00068/10/DE
WP 172

Bericht 01/2010 über die zweite gemeinsame Durchsetzungsmaßnahme:

Erfüllung der nach den innerstaatlichen Rechtsvorschriften über die Vorratsspeicherung von Verkehrsdaten aufgrund der Artikel 6 und 9 der Richtlinie 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation) und der Richtlinie 2006/24/EG (über die Vorratsspeicherung von Daten und zur Änderung der Datenschutzrichtlinie für elektronische Kommunikation) bestehenden Pflichten durch die Telekommunikations-Diensteanbieter und die Internet-Diensteanbieter auf nationaler Ebene

Angenommen am 13. Juli 2010

Zusammenfassung

- Diese Durchsetzungsmaßnahme der Artikel-29-Datenschutzgruppe diente der Untersuchung, ob die mit der Richtlinie 2006/24/EG eingeführten Bestimmungen befolgt werden. Dabei wurden die von der Datenschutzgruppe in ihren früheren Stellungnahmen zu dieser Angelegenheit zum Ausdruck gebrachten Empfehlungen und Bedenken berücksichtigt.

- Die Durchführung der Richtlinie über die Vorratsspeicherung von Daten durch die Anbieter von elektronischen Kommunikationsdiensten und von Internetdiensten ist naturgemäß in hohem Maße mit Risiken verbunden, die angemessene technische und organisatorische Sicherheitsvorkehrungen erforderlich machen. Dies ist dem Umstand geschuldet, dass verfügbare Verkehrsdaten Aufschluss über Auffassungen, Meinungen und Vorlieben geben können und die Verfügbarkeit dieser Daten dementsprechend einen Eingriff in das Privatleben der Benutzer darstellen und sich ganz erheblich auf die Vertraulichkeit der Kommunikation und die Grundrechte, wie das Recht auf freie Meinungsäußerung, auswirken kann.
- Basierend auf einem Fragenkatalog wie auch auf Inspektionen vor Ort, die sich an die wichtigsten innerstaatlichen Telekommunikationsbetreiber und Internet-Diensteanbieter richten, um die erheblichen Marktanteile abzudecken, bringt die Durchsetzungsmaßnahme ein Flickwerk von Durchführungsmaßnahmen an den Tag, so insbesondere im Hinblick auf die vorhandenen Sicherheitsmaßnahmen.

- Es bestehen beträchtliche Unterschiede hinsichtlich der Kategorien der von den Internetdiensten auf Vorrat zu speichernden Verkehrsdaten, und auch hinsichtlich der in den einzelnen Mitgliedstaaten geltenden Speicherungsfristen sind erhebliche Abweichungen festzustellen, während sich hinsichtlich der Kategorien der von den Telefondiensten auf Vorrat zu speichernden Verkehrsdaten ein einheitlicheres Bild ergibt. Von Bedeutung ist auch, dass in den innerstaatlichen Gesetzen vieler Mitgliedstaaten eine kürzere Speicherungsfrist als die von der Richtlinie vorgegebene Höchstfrist gewählt wurde.

- In diesem Zusammenhang ist die Artikel-29-Datenschutzgruppe über die Erkenntnis besorgt, dass die Richtlinie auf der innerstaatlichen Ebene anscheinend nicht kohärent durchgeführt wurde. Insbesondere scheint sie von Mitgliedstaaten so ausgelegt worden zu sein, als ließe sie die Entscheidung über ihren Anwendungsbereich offen – d. h., ob die Richtlinie als Ausnahmeregelung zur allgemeinen Pflicht, Verkehrsdaten mit der Beendigung der elektronischen Kommunikation zu löschen, dienen soll, oder vielmehr als Befugnisnorm für die Vorratsspeicherung all jener Daten, zu deren Speicherung die Diensteanbieter bereits für die in Artikel 6 Absatz 2 der Richtlinie 2002/58 bestimmten Zwecke ermächtigt wurden. Die Datenschutzgruppe spricht sich für die letztere Auslegung aus, die jüngst auch im Urteil des EuGH in der Rechtssache(C-301/06) Irland/Europäisches Parlament, Rat der Europäischen Union für rechtens befunden wurde.

- Die Sicherheitsmaßnahmen fallen, wie es scheint, je nach der Betriebsgröße der Diensteanbieter unterschiedlich umfangreich aus; die logischen Sicherheitsmaßnahmen sind nicht immer angemessen, um mit den in den Verkehrsdaten enthaltenen hochsensiblen Informationen besonders sorgsam umgehen zu können. Es ist von Belang, dass die einschlägigen Verfahren für die Weitergabe der von den gesetzlich ermächtigten

Behörden angeforderten Verkehrsdaten als ziemlich inhomogen anzusehen sind, einschließlich der großen Bandbreite an Sicherheitslösungen und unterschiedlichen Sicherheitsniveaus für die Übermittlung von Verkehrsdaten.

- Die Durchsetzungsmaßnahme brachte zusätzlich zutage, dass nur ein paar Mitgliedstaaten der Kommission die nach der Richtlinie vorgeschriebene jährliche Statistik über die Verwendung der ordnungsgemäß auf Vorrat gespeicherten Verkehrsdaten übermittelt haben, und dass Outsourcing besonders bei kleineren Betreibern eine weitverbreitete Praxis darstellt, was natürlich einige Zweifel hinsichtlich der tatsächlichen Einhaltung der Datenschutzvorschriften aufwirft.

- Das Fehlen einer sachgerechten Statistik ist bei der Beurteilung, ob die Richtlinie ihre Zielsetzung erreicht hat, hinderlich. Die Schlussfolgerungen dieses Berichts zeigen eindeutig, dass die innerstaatliche Durchführung von Vielfalt und mangelnder Harmonisierung geprägt ist. Bis zur Entscheidung der EU-Kommission, ob die Richtlinie geändert oder aufgehoben werden soll[1], hält es die Datenschutzgruppe für zweckdienlich, spezifische Empfehlungen zur Sicherstellung einer stärkeren Harmonisierung, einer sichereren Datenübermittlung und standardisierter Weitergabeverfahren zu formulieren.

- Diese umfassen insbesondere folgende Punkte:
  - ***Kategorien von auf Vorrat gespeicherten Daten:*** Der Katalog der zwingend auf Vorrat zu speichernden Verkehrsdaten ist als erschöpfende Liste anzusehen. Folglich können den Diensteanbietern aufgrund der Richtlinie über die Vorratsspeicherung von Daten keine zusätzlichen Pflichten zur Vorratsdatenspeicherung auferlegt werden.
  - ***Speicherungsfristen:*** Um gleiche Rahmenbedingungen zu erhalten, muss die Höchstfrist für die Vorratsspeicherung verkürzt und eine einheitliche, kürzere Frist gesetzt werden, die von allen Diensteanbietern in der gesamten EU einzuhalten ist, wie die Artikel-29-Datenschutzgruppe bereits in ihrer Stellungnahme WP113 dargelegt hat. Der gesamte Aspekt der Sicherheit von Verkehrsdaten für sich sollte von der Kommission unter einem breiteren Blickwinkel neu überdacht werden.
  - ***Technische und organisatorische Sicherheitsmaßnahmen:*** Im Einzelnen aufgeführt sind spezifische Zusatzmaßnahmen (wie strenge Authentifizierung, Access- und Log-Management in Einzelheiten); zu Zwecken einer schnelleren und zuverlässigeren Datenübermittlung; die die Sammlung von statistischen Informationen und den Nachweis von Zugriffen auf die betreffenden Daten ermöglicht, wurde ferner ein Vorschlag für ein Standardverfahren für die Weitergabe von Verkehrsdaten an die gesetzlich ermächtigten Behörden ausgearbeitet. In diesem Zusammenhang muss der Begriff „schwere Straftat“ auf der Ebene der Mitgliedstaaten klar definiert werden, und die Liste der zum Zugriff auf die betreffenden Daten befugten staatlichen Stellen muss allen relevanten Beteiligten bekannt gegeben werden.

[1] Diesbezüglich erinnert die Artikel-29-Datenschutzgruppe an ihre früheren Stellungsnahmen zu dieser Richtlinie.

I. Hintergrund – Durchsetzung

In ihrem ersten Bericht über die Durchführung der Datenschutzrichtlinie im Mai 2003 ersuchte die Europäische Kommission die Artikel-29-Datenschutzgruppe, zu erwägen, sektorale Untersuchungen auf EU-Ebene durchzuführen und die diesbezüglichen Normen anzugleichen. Die Artikel-29-Datenschutzgruppe legte in ihrer Entschließung vom 25. November 2004 dar, dass die Förderung der einheitlichen Anwendung und der harmonisierten Befolgung des Datenschutzrechts eines ihrer strategischen und ständigen Ziele ist.

Nach der ersten gemeinsamen Durchsetzungsmaßnahme zu privaten Krankenversicherungsunternehmen (Bericht 1/2007, angenommen am 20. Juni - WP137) und aufgrund der dabei gesammelten Erfahrungen beschloss die Datenschutzgruppe – als Teil der in ihrem Arbeitsprogramm dargelegten Prioritäten, die einheitliche Anwendung der auf der Gemeinschaftsebene harmonisierten Datenschutzgrundsätze zu überprüfen – Die die Durchführung einer zweiten gemeinsamen Erhebung und entschied sich dabei für die Untersuchung der Erfüllung der nach den innerstaatlichen Rechtsvorschriften über die Vorratsspeicherung von Verkehrsdaten[2] aufgrund der Artikel 6 und 9 der Richtlinie 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation) und der Richtlinie 2006/24/EG (über die Vorratsspeicherung von Daten und zur Änderung der Datenschutzrichtlinie für elektronische Kommunikation) bestehenden Pflichten durch die Telekommunikations-Diensteanbieter und die Internet-Diensteanbieter auf nationaler Ebene.

Im Juli 2008 beauftragte die Artikel-29-Datenschutzgruppe die Taskforce *Rechtsdurchsetzung* (Enforcement Task Force - ETF) mit der Planung und Umsetzung der Schritte, die nach Maßgabe der in WP152 im Einzelnen beschriebenen Aufgabenstellung für die Durchführung der Durchsetzungsmaßnahme erforderlich sind.

Die in WP101 definierte Kombination von Kriterien legte die Wahl dieses Themenbereichs nahe, wenn auch die Datenschutzgruppe sich der Tatsache bewusst war, dass der Umsetzungsprozess der Richtlinie über die Vorratsspeicherung von Daten noch nicht abgeschlossen ist – entweder wegen innerstaatlicher Verzögerungen oder wegen der unterschiedlichen Fristen, die den Mitgliedstaaten zur Einführung der Vorratsspeicherungspflicht auch in Bezug auf Internet-Verkehrsdaten gesetzt wurden.

Diese Entscheidung wurde getroffen, weil die Richtlinie 2006/24/EG von ihrem Anwendungsbereich her ziemlich spezifisch ist und eine Ausnahmeregelung von dem in der Richtlinie 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation) aufgestellten allgemeinen Grundsatz darstellt, – nach deren Artikel 6 Absatz 1 gilt: „Verkehrsdaten, die sich auf Teilnehmer und Nutzer beziehen und vom Betreiber … eines öffentlich zugänglichen elektronischen Kommunikationsdienstes verarbeitet und gespeichert werden, sind … zu löschen oder zu anonymisieren, sobald sie für die Übertragung einer Nachricht nicht mehr benötigt werden.“ Die einzige allgemeine Pflicht zur Speicherung von Verkehrsdaten ergibt sich aus Artikel 6 Absatz 2, sofern solche Daten „zum Zwecke der Gebührenabrechnung und der Bezahlung von Zusammenschaltungen erforderlich sind“ – diese ist jedoch „nur bis zum Ablauf der Frist zulässig, innerhalb deren die Rechnung rechtlich angefochten oder der Anspruch auf Zahlung geltend gemacht werden kann.“

[2] Der Klarstellung halber sei darauf hingewiesen, dass der Begriff „Verkehrsdaten“ in dieser Stellungnahme die in Artikel 5 der Richtlinie 2006/24/EG genannten Daten umfasst.

