

Von: Eisenreich, Julius
Gesendet: Mittwoch, 3. November 2021 08:42
An: 'Saebisch, Steffen'; 'Bundesvorsitzende'
Cc: Wolfgang.Schmidt@bmf.bund.de
Betreff: Vorgehen der geschäftsführenden Bundesregierung auf EU-Ebene
Anlagen: Non-paper KOM_ Antwortbeitrag.docx; Anlage 1 - Non paper WK 7294-2021.pdf

Lieber Herr Saebisch, lieber Herr Heinrich,

zu den von Ihnen konkret angesprochenen Themen der Europapolitik habe ich folgende Informationen zusammentragen können:

Die verschiedenen KOM-Überlegungen zur Einstufung von Wirtschaftsaktivitäten zu den Umweltzielen 1 und 2 der Taxonomie und deren Auswirkungen sind bereits seit längerem Gegenstand der Diskussionen auf europäischer Ebene und auch der Abwägung und Prüfung der Bundesregierung. Das Verfahren für das Zustandekommen der Delegierten Rechtsakte, deren Rechtsgrundlagen sich in der von EP und Rat beschlossenen und bereits im Juli 2020 in Kraft getretenen Taxonomie-VO finden, ist allerdings weitgehend in der Hand der Europäischen Kommission und die Verfahrensanforderungen für eine Einflussnahme durch EP und Rat sehr hoch. Zum Delegierten Rechtsakt zu den Umweltzielen 1 und 2 muss bis zum 8. Dezember 2021 eine Entscheidung des Rates getroffen werden.

Grundlage der Verhandlungen der bisherigen Bundesregierung im Zusammenhang mit dem „Fit-for-55“-Paket war eine erste gemeinsame Stellungnahme der Ressorts vom Mai dieses Jahres. Die geschäftsführende Bundesregierung wird – entsprechend des politischen Gebots zur Selbstbeschränkung – in den kommenden Verhandlungen auch zu den „Fit-for-55“-Themen keine weitergehenden politischen Festlegungen treffen, die eine künftige Bundesregierung binden.

Bei den von Ihnen hervorgehobenen Themen Energieeffizienz, EE und „Ende des Verbrenners“ bzw. CO₂-Pkw-Standards ist keine Einigung im Rat vor dem nächsten Jahr zu erwarten.

Bei der von Ihnen darüber hinaus angesprochenen „Initiative zur Weiterentwicklung der EU-Battlegroups“ handelte es sich um einen gemeinsam mit Finnland, den Niederlanden, Portugal und Slowenien eingebrachten fachlichen Beitrag des BMVg im Rahmen der sog. „strategischen Dialogphase“ zur Erarbeitung des „Strategischen Kompasses der EU“. Das Gedankenpapier beinhaltete keine neue Positionierung der bisherigen Bundesregierung, sondern einen ergebnisoffenen Beitrag für die laufende Diskussion zur Stärkung des europäischen Krisenmanagements, die innerhalb der EU zwischen den Mitgliedstaaten diskutiert werden.

Mit Blick auf das Thema Geldwäsche hat sich die bisherige Bundesregierung in der Vergangenheit regelmäßig an den Standards der FATF als globaler Standardsetzerin für die Bekämpfung von Geldwäsche und Terrorismusfinanzierung orientiert und zugleich das Ziel verfolgt, die Arbeit der FATF auf EU-Ebene nicht zu duplizieren. Sie hat sich daher insbes. in den Verhandlungen zur AMLR für einen rein technischen Listungsprozess ausgesprochen und die Haltung vertreten, dass Abweichungen von den Empfehlungen der FATF, auch wenn sie zu einer Verschärfung der AML-Gesetzgebung führen würden, dementsprechend gut begründet sein sollten.

Zu den Leitlinien der KOM zur Anwendung der Beihilfavorschriften im Klima-, Umwelt- und Energiebereich (KUEBLL) hat die bisherige Bundesregierung Mitte August eine Stellungnahme an die KOM übermittelt. Der weitere Ausbau der Erneuerbaren, die Steigerung der Energieeffizienz und die Unterstützung des Green Deals zählen zu den zentralen Anliegen, mit denen sich die bisherige Bundesregierung eingebracht hat. Die Mitgliedstaaten waren über die öffentliche Konsultation hinaus nicht formell beteiligt.

