ENGLISCH	DEUTSCH (ausgehend von Google-Übersetzung o_O) (mit # markierte Felder müssen noch geglättet werden...)	Subjektive Anmerkungen, Zusammenfassung zusammengetragen aus der Arbeit mehrerer „Aktivisten“
Brussels, 15 December 2011	Brüssel, den 15. Dezember 2011	
18620/11	18620/11	
LIMITE	LIMITE	
DAPIX 167 TELECOM 214 COPEN 365 DATAPROTECT 156	DAPIX 167 TELECOM 214 COPEN 365 DataProtect 156	
NOTE	**NOTIZ**	
From: Commission Services	Von: Dienststellen der Kommission	
To: Working Party on Data Protection and Exchange of Information	An: Arbeitsgruppe für den Datenschutz und den Austausch von Informationen (DAPIX)	
No. Cion prop.: 9324/11 DAPIX 38 TELECOM 47 COPEN 85	Nr. Kommissionsvorschlag prop:. 9324/11 DAPIX 38 TELECOM 47 COPEN 85	
Subject: Consultation on reform of Data Retention Directive: emerging themes and next steps	Betreff: Anhörung zur Reform der Richtlinie zur Vorratsdatenspeicherung - aufkommende Themen und nächste Schritte	
1. The purpose of this paper is to inform DAPIX of the results of the Commissions consultation on the reform of the Data Retention Directive (DRD), to set out the main problems, and to put specific questions on which the Commission, in determining the way forward, will rely on evidence supplied by Member States.	1. Der Zweck dieses Schreibens ist, DAPIX über die Ergebnisse der Kommissions-Konsultation über die Reform der Richtlinie zur Vorratsdatenspeicherung (DRD) zu informieren, die wichtigsten Probleme offenzulegen und konkrete Fragen zu stellen, anhand derer die Kommission unter Bezug auf die von den Mitgliedstaaten zur Verfügung gestellten Unterlagen, das weitere Vorgehen festlegen wird.	• Es gibt Probleme.

CONSULTATION

2. Following the presentation of its evaluation report on the Data Retention Directive, the Commission has been consulting all interested groups on whether and if so how the DRD should be reformed, including:

- Member States governments and other government e.g. Länder

- Law enforcement including Europol and Eurojust

- Judiciary

- Data protection authorities

- Industry including trade associations

- Consumer associations

- Civil society: privacy-advocates, journalist association, victims groups

- Open public consultation on DG Home website

BERATUNG

2. Nach der Präsentation seines Evaluierungsberichts über die Richtlinie zur Vorratsdatenspeicherung hat die Kommission Konsultationen mit allen interessierten Gruppen darüber aufgenommen, ob und wenn ja, wie die DRD reformiert werden sollte. Zu diesen Gesprächen waren eingeladen:

- Regierungen der Mitgliedstaaten und anderen Bundesländer

- Strafverfolgungsbehörden einschließlich Europol und Eurojust

- Justiz

- Datenschutzbehörden

- Industrie und Wirtschaftsverbände

- Verbraucherverbände

- Zivilgesellschaft: Datenschutz-Anwälte, Journalisten Verband, Opfergruppen

- Öffentlich zugängliche Konsultation via DG Home Webportal

- Übersicht über die bisherige Arbeit der Kommission.

EMERGING THEMES

I. Need to explain better the value of data retention

AUFKOMMENDE THEMEN

I. Notwendigkeit einer besseren Erklärung des Wertes und der Bedeutung der Vorratsdatenspeicherung

- *Die Überschrift nimmt eine (voraus) wertende Haltung ein.*

3. We have received strong views from law enforcement and the judiciary from all Member States that Communications data are crucial for criminal investigations and trials. and that it was essential to guarantee that these data would be available if needed for at least 6 months or at least a l year. We have also received strong qualitative evidence of the value of historic Communications data in specific cases of terrorism. serious crime and crimes using the internet or by telephone - but only from 11 out of 27 Member States.

3. Uns wurde die feste Überzeugung der Strafverfolgungsbehörden und der Justiz aus allen Mitgliedstaaten mitgeteilt, das Kommunikationsdaten ausschlaggebend für strafrechtlichen Ermittlungen und Gerichtsverfahren sein können und dass es wichtig sei, dass diese Daten für mindestens 6 bis 12 Monate gespeichert werden müssten Wir haben auch starke qualitative Belege erhalten, die den Wert der Kommunikationsdatenspeicherung bei der Verfolgung bestimmter Fälle von Terrorismus, schwerer Kriminalität und per Internet oder mit Hilfe des Telefons begangener Verbrechen betonen – derartige Informationen erhielten wir allerdings nur von 11 der 27 Mitgliedstaaten.

