Behörden zu erlassen. Fragen des Zugangs zu Daten, die gemäß dieser Richtlinie von nationalen Behörden für solche Tätigkeiten auf Vorrat gespeichert werden, die in Artikel 3 Absatz 2 Gedankenstrich 1 der Richtlinie 95/46/EG aufgeführt sind, fallen nicht in den Anwendungsbereich des Gemeinschaftsrechts. Sie können aber durch nationales Recht oder Maßnahmen nach Titel VI des Vertrags über die Europäische Union geregelt werden. Derartige Rechtsvorschriften oder Maßnahmen müssen die Grundrechte, wie sie sich aus den gemeinsamen Verfassungstraditionen der Mitgliedstaaten ergeben und durch die EMRK gewährleistet sind, in vollem Umfang wahren. Nach Artikel 8 der EMRK in der Auslegung durch den Europäischen Gerichtshof für Menschenrechte müssen Eingriffe von Behörden in das Recht auf Privatsphäre den Anforderungen der Notwendigkeit und Verhältnismäßigkeit genügen und deshalb festgelegten, eindeutigen und rechtmäßigen Zwecken dienen, wobei sie in einer Weise erfolgen müssen, die dem Zweck des Eingriffs entspricht, dafür erheblich ist und nicht darüber hinausgeht –

HABEN FOLGENDE RICHTLINIE ERLASSEN:

---

[1] ABl. C 321 vom 31.12.2003, S. 1.

Artikel 1

Gegenstand und Anwendungsbereich

1. Mit dieser Richtlinie sollen die Vorschriften der Mitgliedstaaten über die Pflichten von Anbietern öffentlich zugänglicher elektronischer Kommunikationsdienste oder Betreibern eines öffentlichen Kommunikationsnetzes im Zusammenhang mit der Vorratsspeicherung bestimmter Daten, die von ihnen erzeugt oder verarbeitet werden, harmonisiert werden, um sicherzustellen, dass die Daten zum Zwecke der Ermittlung, Feststellung und Verfolgung von schweren Straftaten, wie sie von jedem Mitgliedstaat in seinem nationalen Recht bestimmt werden, zur Verfügung stehen.

2. Diese Richtlinie gilt für Verkehrs- und Standortdaten sowohl von juristischen als auch von natürlichen Personen sowie für alle damit in Zusammenhang stehende Daten, die zur Feststellung des Teilnehmers oder registrierten Benutzers erforderlich sind. Sie gilt nicht für den Inhalt elektronischer Nachrichtenübermittlungen einschließlich solcher Informationen, die mit Hilfe eines elektronischen Kommunikationsnetzes abgerufen werden.

Artikel 2

Begriffsbestimmungen

1. Für die Zwecke dieser Richtlinie finden die Begriffsbestimmungen der Richtlinie 95/46/EG, der Richtlinie 2002/21/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste (Rahmenrichtlinie)1 und der Richtlinie 2002/58/EG Anwendung.

2. Im Sinne dieser Richtlinie bezeichnet der Ausdruck

   a) "Daten" Verkehrsdaten und Standortdaten sowie alle damit in Zusammenhang stehende Daten, die zur Feststellung des Teilnehmers oder Benutzers erforderlich sind;

   b) "Benutzer" jede juristische oder natürliche Person, die einen öffentlich zugänglichen elektronischen Kommunikationsdienst für private oder geschäftliche Zwecke nutzt, ohne diesen Dienst notwendigerweise abonniert zu haben;

   c) "Telefondienst" Anrufe (einschließlich Sprachtelefonie, Sprachspeicherdienst, Konferenzschaltungen und Datenabrufungen), Zusatzdienste (einschließlich Rufweiterleitung und Rufumleitung) und Mitteilungsdienste und Multimediadienste (einschließlich Kurznachrichtendienste (SMS), erweiterte Nachrichtendienste (EMS) und Multimedia-Dienste (MMS));

   d) "Benutzerkennung" eine eindeutige Kennung, die Personen zugewiesen wird, wenn diese sich bei einem Internetanbieter oder einem Internet-Kommunikationsdienst registrieren lassen oder ein Abonnement abschließen;

---

1 ABl. L 108 vom 24.4.2002, S. 33.

e) "Standortkennung" die Kennung der Funkzelle, von der aus eine Mobilfunkverbindung hergestellt wird bzw. in der sie endet;

f) "erfolgloser Anrufversuch" einen Telefonanruf, bei dem die Verbindung erfolgreich aufgebaut wurde, der aber unbeantwortet bleibt oder bei dem das Netzwerkmanagement eingegriffen hat.

Artikel 3

Vorratsspeicherungspflicht

1. Abweichend von den Artikeln 5, 6 und 9 der Richtlinie 2002/58/EG tragen die Mitgliedstaaten durch entsprechende Maßnahmen dafür Sorge, dass die in Artikel 5 der vorliegenden Richtlinie genannten Daten, soweit sie im Rahmen ihrer Zuständigkeit im Zuge der Bereitstellung der betreffenden Kommunikationsdienste von Anbietern öffentlich zugänglicher elektronischer Kommunikationsdienste oder Betreibern eines öffentlichen Kommunikationsnetzes erzeugt oder verarbeitet werden, gemäß den Bestimmungen der vorliegenden Richtlinie auf Vorrat gespeichert werden.

2. Die Verpflichtung zur Vorratsspeicherung nach Absatz 1 schließt die Vorratsspeicherung von in Artikel 5 genannten Daten im Zusammenhang mit erfolglosen Anrufversuchen ein, wenn diese Daten den Anbietern öffentlich zugänglicher elektronischer Kommunikationsdienste oder den Betreibern eines öffentlichen Kommunikationsnetzes im Rahmen der Zuständigkeit des betreffenden Mitgliedstaats im Zuge der Bereitstellung der betreffenden Kommunikationsdienste erzeugt oder verarbeitet und gespeichert (bei Telefoniedaten) oder protokolliert (bei Internetdaten) werden. Nach dieser Richtlinie ist die Vorratsspeicherung von Daten im Zusammenhang mit Anrufen, bei denen keine Verbindung zustande kommt, nicht erforderlich.

Artikel 4

Zugang zu Daten

Die Mitgliedstaaten erlassen Maßnahmen, um sicherzustellen, dass die gemäß dieser Richtlinie auf Vorrat gespeicherten Daten nur in bestimmten Fällen und in Übereinstimmung mit dem innerstaatlichen Recht an die zuständigen nationalen Behörden weitergegeben werden. Jeder Mitgliedstaat legt in seinem innerstaatlichen Recht unter Berücksichtigung der einschlägigen Bestimmungen des Rechts der Europäischen Union oder des Völkerrechts, insbesondere der EMRK in der Auslegung durch den Europäischen Gerichtshof für Menschenrechte, das Verfahren und die Bedingungen fest, die für den Zugang zu auf Vorrat gespeicherten Daten in Fällen, in denen die Anforderungen der Notwendigkeit und der Verhältnismäßigkeit erfüllt sind, einzuhalten sind.

Artikel 5

Datenkategorien, die auf Vorrat zu speichern sind

1. Die Mitgliedstaaten stellen sicher, dass gemäß dieser Richtlinie die folgenden Datenkategorien auf Vorrat gespeichert werden:

   a) zur Rückverfolgung und Identifizierung der Quelle einer Nachricht benötigte Daten:

      1. betreffend Telefonfestnetz und Mobilfunk:

         i) die Rufnummer des anrufenden Anschlusses,

         ii) der Name und die Anschrift des Teilnehmers bzw. registrierten Benutzers;

2. betreffend Internetzugang, Internet-E-Mail und Internet-Telefonie:

   i) die zugewiesene(n) Benutzerkennung(en),

   ii) die Benutzerkennung und die Rufnummer, die jeder Nachricht im öffentlichen Telefonnetz zugewiesen werden,

   iii) der Name und die Anschrift des Teilnehmers bzw. registrierten Benutzers, dem eine Interprotokoll-Adresse (IP), Benutzerkennung oder Rufnummer zum Zeitpunkt der Nachricht zugewiesen war;

b) zur Identifizierung des Adressaten einer Nachricht benötigte Daten:

   1. betreffend Telefonfestnetz und Mobilfunk:

      i) die angewählte(n) Nummer(n) (die Rufnummer(n) des angerufenen Anschlusses) und bei Zusatzdiensten wie Rufweiterleitung oder Rufumleitung die Nummer(n), an die der Anruf geleitet wird,

      ii) die Namen und Anschriften der Teilnehmer oder registrierten Benutzer;

2. betreffend Internet-E-Mail und Internet-Telefonie:

i) die Benutzerkennung oder Rufnummer des vorgesehenen Empfängers eines Anrufes mittels Internet-Telefonie,

ii) die Namen und Anschriften der Teilnehmer oder registrierten Benutzer und die Benutzerkennung des vorgesehenen Empfängers einer Nachricht;

c) zur Bestimmung von Datum, Uhrzeit und Dauer einer Nachrichtenübermittlung benötigte Daten:

1. betreffend Telefonfestnetz und Mobilfunk: Datum und Uhrzeit des Beginns und Endes eines Kommunikationsvorgangs;

2. betreffend Internetzugang, Internet-E-Mail und Internet-Telefonie:

i) Datum und Uhrzeit der An- und Abmeldung beim Internetzugangsdienst auf der Grundlage einer bestimmten Zeitzone, zusammen mit der vom Internetzugangsanbieter einer Verbindung zugewiesenen dynamischen oder statischen IP-Adresse und die Benutzerkennung des Teilnehmers oder des registrierten Benutzers;

ii) Datum und Uhrzeit der An- und Abmeldung für einen Internet-E-Mail-Dienst oder einen Internet-Telefonie-Dienst auf der Grundlage einer bestimmten Zeitzone;

d) zur Bestimmung der Art einer Nachrichtenübermittlung benötigte Daten:

1. betreffend Telefonfestnetz und Mobilfunk: der in Anspruch genommene Telefondienst;