Bekanntlich dient die Richtlinie 2006/24/EG (siehe Artikel 1) aber dem Ziel der Harmonisierung der „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". Die betreffenden Daten dürfen auf Vorrat gespeichert werden „zum Zwecke der Ermittlung, Feststellung und Verfolgung von schweren Straftaten, wie sie von jedem Mitgliedstaat in seinem nationalen Recht bestimmt werden."

Darüber hinaus hat die Artikel-29-Datenschutzgruppe drei Stellungnahmen zur Richtlinie über die Vorratsspeicherung von Daten und zu den Entwürfen der endgültigen Rechtsvorschrift abgegeben[3]. In diesen Stellungnahmen, insbesondere in den Dokumenten WP113 und WP119, äußerte die Datenschutzgruppe Bedenken, da die Bestimmungen der Richtlinie für alle europäischen Bürger und deren Privatsphäre weitreichende Konsequenzen haben werden, denn die Entscheidung, die Telefon- und die Internet-Diensteanbieter zu verpflichten, die Verkehrsdaten aller ihrer Teilnehmer und Nutzer auf Vorrat zu speichern, stellt nach wie vor ein absolutes Novum dar. Sie hat direkte Auswirkungen auf den Alltag jedes einzelnen Bürgers und kann eine Gefahr für die Grundwerte und –freiheiten aller Bürger in Europa darstellen. Folglich vertritt die Datenschutzgruppe in ihren Stellungnahmen „die Ansicht, dass eine einheitliche Auslegung und Umsetzung der Richtlinienbestimmungen ebenfalls sehr wichtig ist, damit die Bürger überall in der Europäischen Union den gleichen Schutz genießen".

Angesichts einer fehlenden gemeinsamen Definition des Begriffs „schwere Straftaten" zeigte die Datenschutzgruppe Besorgnis über den ziemlich unbestimmten Zweck der Vorratsspeicherung, der in der „Ermittlung, Feststellung und Verfolgung von schweren Straftaten" besteht; sie war ebenfalls in Sorge über das Fehlen von spezifischen Leitlinien für die Behörden, die befugt sind, auf die von den Diensteanbietern oder Betreibern auf Vorrat gespeicherten Daten und die für die Vorratsspeicherung solcher Daten eingesetzten Mechanismen zuzugreifen; mit solchen Leitlinien ist sicherzustellen, dass die betreffenden Informationen nur zu den in der Richtlinie 2006/24/EG festgelegten Zwecken verfügbar sind. Die Datenschutzgruppe forderte, dass angemessene und besondere Schutzvorkehrungen mindestens in Bezug auf folgende Belange eingeführt werden: Angabe des Zwecks, Begrenzung des Zugangs, Datensparsamkeit, Verbot des Datenschürfens, richterliche/unabhängige Prüfung der Zugangsgenehmigung, Verbot der Nutzung der Daten, die gemäß der Richtlinie über die Vorratsspeicherung allein zu Zwecken der öffentlichen Ordnung gespeichert wurden, durch die Diensteanbieter oder Betreiber zu anderen Zwecken – dies führte zu der Forderung nach getrennten Systemen und der Festlegung von Mindeststandards, die genau regeln, welche Sicherheitsvorkehrungen die Anbieter oder Betreiber treffen müssen.

Die auf Vorrat gespeicherten Verkehrsdaten ermöglichen die Überwachung und Rückverfolgung des gesamten Beziehungsgeflechts einzelner Personen wie auch die Kartierung ihrer räumlichen Bewegungen und der dabei eingesetzten Ausrüstungen und Hilfsmittel. In einer demokratischen Gesellschaft muss jegliche Einschränkung der Rechte des Einzelnen auf Privatsphäre und Datenschutz erforderlich, angemessen und verhältnismäßig sein und spezifischen Zwecken der öffentlichen Ordnung dienen – so der nationalen Sicherheit, der Landesverteidigung, der öffentlichen Sicherheit oder der

[3] Stellungnahmen 9/2004, 4/2005 und 3/2006

Ermittlung, Feststellung und Verfolgung von Straftaten. Derartige Einschränkungen müssen als bloße Mindestanforderung die in der Charta der Grundrechte der Europäischen Union wie auch in der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten festgeschriebenen Rechte, Freiheiten und Grundsätze achten.

Zu Zwecken der Nachprüfung der von der Datenschutzgruppe geltend gemachten Vorbehalte und der bis jetzt erreichten Harmonisierung galt es folglich, einen genauen Blick auf die Art und Weise zu werfen, wie die Richtlinie im jeweiligen innerstaatlichen Recht bisher umgesetzt und ausgeführt wurde.

Zwar muss der Umsetzungsprozess in der EU erst noch abgeschlossen werden, doch kann die Datenschutzgruppe aufgrund der Ergebnisse dieser Erhebung der Kommission, die ihren Bewertungsbericht bis 15 September 2010 vorzulegen hat, bereits jetzt hilfreiche Informationen liefern.

II. Rechtsrahmen

Wie bereits ausgeführt, besteht die Zielsetzung der Richtlinie 2006/24/EG (nachstehend Richtlinie über die Vorratsspeicherung von Daten) in der Harmonisierung der innerstaatlichen Vorschriften über die für bestimmte Verkehrsdaten geltenden Pflichten zur Vorratsspeicherung. In diesem Zusammenhang kann auf die Artikel 5, 6 und 7 der Richtlinie über die Vorratsspeicherung von Daten verwiesen werden, die die Kategorien der auf Vorrat zu speichernden Daten, die einschlägigen Speicherungsfristen und die Datenschutz- bzw. die Datensicherheitsmaßnahmen festlegen. Bekanntlich hat die mit der Richtlinie eingeführte Vorratsspeicherungspflicht unter Umständen bzw. tatsächlich unterschiedliche Rechtswirkungen, je nachdem wie Artikel 3 dieser Richtlinie ausgelegt und durchgeführt wird – d. h. ob festgelegt wird, dass die Richtlinie eine Ausnahmeregelung vom allgemeinen Grundsatz darstellt, dass Verkehrdaten zu löschen sind, sobald sie für die Übertragung einer Nachricht nicht mehr benötigt werden (gemäß Artikel 6 Absatz 1 der Richtlinie 2002/58/EG), oder vielmehr, dass die Richtlinie nur eine zwingende Speicherungsfrist für diejenigen Verkehrsdaten einführt, die zu den in Artikel 6 Absatz 2 der Richtlinie 2002/58/EG genannten Zwecken von den Diensteanbietern bereits erhoben und gespeichert wurden („Zwecke der Gebührenabrechnung und der Bezahlung von Zusammenschaltungen“).[4]

In Anbetracht dieser Erkenntnisse ist daran zu erinnern, dass die Bestimmungen vorstehender Artikel von den Mitgliedstaaten restriktiv anzuwenden sind – d. h., die Mitgliedstaaten können innerstaatliches Recht zur Durchführung dieser Richtlinie nur insofern erlassen, als dieses Recht mit den Anforderungen der Richtlinie über die Vorratsspeicherung von Daten vollkommen in Einklang steht.

---

[4] Die *Stellungnahme 1/2003 zur Speicherung von Verkehrsdaten zu Zwecken der Gebührenabrechnung, angenommen am 29. Januar 2003* - WP29 – gab eine Richtschnur für die Harmonisierung des Speicherzeitraums vor, in dem Verkehrsdaten rechtmäßig zu Zwecken der Gebührenabrechnung verarbeitet werden dürfen. Die Speicherung zu Zwecken der Gebührenabrechnung sollte normalerweise eine Speicherzeit von 3-6 Monaten nicht überschreiten. Verarbeitet werden dürfen nur die Verkehrsdaten, die in Bezug auf die Zwecke der Gebührenabrechnung und der Bezahlung der Zusammenschaltungen angemessen, zutreffend und nicht überzogen sind. Alle anderen Verkehrsdaten müssen gelöscht oder anonymisiert werden.

Alle Praktiken, die nicht diesen Grundsätzen entsprechen und die nicht aufgrund von Rechtsvorschriften gemäß Artikel 15 der Richtlinie 2002/58/EG eindeutig zulässig sind, sind auf ersten Anschein mit den Anforderungen des Datenschutzrechts der EU unvereinbar.

Es ist darauf hinzuweisen, dass jeder Mitgliedstaat aufgrund der Richtlinie über die Vorratsspeicherung von Daten eine öffentliche Stelle zu benennen hat, die für die Kontrolle der Anwendung der Bestimmungen der Richtlinien 95/46/EG und 2002/58/EG sowie der in Artikel 7 der Richtlinie über die Vorratsspeicherung von Daten aufgeführten Datenschutz- und Datensicherheitsmaßnahmen zuständig ist. Die in Artikel 7 genannten Sicherheitsmaßnahmen sind als von jedem Mitgliedstaat zu gewährleistendes Mindestniveau anzusehen. Von Bedeutung ist auch, dass Artikel 9 der Richtlinie über die Vorratsspeicherung von Daten ausdrücklich festlegt, dass die bestreffenden öffentlichen Stellen auch die entsprechenden nationalen Datenschutzbehörden sein können und ihre Kontrolltätigkeiten in völliger Unabhängigkeit wahrnehmen.

Zusätzlich bestimmt die Richtlinie über die Vorratsspeicherung von Daten, dass die Kommission dem Europäischen Parlament und dem Rat spätestens am 15. September 2010 eine Bewertung der Anwendung dieser Richtlinie sowie ihrer Auswirkungen vorzulegen hat, um festzustellen, ob die Bestimmungen dieser Richtlinie insbesondere in Bezug auf die Kategorien von Daten und die Speicherungsfristen gegebenenfalls geändert werden müssen. Bei dieser Bewertung sollte die Kommission die von den Mitgliedstaaten und der Artikel-29-Datenschutzgruppe vorgebrachten Bemerkungen berücksichtigen, wie auch die Statistik über die Vorratsspeicherung von Daten, die die Mitgliedstaaten der Kommission jährlich gemäß Artikel 10 dieser Richtlinie zu übermitteln haben. Aus dieser Statistik muss insbesondere hervorgehen, in welchen Fällen Daten an die gesetzlich ermächtigten Behörden weitergegeben wurden, wie viel Zeit zwischen dem Zeitpunkt der Vorratsspeicherung der Daten und dem Zeitpunkt, zu dem sie von der gesetzlich ermächtigten Behörde angefordert wurden, vergangen ist, und in welchen Fällen die Anfragen nach Daten ergebnislos geblieben sind.

Wie bereits angemerkt, hatten zum Zeitpunkt der Erstellung dieses Berichts noch nicht alle Mitgliedstaaten die Richtlinie über die Vorratsspeicherung von Daten umgesetzt. In einigen Mitgliedstaaten (Deutschland, Rumänien) haben die Verfassungsgerichte bzw. die Obersten Gerichtshöfe entschieden, dass die betreffenden Rechts- und Verwaltungsvorschriften zur Umsetzung der Richtlinie in einzelstaatliches Recht verfassungsrechtliche Grundsätze verletzten.

III. Durchsetzungsmaßnahme

A. Grundlagen

Die Durchsetzungsmaßnahme diente dem Zweck, zu bewerten, wie die Diensteanbieter von elektronischer Kommunikation und die Internet-Diensteanbieter die Verpflichtungen umgesetzt haben, die ihnen aus der Richtlinie über die Vorratsspeicherung von Daten in Bezug auf die Kategorien von auf Vorrat zu speichernden Verkehrsdaten (Artikel 5), Speicherungsfristen (Artikel 6) und technische und organisatorische Sicherheitsmaßnahmen (Artikel 7) erwachsen. In den Mitgliedstaaten, die diese Richtlinie noch nicht in innerstaatliches Recht umgesetzt hatten, fanden die den vorgenannten Anbietern durch das einschlägige nationale Recht aufgrund der Datenschutzrichtlinie für elektronische Kommunikation (Richtlinie 2002/58/EG) auferlegten Pflichten Berücksichtigung, so insbesondere in Bezug auf deren Artikel 6 und 9. Bezug genommen wurde auch auf die in der Stellungnahme 3/2006 (WP 119) vorgeschlagenen Mindestschutzvorkehrungen.