Zum Green Deal und seinem für die Landwirtschaft besonders wichtigen Bestandteil der Farm-to-Fork-Strategie gibt es bislang keinerlei bindenden EU-Rechtsakt oder auch nur eine umfassende Folgenabschätzung. Beides ist nach Auffassung der bisherigen Bundesregierung aber notwendig, um bei der Beurteilung der nationalen Strategiepläne im Rahmen der GAP 2023 zugrunde gelegt zu werden.

Schließlich zum Spiegelartikel zur Vorratsdatenspeicherung: Er dürfte sich auf die deutsche Antwort auf ein non-paper der EU-Kommission beziehen. Das Papier der EU Kommission stammt aus Juni 2021 und die Antwort aus Juli 2021, also aus der Zeit deutlich vor der Bundestagswahl. Beide Papiere sind auch nicht „geheim“. Das non-paper ist von Netzpolitik.org bereits am 16. Juli veröffentlicht worden. Dass die deutsche Antwort (durch die EU-Kommission) auch veröffentlicht werden kann, hat die Bundesregierung der EU-Kommission im Oktober mitgeteilt. Inhaltlich ist das deutsche Papier im Wesentlichen eine Beantwortung der von der Kommission gestellten Fragen auf der Basis des geltenden Rechts. Konkrete Vorschläge werden nicht gemacht. Ich habe Ihnen beides zur Kenntnis angehängt.

Viele Grüße

Julius Eisenreich

Julius Eisenreich

Sprecher und stellvertretender Büroleiter des Chefs des Bundeskanzleramtes

Tel. 030184002080

julius.eisenreich@bk.bund.de

-----Ursprüngliche Nachricht-----

Von: Robert Heinrich <Robert.Heinrich@gruene.de>

Gesendet: Montag, 25. Oktober 2021 18:27

An: Eisenreich, Julius <Julius.Eisenreich@bk.bund.de>

Cc: Braun, Helge <Helge.Braun@bk.bund.de>; Saebisch, Steffen <steffen.saebisch@fdpbt.de>

Betreff: Vorgehen der geschäftsführenden Bundesregierung auf EU-Ebene

Sehr geehrter Herr Eisenreich,

haben Sie vielen herzlichen Dank für die bisherige stets gute Zusammenarbeit!

Ergänzend zum heutigen Brief der Parteivorsitzenden von GRÜNEN und FDP zur Selbstbeschränkung der geschäftsführenden Bundesregierung erlauben wir uns, einige Hinweise zu geben, wo das aktuelle Handeln der Bundesregierung auf EU-Ebene mit Blick auf das Prinzip der Selbstbeschränkung aus unserer Sicht Fragen aufwirft - bei allem Verständnis, dass das laufende Geschäft natürlich weitergehen muss. Ich wäre dankbar, wenn Sie diese Punkte zeitnah prüfen und uns dazu eine Rückmeldung geben.

Mit freundlichen Grüßen

Robert Heinrich

Büroleiter der Bundesvorsitzenden
Annalena Baerbock und Robert Habeck

Taxonomie: Aktuell macht sich Frankreich dafür stark, dass Atomenergie als "grün" gelabelt werden soll. Andere Länder engagieren sich für Gas als "grünen" Energieträger in der Taxonomie. Beides käme einer Festlegung mit erheblichen Folgen gleich - und wäre kaum noch zu ändern, wenn es einmal in den Entwürfen der Kommission steht.

Wir erwarten, dass sich die geschäftsführende Bundesregierung gegenüber der EU-Kommission mit Nachdruck für eine Verschiebung des KOM-Entwurfs einsetzt, damit wir als neue BR noch entsprechend agieren können. Diese Verschiebung wollen auch Teile der KOM. Mit Blick auf die anstehende Abstimmung (spätestens zum 7.12.) im Rat über die bisher vorliegenden delegierten Rechtsakte zur Taxonomie (also ohne Energie) wird es entscheidend auf

Deutschland ankommen. Die BR muss hier zwingend zustimmen oder sich zumindest enthalten, was ja einer Stillhaltevereinbarung entspräche. Bei einer Ablehnung wäre die "sustainable finance"-Strategie der EU Geschichte.