- Rückmeldungen von nur 11 der 27 Mitgliedstaaten (trotz mehrfacher und -monatiger Verschiebung der Fristen zur Einreichung von Daten und Informationen zu tatsächlichen Erfahrungen mit der Umsetzung der VDS)
- "crimes using telephone" → Nutzung zur Verfolgung nicht schwerer Straftaten (Straftaten, die per TK begangen werden) → Zweckänderung der Richtlinie in der Praxis bewiesen

4. There is a continued perception that there is little evidence at an EU and national level on the value of data retention in terms of public security and criminal justice, nor of what alternatives have been considered. Member States' evidence tends to consist of Statements of the importance of the data. It is unclear whether data requested would be available anyway without the retention Obligation, because there is no logical Separation between data stored and then accessed for a) business purposes, b) for purposes of combating 'serious crime' and c) for purposes other than combating serious crime. There is no agreement on how to report Implementation in qualitative terms. Data Protection Authorities do not know what is being kept or deleted by operators. The statistics required under Article 10 do not, as it is currently interpreted, enable evaluation of necessity and effectiveness.

4. Es ist ständige Wahrnehmung, dass es nur wenige Hinweise (auf EU- und nationaler Ebene) für den Wert der Vorratsdatenspeicherung in Bezug auf die öffentliche Sicherheit und Strafjustiz gibt, noch darüber, ob und welche Alternativen zur Vorratsdatenspeicherung in Betracht gezogen worden sind. Die von den Mitgliedstaaten vorgelegten Belege beschränken sich auf Aussage zu der Wichtigkeit der Daten. Unklar ist, ob die angeforderten Daten nicht ohnehin und auch ohne VDS zur Verfügung stehen würden, da es keine logische Trennung gibt zwischen gespeicherten und dann abgerufenen Daten für a) geschäftliche Zwecke, b) zum Zwecke der Bekämpfung der "schweren Straftat" und c) für andere Zwecke als Bekämpfung von schwerer Kriminalität. Es gibt keine Abstimmung über eine einheitliche qualitative Beschreibung der Umsetzung der VDS. Die Datenschutzbehörden wissen nicht, welche Daten von den Betreibern gespeichert und welche gelöscht werden. Die nach Artikel 10 der aktuellen DRD zu erstellenden Statistiken ermöglichen nach derzeitiger Interpretationslage keine Evaluation der Notwendigkeit oder Effektivität der DRD.

- "Beweis" der Notwendigkeit der VDS scheint größtenteils ein Lippenbekenntnis zu sein
- keine Trennung zwischen Abrechnungs- und Verkehrsdaten
- keine Differenzierung zwischen Zugriff auf VDS-Daten zur Bekämpfung schwerer Straftaten und anderer Straftaten
- keine Richtlinien zur Implementierung der Datenspeicherung und des Datenabrufs
- Datenschutzbehörden sind ratlos und können ihre Aufgaben nicht wahrnehmen
- Die Evaluation nach Artikel 10 ist gescheitert – dieser Teil/diese Bedingung der derzeit gültigen VDS-Richtlinie kann also nicht eingehalten/umgesetzt werden!

5. There is, therefore, currently no monitoring System whereby the citizens can see that a) the data would not have been available to law enforcement without mandatory retention and b) the outcome of using that data in investigations and prosecutions.

5. Es gibt demzufolge zur Zeit kein Beobachtungssystem, das den Bürgern ermöglicht zu sehen dass a) die Daten den Strafverfolgungsbehörden ohne die verpflichtende Vorratsdatenspeicherung nicht zur Verfügung gestanden hätten und b) das diese Daten in Ermittlungs- und Strafverfolgungsmaßnahmen hilfreichen Einsatz gefunden haben.

- mangelnde Transparenz der Bürger und der Datenschutzbeauftragten über Zugriffe

II. Some data categories are being retained unnecessarily, other types of data needed by law enforcement cannot be easily accessed

II. Einige Datenkategorien werden unnötigerweise gespeichert, andere Daten sind für die Strafverfolgungsbehörden nicht immer leicht zugänglich

- *Die Zwischenüberschrift gesteht das Scheitern der bisherigen Richtlinie ein*

6. Law enforcement favour 'technological neutrality' so that their ability to know who communicated with whom, when, where and how is not diminished as technologies develop. However, unclear definitions in the DRD have encouraged heterogeneous interpretations of the scope - both operators and types of data - and this can result in frustration for law enforcement. For example, instant messaging, chat, uploads and downloads (but not anonymous SIM cards) are types of data held by information society Services which is almost identical to traffic data but which is outside the scope of the DRD. There is no Standard EU approach to accessing this data, so some law enforcement find it very difficult to get this data on time for their investigations.

