Rat der
Europäischen Union

Brüssel, den 23. November 2018
(OR. en)

14319/18

LIMITE

COPEN 394
CYBER 277
DAPIX 349
ENFOPOL 561

VERMERK

Absender:	Vorsitz
Empfänger:	Ausschuss der Ständigen Vertreter / Rat
Nr. Vordok.:	13826/18
Betr.:	Vorratsdatenspeicherung – Sachstand

I. Einleitung

Unter maltesischem Vorsitz wurde ein Prozess der gemeinsamen Reflexion über die Vorratsdatenspeicherung zum Zwecke der Verhütung und Verfolgung von Straftaten unter Berücksichtigung der Urteile des Europäischen Gerichtshofs in den Rechtssachen *Digital Rights Ireland*[1] und *Tele 2*[2] eingeleitet; dieser Prozess wurde unter estnischem und unter bulgarischem Vorsitz fortgesetzt.

Der Rat (Justiz und Inneres) hat im Dezember 2017 beschlossen, sich bei den weiteren Arbeiten auf drei Hauptelemente zu konzentrieren: Gewährleistung der Verfügbarkeit von Daten (Kohärenz zu dem Entwurf der Online-Datenschutz-Verordnung); Festlegung von Schutzvorkehrungen für den Zugang; ferner Beschränkung des Geltungsbereichs des Regelungsrahmens für die Vorratsdatenspeicherung unter Berücksichtigung der jüngsten Rechtsprechung[3].

1 C-293/12.
2 C-203/15.
3 Dok. 14480/1/17.

Was die Kohärenz zum Entwurf der Online-Datenschutz-Verordnung anbelangt, so ist im Zusammenhang mit der Debatte über die Vorratsdatenspeicherung die Reform des Rahmens für den Online-Datenschutz von Belang. Im Hinblick darauf hielt die Gruppe der Freunde des Vorsitzes (Informationsaustausch und Datenschutz – Vorratsdatenspeicherung) am 12. Februar und 17. Mai 2018 gemeinsame Sitzungen mit der Gruppe "Telekommunikation" ab. Diesbezüglich wurde die Notwendigkeit, innerhalb der neuen Online-Datenschutz-Verordnung die Flexibilität zu wahren, als unverzichtbares Element dafür anerkannt, eine künftige Weiterentwicklung entweder durch die Rechtsprechung des EuGH oder durch legislative Reformen auf nationaler oder europäischer Ebene zu ermöglichen.

Um das Konzept der beschränkten Vorratsdatenspeicherung (Eingriffsstufe 1) inhaltlich auszugestalten, wurden bestimmte Aspekte wie die Begrenzung der Datenkategorien, Beschränkungen der Dauer der Vorratsdatenspeicherung, die Speicherung im Gebiet der Union und die Speicherung in verschlüsselter Form/Pseudonymisierung, in den Bericht an den Rat zur weiteren Vertiefung aufgenommen. Was das Konzept des gezielten Zugangs zu den auf Vorrat gespeicherten Daten (Eingriffsstufe 2) anbelangt, so wurden verschiedene Vorschläge für inhaltliche und verfahrensbezogene rechtliche Anforderungen unterbreitet. Es sei als Vorbemerkung darauf hingewiesen, dass es die gemeinsame Auffassung der Mitgliedstaaten ist, dass die Schlussfolgerungen des EuGH in den Rechtssachen *Digital Rights Ireland* und *Tele 2* nicht für Teilnehmerdaten, sondern lediglich für Verkehrs- und Standortdaten gelten.

Der bulgarische Vorsitz hat in der Gruppe der Freunde des Vorsitzes (Informationsaustausch und Datenschutz – Vorratsdatenspeicherung) die Diskussionen über die Eingriffsstufe 1 (**beschränkte Vorratsdatenspeicherung**) eingeleitet. Am 18. April 2018 hat Europol über die Ergebnisse des Datenmatrix-Workshops berichtet, und die Delegationen haben das mögliche weitere Vorgehen erörtert. Sie haben auch das Konzept erneuerbarer Speicherungsanordnungen ausgelotet. Am 17. Mai 2018 begannen die Diskussionen über die Dauer der Vorratsdatenspeicherung; diese wurden am 10. Juli 2018 unter österreichischem Vorsitz fortgesetzt. Damit war die Prüfung der Elemente zur Eingriffsstufe 1 abgeschlossen. Am 11. September 2018 hat die Gruppe die inhaltlichen und verfahrensbezogenen rechtlichen Anforderungen geprüft, womit die Beratungen über die Eingriffsstufe 2 (**gezielter Zugang zu den auf Vorrat gespeicherten Daten**) abgeschlossen wurden.