Fit for 55: Die Verhandlungen im Rat beginnen jetzt. Die slowenische Ratspräsidentschaft will zu einigen Dossiers noch vor Ende dieses Jahres zu einem Ratsstandpunkt kommen. Die Position der geschäftsführenden BR muss hier aus unserer Sicht die der neuen BR unbedingt widerspiegeln. Das gilt vor allem für Energieeffizienz und EE, hier besonders die Solar-Initiative, sowie das Ende des Verbrenners.

Verteidigung: Vor rund einer Woche hat die BR gemeinsam mit den Niederlanden, Portugal, Finnland und Slowenien eine Initiative zur Weiterentwicklung der EU-Battlegroups gestartet. Konkret lautet ein Vorschlag, über den noch nie genutzten Artikel 44 des EU-Vertrags Einsätze von Koalitionen der Willigen zu ermöglichen. Das ist ein weitreichender Vorstoß, den wir - unabhängig von der inhaltlichen Positionierung dazu - so kurz vor einem Regierungswechsel als kritisch bewerten.

Geldwäsche: Zehn EU-Mitgliedstaaten inkl. Deutschland haben sich nach unserer Information kürzlich per Brief dagegen verwendet, dass die Kommission im neuen Anti-Geldwäsche-Gesetzespaket die eigene Schwarze Liste über die FATF-Minimalliste hinaus erweitert. Die zehn Staaten haben sich auch gegen eine automatische Verschärfung der Verpflichtungen (verstärkte Sorgfaltspflicht gegenüber Kund*innen) ausgesprochen, die laut Kommission mit der Aufnahme eines Landes in die "graue Liste" einhergehen sollte. Damit zielen aus unserer Sicht auf eine Abschwächung der Anti Geldwäsche-Vorschläge der Kommission ab.

Beihilferecht: Zurzeit arbeitet die KOM an neuen Richtlinien zum Beihilferecht. Es soll Green-Deal-konform ausgerichtet werden. Die geschäftsführende BR sollte auch hier im Sinne der neuen BR agieren und klar Beihilfen für EE unterstützen: eigene Kategorie, Südkategorie, Ausnahmen für energy communities. Auch sollte sie keine falschen Festlegungen vertreten, z.B. Signale für fortgesetzte Beihilfegenehmigungen für fossile Brennstoffe und Atomenergie geben.

Agrar: In Vertretung von Julia Klöckner hat sich deren Staatssekretärin jüngst im Rat gegen den Vorschlag der KOM ausgesprochen, die nationalen Strategiepläne zur GAP auf Grundlage des Green Deal zu prüfen und zu validieren. Das könnte weitreichende Konsequenzen haben, die unseres Erachtens mit einem Selbstbeschränkungs-Ansatz unvereinbar sind.

BÜNDNIS 90/DIE GRÜNEN
Bundesgeschäftsstelle
Platz vor dem neuen Tor 1
10115 Berlin

T: 00493028442129
F: 00493028442249
M: 004917610020596
robert.heinrich@gruene.de

www.gruene.de



Council of the European Union
General Secretariat

Brussels, 10 June 2021

WK 7294/2021 INIT

LIMITE

COPEN

CYBER

ENFOPOL

JAI

DATAPROTECT

WORKING PAPER

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

NOTE

From:	Commission
To:	Delegations

Subject:	Non-paper on the way forward on data retention – Presentation by the Commission and exchange of views
----------	--

Delegations will find in the Annex a Non-paper from the Commission on the above mentioned subject.

Data retention – Commission services non-paper

Contribution to the Council COPEN Working Party meeting of 16 June 2021

This non-paper has not been adopted or endorsed by the European Commission. Any views expressed are the preliminary views of the Commission services and may not in any circumstances be regarded as stating an official position of the Commission.

1. Introduction

The laws of a majority of Member States provide for the retention and use of electronic communications metadata for the protection of national and public security and the fight against crime. At the same time, where such measures include indiscriminate and generalised data retention, they have raised important questions on interference with fundamental rights, including the rights to privacy and protection of personal data.