2. betreffend Internet-E-Mail und Internet-Telefonie: der in Anspruch genommene Internetdienst;

e) zur Bestimmung der Endeinrichtung oder der vorgeblichen Endeinrichtung von Benutzern benötigte Daten:

1. betreffend Telefonfestnetz: die Rufnummern des anrufenden und des angerufenen Anschlusses;

2. betreffend Mobilfunk:

i) die Rufnummern des anrufenden und des angerufenen Anschlusses,

ii) die internationale Mobilteilnehmerkennung (IMSI) des anrufenden Anschlusses,

iii) die internationale Mobilfunkgerätekennung (IMEI) des anrufenden Anschlusses,

iv) die IMSI des angerufenen Anschlusses,

v) die IMEI des angerufenen Anschlusses,

vi) im Falle vorbezahlter anonymer Dienste Datum und Uhrzeit der ersten Aktivierung des Dienstes und die Kennung des Standorts (Cell-ID), an dem der Dienst aktiviert wurde;

3. betreffend Internetzugang, Internet-E-Mail und Internet-Telefonie:

i) die Rufnummer des anrufenden Anschlusses für den Zugang über Wählanschluss,

ii) der digitale Teilnehmeranschluss (DSL) oder ein anderer Endpunkt des Urhebers des Kommunikationsvorgangs;

f) zur Bestimmung des Standorts mobiler Geräte benötigte Daten:

1. die Standortkennung (Cell-ID) bei Beginn der Verbindung,

2. Daten zur geographischen Ortung von Funkzellen durch Bezugnahme auf ihre Standortkennung (Cell ID) während des Zeitraums, in dem die Vorratsspeicherung der Kommunikationsdaten erfolgt.

2. Nach dieser Richtlinie dürfen keinerlei Daten, die Aufschluss über den Inhalt einer Kommunikation geben, auf Vorrat gespeichert werden.

Artikel 6

Speicherungsfristen

Die Mitgliedstaaten sorgen dafür, dass die in Artikel 5 angegebenen Datenkategorien für einen Zeitraum von mindestens sechs Monaten und nicht mehr als zwei Jahren ab dem Zeitpunkt der Kommunikation auf Vorrat gespeichert werden.

Artikel 7

Datenschutz und Datensicherheit

Unbeschadet der zur Umsetzung der Richtlinien 95/46/EG und 2002/58/EG erlassenen Vorschriften stellt jeder Mitgliedstaat sicher, dass Anbieter von öffentlich zugänglichen elektronischen Kommunikationsdiensten bzw. Betreiber eines öffentlichen Kommunikationsnetzes in Bezug auf die nach Maßgabe der vorliegenden Richtlinie auf Vorrat gespeicherten Daten zumindest die folgenden Grundsätze der Datensicherheit einhalten:

a) die auf Vorrat gespeicherten Daten sind von derselben Qualität und unterliegen der gleichen Sicherheit und dem gleichen Schutz wie die im Netz vorhandenen Daten,

b) in Bezug auf die Daten werden geeignete technische und organisatorische Maßnahmen getroffen, um die Daten gegen zufällige oder unrechtmäßige Zerstörung, zufälligen Verlust oder zufällige Änderung, unberechtigte oder unrechtmäßige Speicherung, Verarbeitung, Zugänglichmachung oder Verbreitung zu schützen,

c) in Bezug auf die Daten werden geeignete technische und organisatorische Maßnahmen getroffen, um sicherzustellen, dass der Zugang zu den Daten ausschließlich besonders ermächtigten Personen vorbehalten ist, und

d) die Daten werden am Ende der Vorratsspeicherungsfrist vernichtet, mit Ausnahme jener Daten, die abgerufen und gesichert worden sind.

Artikel 8

Anforderungen an die Vorratsdatenspeicherung

Die Mitgliedstaaten stellen sicher, dass die in Artikel 5 genannten Daten gemäß den Bestimmungen dieser Richtlinie so gespeichert werden, dass sie und alle sonstigen damit zusammenhängenden erforderlichen Informationen unverzüglich an die zuständigen Behörden auf deren Anfrage hin weitergeleitet werden können.

Artikel 9

Kontrollstelle

1. Jeder Mitgliedstaat benennt eine oder mehrere öffentliche Stellen, die für die Kontrolle der Anwendung der von den Mitgliedstaaten zur Umsetzung von Artikel 7 erlassenen Vorschriften bezüglich der Sicherheit der auf Vorrat gespeicherten Daten in seinem Hoheitsgebiet zuständig ist/sind. Diese Stellen können dieselben Stellen sein, auf die in Artikel 28 der Richtlinie 95/46/EG Bezug genommen wird.

2. Die in Absatz 1 genannten Stellen nehmen die dort genannte Kontrolle in völliger Unabhängigkeit wahr.

Artikel 10

Statistik

1. Die Mitgliedstaaten sorgen dafür, dass der Kommission jährlich eine Statistik über die Vorratsspeicherung von in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder eines öffentlichen Kommunikationsnetzes erzeugten oder verarbeiteten Daten übermittelt wird. Aus dieser Statistik muss hervorgehen:

   – in welchen Fällen im Einklang mit dem innerstaatlichen Recht Daten an die zuständigen Behörden weitergegeben worden sind;

   – wie viel Zeit zwischen dem Zeitpunkt der Vorratsspeicherung der Daten und dem Zeitpunkt, zu dem sie von der zuständigen Behörde angefordert wurden, vergangen ist und

   – in welchen Fällen die Anfragen nach Daten ergebnislos geblieben sind.

2. Die Statistik darf keine personenbezogenen Daten enthalten.

Artikel 11

Änderung der Richtlinie 2002/58/EG

In Artikel 15 der Richtlinie 2002/58/EG wird folgender Absatz eingefügt:

"1a. Absatz 1 gilt nicht für Daten, für die in der Richtlinie 2006/.../EG* des Europäischen Parlaments und des Rates vom ...[+] über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder eines öffentlichen Kommunikationsnetzes erzeugt oder verarbeitet werden*, eine Vorratsspeicherung zu den in Artikel 1 Absatz 1 der genannten Richtlinie aufgeführten Zwecken ausdrücklich vorgeschrieben ist.

---

* ABl. ..."[++]

Artikel 12

Zukünftige Maßnahmen

1. Ein Mitgliedstaat, in dem besondere Umstände die Verlängerung der maximalen Speicherungsfrist nach Artikel 6 für einen begrenzten Zeitraum rechtfertigen, kann die notwendigen Maßnahmen ergreifen. Der Mitgliedstaat setzt die Kommission hiervon unverzüglich in Kenntnis und unterrichtet die anderen Mitgliedstaaten über die gemäß dem vorliegenden Artikel ergriffenen Maßnahmen und gibt die Gründe für ihre Einführung an.

[+] ABl. Bitte die Nummer und das Datum der vorliegenden Richtlinie einfügen.

[++] ABl.: Bitte die Amtsblattfundstelle der vorliegenden Richtlinie einfügen.

2. Binnen eines Zeitraums von sechs Monaten nach der Mitteilung nach Absatz 1 billigt die Kommission die betreffenden einzelstaatlichen Maßnahmen oder lehnt diese ab, nachdem sie geprüft hat, ob sie ein Mittel zur willkürlichen Diskriminierung oder eine verschleierte Beschränkung des Handels zwischen den Mitgliedstaaten darstellen und ob sie das Funktionieren des Binnenmarktes behindern. Trifft die Kommission innerhalb dieses Zeitraums keine Entscheidung, so gelten die einzelstaatlichen Maßnahmen als gebilligt.

3. Werden die von den Bestimmungen dieser Richtlinie abweichenden einzelstaatlichen Maßnahmen eines Mitgliedstaats nach Absatz 2 gebilligt, so kann die Kommission prüfen, ob sie eine Änderung dieser Richtlinie vorschlägt.

Artikel 13

Rechtsbehelfe, Haftung und Sanktionen

1. Jeder Mitgliedstaat ergreift die erforderlichen Maßnahmen, um sicherzustellen, dass die einzelstaatlichen Maßnahmen zur Umsetzung von Kapitel III der Richtlinie 95/46/EG über Rechtsbehelfe, Haftung und Sanktionen im Hinblick auf die Datenverarbeitung gemäß der vorliegenden Richtlinie in vollem Umfang umgesetzt werden.

2. Jeder Mitgliedstaat ergreift insbesondere die erforderlichen Maßnahmen, um sicherzustellen, dass jedweder vorsätzliche Zugang zu oder die vorsätzliche Übermittlung von gemäß dieser Richtlinie auf Vorrat gespeicherten Daten, der bzw. die nach den zur Umsetzung dieser Richtlinie erlassenen nationalen Rechtsvorschriften nicht zulässig ist, mit Sanktionen, einschließlich verwaltungsrechtlicher und strafrechtlicher Sanktionen, belegt wird, die wirksam, verhältnismäßig und abschreckend sind.

Artikel 14

Bewertung

1. Die Kommission legt dem Europäischen Parlament und dem Rat spätestens am ...* eine Bewertung der Anwendung dieser Richtlinie sowie ihrer Auswirkungen auf die Wirtschaftsbeteiligten und die Verbraucher vor, um festzustellen, ob die Bestimmungen dieser Richtlinie, insbesondere die Liste von Daten in Artikel 5 und die in Artikel 6 vorgesehenen Speicherungsfristen gegebenenfalls geändert werden müssen; hierbei berücksichtigt sie die Weiterentwicklung der Technologie der elektronischen Kommunikation und die ihr gemäß Artikel 10 zur Verfügung gestellte Statistik. Die Ergebnisse dieser Bewertung werden öffentlich gemacht.

2. Die Kommission prüft zu diesem Zweck sämtliche Kommentare, die ihr von den Mitgliedstaaten oder der gemäß Artikel 29 der Richtlinie 95/46/EG eingesetzten Datenschutzgruppe übermittelt werden.

Artikel 15

Umsetzung

1. Die Mitgliedstaaten setzen die Rechts- und Verwaltungsvorschriften in Kraft, die erforderlich sind, um dieser Richtlinie bis spätestens ...** nachzukommen. Sie setzen die Kommission unverzüglich davon in Kenntnis.