Nach den Richtlinien 2006/24/EG und 2002/58/EG muss die Sicherheit personenbezogener Daten in einem angemessenen Verhältnis zu den Risiken stehen, die aus der Verarbeitung solcher Daten und der Merkmale solcher Daten erwachsen. Unter diesem Gesichtspunkt ist nicht zu bestreiten, dass die Durchführung der Richtlinie über die Vorratsspeicherung von Daten wegen der Beschaffenheit der Verkehrsdaten spezielle Risiken für die betroffenen Personen mit sich bringt. Aus diesem Grund stellte die von den Mitgliedern der Artikel-29-Datenschutzgruppe durchgeführte Erhebung spezieller darauf ab, konkrete Informationen zu diesen Risiken zusammenzutragen, anhand derer zu untersuchen ist, ob die bei früheren Gelegenheiten von der Datenschutzgruppe vorgebrachten Bedenken nach wie vor Bestand haben.

Es wurde bereits angemerkt, dass verfügbare Verkehrsdaten Aufschluss über Auffassungen, Meinungen und Vorlieben geben können und die Verfügbarkeit dieser Daten dementsprechend einen Eingriff in das Privatleben der Benutzer darstellen und sich ganz erheblich auf die Vertraulichkeit der Kommunikation und die Grundrechte, wie das Recht auf freie Meinungsäußerung, auswirken kann. Diese Szenarien können leider eintreten, und zwar sowohl aufgrund absichtlicher Aktivitäten als auch wegen fahrlässig angewandter Mechanismen bei der Vorratsspeicherung der Daten. Die unbefugte Weitergabe von bzw. der unbefugte Zugriff auf Informationen, die mit elektronischer Kommunikation zusammenhängen – und die unter Umständen mit Standortdaten verbunden sind – kann die Privatsphäre der betroffenen Personen erheblich beeinträchtigen. Angesichts der vorstehend beschriebenen Umstände ist die Durchführung der Richtlinie über die Vorratsspeicherung von Daten durch die Anbieter von elektronischen Kommunikationsdiensten und von Internetdiensten naturgemäß mit einem hohen Maß an Risiko verbunden, so dass geeignete technische und organisatorische Sicherheitsmaßnahmen unbedingt erforderlich sind.

Was die Risiken anbelangt, so ist daran zu erinnern, dass die Richtlinie die Vorratsspeicherung von Daten verbietet, die mit dem Inhalt einer Kommunikation im Zusammenhang stehen; auf der Grundlage des Gesamtbildes (z. B. von Verhaltensprofilen einzelner Benutzer), das aus ihren sozialen Interaktionen hergeleitet werden kann, ermöglicht ferner schon die bloße Verfügbarkeit von Verkehrsdaten (d. h. solchen im Sinne von Artikel 5 der Richtlinie) die Rückverfolgung von mehreren Einzelfaktoren personenbezogener Informationen (einschließlich sensibler Informationen) in Bezug auf die jeweils betroffenen Personen. Diese Informationen lassen sich in einen räumlichen und zeitlichen Zusammenhang bringen und mithilfe von Datenschürfungsinstrumenten dank leistungsfähiger EDV-Systeme, die heute über Server und Personal Computer zur Verfügung stehen, in großer Detailgenauigkeit kategorisieren. Diese Techniken erweisen sich als besonders wirksam bei umfangreichen Mengen an Verkehrsdaten, die eine große Zeitspanne abdecken. Im Unterschied zu den Verkehrsdaten beim Telefonfestnetz und Mobilfernsprechen können bei internetgestützten Diensten weitere Risiken auftreten, weil gewisse Informationen, wie z. B. die IP-Adresse des Adressaten, den jeweiligen Inhalt von selbst preisgeben können; wie auch Hinweise zur sozialen Stellung, ja sie können sogar Informationen über die ganz persönlichen Vorlieben der betroffenen Personen an den Tag bringen. Eines der Ziele dieser Durchsetzungsmaßnahme bestand folglich in der Bewertung, inwieweit sich die Anbieter von elektronischer Kommunikation und von Internetdiensten der spezifischen Risiken bewusst sind und die eingeführten Sicherheitsmaßnahmen zur Vermeidung dieser Risiken auch tatsächlich erfüllen.

B. Methode und Arbeitsschritte

Die Untersuchung wurde von den Datenschutzbehörden folgender Staaten durchgeführt: *Belgien, Bulgarien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Irland, Italien, Lettland, Liechtenstein, Litauen, Luxemburg, Malta, Niederlande, Polen, Rumänien, Slowakei, Slowenien, Spanien, Tschechische Republik, Ungarn, Vereinigtes Königreich, Zypern.* Bemerkungen zu den Untersuchungsergebnissen wurden auch von der Schwedischen Agentur für Post und Telekommunikation sowie von der Europäischen Kommission übermittelt.

Aufgrund der Erfahrungen bei der ersten Durchsetzungsmaßnahme und angesichts der Vorschläge im Abschlussbericht dieser Maßnahme beschloss die Artikel-29-Datenschutzgruppe, die zweite Durchsetzungsmaßnahme solle aus zwei Arbeitsschritten bestehen – nämlich der Ausgabe eines Fragenkatalogs, gefolgt von der Auswertung der Antworten der einzelnen Datenschutzbehörden, so auch im Rahmen von Inspektionen vor Ort.

So wurde anhand eines Standardbegleitschreibens ein Standardfragenkatalog (den die Datenschutzgruppe im Dezember 2008 angenommen hatte) an alle in den einzelnen Mitgliedstaaten dafür ausgewählten Anbieter von elektronischen Kommunikationsdiensten und von Internetdiensten ausgegeben. Um die erheblichen nationalen Marktanteile abzudecken, beruhte die Auswahl der damit untersuchten Unternehmen auf folgenden Kriterien: relevanter Markt (Festnetzfernsprechen gegen Mobilfernsprechen, konvergente Betreiber, reine Internet-Diensteanbieter), Unternehmensgröße (kleine Diensteanbieter und große Telekommunikationsbetreiber).

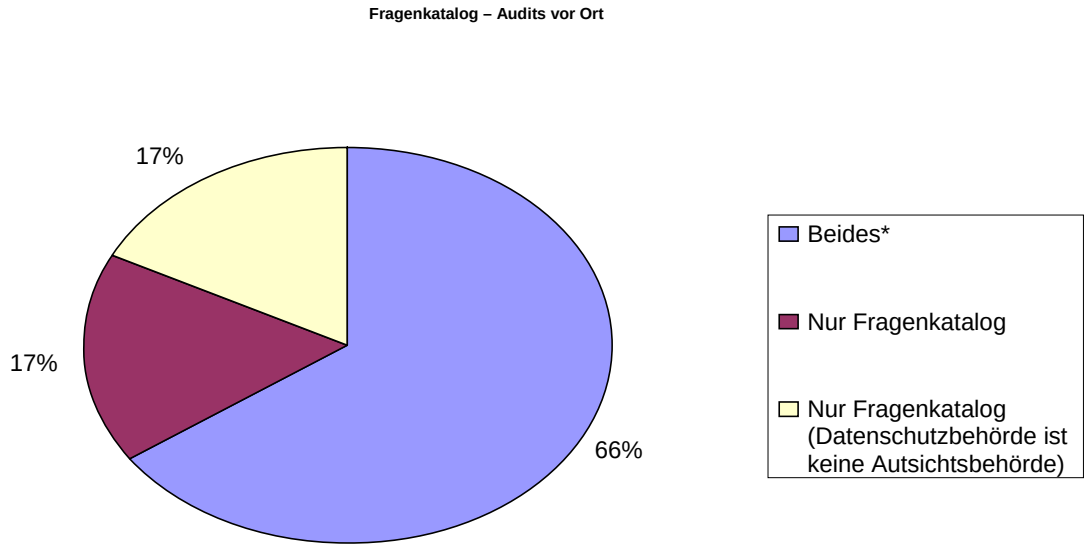
Der Fragenkatalog umfasste 10 Abschnitte zu folgenden Punkten: Art der auf Vorrat gespeicherten Daten, Speicherungsfristen, zu Zwecken der Vorratsspeicherung angewandte technologische Lösungen und außerdem noch besonders wichtige Fragen unter dem Gesichtspunkt der Vorratsspeicherung von Daten (z. B. IT-Sicherheit, logische Zugriffskontrolle, Authentifizierung/Ermächtigung, Zugriffsprotokolle (Logs), Verschlüsselung, Datenweitergabe/Übertragungsprotokolle, physische Schutzmaßnahmen, Sicherungskopie (Back-up)/Datenwiederherstellung bei Systemabsturz). Unter Berücksichtigung der nach der ersten Durchsetzungsmaßnahme berichteten Problempunkte wurde die Anzahl der Fragen gering gehalten und die inhaltliche Fragestellung so klar und bestimmt wie nur möglich formuliert und auch an den für die Antwortgeber geltenden Auswahlkriterien ausgerichtet.

Wann immer es von den Datenschutzbehörden für erforderlich gehalten und kraft der ihnen nach nationalem Recht übertragenen Inspektionsbefugnisse gestattet war, wurden Inspektionen vor Ort durchgeführt, sofern dafür erfahrenes Personal zur Verfügung stand. Solche Inspektionen dienten der Beurteilung der Zuverlässigkeit der Antworten auf den Fragenkatalog und der Beschaffung von noch ausführlicheren Informationen über die Angelegenheiten der Durchführung und erwiesen sich als grundlegend für die Bewertung der Befolgung der einschlägigen Rechtsvorschriften durch die für die Verarbeitung von Daten Verantwortlichen.

Zur Bestandsaufnahme der jeweiligen Situation und der wichtigsten Kritikpunkte wurde danach von jeder der teilnehmenden Datenschutzbehörden ein nationaler Bericht erstellt.

Anhang 1 zu diesem Bericht enthält eine Tabelle mit der Zusammenfassung der von den beteiligten Datenschutzbehörden bereitgestellten Informationen.

Das nachstehende Diagramm zeigt den statistischen Verteilerschlüssel in Bezug auf die Datenschutzbehörden, die die Inspektionen vor Ort vornahmen, im Vergleich zu denen, die den Fragenkatalog ausgaben, und denen, die nicht über die erforderlichen Durchsetzungsbefugnisse verfügen.



C. Schlussfolgerungen[5]

Die Antworten auf den Fragenkatalog brachten ganz allgemein gesagt ein Flickwerk an Durchführungsmaßnahmen an den Tag, so insbesondere im Hinblick auf die vorhandenen Sicherheitsmaßnahmen (siehe Anhang 1, Spalten P und Q). Nur durch gründliche Inspektionen vor Ort war es möglich, festzustellen, dass einige der Antworten unrichtig bzw. ungenau waren, was zur Verhängung von Ad-hoc-Sanktionen und zur Auferlegung von spezifischen technischen und organisatorischen Maßnahmen führte.

Unter Berücksichtigung des unterschiedlichen Informationswertes, den Inspektionen im Vergleich zu einem Fragenkatalog haben, sollten sich besonders die zur Durchführung von Inspektionen befugten Datenschutzbehörden von den inhärenten Risiken einer allgemeinen Pflicht zur Vorratsspeicherung von Verkehrsdaten überzeugt zeigen, indem sie Sensibilisierungskampagnen vorschlagen und ihre Kontrolle der betreffenden Systeme in den Geschäftsräumen der Anbieter von elektronischen Kommunikations- und von Internetdiensten bei Bedarf fortsetzen; zusätzlich ist unbedingt dafür zu sorgen, dass die Durchsetzungstätigkeiten von Datenschutzbehörden nicht durch etwaige Sachzwänge eingeschränkt werden, einschließlich derer im Zusammenhang mit Geschäfts-/ Betriebsgeheimnissen, wenn die besagten Anbieter auf derartige Zwänge vertrauen dürfen, um die angeforderten Informationen nicht weitergeben zu müssen. Daher ist es notwendig,

[5] Für einen ausführlichen Überblick über die einzelstaatlichen Antworten siehe die Tabelle im Anhang I zu diesem Bericht.

den Datenschutzbehörden umfangreiche Durchsetzungsbefugnisse an die Hand zu geben, so auch die Befugnis, sich Zugang zu Geschäfts-/Betriebsgeheimnissen zu verschaffen. Andernfalls wird man sich schwerlich ein eigenständiges Bild machen können.

i. Kategorien von auf Vorrat gespeicherten Daten

Was die Kategorien der unter die Vorratsspeicherungspflicht fallenden Verkehrsdaten anbelangt, so stellte sich heraus, dass die von den einzelnen Anbietern von Telefondiensten auf Vorrat gespeicherten Verkehrsdaten (Anhang 1, Spalten I und J) grundsätzlich in Einklang mit den in Artikel 5 der Richtlinie über die Vorratsspeicherung aufgeführten Daten standen. Umgekehrt bestanden einige beträchtliche Unterschiede hinsichtlich der von den Internetdiensten auf Vorrat zu speichernden Verkehrsdaten (Anhang 1, Spalte K).