Mit dem vorliegenden Dokument stellt der österreichische Vorsitz einen Überblick über den Stand der Erörterungen in der Gruppe der Freunde des Vorsitzes (Informationsaustausch und Datenschutz – Vorratsdatenspeicherung) über die Eingriffsstufen 1 und 2 bereit, zusammen mit den

relevantesten Passagen aus der Rechtsprechung des Gerichtshofs in den Rechtssachen *Digital Rights Ireland* und *Tele 2*. Am 21. November 2018 prüfte der CATS diesen Sachstand zur Vorbereitung der Beratungen im Ausschuss der Ständigen Vertreter am 28. November 2018 und im Rat (Justiz und Inneres) am 6./7. Dezember 2018.

II. Eingriffsstufe 1: beschränkte Vorratsdatenspeicherung

In der Rechtssache *Tele 2* hat sich der EuGH hierzu geäußert; demnach

"(...) untersagt Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 sowie des Art. 52 Abs. 1 der Charta einem Mitgliedstaat nicht, eine Regelung zu erlassen, die zur Bekämpfung schwerer Straftaten vorbeugend die gezielte Vorratsspeicherung von Verkehrs- und Standortdaten ermöglicht, sofern die Vorratsdatenspeicherung ***hinsichtlich Kategorien der zu speichernden Daten****, der erfassten elektronischen Kommunikationsmittel, der betroffenen Personen und der vorgesehenen Dauer der Vorratsspeicherung auf das* ***absolut Notwendige*** *beschränkt ist."*[4]

In den folgenden Absätzen wird auf verschiedene Optionen für die beschränkte Vorratsdatenspeicherung (Eingriffsstufe 1) eingegangen:

1. Begrenzung der Datenkategorien – von Europol koordinierte Arbeiten an einer "Datenmatrix"

Mit dem Konzept der **Begrenzung der Datenkategorien** soll ausgelotet werden, ob Daten, die für die Zwecke der Verhütung und Verfolgung von Straftaten und der Wahrung der öffentlichen Sicherheit nicht absolut unerlässlich und objektiv notwendig sind, von vornherein aus dem Regelungsrahmen für die Vorratsdatenspeicherung ausgeschlossen werden können. Als Mittel zur Begrenzung der Datenkategorien wurden Arbeiten zu einer "Datenmatrix" durchgeführt. Zu diesem Zweck wurde Europol ermutigt, die Vorbereitungsarbeiten für eine solche Datenmatrix auf technischer Ebene in enger Zusammenarbeit mit Experten aus den Mitgliedstaaten mit Blick auf eine weitere Prüfung in der Gruppe der Freunde des Vorsitzes (Informationsaustausch und Datenschutz) voranzubringen[5]. 2018 fanden im März und im Mai im Europol-Hauptquartier in Den Haag zwei Workshops mit nationalen Experten und Ermittlern im Bereich Cyberkriminalität statt.

---

4 *Tele 2*, Randnr. 108.
5 Dok. 14480/1/17 REV 1.

Ein wichtiges Ergebnis der Workshops bestand darin, dass die einschlägigen ETSI-Normen, die als Diskussionsgrundlage dienen, bereits eine "Filterung" der technisch verfügbaren Datensätze bewirkten. Dies bedeutet, dass die Datenkategorien, die als für die Ermittlung und Verfolgung von Straftaten nicht erforderlich erachtet werden, bereits von vornherein aus der Liste ausgeschlossen wurden. Im Ergebnis gelangten die Experten zu dem Schluss, dass nur sehr wenige weitere Datenkategorien als nicht notwendig für die Ermittlung und Verfolgung von Straftaten von den der Liste ausgeschlossen werden könnten. Dies geht auch darauf zurück, dass von Mitgliedstaat zu Mitgliedstaat für verschiedene Strafermittlungen und Ermittlungstechniken unterschiedliche Datenkategorien benötigt werden. Unter anderem wurden diese Ergebnisse von Europol in zwei Dokumenten zusammengefasst und der Gruppe der Freunde des Vorsitzes (Informationsaustausch und Datenschutz – Vorratsdatenspeicherung) vorgelegt[6].