---

* Drei Jahre nach dem in Artikel 15 Absatz 1 genannten Zeitpunkt.

** 18 Monate nach der Annahme dieser Richtlinie.

Wenn die Mitgliedstaaten diese Vorschriften erlassen, nehmen sie in den Vorschriften selbst oder durch einen Hinweis bei der amtlichen Veröffentlichung auf diese Richtlinie Bezug. Die Mitgliedstaaten regeln die Einzelheiten der Bezugnahme.

2. Die Mitgliedstaaten teilen der Kommission den Wortlaut der wichtigsten innerstaatlichen Rechtsvorschriften mit, die sie auf dem unter diese Richtlinie fallenden Gebiet erlassen.

3. Bis .....* kann jeder Mitgliedstaat die Anwendung dieser Richtlinie auf die Speicherung von Kommunikationsdaten betreffend Internetzugang, Internet-Telefonie und Internet-E-Mailaufschieben. Beabsichtigt ein Mitgliedstaat, den vorliegenden Absatz in Anspruch zu nehmen, so unterrichtet er den Rat und die Kommission hiervon mittels einer Erklärung bei der Annahme dieser Richtlinie. Die Erklärung wird im Amtsblatt der Europäischen Union veröffentlicht.

Artikel 16

Inkrafttreten

Diese Richtlinie tritt am zwanzigsten Tag nach ihrer Veröffentlichung im Amtsblatt der Europäischen Union in Kraft.

---

* 36 Monate nach der Annahme dieser Richtlinie.

Artikel 17

Adressaten

Diese Richtlinie ist an die Mitgliedstaaten gerichtet.

Geschehen zu Brüssel am

In Namen des Europäischen Parlaments	*Im Namen des Rates*
Der Präsident	*Der Präsident*

RAT DER EUROPÄISCHEN UNION

Brüssel, den 20. Februar 2006 (21.02)
(OR. fr,en)

5777/06
ADD 2 REV 2 COR 1

Interinstitutionelles Dossier: 2005/0182 (COD)

COPEN 7
TELECOM 3
CODEC 78

KORRIGENDUM ZUR ÜBERARBEITETEN FASSUNG DES ADDENDUMS ZUM I/A-PUNKT-VERMERK

des	Generalsekretariats des Rates
für	den AStV / RAT
Nr. Kommissionsvorschlag:	12671/05 COPEN 150 TELECOM 96 CODEC 803
Betr.:	Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG [erste Lesung] – Erklärungen der Delegationen gemäß Artikel 15 Absatz 3 des Richtlinienvorschlags

Auf Seite 5 werden folgende Erklärungen hinzugefügt:

Erklärung Finnlands

Gemäß Artikel 15 Absatz 3 der Richtlinie über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt und verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG erklärt Finnland, dass es die Anwendung dieser Richtlinie auf die Speicherung von Kommunikationsdaten betreffend Internetzugang, Internet-Telefonie und Internet-E-Mail aufschieben wird.

Erklärung Deutschlands

gemäß Artikel 15 Abs. 3 RL 2006/…/EG

Deutschland behält sich das Recht vor, die Anwendung dieser Richtlinie auf die Speicherung von Kommunikationsdaten betreffend Internetzugang, Internet-Telefonie und Internet-E-Mail für einen Zeitraum von 18 Monaten ab dem in Artikel 15 Abs. 1 Satz 1 genannten Zeitpunkt zurückzustellen.

Bundeskriminalamt

Eva Mahnken

Mindestspeicherungsfristen für Telekommunikationsverbindungsdaten

Rechtstatsachen zum Beleg der

defizitären Rechtslage

Stand: 15. November 2005

BKA

Gliederung

III. Auftrag/Hintergrund

Im April 2004 legten die Französische Republik, die Republik Irland, das Königreich Schweden und das Vereinte Königreich dem Rat der Europäischen Union den Entwurf eines Rahmenbeschlusses über

„*die Vorratsspeicherung von Daten, die in Verbindung mit der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet und aufbewahrt werden, oder von Daten, die in öffentlichen Kommunikationsnetzen vorhanden sind, für die Zwecke der Vorbeugung, Untersuchung, Feststellung und Verfolgung von Straftaten einschließlich Terrorismus*“

vor[1].

Dies löste in Deutschland erneut eine Debatte über die Sinnhaftigkeit/Notwendigkeit, Rechtmäßigkeit, Wirtschaftlichkeit und datenschutzrechtliche "Gefährlichkeit" einer solchen Regelung aus.

Mindestspeicherungsfristen für Telekommunikationsdaten wurden in Deutschland bereits wiederholt von den Strafverfolgungs- und Sicherheitsbehörden gefordert; Pflichten zur Speicherung bestehen aber bisher lediglich punktuell im Wertpapierhandelsgesetz[2].

Die Einführungsvorschläge stoßen teilweise auf Kritik. Insbesondere aus den Reihen der Beauftragten für den Datenschutz in Bund und Ländern werden massive Eingriffe in die Grundrechte der Bürger beklagt.
Die Betreiberwirtschaft sieht dazu hohe Kosten für die Schaffung von neuen Speicherkapazitäten auf sich zukommen. Eine nicht zu vermeidende Steigerung der Betriebskosten führe zu einem Abbau von Arbeitsplätzen und zu einer weiteren Verschlechterung des Standorts Deutschland. Es wird zudem der praktische Bedarf für eine Speicherung von Verkehrsdaten angezweifelt. Auch seien mildere Maßnahmen (z.B. sog. „Data Freeze“[3]) der angestrebten generellen Speicherverpflichtung vorzuziehen.
Aus Sicht der Strafverfolgungs- und Sicherheitsbehörden ist dagegen eine gesetzliche Regelung der Speicherpflichten und -fristen hinsichtlich Art und Dauer zwingend erforderlich. Oftmals sind Ermittlungsverfahren nicht erfolgreich zu führen, weil Verkehrsdaten als einzige

[1] Ratdok. 8958/04, http://register.consilium.eu.int/pdf/de/04/st08/st08958.de04.pdf
[2] Nach § 16b WpHG kann die Aufbewahrung von bereits existierenden Verbindungsdaten über den Fernmeldeverkehr verlangt werden.

Ermittlungsansätze zur Verfügung stehen, diese Daten aber in vielen Fällen gar nicht oder nicht mehr gespeichert sind und die Auskunftsersuchen der Behörden damit ins Leere gehen. Durch eine einheitliche gesetzliche Regelung könnte diese defizitäre Lage beseitigt werden.

Das vorliegende Projekt soll dazu dienen, die Argumentationen der Kritiker zu überprüfen, und zugleich Beweis für den Bedarf der polizeilichen Praxis durch eine solide Rechtstatsachenbasis antreten.
Um im Rahmen der nationalen wie internationalen Willensbildung rechtstatsächliches Material zu gewinnen und die bei der geltende Rechtslage bestehenden Ermittlungsdefizite darstellen zu können, ist das Bundeskriminalamt durch die Abteilung P des Bundesministeriums des Innern ersucht worden, eine Erhebung von Rechtstatsachen bei den Polizeien des Bundes und der Länder durchzuführen.
Die Kommission Einsatz- und Ermittlungsunterstützung (KEEU) hat dem BKA das entsprechende Mandat mit Beschluss vom 11. März 2005 erteilt.

Ziel des Projekts ist sowohl die rechtswissenschaftliche Aufbereitung der Thematik als auch die umfassende Erhebung der Rechtstatsachen. Aufgrund der bereits jetzt bestehenden Diskussion hat das BKA den politischen Entscheidungsträgern Rechtstatsachen und Argumentationen an die Hand zu geben, die die Erforderlichkeit und Effektivität einer gesetzlichen Speicherpflicht und derzeit bestehende Defizite belegen. Der Abschlussbericht soll den Entscheidungsträgern dabei als Argumentationsgrundlage dienen, entsprechende gesetzliche Regelungen vor dem Hintergrund des Entwurfs des EU-Rahmenbeschlusses bzw. der EU-Richtlinie einzuführen.

Der nachfolgende Bericht beschreibt die Methodik der Fallerhebung und stellt das Ergebnis der Auswertung dar.

IV. Evaluation

4. Hintergrund

Jedes neue Gesetz und jede Gesetzesänderung hat sich am Maßstab des Grundgesetzes zu orientieren. Zentral ist dabei die Frage der Verhältnismäßigkeit. Ein Gesetz, das keinen positiven Einfluss auf den legitimen Zweck hat, zu dem es erlassen wurde, ist nicht notwendig und damit nicht verhältnismäßig. Aus dem Rechtsstaatsprinzip (Art. 20 GG) ergibt sich, dass sie nur soweit von der öffentlichen Gewalt eingeschränkt werden dürfen, als es zum Schutz der öffentlichen Interessen notwendig ist[4].

In Hinblick auf die Erörterung, ob man eine gesetzliche Mindestspeicherungsfrist benötigt, stellt sich die Frage, ob der Nutzen, der hieraus gezogen werden kann, auch den Eingriff in die Grundrechte rechtfertigt.

Im Zusammenhang mit der Erstellung des „Sicherheitspaketes 1994“ wurde aus politischer Sicht der konkrete Nachweis für angestrebte Gesetzesänderungen anhand von tatsächlichen Sachverhalten aus der Praxis für erforderlich gehalten[5]. Gleiches wird auch vom Datenschutz gefordert.

5. Ziel

Rechtstatsachenforschung stellt eine Wissenschaft dar, die sich mit Lebenssachverhalten beschäftigt, die Gegenstand bestehender oder geplanter rechtlicher Regelungen sind, sowie mit deren Anwendung, Durchführung, Wirkung und Erfolg. Dabei soll nicht nur die zur Setzung und Evaluation der rechtlichen Regelung notwendige Empirie beigesteuert und sich nicht auf eine Beschreibung der Lebenswirklichkeit beschränkt werden. Es ist gerade auch Aufgabe der Rechtstatsachenforschung, durch Erklärungen und Prognosen zur Erkenntnissteigerung beizutragen[6].