Bis auf wenige Ausnahmen (es handelt sich insbesondere um einen Fall in einem Mitgliedstaat, in dem festgestellt wurde, dass der Inhalt von SMS-Mitteilungen zur Erleichterung der Tätigkeiten der Sicherheitsdienste über mehrere Monate auf Vorrat gespeichert und zugänglich gemacht wurde), werden in Bezug auf die Telefondienste die zur Identifizierung der Quelle und des Adressaten einer Nachricht benötigten Daten, der Beginn und das Ende der Nachrichtenübermittlung, der von den Benutzern in Anspruch genommene Telefondienst und die dafür eingesetzten Endgeräte ordnungsgemäß auf Vorrat gespeichert. Ein besonderer Grund zur Besorgnis hängt mit der Vorratsspeicherung von Standortdaten zusammen, wenn diese Daten während eines Anrufs oder einer Internetsitzung fortlaufend erhoben werden, und zwar wegen der Rückverfolgbarkeit der Mobilität des Benutzers.

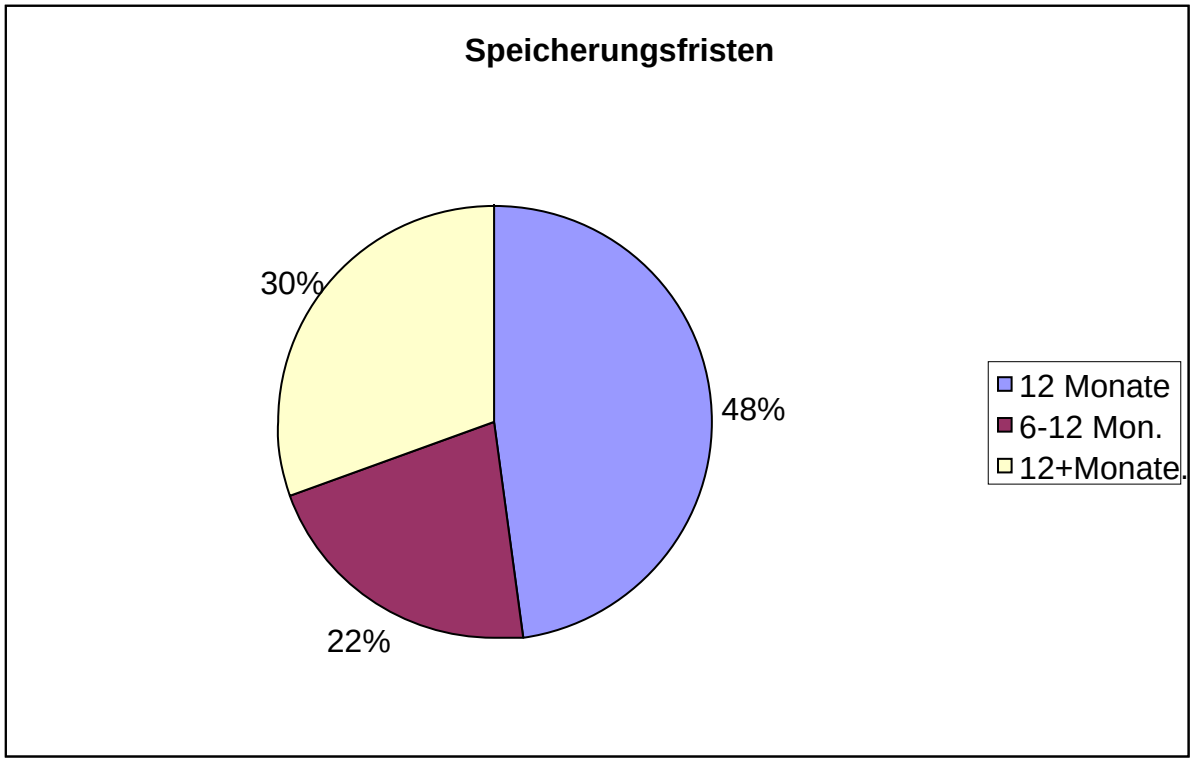
Hinsichtlich der von den Internetdiensten auf Vorrat zu speichernden Verkehrsdaten ist die Lage jedoch anders. Ebenso wie die in Artikel 5 der Richtlinie aufgeführten Kategorien von Daten werden in einigen Fällen außerdem noch zusätzliche Kategorien von Daten auf Vorrat gespeichert, bei denen es um den Inhalt von Kommunikationsvorgängen geht und die dadurch außerhalb des Anwendungsbereichs des geltenden Rechtsrahmens liegen (siehe Anhang 1, Spalte K). In dieser Hinsicht kann auf die IP-Adresse des Adressaten und die URL-Internetadresse von Websites, die Kopfzeilen von E-Mail-Mitteilungen, die Liste aller Empfänger von E-Mail-Mitteilungen im „Cc“-Modus beim Mail-Server des Adressaten und die den Benutzern vom Internet-Diensteanbieter zugeteilte Port-Nummer Bezug genommen werden.

In diesem Zusammenhang ist daran zu erinnern, dass die Richtlinie 2006/24/EG eine Ausnahmeregelung von den Bestimmungen der Richtlinie 2002/58/EG darstellt und der Katalog der zwingend auf Vorrat zu speichernden Verkehrsdaten als erschöpfend anzusehen ist – d. h., den Diensteanbietern auf der Grundlage der Richtlinie über die Vorratsspeicherung von Daten keine zusätzlichen Pflichten zur Vorratsdatenspeicherung auferlegt werden dürfen.

Andererseits ist sich die Artikel-29-Datenschutzgruppe der Streitfragen im Zusammenhang mit einer möglichen Erweiterung des Anwendungsbereichs der Richtlinie über die Vorratsspeicherung von Daten nach innerstaatlichem Recht bewusst – so insbesondere, ob die gesetzlich ermächtigten Behörden nur die Verkehrsdaten zusammentragen dürfen, deren Vorratsspeicherung den Diensteanbietern nach Artikel 6 Absatz 2 der Richtlinie 2002/58/EG gestattet ist, oder auch zusätzliche Verkehrsdaten, die nicht in den einschlägigen Bestimmungen der Richtlinie 2002/58/EG genannt sind.

ii. Speicherungsfristen

Zu Zwecken dieser Analyse und aufgrund der Ergebnisse der Durchsetzungsmaßnahme wurde die für die Vorratsdatenspeicherung mögliche Zeitspanne (6 bis 24 Monate) in drei etwaige Zeitkomplexe unterteilt, nämlich in eine Vorratsdatenspeicherung von a) 12 Monaten; b) unter 12 Monaten und c) über 12 Monaten. Es zeigte sich, dass 48% der Antwortgeber die Daten für einen Zeitraum von 12 Monaten auf Vorrat speicherten, bei immerhin vergleichsweise hohen Prozentsätzen von 22% für "frische Daten" (Gruppe b)) und von 30% für "reife Daten" (Gruppe c)). Das nachstehende Diagramm zeigt die entsprechende prozentuale Verteilung für die EU-Mitgliedstaaten:



Die von den jeweiligen nationalen Gesetzgebern in Umsetzung der Richtlinie über die Vorratsspeicherung von Daten festgelegten Speicherungsfristen weisen von Mitgliedstaat zu Mitgliedstaat erhebliche Abweichungen auf (siehe Anhang 1, Spalten L, M, N), obwohl sich in vielen Ländern (siehe nachstehendes Diagramm) ein kürzerer Zeitraum als die erlaubte Höchstfrist als bevorzugte Praxis erwies, was nahelegt, dass sich die in der Richtlinie festgelegte Spanne des Speicherungszeitraums noch weiter angleichen lässt.

Dazu ***sollte vorzugsweise in Betracht gezogen werden, die Höchstfrist für die Vorratsspeicherung zu verkürzen und eine einheitliche, kürzere Frist zu setzen, die von allen Diensteanbietern in der gesamten EU einzuhalten ist, wie die Artikel-29-Datenschutzgruppe bereits in ihrer Stellungnahme WP113 dargelegt hat[6].***

[6] WP 113: „In jedem Fall muss eine allgemeine Aufbewahrungsfrist klar geregelt werden. Sie sollte möglichst kurz sein und weitestgehend mit der Aufbewahrungsfrist übereinstimmen, die für die ursprünglichen Zwecke gilt, zu denen die Daten von den Kommunikationsdiensteanbietern aufgezeichnet werden."

Den Schlussfolgerungen dieser Durchsetzungsmaßnahme zufolge erfüllten die per Fragenkatalog kontaktierten und/oder inspizierten/kontrollierten Diensteanbieter die oben angeführten Vorratsspeicherungspflichten. In sehr wenigen Fällen erwies sich die De-facto-Situation jedoch als unterschiedlich, und zwar wegen der unterschiedlichen Speicherungspraktiken und/oder –pflichten, die für Verkehrsdaten zu gewerblichen/kommerziellen Zwecken gelten, wodurch solche Daten in der Tat für längere Zeiträume gespeichert werden als die in der Richtlinie geregelten Daten. In einigen Fällen erstrecken sich solche Zeiträume über bis zu 36 Monate, und in einem Fall wurde sogar ein Speicherungszeitraum von insgesamt 10 Jahren festgestellt.

Darüber hinaus wurde festgestellt, dass bei Ablauf der jeweiligen Speicherungsfristen in vielen Fällen keine automatisierten Datenlöschungsverfahren existieren. Diesbezüglich muss daran erinnert werden, dass der Einsatz von manuellen bzw. von Menschenhand eingeleiteten Verfahren nicht als mit der Richtlinie über die Vorratsspeicherung von Daten in Einklang stehend anzusehen ist, da er eine Verlängerung der Speicherungsfristen auf eine unbestimmte Zeitspanne möglich macht, die vom Ablauf der betreffenden Speicherungsfrist bis zum Start des manuellen Löschungsverfahrens reicht.
Automatisierte Verfahren sind auch für die Erstellung von Sicherungskopien (Back-ups) anzuwenden.

Diesbezüglich ist auch darauf hinzuweisen, dass die Anbieter von elektronischen Kommunikations- und von Internetdiensten die Verkehrsdaten in mehreren Systemen speichern und diese Daten dann für vielfältige operative und verwaltungstechnische Zwecke nutzen, die in einigen Fällen aufgrund von Rechtsvorschriften vorgegeben sowie im Rahmen von Dienstgütevereinbarungen und Dienstleistungsverträgen geregelt sind. Ferner wurden alle Verkehrsdaten, die in für die gesetzlich ermächtigten Behörden zugänglichen Systemen gespeichert sind, in der Tat schon vorher auch in anderen Systemen gespeichert; diese Systeme gewährten zu verschiedenartigen Zwecken Zugang, so z. B. zur Problem-/ Konfliktlösung, Betrugsaufdeckung, Gebührenabrechnung usw. durch verschiedene Arbeitseinheiten in der Organisation des Diensteanbieters, die ganz häufig auch weniger strengen Kontrollen unterlagen.