6. Strafverfolgungsbehörden bevorzugen eine „technologische Neutralität“, so dass ihr Zugang zu den Daten, wer wann mit wem und von wo aus kommuniziert hat auch mit fortschreitender technologischer Fortentwicklung nicht eingeschränkt wird. Allerdings haben unklare Definitionen der DRD zu einer uneinheitlichen Interpretation der Reichweite der Datenerfassung geführt, was Frustration bei den Strafverfolgungsbehörden zur Folge hatte.
Zum Beispiel sind Instant Messaging, Chat, Uploads und Downloads (allerdings nicht anonyme SIM-Karten) Arten von Daten, die von TK-Anbietern erfasst sind oder erfassbar wären, die bis jetzt aber nicht durch die DRD abgedeckt werden, obwohl es sich um ähnliche Verbindungsdaten handelt. Es gibt derzeit keinen EU-einheitlichen Ansatz zur Ermöglichung des Zugriffs auf diese speziellen Daten, so dass die Strafverfolgungsbehörden einzelner Länder Probleme haben, an diese Daten zu gelangen.

- nicht-eindeutige Definition von Verkehrsdaten führt zu Zugriff auf weitere Daten durch die Sicherheitsbehörden
- man bedauert, dass es im Rahmen der VDS-Richtlinie noch keine zwingende Erfassung von Instant-Messaging, Chat-, Upload- und Download-Daten gibt und wünscht sich eine entsprechende Erweiterung, da es länderweise bislang schwierig sei, an diese Daten heranzukommen (!)
- es droht also eine Ausweitung der Richtlinie aufgrund des Drucks einzelner Länder, in denen das aufgrund nationaler Gesetzgebung nicht möglich ist! Das ist ein Missbrauch der Richtlinie.

7. The majority of requests received for internet data are to resolve IP addresses to a subscriber, with other requests for email traffic data not as common. However, this could be an issue of lack of training or weakness in forensic capacity.

7. Die meisten Anträge auf Internet-Daten erfolgen mit dem Zweck, den IP-Inhaber zu ermitteln und weniger oft zur Klärung von E-Mail-Verkehrsdaten. Dieses könnte allerdings auch an mangelhafter Ausbildung oder Ausstattung der forensischen Abteilungen liegen.

- Häufig: Abfrage von Daten zur Ermittlung von IP-Adressen-Inhabern.

8. Business-to-busmess Service providers very rarely receive requests for data which they retain. Small and medium operators also tend to receive requests for data very rarely.

8. Business-to-business Dienstleister erhalten nur sehr selten Anträge zur Herausgabe von VDS-Daten. Ähnliches gilt für kleine und mittelgroße TK-Dienstleister und Provider.

- Häufigste VDS-Datenabfrage hauptsächlich bei den großen TK-Dienstleistern/Providern.

III. Concern about proportionality, legal precision and data protection

III. Die Sorge um Verhältnismäßigkeit, der Rechtsgenauigkeit und des Datenschutzes

- *Datenschutzrechtliche Bedenken*

9. The DRD purpose (Article 1) concerns 'serious crime', which is not defined at EU level or in many Member States, although the Council Statement on adoption of the Directive said that MS should have 'due regard to the crimes listed in ... the European Arrest Warrant ... and crime involving telecommunication'. Certain crimes, e.g. hacking, may not be deemed 'serious' but can only be tackled through telecoms data. The DRD does not cover urgent cases for protection of life and limb not related to crime e.g. suicide / self harm, missing persons, emergencies. There are also some calls for extension of the purpose to include Copyright infringements, which may include illegal downloads / piracy.

9. Der in Artikel 1 der DRD definierte Zweck der Richtlinie betrifft „schwere Straftaten“ - ein Begriff, der auf EU-rechtlicher Ebene und in vielen Mitgliedstaaten allerdings nicht vereinheitlicht ist, trotzdem der Ministerrat im Rahmen der Verabschiedung der DRD erklärt hatte, die Mitgliedstaaten sollten dieses "unter Beachtung der Verbrechen aufgelistet im ... Europäischen Haftbefehl“ definiert haben. Auch dazu gehören sollte „... Kriminalität, die Telekommunikation als Tatmittel nutzt". Bestimmte Verbrechen wie z.B. das „Hacken“ mögen zwar nicht schwerwiegend sein, können allerdings nur durch TK-Daten nachgewiesen werden. Die DRD darf nicht dringende Fälle zum Schutz von Leib und Leben herhalten, die nicht im Zusammenhang mit z.B. Selbstmord, Selbstverletzung, vermissten Personen und Notfällen stehen. Ebenso wird verlangt, die DRD zum Einsatz im Zusammenhang mit Urheberrechtsverletzungen auszuweiten (z.B. für illegale Downloads bzw. Download-Piraterie).