Ziel dieser Fallerhebung ist es, einen Überblick über die derzeit bestehende Rechtswirklichkeit zu geben und zugleich die Defizite wie auch positiven Regelungen der heutigen Gesetzeslage aufzuzeigen und nachvollziehbar zu beweisen. Dies kann nur auf Grundlage einer soliden Datenbasis erfolgen.

Die Fälle können und sollen eine Argumentationshilfe für den Gesetzgeber bilden. Dabei ist klar, dass eine Fallerhebung immer nur ein Mosaikstein im Argumentationsgefüge sein kann.

---

[4] BVerfGE 19, 342 (348f.); Jarass/Pieroth Art. 20 GG Rn. 80
[5] Kriminalistik Lersch 99, 579; Kriminalistik Nüßer 05, 76ff.
[6] Albrecht S. 25

Einer der Hauptkritikpunkte bei einer gesetzlichen Einführung von Mindestspeicherungsfristen ist aber gerade die angeblich mangelnde Notwendigkeit einer solchen Verpflichtung. Insbesondere wird angeführt, die von den Strafverfolgungsbehörden begehrten Daten lägen auch bereits nach der heutigen Speicherpraxis vor und könnten somit beauskunftet werden. Dies soll hiermit überprüft werden.

6. Methodik

Anhand einer Bund-Länder-Befragung sollten die derzeitigen Rechtsdefizite ermittelt werden. Als Erhebungsinstrument wurde ein standardisierter Fragebogen gewählt. Die Fragebögen an die Länder wurden über die Landeskriminalämter an die Polizeidienststellen gesteuert.
Der Fragebogen ist vom BKA, Abteilung Kriminalistisches Institut – KI 15 in Abstimmung mit der Kommission Einsatz- und Ermittlungsunterstützung (KEEU), dem Bundesministerium der Justiz und dem Bundesministerium des Innern entworfen worden. Neben geschlossenen Fragen wurden auch offene Fragen gestellt, um auf etwaige Besonderheiten des Einzelfalls eingehen zu können.
Die erhobene Datenmenge dient als Grundlage für die statistische Auswertung.
Die zugelieferten Fälle wurden in eine Access-Datenbank eingestellt und ausgewertet.
Die Erhebung erfolgte vom 01. April 2005 bis zum 30. September 2005. Dies darf aber nicht mit dem Zeitraum der tatsächlichen Geschehen verwechselt werden. Die Bedarfsträger sollten vielmehr auch Fälle, die vor dem 01. April 2005 lagen, zuliefern. Es handelt sich mithin um einen Meldezeitraum, nicht um einen Ereigniszeitraum.

Dabei war uns bewusst, dass gerade die Frage, ob ein nicht vorhandenes Datum nützlich gewesen wäre, schwierig zu beantworten ist, da es ja gerade nicht zur Analyse vorliegt und man sich deshalb im Bereich des Hypothetischen bewegt.

14. Auswertung

Insgesamt wurden **381** Fälle bis zum 31. Oktober 2005 gemeldet. Dabei war nur ein Fall dem Bereich der Gefahrenabwehr und ein Fall dem Bereich der internationalen Rechtshilfe zuzuordnen. Der Rest betraf den Bereich der Strafverfolgung. Alle Fragebögen wurden in Access erfasst und ausgewertet.

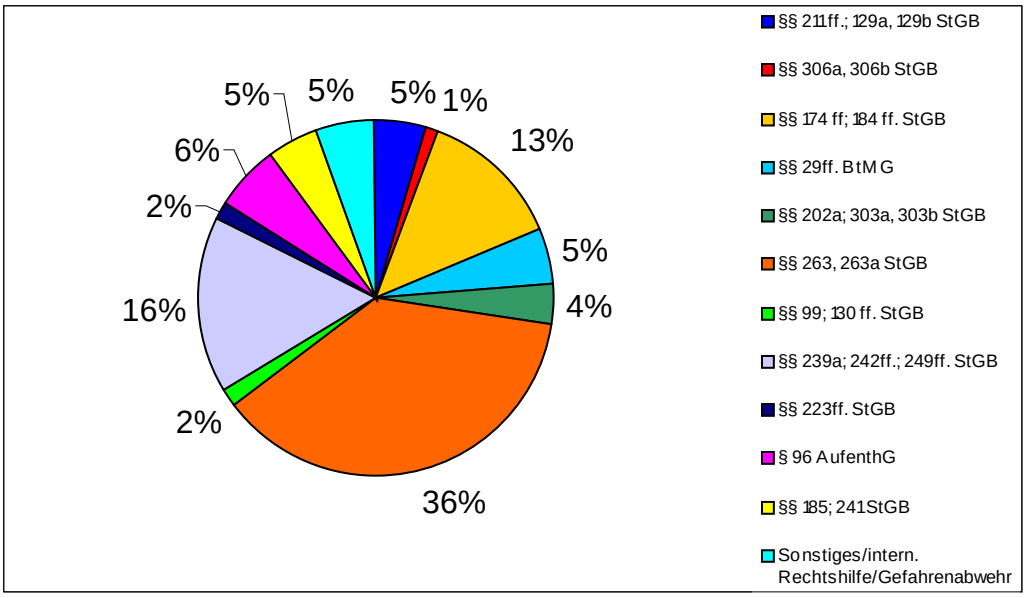
Die folgende Auswertung soll das Bedürfnis für die Einführung einer gesetzlichen Mindestspeicherungsfrist aufzeigen, darüber hinaus wird ein Überblick u.a. über die Häufigkeit der gemeldeten Straftaten, die Art der ersuchten Daten sowie über die

gewünschten Speicherzeiten und die Möglichkeit von alternativen Ermittlungsmethoden und deren Erfolg gegeben.

15. Straftaten

381 Fälle wurden gemeldet; die untenstehende Tabelle zeigt die Häufigkeit der Straftatbestände. Schwerpunkte liegen im Bereich der Straftaten gegen die sexuelle Selbstbestimmung, Betrugsdelikten und Straftaten gegen das Eigentum. Gleichfalls ersichtlich ist aber auch, dass die Notwendigkeit von Verkehrsdaten sich nicht allein auf diese Delikte bezieht, sondern eine Relevanz bei fast jeder Straftat haben können. Dies bestätigt, dass Internet und Telefon, ob fest oder mobil, bei allgemeinen Straftaten und nicht nur bei Straftaten "gegen den Computer" selbst, eine große Rolle spielen.

Straftatbestände	Fallzahlen	Prozentangaben
§§ 211 ff. StGB	16	4,2 %
§§ 174 ff; 184 ff. StGB	50	13,1 %
§§ 129a, 129b StGB	2	0,5 %
§§ 306a, 306b StGB	4	1,0 %
§ 239a StGB	2	0,5%
§§ 29 ff. BtMG	19	5,0 %
§§ 202a; 303a, 303b StGB	14	3,7 %
§§ 263, 263a StGB	141	37,0 %
§§ 242 ff.; 249 ff. StGB	59	15,5 %
§§ 223 ff. StGB	7	1,8 %
§ 96 AufenthG	23	6,0 %
§§ 185; 241 StGB	18	4,7 %
§§ 99; 130 ff. StGB	6	1,6 %
Sonstiges/intern. Rechtshilfe	19	5,0 %
Gefahrenabwehr	1	0,3 %
Kontrollsumme	381	100 %



Die Straftatbestände sind für die Diagrammdarstellung zum Teil zusammengefasst worden, um die Übersichtlichkeit zu gewährleisten.

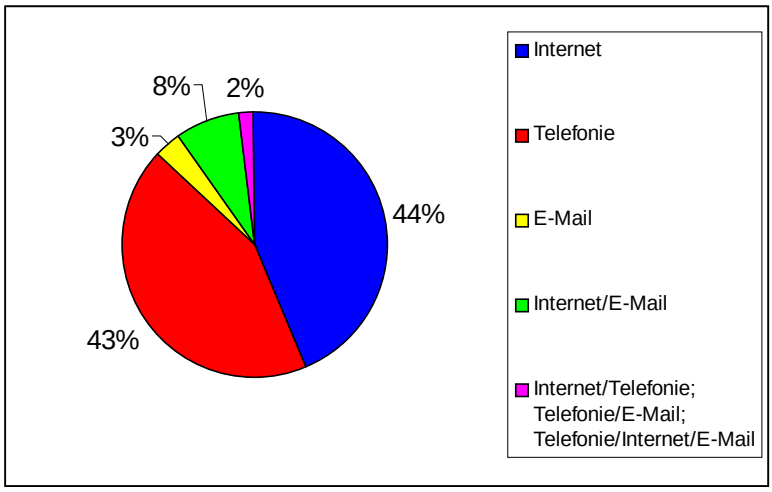
16. Ersuchen der Strafverfolgungsbehörden betraf folgende Daten

e. Telefonie/E-Mail/Internet/Sonstiges

Die Frage beinhaltete die Option „sonstige Daten“. Die hier erfassten Daten (16 Fälle) wurden nachkontrolliert und betrafen den Bereich Telefon und Internet. Per Hand wurden die Daten nacherfasst und den entsprechenden Bereichen zugeordnet.
Fast gleichhäufig wurden Daten abgefragt, die den Bereich des Internets und den Bereich der Telefonie betrafen. In lediglich 2% der Fälle wurden sowohl Verkehrsdaten von Internet/Telefonie, Telefonie/E-Mail oder Telefonie/Internet/E-Mail abgefragt.