Daher ist mit Nachdruck auf die Notwendigkeit hinzuweisen, dass die Kommission und die anderen Institutionen, die für die Bewertung der Funktionsfähigkeit der Richtlinie über die Vorratsspeicherung von Daten zuständig sind, die umfassende Empfindlichkeit von Verkehrsdaten an sich berücksichtigen und deren gesamte Sicherheitslage neu überdenken, und zwar unabhängig davon, ob diese Daten in anderen Systemen und zu anderen Zwecken als den in der Richtlinie bestimmten gespeichert werden – und dies schon im Hinblick auf die Gesamtbewertung der Durchführung dieser Richtlinie. Lässt man bei den Systemen mit den Kategorien von Verkehrsdaten, die in der Richtlinie aufgeführt sind, andere Sicherheitsniveaus und Speicherungsfristen zu als bei den Systemen mit den Verkehrsdaten, die für andere, unternehmensbezogene Zwecke genutzt werden, so bedeutet dies insgesamt eine Absenkung der Sicherheit der Verkehrsdaten und letztendlich das Scheitern, die in der Richtlinie festgelegten Anforderungen zu erfüllen – d. h., Verkehrsdaten nur für begrenzte Zeiträume auf Vorrat zu speichern und nur aufgrund von spezifischen Sachzwängen zugänglich zu machen.

iii. Technische und organisatorische Sicherheitsmaßnahmen

Artikel 7 Buchstabe b) der Richtlinie über die Vorratsspeicherung von Daten verlangt, die Verkehrsdaten derart auf Vorrat zu speichern, dass geeignete technische und organisatorische Maßnahmen vorhanden sind, um das Risiko der zufälligen oder unrechtmäßigen und/oder unberechtigten Zerstörung oder der Änderung der Daten und ferner das Risiko der unberechtigten Zugänglichmachung und/oder Verarbeitung möglichst gering zu halten.
Die Richtlinieverlangt keine zusätzlichen Sicherheitsmaßnahmen zur Aufstockung derer nach der Richtlinie 2002/58/EG und der Richtlinie 95/46/EG. Wie bereits in den oben angeführten Stellungnahmen der Artikel-29-Datenschutzgruppe herausgestellt wurde, ist jedoch zu bedenken, dass es das mit den Verkehrsdaten an sich zusammenhängende Risikoniveau ist, das unter Berücksichtigung der Art und Beschaffenheit dieser Daten, der Menge der gespeicherten Daten und der Speicherungsfristen den Auftrag zur Anwendung strenger, risikogewichteter Sicherheitsstandards begründet.
In diesem Zusammenhang hat die Durchsetzungsmaßnahme gezeigt, dass die technischen und organisatorischen Sicherheitsmaßnahme die von den Anbietern von elektronischen Kommunikations- und von Internetdiensten durchgeführt werden, deren Bewusstsein in Bezug auf das/die Risiko/Risiken widerspiegeln, das/die mit den Verkehrsdaten von Telefonnetzen und Internet verbunden ist/sind. Wenn keine ausführlichen Beratungen/Hilfestellungen gegeben oder die lauernden Risken unterschätzt werden, besteht eine große Wahrscheinlichkeit, dass unzulängliche Maßnahmen ergriffen werden.

Um die Anforderungen der Richtlinie über die Vorratsspeicherung von Daten zu erfüllen, sollten die Anbieter von elektronischen Kommunikations- und von Internetdiensten die mit Verkehrsdaten verbundenen Risiken regelmäßig und möglichst objektiv bewerten, damit sie alle relevanten Risikofaktoren und deren mögliche Auswirkungen feststellen können, und dabei der Zugriffskontrolle und der Verfügbarkeit von Daten besondere Aufmerksamkeit widmen. Regelmäßige externe Audits dürften einen Beitrag zu einer unabhängigen und objektiven Risikobewertung leisten.

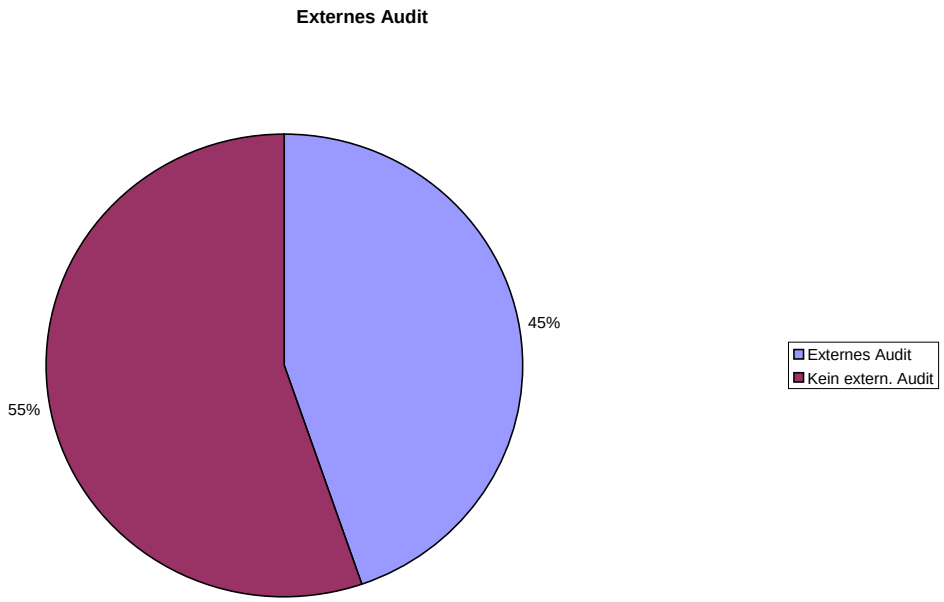
Hinsichtlich der Informationssicherheit wurde bei der Durchsetzungsmaßnahme kein homogenes Bild vorgefunden; aufgrund der Antworten auf den Fragenkatalog (siehe Anhang 1, Spalten P und Q) wie auch der Inspektionen vor Ort kann in der Tat die Aussage getroffen werden, dass die Sicherheitsmaßnahmen je nach der Betriebsgröße der Diensteanbieter unterschiedlich umfangreich ausfallen.

Ein hohes Sicherheitsniveau war in Bezug auf die physischen Zugriffskontrollen bei den Systemen zur Vorratsspeicherung von Verkehrsdaten zu finden (siehe Anhang 1,Spalte Q). Von geringfügigen Unterschieden abgesehen, bauen die meisten Anbieter von elektronischen Kommunikations- und von Internetdiensten auf die Videoüberwachung, spezialisiertes Überwachungspersonal, Zugriffskontrollsysteme und notfallgetriggerte Eskalationsverfahren, um die kontinuierliche Überwachung besagter Systeme sicherzustellen.

Während größere Diensteanbieter tatsächlich technische und organisatorische Maßnahmen einsetzen, die ein angemessenes Sicherheitsniveau für die auf Vorrat gespeicherten Verkehrsdaten sicherstellen können, dürften kleinere Anbieter sich nur geringere Sicherheitsstandards leisten können; und in der Tat sind die meisten von ihnen – vor allem wegen Kostendämpfungsstrategien – nicht in der Lage, Spitzen-IT-Sicherheitslösungen einzusetzen, die die Verkehrsdaten mit dem gleichen Maß an Komplexität schützen wie bei den Marktführern üblich. In letzterem Fall können sich die Aufgaben, die dem die

betreffenden personenbezogenen Daten verarbeitenden Personal anvertraut wurden, überschneiden, wodurch einige Angehörige des Personals Zugang zu verschiedenen Systemen haben, die Verkehrsdaten zu unterschiedlichen Zwecken speichern. Nicht alle Systeme, die Verkehrsdaten zu kommerziellen Zwecken verarbeiten, wurden so konzipiert und/oder in die Praxis umgesetzt, dass man dabei immer die Notwendigkeit im Auge behielt, ein angemessenes Sicherheitsniveau für die Verkehrsdaten zu gewährleisten. Für die Risiken, die mit der Vorratsspeicherung von Verkehrsdaten verbunden sind, scheint es keinerlei Standardbewusstsein zu geben.

Was insbesondere die Vorlaufphase der Risikoabschätzung anbelangt, wurde herausgefunden, dass es sich dabei um eine Aufgabe handelt, die in der Regel innerbetrieblich bei der betreffenden Gesellschaft ausgeführt wird – was unter Umständen Parteilichkeit und Voreingenommenheit begünstigt und das Risiko mit sich bringt, Anfälligkeiten und Schwachstellen zu unterschätzen. Das nachstehende Diagramm zeigt die jeweiligen Prozentsätze in Bezug auf die Diensteanbieter, die auf externe Audits und/oder Sicherheitszertifizierung durch unparteiische Dritte setzen, im Verhältnis zur Gesamtzahl der in Betracht kommenden Diensteanbieter.



Die Verkehrsdaten sind von Natur aus als sehr sensible Daten anzusehen. Sie müssen daher in einer Art und Weise behandelt werden, die der der in Artikel 8 der Richtlinie 95/46/EG aufgeführten besonderen Kategorien personenbezogener Daten vergleichbar ist. Die Vorratsspeicherung dieser Daten sollte nicht nur ihrer sensiblen Natur angepasst werden, sondern hinsichtlich ihrer Zugänglichkeit durch und ihrer Weiterübermittlung an die gesetzlich ermächtigten Behörden bedarf es auch noch zusätzlicher Aufmerksamkeit. Um sicherzustellen, dass diese auch gewährt wird, müssen die Voraussetzungen für die Zugänglichkeit und die Weiterübermittlung der auf Vorrat gespeicherten Daten gesetzlich klar umrissen werden. Die Richtlinie über die Vorratsspeicherung von Daten ist ein Rechtsinstrument, das in den Jahren vor Inkrafttreten des Lissabon-Vertrags im Rahmen einer anderen Aufteilung der Rechtszuständigkeiten ausgearbeitet wurde und enthält keine besonderen Regelungen zu diesem Punkt – obwohl die Datenschutzgruppe die Ausarbeitung derartiger Regelungen gefordert hatte. Ferner lässt sich anführen, dass eine Selbstregulierung in diesem Zusammenhang nicht ausreichend wäre, und zwar hauptsächlich wegen des ungleichen Kräfteverhältnisses zwischen den Diensteanbietern auf der einen Seite und den gesetzlich ermächtigten Behörden auf der anderen Seite. Die Diensteanbieter sind nicht in der Lage, ihre eigenen Sicherheitsmaßnahmen im Umgang mit den gesetzlich ermächtigten Behörden ‚durchzudrücken'.

Zusätzlich zu einigen derzeit praktizierten Sicherheitsmaßnahmen können noch weitere Maßnahmen vorgeschlagen werden, die man in vollkommener Übereinstimmung mit dem Grundsatz der Technologieneutralität ergreifen kann, um gemäß Artikel 7 Buchstabe c) der Richtlinie über die Vorratsspeicherung von Daten sicherzustellen, dass der Zugang zu den betreffenden Daten ausschließlich ordnungsgemäß ermächtigtem Personal vorbehalten ist; derzeit ergreifen indes nicht alle infrage kommenden Diensteanbieter diese Maßnahmen:

- ***Strenge Kontrolle des Zugriffs auf die auf Vorrat gespeicherten Daten im Rahmen der Festlegung von Benutzerpflichten und Benutzerprofilen mit unterschiedlichen Benutzerberechtigungen;***
- ***strenge Authentifizierung für den Zugang zum betreffenden System, basierend auf doppelten Authentifizierungsmechanismen (d. h. Passwort + biometrischen Daten oder Passwort + Token), um die körperliche Anwesenheit der für die Verarbeitung der Verkehrsdaten verantwortlichen Person sicherzustellen;***
- ***detailgenaue Rückverfolgung der Arbeitsgänge bei Zugriff und Verarbeitung im Wege der Log-Vorratsspeicherung mithilfe von Zugriffsprotokollen (Logs), die zumindest die Benutzeridentität, die Zugriffszeit und die vom Zugriff betroffene Datei aufzeichnen;***
- ***Einsatz von Log-Management-Lösungen zur Gewährleistung der Log-Integrität mithilfe von Verschlüsselungstechnologie oder Maßnahmen, die ein gleichwertiges Schutzniveau bieten;***
- ***logische Trennung von anderen Systemen, die Verkehrsdaten zu kommerziellen Zwecken verarbeiten;***
- ***zusätzliche Maßnahmen, die unter Umständen zur Sicherstellung der Vertraulichkeit von Daten nötig sind .***

Unter dem Gesichtspunkt Organisation/Management sollte ferner den Systemadministratoren besondere Bedeutung beigemessen werden, die mit Systemen zu tun haben, in denen Verkehrsdaten zu Zwecken gespeichert werden, die mit der gesetzlich ermächtigten Behörde zusammenhängen; ***die Rollen und Funktionen, die solchen Administratoren zukommen,***

sind in Einzelheiten darzustellen, so auch anhand von Ad-hoc-Berichten, und alle Instandhaltungsaktivitäten, die an solchen Systemen durchgeführt werden, sollten eingehenden Kontrollen unterliegen.