- keine klare Definition schwerer Straftaten → Intransparenz, nicht rechtmäßige Zugriffe
- Was sind „emergencies“, die nach Meinung der Kommission den Abruf und die Verwendung der VDS-Daten rechtfertigen?
- Auch zur Strafverfolgung von „hacking“ soll die VDS in Zukunft herhalten!
- (Ganz nebenbei: wie lautet die juristische Definition eines solchen Straftatbestandes auf europäischer Rechtsebene?)
- Forderung der Ausweitung der VDS-Richtlinie für den Einsatz bei Urheberrechtsverfahren → drohende Kriminalisierung der Mehrheit der Nutzer

10. Data protection authorities and NGOs are concerned at the lack of a clear limitation of the purposes for which data may be retained. In some Member States, the retention requirement is not limited to a specific purpose. The European Court of Justice has ruled that the use of personal data in civil proceedings is not prevented by the DRD. Such a lack of clarity, it is claimed, leads to risk or fear of 'function creep'. This endangers the principles of finality and predictability.

10. Datenschutzbehörden und NGOs sind über den Mangel an einer klaren Begrenzung der Zwecke, für die Daten beibehalten werden dürfen, besorgt. In einigen Mitgliedstaaten ist die VDS nicht auf bestimmte Zwecke beschränkt worden. Der Europäische Gerichtshof hat entschieden, dass die Verwendung von personenbezogenen Daten in Zivilverfahren nicht durch die DRD verhindert wird. Solch ein Mangel an Klarheit, so wird behauptet, führt zu Risiko oder die Angst vor "Zweckentfremdung" der Daten. Dies gefährde die Prinzipien der Zielgerichtetheit und Berechenbarkeit der VDS.

- Bedenken der Datenschutzbehörden und NGO's werden hier leider nur bruchteil- bzw. bruchstückhaft wiedergegeben.

11. Operators do not provide consistent notification to users in contracts of potential data disclosure to authorities. There is no procedure for reporting and redressing data breaches. There is no clear distinction between data kept for commercial purposes, and data kept under the retention requirement. Citizens often do not know who has access to the data. The absence of Standard procedures means that access cannot be monitored and audited.

11. Bei den TK-Dienstleistern gibt es keine einheitliche Vorgaben zum Umgang mit Kunden bzw. der Aufklärung ihrer Kunden über die Praxis und Bedeutung der von ihnen betriebenen VDS. Es gibt keinerlei Standards oder Vorgaben zur Meldung von Datenmissbrauch oder -diebstahl. Ebensowenig gibt es eine klare Unterscheidung der gespeicherten Daten hinsichtlich ihres eigentlichen Zwecks (zum Zwecke der Aufrechterhaltung der Aufgaben der TK-Anbieter einerseits und für die VDS andererseits). Vom Datenabruf betroffene Bürger erhalten meistens nichts darüber, dass persönliche Daten von ihnen weitergegeben worden sind. Das Fehlen jeglicher Standards zu diesen Punkten bedeutet, dass der Datenzugriff auf persönliche Daten weder überwacht noch bewertet werden kann.

- Offenbarung schwerwiegender grundrechtlicher Probleme:
- keine Standards hinsichtlich der Datentrennung bei den TK-Dienstleistern
- keine obligatorischen Pflichten zur Meldung von Datenmissbrauch oder -diebstahl, auch keinerlei Bußgeldbewährung
- keine Benachrichtigung der vom Datenabgriff betroffenen Menschen
- keine Aufklärung der Kunden über das Stattfinden und/oder Umfang der VDS
- und deswegen:
- keinerlei Evaluation/Kontrolle/Bewertung hierzu möglich!

IV. Difficulties in police and judicial cross-border cooperation

12. Law enforcement finds it difficult and inefficient to share acquired data across borders, including for joint investigations by Europol. This is often due to divergences in data retention, especially where Member States have not transposed at all and therefore cannot participate in joint operations. However, where there is a good level of tmst data is more likely to be exchanged. The EIO may assist if and when it is adopted and fully implemented, where there will be an assumption that a request for evidence will be executed where it concerns 'the identification of persons holding a subscription of a specified phone number or IP address.