Ersuchen betraf:	Fallzahlen	Prozent
Internet	166	43,6 %
Telefonie	165	43,3 %
E-Mail	13	3,4 %
Internet/E-Mail	31	8,1 %
Internet/Telefonie	1	0,3 %
Telefonie/E-Mail	2	0,5 %
Telefonie/Internet/E-Mail[7]	3	0,8 %
Kontrollsumme	381	100,0 %

[7] zusammengefasste Begriffe im Sinne der Kumulation

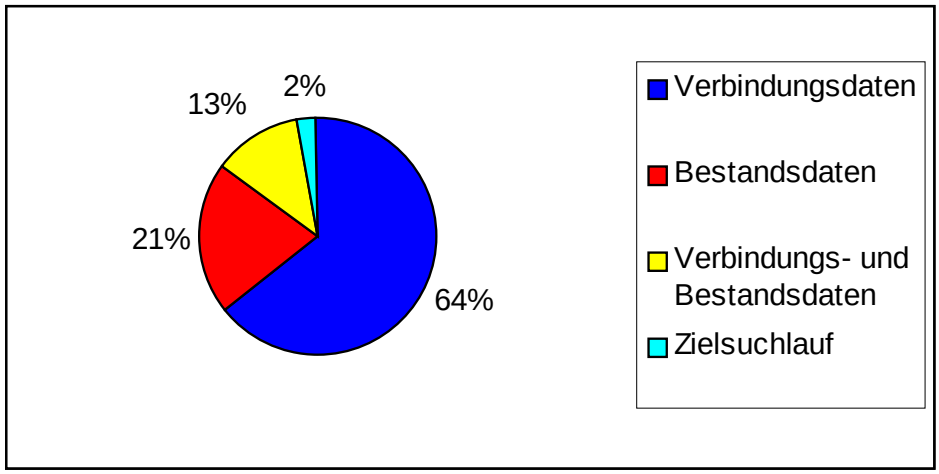


f. Datenart

Bei der Frage nach der genauen Bezeichnung der Daten, die beauskunftet werden sollten, handelte es sich um eine offene Frage. Als Cluster wurden die Kategorien „Verbindungsdaten iSd § 100g Abs. 3 StGB“, „Bestandsdaten“, „Verbindungs- und Bestandsdaten“, „Zielsuchlauf iSd § 100g Abs. 2 StGB“ sowie „keine Angaben“, die unter „non-values“ erfasst wurden, zusammengefasst.

Die untenstehende Übersicht soll einen Eindruck von der Häufigkeit der abgefragten Datenarten geben.

Art der angeforderten Daten	Anfragen	Prozent ohne non-values (372 Fälle)
Verbindungsdaten	238	64,0 %
Bestandsdaten	78	21,0 %
Verbindungs- und Bestandsdaten	47	12,6 %
Zielsuchlauf	9	2,4 %
non values	9	
Kontrollsumme	381	100,0 %



Die Verbindungsdaten umfassen dabei neben Rufnummern auch die Funkzellenabfrage, IP-Adressen, IMEI und log-files.

In fünf Fällen sind sowohl Verbindungsdaten als auch Zielsuchläufe durchgeführt worden. Diese fünf Fälle sind unter den „Verbindungsdaten“ erfasst worden.

g. Ankommende Verbindungsdaten

In dem Fragebogen wurde nicht isoliert nach der Relevanz ankommender Verbindungsdaten gefragt. Deshalb wurden lediglich in 26 Fällen explizit auf diese Daten hingewiesen. Es ist davon auszugehen, dass sie aber ebenfalls in der allgemeinen Bezeichnung „Verbindungsdaten“ enthalten sind.

h. Erfolg der Datenauskunft

Von Interesse ist auch die Frage, inwieweit die Betreiberwirtschaft den Auskunftsersuchen der Ermittlungsbehörden nachkommt. Als Cluster wurden dabei „Auskunft (teilweise) erteilt“, „Daten wurden nicht beauskunftet“ und „keine Zuordnung“ gebildet. War eine eindeutige Zuordnung nicht möglich, wurden die Angaben unter dieser Kategorie erfasst.
Bei den Prozentangaben handelt es sich daher um Größenordnungen.

Auskunft wurde (teilweise) entsprochen:	12 %
Daten wurden nicht beauskunftet:	70 %
keine Zuordnung:	19 %

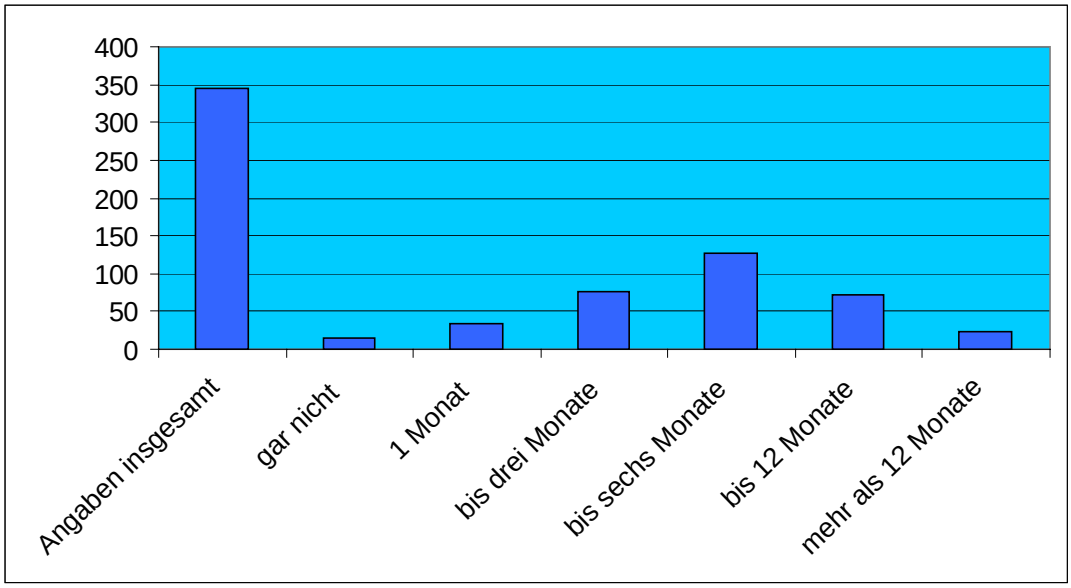
Hauptsächlich war eine negative Bescheidung des Ersuchens auf zu kurze Speicherfristen bzw. überhaupt fehlende Speicherung (Flatrate, Prepaid-Handy) zurückzuführen.

17. Idealzeitraum

i. Beauskunftete Fälle insgesamt

Insgesamt wurden 381 Ermittlungsverfahren mitgeteilt. In 35 Fällen (non-values) wurden keine Auskünfte zu einer Idealspeicherzeit gemacht. Durchschnittlich sehen die Strafverfolgungsbehörden eine Speicherzeit von bis zu sechs Monaten (ohne non-values) als wünschenswert an.

Die Wert in den Diagrammen „Angaben insgesamt“ sind alle Fälle ohne die non-values.

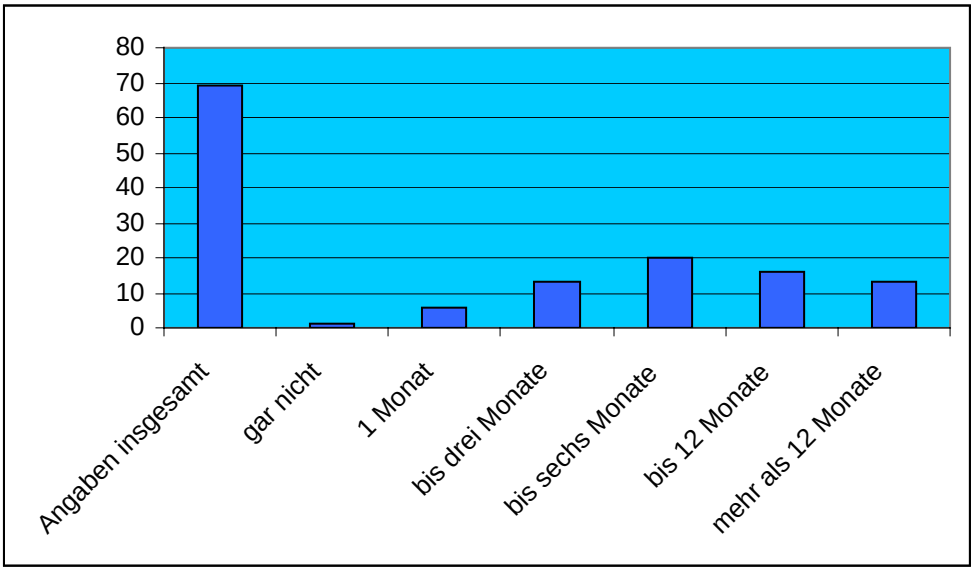


Idealspeicherzeit	Fallzahlen	Prozent ohne non-values (346 Fälle)
gar nicht	15	4,3 %
1 Monat	33	9,5 %
bis drei Monate	77	22,3 %
bis sechs Monate	127	36,7 %
bis 12 Monate	71	20,5 %
mehr als 12 Monate	23	6,6 %
non-values	35	
Kontrollsumme	381	100,0 %

j. Verbrechen

Insgesamt wurden 72 Ermittlungsverfahren wegen Verbrechenstatbeständen beauskunftet, in drei Fällen wurden keine Angaben zur Idealspeicherzeit (non-values) gemacht.

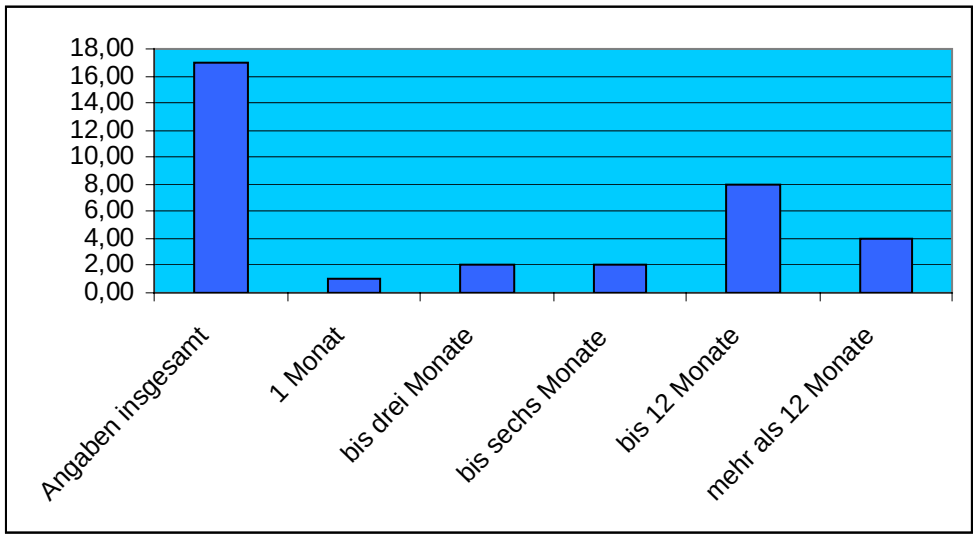
Durchschnittlich wurde eine Speicherzeit (ohne non-values) von bis zu sechs Monaten befürwortet.