Zur Verbesserung der auf die Verkehrsdaten anzuwendenden Sicherheitsmaßnahmen sind Mehrfachaktionen erforderlich, die gut zu koordinieren sind; ***ihre Durchführung durch die Diensteanbieter kann erleichtert werden, wenn sowohl innerbetriebliche Maßnahmen als auch die eigentlichen technologischen Maßnahmen in ein Sicherheitszertifizierungsprogramm eingebettet werden, das in regelmäßigen Zeitabständen durchzuführen ist – vorzugsweise durch einen externen Dritten und in Übereinstimmung mit den international vereinbarten Standards – um die Robustheit der Maßnahmen zu bewerten, die gegenüber den sich wandelnden Formen von Risiken und Anfälligkeiten/Schwachstellen zum Einsatz kommen. Auch andere Maßnahmen könnten sich als für diesen Zweck tragfähige Lösung erweisen, so z. B., dass man den Datenschutzbehörden die Möglichkeit gibt, Audits selbst durchzuführen, oder den Datenschutzbehörden die Audits Dritter zur Verfügung stellt.***

Die nichthomogene Erfüllung der technischen und organisatorischen Sicherheitspflichten führt zu dem Scheitern, das mit der Richtlinie verfolgte Harmonisierungsziel uneingeschränkt zu erreichen, und wirkt sich auf die Kosten aus, die durch die einzelnen Akteure aufgrund ihrer unterschiedlichen Größe und Marktstellung wie auch der sich verändernden Marktdynamik anfallen, was letztlich zu einer nicht harmonisierten Anwendung der Richtlinie über die Vorratsspeicherung von Daten führt und die EU-Bürger davon abhält, ein gleich hohes Schutzniveau genießen zu können.

Der Fall des Artikel 7 Buchstabe d) der Richtlinie über die Vorrangspeicherung von Daten (abgerufene Daten): Artikel 7 Buchstabe d) dieser Richtlinie sieht eine Ausnahme vor, die für die Vorratsspeicherung der von den gesetzlich ermächtigten Behörden abgerufenen Daten gilt, die *de facto* für einen unbestimmten zusätzlichen Zeitraum gespeichert werden können.

Man könnte überlegen, ob die Anbieter von elektronischen Kommunikations- und von Internetdiensten aufgefordert werden sollten, zusätzliche Sicherheitsmaßnahmen zu entwickeln, die auf diese Kategorie der „abgerufenen Daten“ abstellen, da in der Richtlinie keine speziellen Anforderungen festgelegt sind, ob nun diese Daten später in die betreffenden Falldateien aufgenommen und die anzuwendenden Sicherheitsmaßnahmen den zuständigen Behörden übertragen werden sollten (was der Fall zu sein scheint). An den betreffenden Daten macht sich eine Menge wesentlicher Kritikpunkte fest, auch weil diese Daten wichtige Informationen über die Benutzer preisgeben können (wozu unter Umständen auch sensible Informationen gehören).

Massive Zugriffe auf Verkehrsdaten und eine erweiterte Vorratsspeicherung solcher Daten könnten als Mechanismen zur Umgehung der in der Richtlinie festgelegten Pflichten angesehen werden. ***Die Notwendigkeit, erweiterte Speicherungsfristen für abgerufene Daten ins Auge zu fassen, ist anhand von scharf umrissenen Kriterien zu bewerten, die auf alle Fälle auch die Löschung abgerufener Daten im Lichte der Anforderungen gemäß der Richtlinie 95/46/EG wie auch der internationalen Instrumente (einschließlich der Empfehlung R(87)15 des Europarates) vorsehen sollten.***

iv. Weitergabeverfahren

Die Weitergabeverfahren, die für die von den gesetzlich ermächtigten Behörden angeforderten Verkehrsdaten gelten, wurden als ziemlich inhomogen empfunden. So wurde eine große Bandbreite von Lösungen mitgeteilt und sowohl im Rahmen des Fragenkatalogs als auch bei den Inspektionen vor Ort beschrieben – so auch Weitergabeverfahren auf der Grundlage von handgeschriebenen Dokumenten, Kurierdienst oder Standardpostsendung – außerdem unterschiedliche Niveaus der Übertragungssicherheit, die von der Übermittlung per E-Mail- und/oder Fax-Nachrichten bis hin zur Nutzung von zweckbestimmten, verschlüsselungsgeschützten Übertragungskanälen reichen. ***Auf diesem Gebiet gilt es daher, der Verwirklichung der Harmonisierung durch die Entwicklung von standardisierten Datenweitergabeverfahren für gesetzlich ermächtigte Behörden besondere Bedeutung beizumessen.***

In diesem Zusammenhang ist darauf hinzuweisen, dass die Richtlinie über die Vorratsspeicherung von Daten eine erschöpfende Liste über die Daten enthält, die den gesetzlich ermächtigten Behörden von den Diensteanbietern übermittelt werden dürfen und die eine abschließende Menge von Elementen bilden; ferner sollten die unter die Weitergabe auf Anforderung fallenden schweren Straftaten durch innerstaatliche Gesetze scharf umrissen werden, während die öffentlichen Stellen (Justizbehörden), die ermächtigt sind, den Zugriff auf solche Daten zu genehmigen, oder die speziellen Zugriffsmöglichkeiten kraft Gesetzes eindeutig und erschöpfend geregelt werden sollten.

Ein auf obigen Annahmen basierendes Datenaustauschprotokoll könnte zu einem IT-Standardverfahren weiterentwickelt werden, während dies derzeit dem Ermessen der einzelnen Beteiligten überlassen bleibt – so jedenfalls nach den verfügbaren Informationen. Durch die Festlegung eines Weitergabestandardverfahrens, das auch die Ausrichtung der Datenübermittlung (die auf PUSH-Protokollen basieren sollte) mit berücksichtigt, würden schnellere, zuverlässigere Datenübertragungen ermöglicht und bei allen relevanten Beteiligten (Diensteanbietern und gesetzlich ermächtigten Behörden) niedrigere Kosten anfallen; denn in der Tat könnten Letztere von Standardlösungen profitieren, die auf der Grundlage eines vereinheitlichten Referenzrahmens entworfen und in großem Umfang umgesetzt würden. Diese wären weit entfernt von den derzeit auf dem Markt verfügbaren Lösungen, die beide von ihrer Art her ganz anders und teurer sind.

- Es muss betont werden, dass eine eindeutige Spezifizierung sowohl der Beteiligten als auch der Datensätze, die diese Beteiligten dann austauschen können, das gesamte Sicherheitsniveau des Weitergabeverfahrens erheblich verbessern würde. Dafür lassen sich mehrere Gründe anführen: Die gegenseitige Authentifizierung würde ermöglicht; die Voraussetzungen für die Durchführung von verschlüsselten Verbindungen würden erfüllt und vertrauenswürdige und sichere Kommunikationskanäle auf Verbindungen mit Signaturschlüssel- und digitalen Signatur-Zertifikaten gestützt, was Integrität, Vertraulichkeit und Sende- und Empfangsbeweis von Datenübertragungen sicherstellen würde; die Risiken von Man-in-the-middle-Angriffen – Dazwischenschalten zum Einsehen/Abhören des Kommunikationskanals und zur Aneignung und/oder Vervielfältigung der übermittelten Inhalte– würden erheblich reduziert; alle für effiziente Datenzugriffserfassungen benötigten Instrumente könnten dazugeschaltet werden; die einzelnen Beteiligten könnten die Weitergabeverlangen nach ihrem Zweck und/oder nach der Kategorie der angeforderten Daten kategorisieren, was zur Erleichterung der Erstellung von homogenen statistischen

Berichten in den Mitgliedstaaten vernünftigerweise erwartet werden kann. Wenn sie zum Einsatz kommen, wäre es mit allen diesen Optionen möglich, die Anzahl der unangemessenen Datenzugriffe zu reduzieren und die Datenschutzbehörden in die Lage zu versetzen, Datenzugriffe effizient zu überprüfen. Auch die Justizbehörden sollten in das Weitergabeverfahren mit einbezogen werden, nämlich in ihrer Eigenschaft als vertrauenswürdige staatliche Stellen, die jeweils im Einzelfall entscheiden könnten, welche Daten den gesetzlich ermächtigten Behörden unter welchen Bedingungen bereitgestellt werden dürfen. Der jeweilige Zweck sollte aus einer öffentlich bekannten Liste schwerer Straftaten ausgewählt werden, um das in der Richtlinie für die Verkehrsdaten vorgesehene Datenübermittlungsverfahren getreu widerzuspiegeln.

Aus vorstehend genannten Gründen könnte ein europaweiter Weitergabestandard folgende Punkte umfassen:

- eine einheitliche Anlaufstelle bei jedem Diensteanbieter;
- ein einheitliches Datenweitergabeformat einschließlich zumindest folgender Felder zur Ermöglichung eines sicheren, zuverlässigen Verkehrsdatenaustauschs/-zugriffs unter den Beteiligten:
    - Benutzerdaten mit einer bekannten, abschließenden Anzahl von Feldern in Bezug auf das Abonnement des Kommunikationsdienstes und die den Benutzern zur Verfügung gestellten Endgeräte;
    - Verkehrsdaten mit einer bekannten, abschließenden Anzahl von Feldern in Bezug auf die innerstaatliche Umsetzung der in Artikel 5 der Richtlinie über die Vorratsspeicherung von Daten dargelegte Datenliste;
    - Kenncode des Diensteanbieters mit einer EU-weit einheitlichen ID-Kennung (Identifizierungsnummer) zur Identifizierung des jeweiligen Anbieters von elektronischen Kommunikationsdiensten und/oder Anbieters von Internet-Diensten;
    - Kenncode der gesetzlich ermächtigten Behörde mit einer ID-Kennung (Identifizierungsnummer) zur Identifizierung der jeweiligen zum Zugriff auf Verkehrsdaten ermächtigten Behörde;
    - Kenncode der Justizbehörde mit einer EU-weit einheitlichen ID-Kennung (Identifizierungsnummer) zur Identifizierung der jeweiligen Justizbehörde, die zur Genehmigung des Zugriffs auf die Verkehrsdaten ermächtigt ist;
    - Zeitstempel und Nummer der Datenanforderung zur Identifizierung des Zeitpunktes und der Reihenfolge der Datenzugriffsersuchen wie auch der betreffenden Genehmigungen;
    - Art des Ersuchens zur genauen Angabe der Kategorie der Datenanforderung (z. B. Einordnung nach schwerer Straftat oder nach Anzahl der angeforderten Verkehrsdaten).

Durch die Einführung eines Datenaustauschprotokolls mit den vorstehenden Merkmalen wäre es möglich, einige Kritikpunkte, auf die mehrere Datenschutzbehörden im Laufe dieser Durchsetzungsmaßnahme hingewiesen haben, auf ein Minimum zu reduzieren, so z. B. den Druck, der von den gesetzlich ermächtigten Behörden auf die Diensteanbieter ausgeübt wird, um zusätzliche benutzerbezogene Daten zu erlangen, die nicht in der Richtlinie über die Vorratsspeicherung von Daten aufgeführt sind, die Einreichung von Zugriffsersuchen trotz fehlenden förmlichen Durch-/Haussuchungsbefehls oder die Einreichung von

Zugriffsersuchen durch nicht ermächtigte staatliche Stellen (d. h. durch eine nicht gesetzlich ermächtigte Behörde).