IV. Schwierigkeiten bei der polizeilichen und justiziellen grenzüberschreitende Zusammenarbeit

12. Strafverfolgungsbehörden erleben es als schwierig und ineffizient, Daten über nationale Grenzen hinweg auszutauschen, das gilt auch für die Zusammenarbeit im Rahmen von Europol. Das hängt oft von den sehr unterschiedlichen Länderregelungen zur VDS ab, insbesondere wenn einzelne Staaten gar keine Umsetzung vorgenommen haben und deswegen an gemeinsamen Aktionen nur beschränkt teilnehmen können. Im Falle des Vorhandenseins von Daten werden die Daten dagegen mit hoher Wahrscheinlichkeit ausgetauscht. Das EIO kann unterstützend tätig werden und im Fall der berechtigten Anforderung personenspezifischer Daten zur Aufklärung der Identitäten von Telefonnummern und IP-Adressen weiterhelfen.

- *Transnationale Probleme / Europäischer Datenverkehr*

- Klage über uneinheitliche Umsetzung der VDS-Richtlinie (DRD)
- Intensiver Austausch von TK-Daten auch über Nationalstaatengrenzen hinweg sei ansonsten kein Problem...

V. Effect on industry: Uneven data retention practices continue to impede and distort the internal market

13. Businesses in the telecommunications sector complain about legal uncertainty, saying that it is often unclear which data should be stored. Some Member States consider that the data categories in Article 5 of the DRD are not exhaustive but rather the minimum requirement. The Article 29 Working Party has argued that unsuccessful communication attempts (which are covered by Article 3 (2)) should not be stored. Electronic Communications Service and Internet email have been interpreted in certain Member States as including webmail and social networking sites which provide email exchange Services, instant messaging, chat and video conferencing. There is some confusion about the distinction between 'Electronic mail1 (Directive

V. Auswirkungen auf die Industrie: Ungleiche Vorratsdatenspeicherungs-Praktiken behindern und verzerren den Binnenmarkt nach wie vor

13. TK-Dienstleister beklagen die Unsicherheiten der gesetzlichen Rahmenbedingungen. Es sei z.B. unklar, welche Daten im Detail erfasst und gespeichert werden sollten. Einige Mitgliedstaaten sind der Ansicht, dass die Datenkategorien gemäß Artikel 5 des DRD nicht das Maximale sondern die Mindestanforderung zu den zu speichernden Daten darstellen würden.. Die Artikel 29-Datenschutzgruppe hat argumentiert, dass erfolglose Kommunikationsversuche (die unter Artikel 3 (2) fallen) nicht gespeichert werden sollten. Mancherorts wurde die Richtlinie derart interpretiert, dass sogar Webmail und „Soziale Netzwerke“, die E-Mail-Angebot, Instant Messaging, Chat und Videokonferenzen anbieten, nun ebenfalls

- *Sichtweise der TK-Dienstleister / Provider*

- Ausweitung der VDS-Daten über "Minimum" in der Richtlinie wird teilweise praktiziert → verletzt Grundrechte und EU-Datenschutzrichtlinie
- Forderung der Art. 29-Gruppe (EU-Datenschutzgruppe) nach Nicht-Speicherung erfolgloser Kommunikationsversuche (erfolglose Telefonanrufe z.B.)
- Auch soziale Netzwerke sind – entgegen der ursprünglichen Absicht – in einigen Ländern vermehrt von VDS betroffen.
- Unklarheit in der Bewertung von Instant Messaging.
- Doppelte Speicherung der

2002/58/EC Article 2 (h)) which could be deemed to include instant messaging, and 'internet email' which may not. While the intention of the DRD was that data should only be retained once, in reality data is stored by the operators of the sender and receiver of communication, and each Server is backed up.

von der VDS-Speicherung betroffen sind. Es gibt einige Verwirrung über die Unterscheidung zwischen einer "Elektronische Mail" (Richtlinie 2002/58/EG Artikel 2 (h)), zu der Instant-Messaging gehören könnte, und "Internet-E-Mail ", bei der das nicht gilt. Während es die Absicht der DRD ist, dass TK-Daten nur einmal und an einer Stelle erfasst und gespeichert werden sollten, ist dieses in Wirklichkeit anders: sowohl Sender als auch Empfänger der TK-Verbindung speichern nun dieses Daten auf ihrem jeweiligen Server.

Verbindungsdaten bei E-Mails und anderen TK-Verbindungen (sowohl beim Sender- als auch beim Empfänger-Provider), was der Absicht der Richtlinie widerspricht.

14. The industry has also provided evidence of considerable costs of compliance. The Data Retention Expert Group has recently approved a document describing these costs (list at Annex A) and various operators have provided confidential information on costs. The cost to the operator stems from having to retain it in such a way as to ensure it is available and valuable to competent authorities, which is explicitly required by the DRD Article 8. It is a pure overhead if no reimbursement. There is a disproportionately high cost for smaller enterprises. The Commission is comparing and testing the cost estimates provided.