Daher kann, soweit der Aspekt der Begrenzung der Datenkategorien betroffen ist, die Schlussfolgerung getroffen werden, dass es schwierig, wenn nicht gar unmöglich wäre, eine nennenswerte Zahl weiterer Datenkategorien von vornherein von der Speicherung auszuschließen. Der Grund hierfür ist, dass anhand der einschlägigen ETSI-Normen die technisch verfügbaren umfassenderen Datensätze bereits "herausgefiltert" worden sind, da sie speziell für Strafverfolgungszwecke entwickelt wurden. Eine weitere Begrenzung der Kategorien der auf Vorrat gespeicherten Daten würde sich daher nachteilig auf die Wirksamkeit strafrechtlicher Ermittlungen auswirken. Ferner erfordern unterschiedliche Strafermittlungen und Ermittlungstechniken in den Mitgliedstaaten auch unterschiedliche Datenkategorien. Da die für Strafverfolgungszwecke nicht erforderlichen Datenkategorien bereits ausgeschlossen sind, gibt es keine allgemeine und unterschiedslose Vorratsdatenspeicherung im Sinne des EuGH-Urteils in der Rechtssache *Tele 2*.

---

6 Für weitere Einzelheiten siehe folgende Dokumente: WK 4507/2018 INIT (Ergebnisse des ersten Workshops) und WK 5900/2018 INIT (Ergebnisse des zweiten Workshops).

2. Erneuerbare Speicherungsanordnungen (RRW)

Im Arbeitsdokument WK 3974/2018 INIT stellte der bulgarische Vorsitz das Konzept der erneuerbaren Speicherungsanordnungen (RRW) vor. Auch wenn der EuGH in seiner Rechtsprechung nicht auf diesen Aspekt eingegangen war, wurde es für sinnvoll erachtet, dieses Konzept auszuloten. Für die Zwecke der Beratungen wurde eine RRW definiert als

"von einer zuständigen nationalen Behörde an einen bzw. mehrere im Hoheitsgebiet eines Mitgliedstaats tätige(n) Erbringer elektronischer Dienstleistungen gerichtete Anordnung, mit der der bzw. die Erbringer dazu verpflichtet wird bzw. werden, (bestimmte Kategorien von) Daten auf Vorrat zu speichern, und die für einen bestimmten Zeitraum gültig ist, innerhalb dessen sie erneuert werden kann, wenn sie die durch nationale Rechtsvorschriften vorgeschriebenen Bedingungen – einschließlich derjenigen, dass ihre Verhältnismäßigkeit und Notwendigkeit auf der Grundlage einer vorangegangenen Bedrohungsanalyse gerechtfertigt und durch eine anschließende Bedrohungsanalyse bestätigt worden sind – für eine Erneuerung erfüllt."[7]

Somit würde eine RRW die Menge der auf Vorrat gespeicherten Daten begrenzen – aufgrund ihrer festgelegten Geltungsdauer, ihrer Beschränkung auf bestimmte Erbringer elektronischer Dienstleistungen (beispielsweise durch Nichteinbeziehung kleinerer Erbringer elektronischer Dienstleistungen) und/oder der Möglichkeit einer Begrenzung der RRW auf die Vorratsspeicherung von Daten nur bestimmter Kategorien. Ferner würde die für RRW geltende Anforderung, dass sie von einem Justizangehörigen genehmigt werden müssen und dass sie nach Ablauf der Geltungsdauer erneuert werden müssen und/oder andere Verfahrensgarantien eine regelmäßige Überprüfung der Maßnahme sicherstellen.