In diesem Zusammenhang ist es angebracht, daran zu erinnern, dass ***der Katalog der schweren Straftaten, die eine Vorratsdatenspeicherung im Rahmen dieser Richtlinie rechtfertigen, auf innerstaatlicher Ebene auf der Grundlage von nationalem Recht erstellt werden sollte, und zwar unter Berücksichtigung der Erwägungen in den Dokumenten WP113 und WP119 hinsichtlich der Notwendigkeit, klar zu umreißen und näher zu bestimmen, was unter „schweren Straftaten" zu verstehen ist. Die erschöpfende Liste der staatlichen Stellen, die zum Zugriff auf die gemäß der einschlägigen Richtlinie auf Vorrat gespeicherten Daten ermächtigt sind, ist allen relevanten Beteiligten bekannt zu gegeben.***

In dieser Hinsicht lohnt noch zu erwähnen, dass das Europäische Institut für Telekommunikationsnormen (ETSI) ein eindrucksvolles Referenzmodell für die Weitergabe von Verkehrsdaten an gesetzlich ermächtigte Behörden erarbeitet hat, das jetzt weiter studiert und evaluiert werden kann..

D. Statistik gemäß Artikel 10 der Richtlinie über die Vorratsspeicherung von Daten

Nach Artikel 10 dieser Richtlinie sorgen die Mitgliedstaaten dafür, dass der Kommission jährlich eine Statistik über die Verwendung der nach den einschlägigen Vorschriften auf Vorrat gespeicherten Verkehrsdaten übermittelt wird. Nach Artikel 14 ist diese Statistik (die von den Mitgliedstaaten zur Verfügung gestellt wird) bei jeglicher Änderung der Richtlinie zu berücksichtigen. Von sehr wenigen Ausnahmen abgesehen, kann nicht bestätigt werden, dass dieser Mitteilungspflicht nachgekommen wurde.

Auch nur wenige Mitgliedstaaten haben die verlangten Informationen zu folgenden Themen vorgelegt: Anzahl der bei Diensteanbietern eingereichten Datenanforderungen; Fälle, in denen die angeforderten Informationen gegeben wurden, und Fälle, in denen der Anbieter nicht in der Lage war, die angeforderten Daten zur Verfügung zu stellen; wie viel Zeit zwischen dem Zeitpunkt der Vorratsspeicherung der Daten und dem Zeitpunkt, zu dem sie von der zuständigen Behörde angefordert wurden, vergangen ist.

Zwar kann die Statistik nach Artikel 10 nicht die einzige Grundlage für die Entscheidung über die Zukunft der Richtlinie über die Vorratsspeicherung von Daten bilden, doch sind die Verfügbarkeit und die angemessene Bewertung der betreffenden Informationen von wesentlicher Bedeutung für die Beurteilung, ob die der Richtlinie zugrunde liegenden Ziele auch erreicht wurden; so z. B. die notwendige Einführung harmonisierter Grundsätze, die für alle EU-Mitgliedstaaten gelten sollen – eine Beurteilung, die zum Teil auch im Lichte der Kritikpunkte geführt werden muss, auf die während der gesamten Diskussion vor ihrer Annahme und auch danach noch aufmerksam gemacht wurde (siehe die Entscheidungen einiger europäischer Verfassungsgerichte und Oberster Gerichtshöfe).

Das Fehlen einer sachgerechten Statistik könnte das gesamte Bewertungsvorhaben behindern, denn hier geht es um eine wichtige Voraussetzung für eine etwaige Änderung der Richtlinie – insbesondere insofern als die Liste der Daten in Artikel 5 und die Speicherungsfristen in Artikel 6 davon betroffen sind.

Die Verwendung einer partiellen und/oder inhomogenen Statistik kann zu Entscheidungen führen, die merkliche Auswirkungen auf die Privatsphäre der betroffenen Personen haben, ohne jedoch einen Unterschied für die mit der Richtlinie verfolgte bessere Harmonisierung zu machen.

Wiederum macht es Sinn, davon auszugehen, dass sich mehrere Hindernisse beseitigen ließen, wenn ein standardisiertes Weitergabeverfahren entwickelt würde. Angesichts der Verfügbarkeit spezieller Regeln für die Datenweitergabe könnte jeder Akteur eine Statistik erstellen, die mit den Statistiken der übrigen Akteure kohärent wäre – was einen besseren, und zuverlässigen Überblick über die Verwendung und die Leistungsfähigkeit von Verkehrsdaten bei der Verfolgung von „schweren Straftaten" möglich machte.

Im Hinblick auf die erste Bewertung der Durchführung der Richtlinie 2006/24/EG, die die Kommission bis 15. September 2010 vorzunehmen hat, ist es für jeden einzelnen Mitgliedstaat, der die Richtlinie durchgeführt hat, von wesentlicher Bedeutung, die erforderliche Statistik beizubringen. Die Artikel-29-Datenschutzgruppe hält es für absolut notwendig, dass diese Informationen bereitgestellt werden, um objektiv dabei zu helfen, die Notwendigkeit und Wirksamkeit der Richtlinie über die Vorratsspeicherung von Daten unter Beweis zu stellen.

Darüber hinaus ist es auch wesentlich, dass diese Statistik von Informationen über die von den betreffenden Daten ausgelösten Auswirkungen begleitet wird, und zwar aufgegliedert nach dem Alter der Daten zum Thema Behandlung schwerer Straftaten.

E. Outsourcing-Angelegenheiten

Bei dieser Durchsetzungsmaßnahme wurde herausgefunden, dass man sich zur Durchführung verschiedener Tätigkeiten im Zusammenhang mit der Vorratsspeicherung von Verkehrsdaten mehr und mehr des Outsourcings bedient. – so insbesondere, was kleinere Betreiber betrifft, die eine Politik der Kostendämpfung betreiben. Nicht immer geht diese Praxis Hand in Hand mit der genauen Definition der jeweiligen Rolle, so insbesondere was die Befolgung des innerstaatlichen Datenschutzrechts und die Bestellung von Auftragsverarbeitern und/oder die Zuteilung von Verarbeitungsaufgaben an das zuständige Personal anbelangt.

Bekanntlich setzt sich der Markt für elektronische Kommunikationsnetze und –dienste aus einer Vielfalt von Einheiten zusammen, die auf auffällig unterschiedliche menschliche und finanzielle Ressourcen zählen können; dies ist ein eindeutiges Hindernis für die Erreichung des von der Richtlinie über die Vorratsspeicherung von Daten verfolgten Harmonisierungsziels. Beispielsweise wurde herausgefunden, dass die Unternehmensgröße der Einheit, die die Daten auf Vorrat speichert, in einigen Fällen merklich größer war als die Einheit des Anbieters von elektronischen Kommunikationsdiensten – was es für Letzteren, also für den für die Verarbeitung Verantwortlichen, offensichtlich schwer macht, die Verarbeitungsvorgänge, die vom ‚Outgesourcten' vorgenommen werden, sorgfältig zu überwachen. Zusätzliche Kritikpunkte tauchen dann auf, wenn die Verkehrsdaten außerhalb der Inlandsgrenzen auf Vorrat gespeichert werden, was nicht so ganz unüblich ist (siehe nachstehendes Diagramm), auch wenn sich dies meist auf einige große Akteure beschränkt, die in kleineren Mitgliedstaaten arbeiten und sich der Dienste bedienen, die am Hauptsitz des jeweiligen Unternehmens geleistet werden.. Dabei handelt es sich um eine Option, auf die auch kleinere Diensteanbieter und/oder virtuelle Betreiber setzen, die auf die Dienste multinationaler Gesellschaften zurückgreifen, die auf IT-Lösungen spezialisiert sind. Bei

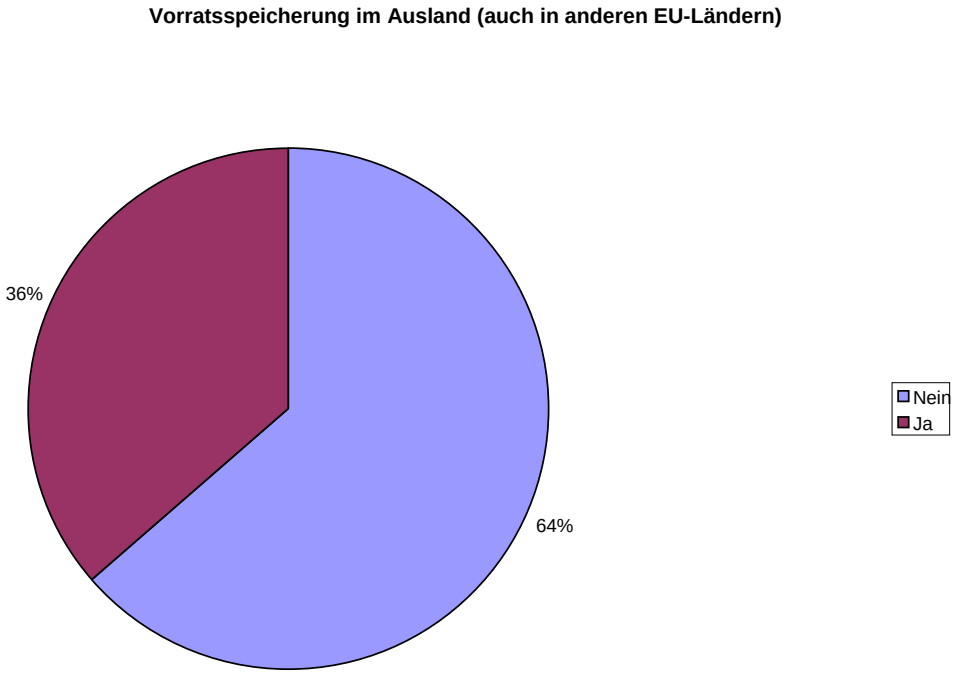
solchen Fallkonstellationen sind die Aufsichtsbehörden zu einem erhöhten Maß an gegenseitiger Amtshilfe und an Zusammenarbeit aufgerufen, um den Datenzugriff gewähren und die notwendigen Durchsetzungsbefugnisse ausüben zu können.

Um in Erfüllung der Anforderungen der Richtlinie die Kostenentwicklung in Grenzen zu halten, könnte auf Verbundlösungen zurückgegriffen werden, die hauptsächlich auf der Inlandsebene bereits umgesetzt wurden, und zwar durch kleine Internet-Diensteanbieter – wobei einer der im Verbund arbeitenden Diensteanbieter oder ein delegierter Dritter das System für die Vorratsspeicherung von Verkehrsdaten konzipiert und durchführt, die Authentifizierungsphasen steuert und die jedem einzelnen Internet-Diensteanbieter zugewiesenen Datenspeicher aufteilt. Dieses Konzept sollte positiv betrachtet werden, wenn es auch eines ausreichend harmonisierten, formalisierten und detaillierten Regelungswerks bedarf.

Die Übermittlung von auf Vorrat gespeicherten Daten in andere Länder sollte jederzeit die Voraussetzungen der Richtlinie 95/46/EG erfüllen. Insbesondere die Übermittlung von auf dem Gebiet der EU erzeugten Verkehrsdaten, die außerhalb der EU verwendet werden sollen, muss gemäß dieser Richtlinie einer Bewertung der Angemessenheit des Schutzniveaus, das das Drittland bietet, unterzogen werden.

Darüber hinaus können die Bestimmungen der Richtlinie 95/46/EG, die sich auf die Übermittlung personenbezogener Daten in Drittländer beziehen, nicht getrennt von den anderen Bestimmungen dieser Richtlinie angewandt werden, einschließlich der Bestimmungen über das Verhältnis zwischen dem für die Verarbeitung Verantwortlichen und dem Auftragsverarbeiter.[7]

[7] Für eine ausführlichere Analyse der rechtlichen Aspekte der Outsourcing-Angelegenheiten verweist die Artikel-29-Datenschutzgruppe auf den Abschnitt 4.6 ‚Grenzüberschreitender Datenfluss' ihrer Stellungnahme 10/2006 zur Verarbeitung von personenbezogenen Daten durch die SWIFT. Auch kann sie auf ihre Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter" (WP169) verweisen.