14. Die Industrie hat auf ihre erheblichen Kosten für die Einhaltung der VDS hingewiesen und diese dokumentiert. Im Anhang A findet sich ein Dokument der „Data Retention Expert Group", das zur Aufschlüsselung dieser Kosten dienen soll. Verschiedene TK-Dienstleister haben vertrauliche Informationen über Kosten zur Verfügung gestellt. Diese Kosten entstehen durch Erfassung, Speicherung und Bereitstellung der VDS-Daten. Es handelt sich um unverhältnismässig hohe Kosten, falls es keine Entschädigungszahlungen gibt. Die Kommission prüft und vergleicht die ihr zur Verfügung gestellten Detaildaten.

- TK-Dienstleister beklagen hohe Kosten, die z.T. nicht erstattet werden würden.
- Der Kommission liegen vertrauliche Kostenrechnungen einzelner Provider vor, die derzeit geprüft und ausgewertet werden.

15. At the same time, some Member States argue that data retention is a Standard overhead for an enterprise that decides to establish its operations in their territory. Therefore, there is no level playing field for industry because inconsistent cost recovery. Furthermore, operators claim that the requirement to invest in data retention Systems means those resources cannot be dedicated to research and innovation into client-facing products.

15. Gleichzeitig argumentieren einige Mitgliedstaaten, dass die Vorratsspeicherung den davon betroffenen Unternehmen einen erheblichen Kostenzuschlag bedeutet. Dieses beeinträchtige die Wettbewerbsgleichheit aufgrund der von Land zu Land unterschiedlichen Systemen von Kostenerstattungen. Außerdem beklagen die TK-Dienstleister, dass ihnen aufgrund der VDS-Kosten Geld für Forschung und Weiterentwicklung ihrer Systeme fehlen würde.

- Klage über Wettbewerbsverzerrungen und mangelnde Kostenerstattung

16. There is no Standard for handover and use. Operators say that they are not always aware of law enforcement powers, which raises questions of liability. The ETSI Technical Committee on Lawful Interception handover Standard aims to provide a two-way user-friendly gateway between the operators and authorities. But these Standards are not mandatory and are followed only in a few Member States. Where there is no cost recovery, it is difficult to agree Standards for handover. Competent authorities do not appreciate the economic value of the data they request, which could otherwise moderate their requests and make them more proportionale. In certain Member States it is unclear to operators which authorities are competent to request data - this puts operators in an invidious position and generates additional legal costs.

16. Es gibt keinen Standard für die Übergabe und Nutzung der Daten. Die Betreiber sagen, dass sie nicht immer im Klaren über die tatsächlichen Befugnisse der Strafverfolgungsbehörden seien, was entsprechende Haftungsfragen aufwirft. Die ETSI Technical Committee auf Lawful Interception Übergabenorm zielt darauf ab, eine anwendungsfreundliche Schnittstelle zwischen TK-Dienstleistern und Behörden zu definieren. Aber diese Standards sind nicht verbindlich und werden nur in wenigen Mitgliedstaaten angewendet. Ohne gleichzeitige Kostenerstattung sei es schwierig, Standards für die Übergabe zwingend zu vereinbaren. Die zuständigen Behörden würden den wirtschaftlichen Wert der Daten nicht schätzen können. Ein neues bessere behördliches Bewußtsein darüber würde den von ihnen angeforderten Umfang an VDS-Daten vermutlich reduzieren und verhältnismäßiger gestalten. In manchen Ländern ist ungeklärt, welche Behörden im Detail überhaupt das Recht auf Datenabgriff besitzen – dieser Zustand versetzt die TK-Dienstleister in eine unbeliebte Situation und erzeugt zusätzliche Verfahrenskosten.

- Übermittlung der Daten nicht ausreichend geregelt --> Datensicherheit, Transparenz?
- Unklarheit darüber, wer Daten anfordern darf --> Risiko von nicht-rechtmäßigen Zugriffen
- TK-Dienstleister beklagen rechtliche Grauzonen, Ärger mit den Behörden und einen unverhältnismäßig hohen Datenabgriff, weil Geld (für die ermitelnden Behörden) bislang keine Rolle spielt.

17. Where there are no agreements among the operators and between them and authorities, it can be very difficult for the latter to obtain the data, especially where communication equipment is owned by different legal entities. Therefore, in at least three Member States, each request for data is sent to all major operators in the jurisdiction, distorting the statistics and giving misleading messages.

17. Ohne das Vorhandensein einheitlicher Regelungen zwischen TK-Dienstleistern und Behörden kann es zu Problemen bei der Zurverfügungstellung der Daten kommen. Das gilt insbesondere dann, wenn die Technik und ihre Zuständigkeit mehrteilig ist und unterschiedlichen juristischen Personen zugeordnet ist. Das führte dazu, dass in mindestens drei Mitgliedstaaten jede Datenanfrage an alle großen TK-Anbieter gesendet wird, was die Statistik erheblich verfälscht und zu irreführenden Ergebnissen führt.