Idealspeicherzeit	Fallzahlen	Prozent ohne non-values (72 Fälle)
gar nicht	1	1,4 %
1 Monat	6	8,7 %
bis drei Monate	13	18,8 %
bis sechs Monate	20	29,0 %
bis 12 Monate	16	23,2 %
mehr als 12 Monate	13	18,8 %
non-value	3	
Kontrollsumme	72	100,0 %

k. BtMG

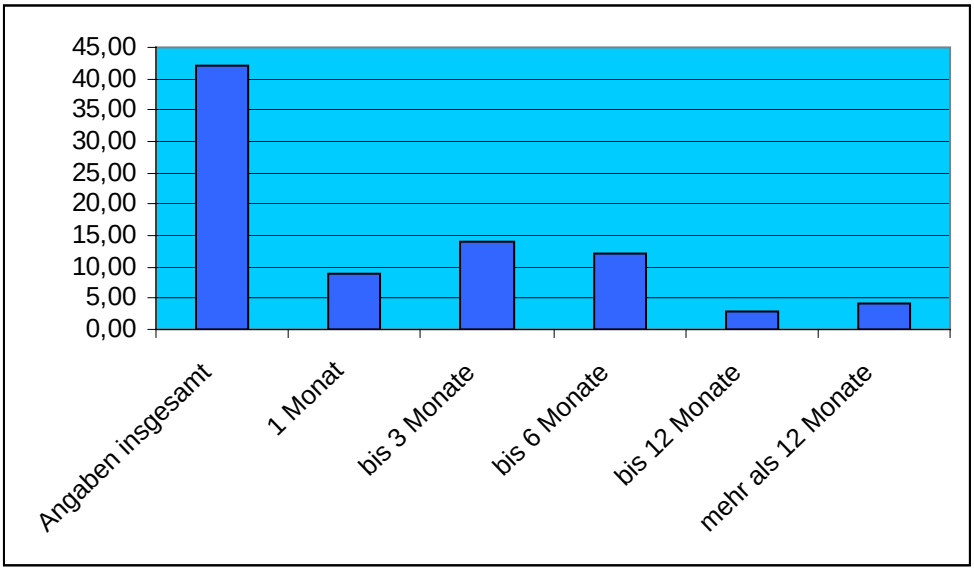
Insgesamt betrafen 19 Ermittlungsverfahren das BtMG, in zwei Fällen wurden keine Angaben zu einer Idealspeicherzeit gemacht. Durchschnittlich wird eine Speicherzeit in diesem Deliktsbereich von bis zu 12 Monaten gefordert.



Idealspeicherzeit	Fallzahlen	Prozent ohne non-values (17 Fälle)
1 Monat	1	5,9 %
bis drei Monate	2	11,8 %
bis sechs Monate	2	11,8 %
bis 12 Monate	8	47,1 %
mehr als 12 Monate	4	23,5 %
non-value	2	
Kontrollsumme	19	100 %

I. Sexualstraftaten

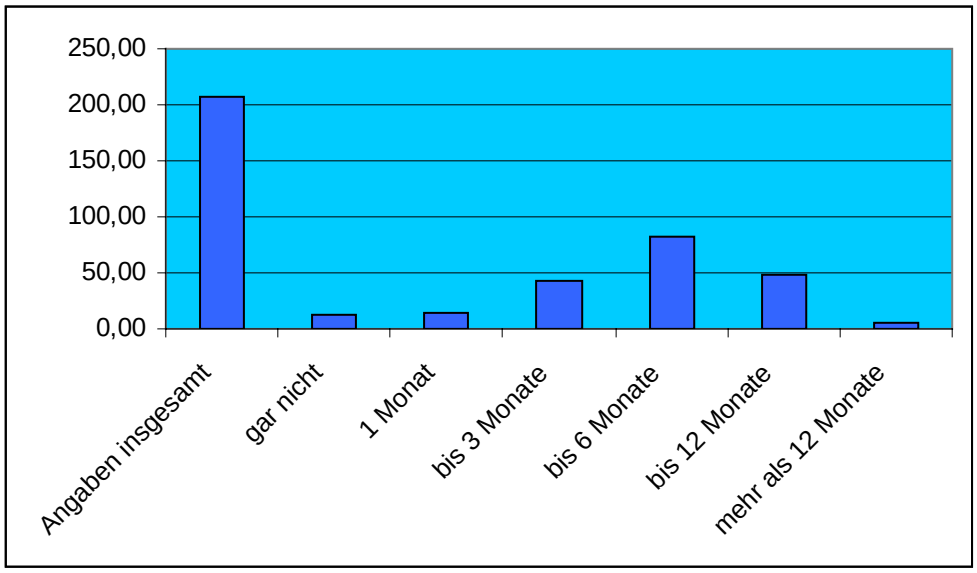
Insgesamt wurden 50 Ermittlungsverfahren beauskunftet, in acht Fällen wurden keine Angaben über eine Idealspeicherzeit gemacht (non-values). Durchschnittlich wird ein Speicherzeit von drei bis zu sechs Monaten für wünschenswert gehalten.



Idealspeicherzeit	Fallzahlen	Prozent ohne non-values (42 Fälle)
1 Monat	9	21,4 %
bis 3 Monate	14	33,3 %
bis 6 Monate	12	28,6 %
bis 12 Monate	3	7,1 %
mehr als 12 Monate	4	9,5 %
non-value	8	
Kontrollsumme	50	100,0 %

m. Vergehen, deren Strafmaß neben Geldstrafe auch Freiheitsstrafe ist

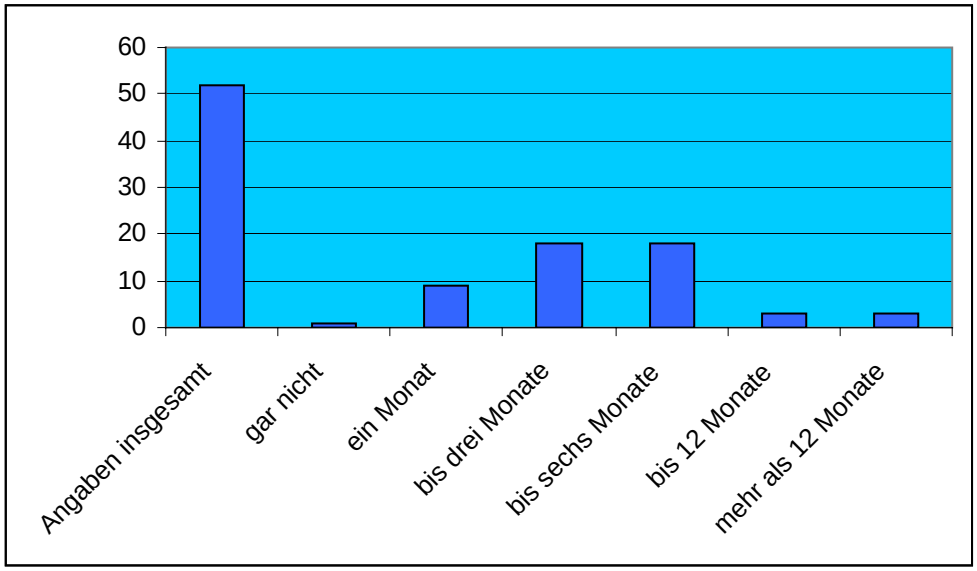
Insgesamt wurden 227 Ermittlungsverfahren beauskunftet, in 19 Fällen wurden keine Angaben zu einem Idealspeicherzeitraum gemacht (non-values). Durchschnittlich wird eine Speicherfrist bis zu sechs Monaten als sinnvoll erachtet.



Idealspeicherzeit	Fallzahlen	Prozent ohne non-values (227 Fälle)
gar nicht	13	6,3 %
1 Monat	14	6,7 %
bis 3 Monate	43	20,7 %
bis 6 Monate	83	39,9 %
bis 12 Monate	49	23,6 %
mehr als 12 Monate	6	2,9 %
non-value	19	
Kontrollsumme	227	100,0 %

n. Vergehen mit im Mindestmaß erhöhter Freiheitsstrafe von drei Monaten bis zu fünf bzw. 10 Jahren

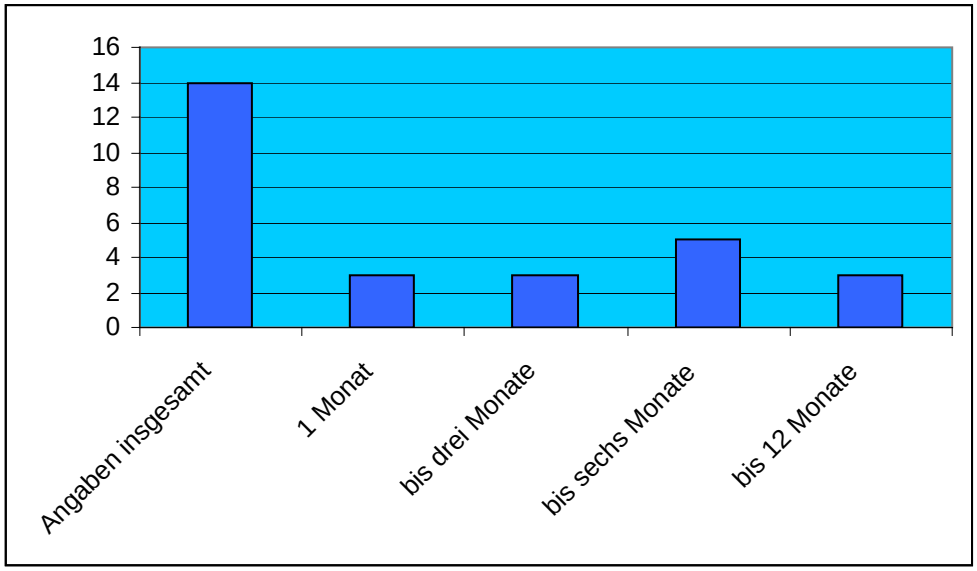
Insgesamt wurden Ersuchen aus 61 Ermittlungsverfahren beauskunftet, in neun Fällen wurde keine Auskunft über eine Idealspeicherzeit erteilt (non-values)
Im Bereich dieser Straftaten wird eine durchschnittliche Speicherdauer von drei bis sechs Monaten als sinnvoll erachtet.