Die Outsourcing-Angelegenheiten sollten Thema einer ausführlicheren Analyse durch die Datenschutzbehörden sein, um die Erfüllung der Pflichten nach innerstaatlichem Recht (beispielsweise hinsichtlich der Bestellung von Auftragsverarbeitern), einschließlich vertraglicher Bestimmungen, einer effektiveren Beurteilung zu unterziehen, die auf bestimmte, angemessene Sicherheitsmaßnahmen eingehen sollte.

IV. Weitere Aktionen und Empfehlungen

Angesichts der Schlussfolgerungen dieser gemeinsamen Erhebung lassen sich unter Berücksichtigung der einzelnen geprüften Punkte die folgenden spezifischen Empfehlungen abgeben: Zwar richten sich die meisten von ihnen an die Diensteanbieter, die über die technischen Mittel für ihre Umsetzung verfügen, doch bringen sie nichtsdestoweniger auch die Rolle der öffentlichen Behörden ins Spiel, so die Europäische Kommission, die Mitgliedstaaten und die nationalen Datenschutzbehörden – nicht zuletzt wegen der Kostenfragen, die einerseits eine geringere Aufmerksamkeit für den Einsatz der nötigen Instrumente zum Schutz der Privatsphäre wie auch der nötigen Sicherheitsinstrumente zur Folge haben und andererseits auch zu Marktverzerrungen führen können. **Ferner möchte die Datenschutzgruppe daran erinnern, dass in diesem Zusammenhang die Selbstregulierung allein nicht ausreichend ist, vor allem wegen des unausgewogenen Kräfteverhältnisses zwischen den Diensteanbietern auf der einen Seite und den gesetzlich ermächtigten Behörden auf der anderen Seite, und weil Angelegenheiten, die mit Wettbewerb und Kosten verbunden sind, mitunter nicht zu einem Konzept der Selbstregulierung unter Gewährleistung hoher Sicherheitsstandards führen können.**

- Kategorien von auf Vorrat gespeicherten Daten

Da die Richtlinie 2006/24/EG eine Ausnahmeregelung zu den Bestimmungen der Richtlinie 2002/58/EG darstellt, ist die Liste der Verkehrsdaten, die zwingend auf Vorrat zu speichern sind, als erschöpfend anzusehen. Folglich dürfen den Diensteanbietern nach der Richtlinie über die Vorratsspeicherung von Daten keine zusätzlichen Pflichten zur Vorratsdatenspeicherung durch innerstaatliche Gesetze auferlegt werden. Auf der anderen Seite möchte die Artikel-29-Datenschutzgruppe betonen, dass die gesetzlich ermächtigten Behörden auf der Grundlage dieser Richtlinie nicht berechtigt sind, den Diensteanbietern aufzutragen, Daten zu sammeln, die außerhalb des Anwendungsbereichs der in der Richtlinie aufgeführten Kategorien liegen.

- Speicherungsfristen

a. Der Mangel an Harmonisierung, auf den durch diese Erhebung in Bezug auf die Speicherungsfristen hingewiesen wurde, stellt eine merkliche Belastung des Grundsatzes dar, demzufolge EU-Bürger „überall in der Europäischen Union das gleiche Schutzniveau genießen“; dies ist zum Teil der Fall, weil die einzelnen Beteiligten aufgrund der damit zusammenhängenden Kosten und Wettbewerbsfähigkeit erhebliche Beeinträchtigungen in wirtschaftlicher Hinsicht erfahren können. Die Datenschutzgruppe ist in diesem Zusammenhang der Auffassung, dass es von Vorteil wäre, eine Kürzung der maximalen Speicherungsfrist in Betracht zu ziehen und eine einheitliche, kürzere Frist zu setzen, die von allen Diensteanbietern überall in der EU einzuhalten ist, wie die Datenschutzgruppe bereits in ihrer Stellungnahme WP113 dargelegt hat.

b. Da unterschiedliche Speicherungszwecke und Speicherungsfristen im Raum stehen (kommerzielles Interesse gegen Rechtsdurchsetzung), dürfte der Vorschlag Sinn machen, dass die Kommission die Gesamtsituation der Sicherheit von Verkehrsdaten an sich neu überdenkt, und zwar schon im Hinblick auf die Gesamtbewertung der Durchführung der Richtlinie über die Vorratsspeicherung von Daten. Es darf nicht zugelassen werden, dass je nachdem, welcher Zweck dem zugrunde liegt, unterschiedliche Sicherheitsniveaus und Speicherungsfristen gelten, Nach der Richtlinie über die Vorratsspeicherung von Daten sind Verkehrsdaten zu Zwecken der Rechtsdurchsetzung für einen begrenzten Zeitraum auf Vorrat zu speichern; Zugang besteht im Rahmen einer bestimmten Rechtsgrundlage zu speziellen Zwecken der Rechtsdurchsetzung.

- Technische und organisatorische Sicherheitsmaßnahmen

a. Anbieter von elektronischen Kommunikations- und von Internetdiensten sollten die mit den Verkehrsdaten zusammenhängenden Risiken regelmäßig und möglichst objektiv bewerten, damit sie alle relevanten Risikofaktoren und deren mögliche Auswirkungen feststellen können, und dabei der Zugriffskontrolle und der Verfügbarkeit von Daten besondere Aufmerksamkeit widmen. Regelmäßige externe Audits dürften einen Beitrag zu einer unabhängigen und objektiven Risikobewertung leisten.

b. Zusätzlich zu einigen derzeit praktizierten Sicherheitsmaßnahmen können noch weitere Maßnahmen vorgeschlagen werden, die man in vollkommener Übereinstimmung mit dem Grundsatz der Technologieneutralität ergreifen kann, um gemäß Artikel 7 Buchstabe c) der Richtlinie über die Vorratsspeicherung von Daten sicherzustellen, dass der Zugang zu den

betreffenden Daten ausschließlich ordnungsgemäß ermächtigtem Personal vorbehalten ist; derzeit ergreifen indes nicht alle infrage kommenden Diensteanbieter diese Maßnahmen:

- Strenge Kontrolle des Zugriffs auf die auf Vorrat gespeicherten Daten im Rahmen der Festlegung von Benutzerpflichten und Benutzerprofilen mit unterschiedlichen Benutzerberechtigungen;
- strenge Authentifizierung für den Zugang zum betreffenden System, basierend auf doppelten Authentifizierungsmechanismen (d. h. Passwort + biometrischen Daten oder Passwort + Token), um die körperliche Anwesenheit der für die Verarbeitung der Verkehrsdaten verantwortlichen Person sicherzustellen;
- detailgenaue Rückverfolgung der Arbeitsgänge bei Zugriff und Verarbeitung im Wege der Log-Vorratsspeicherung mithilfe von Zugriffsprotokollen (Logs), die zumindest die Benutzeridentität, die Zugriffszeit und die vom Zugriff betroffene Datei aufzeichnen;
- Einsatz von Log-Management-Lösungen zur Gewährleistung der Log-Integrität mithilfe von Verschlüsselungstechnologie;
- logische Trennung von anderen Systemen, die Verkehrsdaten zu kommerziellen Zwecken verarbeiten;
- zusätzliche Maßnahmen, die unter Umständen zur Sicherstellung der Vertraulichkeit von Daten nötig sind.

c. Die Rollen und Funktionen, die den Systemadministratoren zukommen, sind in Einzelheiten darzustellen, so auch anhand von Ad-hoc-Berichten, und alle Instandhaltungsaktivitäten, die an solchen Systemen durchgeführt werden, sollten eingehenden Kontrollen unterliegen.

d. Zur Verbesserung der auf die Verkehrsdaten anzuwendenden Sicherheitsmaßnahmen sind Mehrfachaktionen erforderlich, die gut zu koordinieren sind; ihre Durchführung durch die Diensteanbieter kann erleichtert werden, wenn sowohl innerbetriebliche Maßnahmen als auch die eigentlichen technologischen Maßnahmen in ein Sicherheitszertifizierungsprogramm eingebettet werden, das in regelmäßigen Zeitabständen durchzuführen ist – vorzugsweise durch einen externen Dritten und in Übereinstimmung mit den international vereinbarten Standards – um die Robustheit der Maßnahmen zu bewerten, die gegenüber den sich wandelnden Formen von Risiken und Anfälligkeiten/Schwachstellen zum Einsatz kommen. Auch andere Maßnahmen könnten sich als für diesen Zweck tragfähige Lösung erweisen, so z. B., dass man den Datenschutzbehörden die Möglichkeit gibt, Audits selbst durchzuführen, oder den Datenschutzbehörden die Audits Dritter zur Verfügung stellt.

e. Die Notwendigkeit, erweiterte Speicherungsfristen für abgerufene Daten ins Auge zu fassen, ist anhand von scharf umrissenen Kriterien zu bewerten, die auf alle Fälle auch die Löschung abgerufener Daten im Lichte der Anforderungen gemäß der Richtlinie 95/46/EG wie auch der internationalen Instrumente (einschließlich der Empfehlung R(87)15 des Europarates) vorsehen sollten.

- Weitergabeverfahren

a. Zur Ankurbelung der Harmonisierung sind standardisierte Datenweitergabeverfahren für gesetzlich ermächtigte Behörden auf europäischer Ebene zu entwickeln. Das Datenaustauschprotokoll könnte zu einem IT-Standardverfahren weiterentwickelt werden, wobei auch die Ausrichtung der Datenübermittlung (die auf PUSH-Protokollen basieren

sollte) mit zu berücksichtigen ist. Damit würden schnellere, zuverlässigere Datenübertragungen ermöglicht und bei allen relevanten Beteiligten (Diensteanbietern und gesetzlich ermächtigten Behörden) niedrigere Kosten anfallen. Dieser Weitergabestandard sollte mindestens folgenden Parameter oder Ereignissen auf der Spur bleiben: Benutzerdaten, Art der Verkehrsdaten, Kenncode des Diensteanbieters, Kenncode der gesetzlich ermächtigten Behörde, Kenncode der Justizbehörde, Zeitstempel, Nummer und Art der Datenanforderung.

b. Der Katalog der schweren Straftaten sollte auf innerstaatlicher Ebene auf der Grundlage von nationalem Recht und unter Berücksichtigung der Erwägungen in den Dokumenten WP113 und WP119 erstellt werden. Die erschöpfende Liste der staatlichen Stellen, die zum Zugriff auf die gemäß der einschlägigen Richtlinie auf Vorrat gespeicherten Daten ermächtigt sind, ist allen relevanten Beteiligten bekannt zu gegeben.

- Statistik

Die Mitgliedstaaten sollten der Kommission die benötigte Statistik in jedem Fall so schnell wie möglich übermitteln; am besten noch vor Ablauf der Vorlagefrist für den Bewertungsbericht, den die Kommission über die Richtlinie über die Vorratsspeicherung von Daten erstellen muss. Diese Statistik sollte möglichst zusammen mit Informationen über die Auswirkungen infolge von auf Vorrat gespeicherten Verkehrsdaten über die Behandlung schwerer Straftaten, nach Alter der Daten aufgegliedert, vorgelegt werden.

- Outsourcing

a. Die Outsourcing-Angelegenheiten sollten Thema einer ausführlicheren Analyse durch die Datenschutzbehörden sein, um die Erfüllung der Pflichten nach innerstaatlichem Recht (beispielsweise hinsichtlich der Bestellung von Auftragsverarbeitern), einschließlich vertraglicher Bestimmungen, einer effektiveren Beurteilung zu unterziehen, die auf bestimmte, angemessene Sicherheitsmaßnahmen eingehen sollte.

b. Man könnte auf Verbundlösungen zurückgreifen, die auf der Inlandsebene durch kleine Internet-Diensteanbieter bereits umgesetzt wurden.

ANHANG I

Data Retention_DraftFinall