- In „mindestens drei Ländern“ gibt es massive Probleme in der Praxis der VDS-Datenabfrage und im Umgang mit den Daten.
- Das führt zu verfälschten, unbrauchbaren Statistikdaten (und dürfte auch die „Evaluation“ beeinflusst haben...)

QUESTIONS FOR DISCUSSION

18. The following questions are suggested for the working group's discussion:

- How should the EU - at European and national level - address the concerns expressed by law enforcement, data protection authorities and industry, without limiting the operational effectiveness of law enforcement?

- What are the most effective ways of demonstrating value of data retention in general and of the DRD itself?

- What could be the most effective ways of ensuring data security?

- How can the exchange of retained data be best facilitated?

- How can the EU facilitate access for law enforcement to communications data held by information society Services where needed?

ZU DISKUTIERENDE FRAGEN

18. Die folgenden Fragen sind für die Besprechungen der Arbeitsgruppe vorgeschlagen:

- Wie sollte die EU - auf europäischer und nationaler Ebene - die Anliegen und Bedenken der Strafverfolgungsbehörden, Datenschutzbehörden und der Industrie zum Ausdruck bringen, ohne die operative Effizienz der Strafverfolgung zu beschränken?

- Was sind die effektivsten Möglichkeiten zu demonstrieren, welchen Wert die Vorratsdatenspeicherung im Allgemeinen und die DRD selbst haben?

- Was könnten die wirksamsten Möglichkeiten zur Gewährleistung der Datensicherheit sein?

- Wie kann der Austausch von auf Vorrat gespeicherten Daten am besten gefördert werden?

- Wie kann die EU dort den Zugang der Strafverfolgungsbehörden zu den bei den Providern gespeicherten Verkehrsdaten erleichtern, wo es nötig ist?

- grundlegende Fragen, die VOR der Verabschiedung einer solchen Richtlinie geklärt hätten werden müssen. Teilweise sind sie nicht aufzulösen
- Ausblendung der Frage nach dem Nachweis einer vernünftigen, das heißt: im Verhältnis stehenden Effektivität der VDS. Eine Frage, die ebenfalls VOR der VDS-Richtlinie hätte positiv beantwortet werden müssen, die aber selbst jetzt, fünf Jahre nach ihrer europaweit verpflichteten Einführung NOCH IMMER NICHT beantwortet werden kann!
- Die Frage nach der „effektivesten und beispielgebendsten Möglichkeit zur Verdeutlichung des Wertes der VDS“ nimmt eine nüchterne und neutrale Bewertung der Maßnahme vorweg und beantwortet sie implizierend als positiv.
- Ebenso wird die Rechtsstaatlichkeit der inner-EU-europäischen Austausches personenbezogenener Daten nicht einmal zur Bewertung in Frage gestellt ...

NEXT STEPS

19. A number of possible policy options for reforming the DRD have been identified in response to feedback from stakeholders during the consultation process since May 2011, and taking into account views expressed by MEPs and Member States. At present, the evidence gathered appears to reinforce the conclusions of the evaluation report, namely that data retention remains a valuable tool, but that there are serious shortcomings with the EU framework - including retention periods, clarity of purpose limitation and scope, lack of reimbursement of cost to industry. safeguards for access and use - which must be addressed. In particular. all Member States - not just a minority - need to provide convincing evidence of the value of data retention for security and criminal justice.

20. The Commission is now carrying out an impact assessment on the future options. It has also commissioned a study into approaches to, and the costs and benefits of, data preservation in the EU and around the world. Both exercises should be completed by May 2012, in time for a Commission proposal in July 2012.

NÄCHSTE SCHRITTE

19. Eine Reihe von möglichen politischen Optionen für eine Reform der DRD sind in Reaktion auf das Feedback der Beteiligten während des Konsultationsprozesses seit Mai 2011 erkannt und unter Berücksichtigung der Standpunkte der Abgeordneten und der Mitgliedstaaten zum Ausdruck gebracht worden. Derzeit scheinen genügend Beweise gesammelt worden zu sein, um die Schlussfolgerungen der Evaluierung zu stärken, nämlich dass die Vorratsspeicherung von Daten ein wertvolles Werkzeug bleibt, dass es aber gravierende Mängel bei den EU-Rahmenbedingungen gibt - inklusive Aufbewahrungsfristen, die Klarheit der Zweckbindung und der Umfang, der Mangel an Kostenerstattung für die Industrie und der Sicherheit des Zugangs und der Nutzung - die angegangen werden müssen. Im Besonderen müssen alle Mitgliedstaaten – und nicht nur eine Minderheit - überzeugende Beweise für den Wert der Vorratsdatenspeicherung für die Sicherheit und Strafjustiz liefern.