Idealspeicherzeit	Fallzahl	Prozentzahlen ohne non-value (52 Fälle)
gar nicht	1	1,9 %
ein Monat	9	17,3 %
bis drei Monate	18	34,6 %
bis sechs Monate	18	34,6 %
bis 12 Monate	3	5,8 %
mehr als 12 Monate	3	5,8 %
non-value	9	
Kontrollsumme	61	100,0 %

o. Straftaten mit im Mindestmaß erhöhter Freiheitsstrafe von sechs Monaten bis zu 10 Jahren

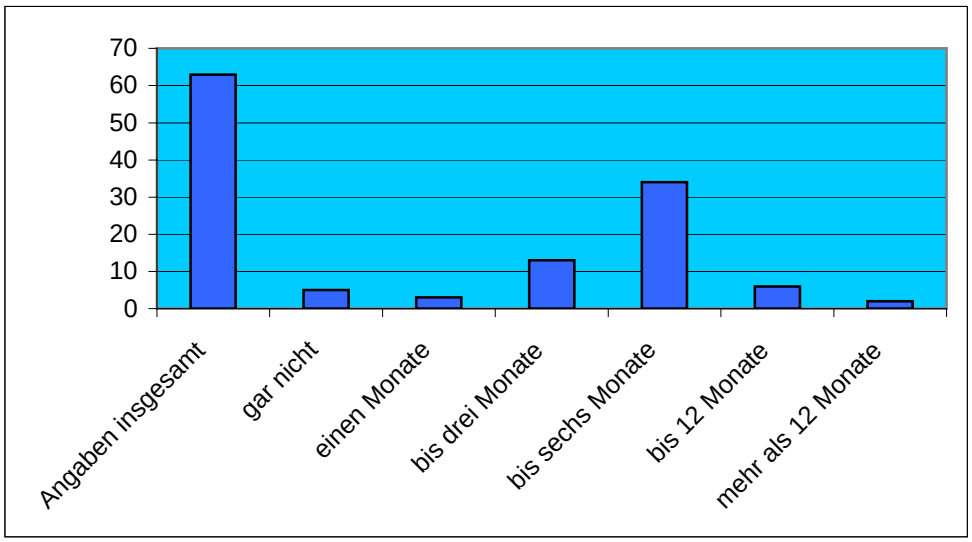
Insgesamt wurden 17 Fälle beauskunftet, in drei Fällen wurden keine Angaben zu einer gewünschten Speicherfrist gemacht. Durchschnittlich wird ein Speicherzeitraum von bis zu sechs Monaten gefordert.



Idealspeicherzeit	Fallzahlen	Prozent ohne non-values (14 Fälle)
1 Monat	3	21,4 %
bis drei Monate	3	21,4 %
bis sechs Monate	5	35,7 %
bis 12 Monate	3	21,4 %
non-values	3	
Kontrollsumme	17	100,0 %

p. Computerstraftatbestände

In diese Übersicht wurden Ermittlungsverfahren erfasst, die sich explizit auf Computerstraftaten nach §§ 202a, 303a, 303b, 263a StGB und dem UrhG beziehen.
Insgesamt wurden 69 Fälle beauskunftet, in sechs Fällen wurden keine Angaben zu einer gewünschten Speicherzeit gemacht (non-values).
Durchschnittlich wird von den Ermittlungsbehörden eine Speicherdauer von bis zu sechs Monaten gefordert.



Idealspeicherzeit	Fallzahlen	Prozent ohne non-values (63 Fälle)
gar nicht	5	7,9 %
einen Monate	3	4,8 %
bis drei Monate	13	20,6 %
bis sechs Monate	34	54,0 %
bis 12 Monate	6	9,5 %
mehr als 12 Monate	2	3,2 %
non-values	6	
Kontrollsumme	69	100,0 %

Übersicht:

Art der Straftaten	Idealspeicherzeitraum
alle Straftatbestände	bis zu drei Monate
Verbrechen	bis zu sechs Monate
BtMG	bis zu 12 Monaten
Sexualstraftaten	bis zu sechs Monaten
Vergehen, deren Strafmaß neben Geld- auch Freiheitsstrafe ist	bis zu sechs Monaten
Vergehen mit im Mindestmaß erhöhter Freiheitsstrafe von drei Monaten bis zu fünf bzw. 10 Jahren im Höchstmaß	drei bis sechs Monate
Vergehen mit im Mindestmaß erhöhter Freiheitsstrafe von sechs Monaten bis zu 10 Jahren im Höchstmaß	bis zu sechs Monaten
Computerstraftatbestände	bis zu sechs Monate

18. Tatsächlich war Auskunft über wie viele Monate möglich?

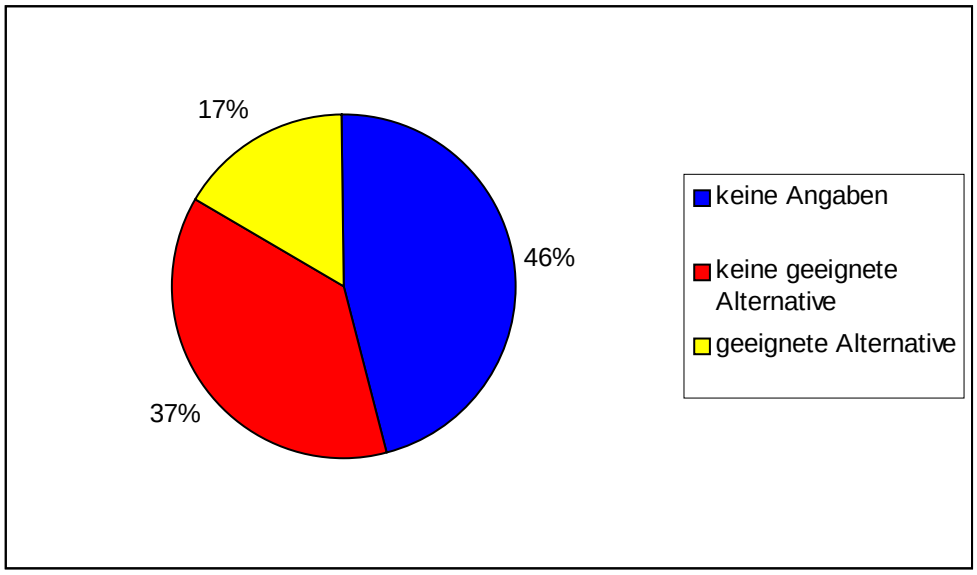
Sowohl hinsichtlich Verbindungsdaten als auch Bestandsdaten und Zielsuchlauf sind die Speicherzeiträume der einzelnen Betreiber sehr unterschiedlich. Bei Flatrateangeboten werden Daten zumeist nicht gespeichert. Im Übrigen unterscheiden sich die Speicherzeiträume von Anbieter zu Anbieter und liegen zwischen 72 Stunden und bis zu drei oder sechs Monaten. Zusätzliches Problem in einer Vielzahl der Fälle war, dass, wenn Daten hätten beauskunftet werden können, diese in den letzten drei Stellen anonymisiert worden waren und damit ebenfalls nicht zur Ermittlung herangezogen werden konnten. Häufig wurde mitgeteilt, dass eine Auskunft deswegen nicht möglich sei, weil die Betreiber von dem Datenschutzbeauftragen in Schleswig-Holstein angewiesen wurden, die Daten zu löschen.

19. Wäre Data Freeze eine geeignete Alternative gewesen?

Die Frage wurden von einem Großteil der Befragten nicht eindeutig mit ja oder nein beantwortet, sondern es wurden offene Antworten gegeben. Um überhaupt einen Überblick zu ermöglichen, wurden die Antworten per Hand ausgewertet. Als Cluster wurden „ja/nein“ und „keine Angaben“-Kategorien gebildet. Bei eindeutigen ja/nein-Antworten wurden diese übernommen. War die Antwort nicht eindeutig bzw. wurde keine Auskunft gegeben, sind diese Fälle unter „keine Angaben“ erfasst; bei den Prozentzahlen handelt es sich daher um Größenordnungen.