In der Sitzung der Gruppe der Freunde des Vorsitzes (Informationsaustausch und Datenschutz – Vorratsdatenspeicherung) vom 18. April 2018 war die große Mehrheit der Mitgliedstaaten skeptisch, ob die Idee von RRW als Mittel zur Begrenzung der Menge der auf Vorrat gespeicherten Daten akzeptabel ist[8]. Nur ein Mitgliedstaat, der ein ähnliches System verwendet, äußerte sich zustimmend zu der Idee. Die Hauptargumente der Mitgliedstaaten, die RRW ablehnten, bestanden darin, dass unter ihren nationalen Gegebenheiten der Ansatz zu komplex und zu ineffizient wäre und er in keinerlei Hinsicht in ihr nationales Strafrechtssystem, insbesondere in ihre

---

7 Dok. WK 3974/2018 INIT, S. 1.

8 Zurückhaltung in Bezug auf das Konzept der RRW war auch bereits in der Sitzung vom 6. November 2017 zum Ausdruck gekommen, als das Konzept vom estnischen Vorsitz in Dokument 13845/17 zusammen mit zahlreichen anderen Vorschlägen für die künftigen Arbeiten eingeführt worden war.

Strafprozessordnungen, passen würde.

In Anbetracht der zurückhaltenden Reaktion der meisten Mitgliedstaaten auf die RRW und des Umstands, dass das Konzept in keinerlei Hinsicht vom EuGH erwähnt worden war, erscheint eine weitere Auslotung nicht sinnvoll.

3. Begrenzte
Speicherungsfristen

3.1. Dauer der Speicherung

In der Sitzung vom 17. Mai 2018 bat der bulgarische Vorsitz die Delegationen um Auskunft über die Speicherungsfristen in ihren jeweiligen Mitgliedstaaten ersucht. Die Fristen reichten von einigen Wochen bis zu drei Jahren, doch in den meisten Mitgliedstaaten (die über eine Regelung zur Vorratsdatenspeicherung verfügen) beträgt die Speicherungsfrist entweder sechs oder zwölf Monate.

In der Sitzung vom 10. Juli 2018 ersuchte der österreichische Vorsitz diejenigen Mitgliedstaaten, deren nationale Regelung zur Vorratsdatenspeicherung vor dem Verfassungsgericht oder einem anderen letztinstanzlichen Gericht angefochten worden war, um Auskunft über die Urteile, insbesondere im Hinblick auf die Speicherungsfristen. Es stellte sich heraus, dass die Dauer der Speicherung in den Mitgliedstaaten, die sich zu diesem Thema äußerten, – mit einer Ausnahme – kein zentrales bzw. überhaupt kein Thema in den Erwägungen der zuständigen nationalen Gerichte war, unabhängig davon, ob die Regelung zur Vorratsdatenspeicherung bestätigt oder für ungültig erklärt wurde. Nur in einem Mitgliedstaat wurde die Speicherungsfrist infolge des Verfahrens vor dem nationalen Verfassungsgericht von zwölf Monaten auf sechs Monate verkürzt; in einem anderen Mitgliedstaat wurde die Speicherungsfrist auf Vorschlag des nationalen Verfassungsausschusses verkürzt.

Die Erwägungen des EuGH in *Tele 2* zur Speicherungsfrist beschränken sich auf die Aussage, dass die vorgesehene Dauer der Vorratsspeicherung auf das absolut Notwendige beschränkt sein muss[9]. Mehrere Mitgliedstaaten betonten, dass eine Speicherungsfrist von mindestens zwölf Monaten für eine wirksame Strafverfolgung ihrer Ansicht nach unbedingt notwendig ist.

Folglich lässt sich festhalten, dass die Dauer der Speicherung im Hinblick auf die Rechtsprechung des EuGH ein weniger kritisches Thema zu sein scheint; hingegen ist es von entscheidender Bedeutung, dass Daten für Strafverfolgungszwecke über einen angemessenen Zeitraum zur Verfügung stehen.

9 *Tele 2*, Randnr. 108.

3.2. Unterscheidung zwischen Datenkategorien auf Speicherungsebene

In der Sitzung vom 10. Juli 2018 fragte der österreichische Vorsitz die Delegationen, ob in ihren nationalen Systemen unterschiedliche Speicherungsfristen für verschiedene Datenkategorien vorgesehen sind. Die meisten Mitgliedstaaten gaben an, dass sie hinsichtlich der Speicherung nicht zwischen verschiedenen Datenkategorien unterschieden; nur wenige Mitgliedstaaten gaben an, dass ihre nationalen Rechtsvorschriften derzeit oder in Zukunft eine Unterscheidung vorsähen. Der EuGH äußert sich nicht ausdrücklich zu unterschiedlichen Speicherungsfristen für verschiedene Arten von Datenkategorien, sondern erwähnt nur die Möglichkeit, zwischen verschiedenen Datenkategorien zu unterscheiden[10]. Daraus folgt nicht unbedingt, dass sich die Unterscheidung auf unterschiedliche Fristen für verschiedene Datenkategorien beziehen muss.