20. Die Kommission wird nun mit der Durchführung einer Bewertung der Auswirkungen auf die Optionen für die Zukunft beginnen. Es wurde auch eine Studie über Ansätze zur Inbetriebnahme, und die Kosten und Nutzen der, Daten-Erhaltung in der EU und der ganzen Welt in Auftrag gegeben. Beide Studien sollten bis Mai 2012 abgeschlossen sein, rechtzeitig für einen Vorschlag der neuen Richtlinie der Kommission, der für den Juli 2012 geplant ist.

- Notwendigkeit der VDS offensichtlich schwer belegbar

- Kommission führt derzeit zwei Studien durch (wer, auf welcher Datenbasis, mit welcher Transparenz?)
- Studien sollen bis Mai 2012 vorliegen
- neuer Kommissions-Vorschlag für VDS-Richtlinie ist für Juli 2012 geplant

ANNEX A

DATA RETENTION EXPERT GROUP: LIST OF COST ELEMENTS FOR COMPLYING WITH DATA RETENTION

21. There is not only the cost for development, maintenance and Operation of data retentipn tools within a provider's PCN/PCS infrastructure but also die cost to the provider's business insofar as the delivery of new innovative Services being negatively impacted by the need to implement DR functionality and integrate new equipment into the network whilst maintaining a data retention capability.

TABLE:

COST TYPES vs. COST ITEM (EXAMPLES)

COST TYPE:
Capital expentiture

COST ITEM:
Training
Testing
Performance
Quality control
Continuity
Procedures for faulty management
Hardware
Software
Retrieval database enabling convenient and timely search and retrieval of data
Collection equipment/ manage acquisition
Secure storage equipment

ANHANG A

VORRATSDATENSPEICHERUNG EXPERTEN-GRUPPE: LISTE DER KOSTENARTEN ZUR EINHALTUNG VORRATSDATENSPEICHERUNG

21. Es gibt nicht nur die Kosten für Entwicklung, Wartung und Betrieb von Datenspeicherungsausrüstung innerhalb einer PCN / PCS-Infrastruktur des Providers, sondern auch abzuschreibende Kosten für das Geschäft des Anbieters, soweit die Lieferung von neuen, innovativen Dienstleistungen nicht negativ durch die Notwendigkeit, DR Funktionalität zu implementieren beeinflusst und durch Integration neuer Geräte in das Netzwerk die Fähigkeit einer Vorratsdatenspeicherung beibehalten bleibt.

TABELLE:

KOSTENTYPEN gegenüber KOSTENDETAIL

KOSTENTYP:
Investitionskosten

KOSTENDETAIL:
Training
Testen
Performance
Qualitätskontrolle
Kontinuität
Verfahren für die fehlerhafte Verwaltung
Hardware
Software
Retrieval-Datenbank ermöglicht bequeme und rechtzeitige Suche und Abruf von Daten
Ausrüstungszusammenstellung / Verwaltung des Einkaufs
Sichere Speicherung Ausrüstung

Security and encryption tools
Development of'existing network elements' to enable integration/ interface with 'DR elements'/ collection and delivery Interfaces/ reengineering of System Interfaces following network Updates, network expansions or changes to network architectures security and access procedures
Continuing Integration

Sicherheits-und Verschlüsselungs-Tools
Entwicklung bestehender Netzwerkelemente. damit Integration / Schnittstelle mit "DR-Elemente" / Einkauf und Lieferung Interfaces / Reengineering von Systemschnittstellen folgende Netzwerk-Updates, Netzwerk-Erweiterungen oder Änderungen Netzwerkarchitekturen Sicherheit und Zugangsverfahren
KontinuierlicheIntegration

COST TYPE:
Operational expentiture

KOSTENTYP:
Laufende Kosten

COST ITEM:
Wages of operations staff
Maintenance of data retention Systems equipment
Training
Operations
Testing
Performance
Quality control
Continuity
Procedures for faulty management
Liaison with competent authorities
security and access procedures
Continuing integration

KOSTENDETAIL:
Die Löhne der IT-Mitarbeiter
Wartung der Vorratsdatenspeicherung-Systeme
Training
Operationen
Testen
Performance
Qualitätskontrolle
Kontinuität
Verfahren für das Problemmanagement
Zusammenarbeit mit den zuständigen Behörden
Sicherheits- und Zugangsverfahren
Fortschreitende Integration