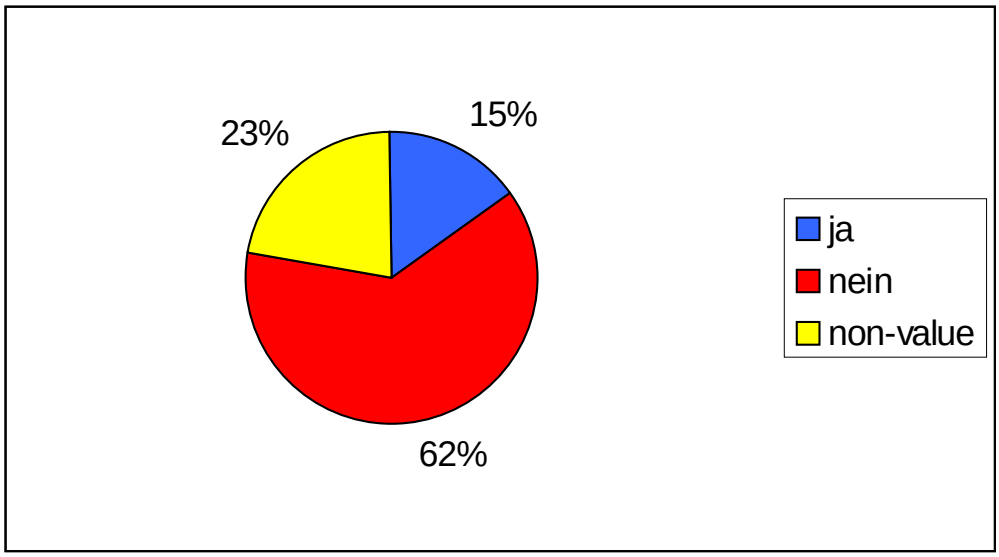
Häufig wurde mitgeteilt, dass Data Freeze eine Alternative hätte sein können, wenn die Daten überhaupt gespeichert worden wären. Da dies aber nicht erfolgt sei, wäre auch ein Data Freeze „ins Leere“ gelaufen. Zudem wurde angeführt, dass wenn schon keine Mindestspeicherungsfrist bestände, zumindest die Möglichkeit eines Data Freeze wünschenswert gewesen wäre.

Fälle insgesamt	381
keine Angaben	175
keine geeignete Alternative	142
geeignete Alternative	64



20. a. Gab es alternative Ermittlungsinstrumente?

Bei dieser Angabe handelt es sich um eine offene Fragestellung. Die Daten wurden insoweit per Hand nachbearbeitet. Als Cluster wurden „ja/nein“ und „keine Angaben“-Kategorien gebildet. Bei eindeutigen ja/nein-Antworten wurden diese übernommen. War die Antwort nicht eindeutig bzw. wurde keine Auskunft gegeben, sind diese Fälle unter „keine Angaben“ erfasst; bei den Prozentzahlen handelt es sich daher um Größenordnungen.
Hauptsächlich wurden Zeugenvernehmungen und generell andere operative Maßnahmen angeführt.



b. Wenn es keine alternativen Ermittlungsinstrumente gab, warum nicht?

Auch dies wurde als offene Frage gestellt. Überwiegend wurde angeführt, dass Verbindungsdaten der einzige Ermittlungsansatz waren, da Personaldaten bei Registrierungen oftmals falsch waren, kein anderweitiger Täter-Opfer-Kontakt stattfand oder sich die Beschuldigten im Ausland aufhielten. Daneben waren Zeugen und Beschuldigte nicht gesprächsbereit bzw. andere Maßnahmen waren nicht verhältnismäßig oder aus Ermittlungstaktik nicht einsetzbar.

c. Wenn es alternative Ermittlungsinstrumente gab, waren diese für den Erfolg der Maßnahme unwichtig (Note 0) bis wichtig (Note 5)?

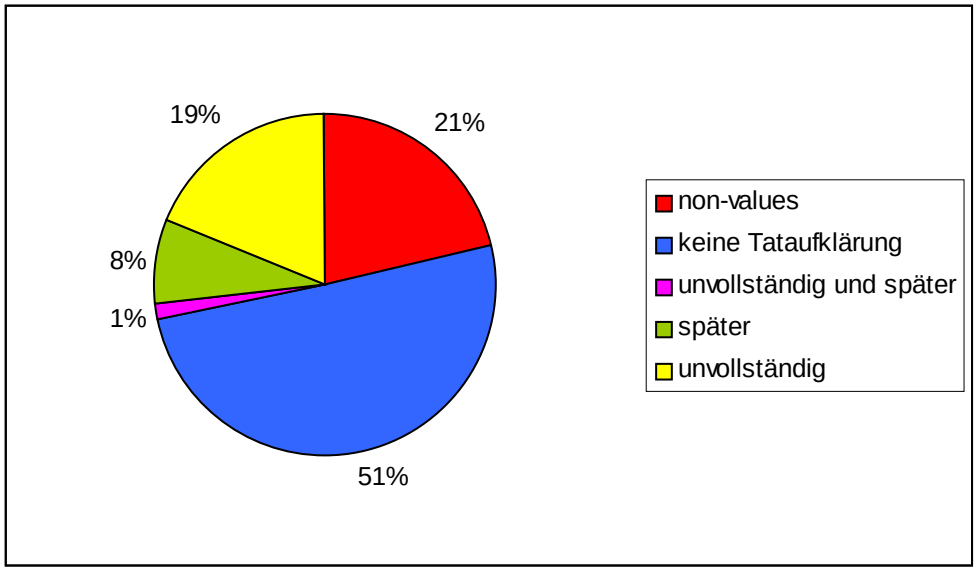
Diese Frage wurde überwiegend auch beantwortet, wenn zuvor das Vorhandensein von alternativen Ermittlungsinstrumenten verneint wurde. Deswegen beschränkt sich die unten

stehende Tabelle nur auf 59 Fälle, in denen eindeutig alternative Ermittlungsinstrumente bejaht wurden.

alternatives Ermittlungsinstrument war für den Erfolg der Maßnahme	Fallzahlen	Prozent
Note 0 (unwichtig)	4	6,8 %
Note 1	4	6,8 %
Note 2	8	13,6 %
Note 3	9	15,3 %
Note 4	12	20,3 %
Note 5 (wichtig)	14	23,7 %
non-value	8	13,6 %
Kontrollsumme	59	100 %

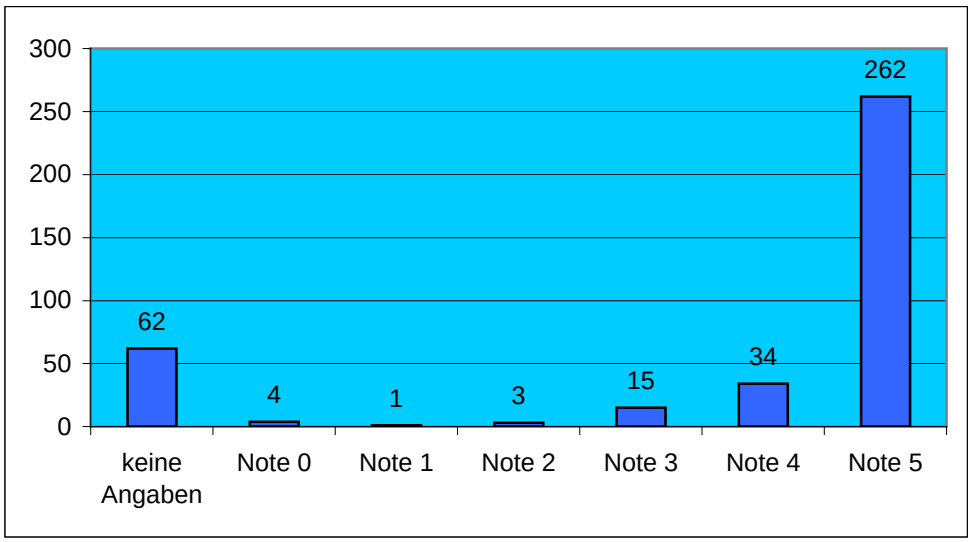
21. Die Taten konnten nicht/unvollständig/später aufgeklärt werden:

Von den insgesamt beauskunfteten 381 Fällen, haben 81 keine Angaben zur Tataufklärung gemacht (non-values).



22. Verkehrsdaten waren für den Erfolg der Maßnahme wie wichtig?

Von allen beauskunfteten Fällen haben 62 keine Angaben zur Einschätzung der Verkehrsdaten gegeben (non-values).



Notenskala		Fallzahlen	Prozent
keine Angaben		62	16,3 %
Note	0 (unwichtig)	4	1,0 %
Note	1	1	0,3 %
Note	2	3	0,8 %
Note	3	15	3,9 %
Note	4	34	8,9 %
Note	5 (sehr wichtig)	262	68,8 %
Kontrollsumme		381	100 %

23. Zusammenfassung

Die Evaluation zeigt, dass fast alle Straftatkategorien eine Relevanz bei der Frage der Mindestspeicherungsfristen für Verkehrsdaten haben. Nicht nur eindeutige Computerstraftatbestände wie §§ 303a, 303b, 202a StGB finden sich, sondern auch Körperverletzung, Diebstahl etc. Es zeigt sich auch, dass die Daten besondere Bedeutung erlangen, wenn kein weiterer Täter-Opfer-Kontakt stattgefunden hat oder um die Tatumstände genauer zu erhellen.
Schwerpunkt der Delikte lag aber bei Betrugstatbeständen und Straftaten gegen die sexuelle Selbstbestimmung.
Obwohl in 78% der Fälle die Strafverfolgungsbehörden Verkehrsdaten als wichtig bis sehr wichtig erachten, führte dies nicht zu Forderungen von sehr langen Speicherfristen, was auf einen sensiblen, problembewussten Umgang der Polizei mit rechtspolitischen Forderungen mit datenschutzrechtlicher Relevanz schließen lässt.

Dass als Idealspeicherzeitraum weitestgehend von den Ermittlungsbehörden eine Zeit von bis zu sechs Monaten gefordert wird, zeigt, dass sich die Ermittlungsbehörden des Grundrechtseingriffs sehr wohl bewusst sind und diesen bei ihren Forderungen auch beachten. Auch die ebenfalls häufige Angabe, ein zwölfmonatiger Speicherzeitraum sei ausreichend, kann als ausgesprochen moderat bezeichnet werden.

Die Evaluation zeigt aber auch statistisch, dass das „Data Freeze“, wie bereits oben ausgeführt, keine geeignete Alternativmethode ist. Lediglich 17% sahen es als gleich geeignet an.

Die Rechtstatsachen belegen, dass es ein Bedürfnis für die Einführung von Mindestspeicherungsfristen gibt und dieses bei der Ermittlung von Straftaten auch dringend erforderlich ist.

-