Eine andere Möglichkeit als die Unterscheidung zwischen Datenkategorien auf Speicherungsebene wären unterschiedliche Fristen auf Zugangsebene (siehe unten).

3.3. Löschung der Daten nach Ablauf der Speicherungsfrist

In *Digital Rights Ireland* kritisiert der EuGH, dass die Richtlinie 2006/24/EG (Richtlinie über die Vorratsspeicherung von Daten, mit dem Urteil in der genannten Rechtssache für ungültig erklärt) nicht gewährleistet, *"dass die Daten nach Ablauf ihrer Speicherungsfrist unwiderruflich vernichtet werden"*[11]. Demzufolge muss eine Regelung zur Vorratsdatenspeicherung eine konkrete Vorschrift zur Löschung der Daten nach Ablauf der Speicherungsfrist enthalten.

In der Sitzung vom 10. Juli 2018 erklärten alle an der Aussprache beteiligten Mitgliedstaaten, dass sie über **spezifische Vorschriften zur Löschung (oder in einigen Fällen zur Pseudonymisierung) der Daten nach Ablauf der Speicherungsfrist verfügen**. Darüber hinaus berichtete eine Reihe von Mitgliedstaaten, dass die Speicherung der Daten nach Ablauf der vorgeschriebenen Speicherungsfrist gemäß ihren nationalen Rechtsvorschriften zulässig ist, wenn sie für die Geschäftszwecke der Anbieter erforderlich ist. Strafverfolgungsbehörden können auf solche Daten zugreifen, solange das jeweilige Strafprozessrecht eingehalten wird.

10 Siehe Fußnote 2 (*Tele 2*, Randnr. 108).
11 Siehe auch *Tele 2*, Randnr. 122.

4. Anforderungen an die Datensicherheit – Speicherung im Gebiet der Union und Speicherung in verschlüsselter Form/Pseudonymisierung

4.1. Speicherung der Daten im Gebiet der Europäischen Union

In *Tele 2* erklärt der EuGH Folgendes:

"Unter Berücksichtigung der Menge an gespeicherten Daten, ihres sensiblen Charakters und der Gefahr eines unberechtigten Zugangs zu ihnen müssen die Betreiber elektronischer Kommunikationsdienste, um die Unversehrtheit und Vertraulichkeit der Daten in vollem Umfang zu sichern, durch geeignete technische und organisatorische Maßnahmen ein besonders hohes Schutz- und Sicherheitsniveau gewährleisten. ***Die nationale Regelung muss insbesondere vorsehen, dass die Daten im Unionsgebiet zu speichern*** *und nach Ablauf ihrer Speicherungsfrist unwiderruflich zu vernichten sind"*[12].

In der Sitzung vom 10. Juli 2018 (Arbeitspapier WK 7875/2018 INIT) fragte der österreichische Vorsitz die Mitgliedstaaten, ob ihre nationalen Regelungen zur Vorratsdatenspeicherung eine obligatorische Speicherung der Daten im Gebiet der Europäischen Union vorsehen. Von den Delegationen, die sich an der Aussprache beteiligten, berichtete eine knappe Mehrheit, dass eine Speicherung innerhalb der EU (oder, in einem Fall, innerhalb des EWR) obligatorisch sei. In der Hälfte dieser Fälle müssen die Daten sogar im Mitgliedstaat selbst gespeichert werden. Einige der Mitgliedstaaten ohne rechtliche Verpflichtung zur Speicherung der Daten innerhalb der EU äußerten Bedenken hinsichtlich einer solchen Verpflichtung, da sie zu einer unterschiedlichen Behandlung in- und ausländischer Anbieter führen könnte.

Folglich divergieren die Standpunkte der Mitgliedstaaten und die nationalen Regelungen zur Vorratsdatenspeicherung im Hinblick auf die obligatorische Speicherung der Daten innerhalb der EU.

4.2. Speicherung der Daten in verschlüsselter Form/Pseudonymisierung

Der Vorschlag, Daten verschlüsselt zu speichern oder durch Pseudonymisierung zu schützen, geht nicht unmittelbar auf *Digital Rights Ireland* oder *Tele 2* zurück, sondern war einer der Diskussionsvorschläge des estnischen Vorsitzes, um die Forderung des EuGH nach

12 *Tele 2*, Randnr. 122.

Mindesterfordernissen in Bezug auf die Datensicherheit zu erfüllen[13].

[13] Siehe Dok. WK 13845/17, S. 6.

Bei den Beratungen am 10. Juli 2018 gaben nur sehr wenige Mitgliedstaaten an, dass sie Erfahrungen mit Datensicherheitsmaßnahmen wie verschlüsselter Speicherung oder Pseudonymisierung haben. Die meisten an der Aussprache beteiligten Mitgliedstaaten erklärten, dass ihre nationalen Rechtsvorschriften keine Sicherheitsmaßnahmen im Detail vorsehen oder beschreiben. Einige von ihnen fügten hinzu, dass sie solche Maßnahmen kritisch sehen, andere hingegen gaben an, dass sie Maßnahmen wie die Verschlüsselung oder Pseudonymisierung gespeicherter Daten bereits geprüft hätten bzw. derzeit prüften.

Als Antwort auf eine allgemeinere Frage zu technischen Datenschutzmaßnahmen erklärten die meisten Mitgliedstaaten ferner, dass ihre nationalen Rechtsvorschriften zur Vorratsdatenspeicherung keine spezifischen Vorschriften zur sicheren Speicherung der Daten enthielten, sondern dass allgemeine Vorschriften angewandt würden; einige Mitgliedstaaten überlassen es dem Ermessen der Anbieter, angemessene Maßnahmen zur Datensicherheit zu treffen. Nur wenige Mitgliedstaaten gaben an, dass es in ihren Gesetzen und/oder technischen Vorschriften spezifische Anforderungen an die sichere Speicherung von Daten im nationalen System der Vorratsdatenspeicherung gibt.

Generell ist die Frage der Datensicherheit ein aktuelles und wichtiges Thema für die Mitgliedstaaten. Zugleich scheint die Speicherung von Daten in verschlüsselter Form bzw. deren Pseudonymisierung – unter Berücksichtigung der Sichtweise vieler Mitgliedstaaten und der Tatsache, dass der EuGH die verschlüsselte Speicherung von Daten bzw. deren Pseudonymisierung nicht ausdrücklich als spezifische Anforderung nennt[14] – bei der Ermittlung spezifischer Anforderungen an eine Regelung zur Vorratsdatenspeicherung keine vorrangige Frage zu sein.

4.3. Überwachung der Garantien gegen den Missbrauch der Daten durch eine unabhängige Stelle

In *Tele 2* verweist der EuGH ausdrücklich auf die Notwendigkeit, die Einhaltung der Datenschutzgarantien durch eine unabhängige Stelle zu überwachen[15].

---

14 Der EuGH verweist nur allgemein auf Sicherheitsmaßnahmen als unverzichtbare Anforderung an eine künftige Regelung zur Vorratsdatenspeicherung, *Tele 2*, Randnr. 122.

15 *Tele 2*, Randnr. 123.

Bei der Aussprache am 10. Juli 2018 erklärten alle beteiligten Mitgliedstaaten, dass eine nationale Stelle befugt sei, die Garantien der Anbieter in Bezug auf die Vorratsdatenspeicherung zu überwachen. Einige Mitgliedstaaten unterstützten ausdrücklich die Aussage, dass eine solche Überwachung durch eine unabhängige Stelle als Argument zur Verteidigung nationaler Rechtsvorschriften für die Vorratsdatenspeicherung herangezogen werden könnte. **Eine Regelung zur Vorratsdatenspeicherung, die im Einklang mit dem Unionsrecht steht, sollte daher eine Bestimmung enthalten, nach der eine unabhängige nationale Stelle die Einhaltung der Garantien überwacht.**