In its recent judgements¹, the Court of Justice of the European Union (CJEU) confirmed its previous jurisprudence² that electronic communications data are confidential and that, in principle, traffic and location data cannot be retained in a general and indiscriminate manner. At the same time, the CJEU identified certain situations where retention is permissible, based on clear and proportionate obligations laid down in law and subject to strict substantive and procedural safeguards. There are three data retention cases from Germany³, Ireland⁴ and France⁵ still pending before the CJEU.

On 11 March 2021, Justice Ministers exchanged views on the retention of electronic communications (meta) data. There was broad support among Member States to explore the possibilities of new EU legislation on data retention, while some considered it necessary to have more discussions on how to ensure compliance with the various CJEU rulings before moving to the next step.

On 17 December 2020, the European Parliament adopted a resolution on the EU Security Union Strategy noting that in its October 2020 rulings, the CJEU upheld previous case law, concluding that only a targeted retention of data limited to specific persons or a specific geographical area is allowed but also specified that IP addresses assigned to the source of a communication may be subject to generalised and indiscriminate retention for the purpose of combating serious crime and serious threats to public security, subject to strict safeguards. The European Parliament adopted a resolution of 26 November 2020 on the situation of fundamental rights in the EU in 2018-2019 in which it calls on the European Commission to launch infringement procedures against Member States whose laws implementing the invalidated Data Retention Directive have not been repealed to bring them into line with the CJEU case law. In its resolution of 12 December 2018 on findings and recommendations of the Special Committee on Terrorism, the European Parliament urges the Commission to evaluate a

¹ Judgments in Case C-623/17, *Privacy International* and Joined Cases C-511/18, C-512/18 and C-520/18 *La Quadrature du Net a.o.* of 6 October 2020 and Case C-746/18 *Prokuratuur* of 2 March 2021.

² Judgments in Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland a.o.* of 8 April 2014, Joined Cases C-203/15 and C-698/15, *Tele2 Sverige a.o.* of 21 December 2016 and Case C-207/16 *Ministerio Fiscal* of 2 October 2018.

³ Joined Cases C-793/19 and C-794/19 - *SpaceNet a.o.*

⁴ Case C-140/20 *Dwyer*.

⁵ Joined cases C-339/20 and C-397/20 *VD a.o.*

I. Allgemeine Anmerkungen

Die Entscheidung über ein europäisches Instrument der Vorratsdatenspeicherung kann erst dann getroffen werden, wenn die sich aus den Entscheidungen des Europäischen Gerichtshofs ergebenden noch offenen Fragen geklärt sind und insbesondere Einigkeit zwischen den Mitgliedstaaten über das ob und wie einer europäischen Regelung besteht.

Das hat Deutschland im Rahmen der Informellen Sitzung der Justizminister am 11. März 2021 betont. An dieser Einschätzung halten wir weiterhin fest.

Dass die Möglichkeiten und die Reichweite einer europäischen Lösung angesichts der derzeit noch anhängigen Verfahren vor dem Europäischen Gerichtshof noch nicht endgültig eingeschätzt werden können, gilt insbesondere mit Blick auf das deutsche Vorlageverfahren. Unter Berücksichtigung dessen, dass die deutsche Regelung zur Vorratsdatenspeicherung im europäischen Vergleich besonders restriktiv ausgestaltet ist, gehen wir davon aus, dass der Gerichtshof diese als europarechtskonform anerkennen wird und wir erwarten insbesondere von dieser Entscheidung weitere Erkenntnisse und die Klärung noch offener Fragen.

Einen rein nationalen Ansatz der Vorratsdatenspeicherung lehnen wir allerdings ab. Zwar würde ein rein nationaler Ansatz ein höheres Maß an Flexibilität ermöglichen und hätte zur Folge, dass auf die unterschiedlichen nationalen Besonderheiten und Bedürfnisse näher eingegangen werden könnte. Gleichzeitig führt dieser Ansatz jedoch zu stark voneinander divergierender Regelungen innerhalb der einzelnen Mitgliedstaaten. Damit würde das ursprünglich verfolgte Ziel, einer Harmonisierung im Bereich der Strafverfolgung, aufgegeben. Zudem sendet ein solcher Schritt aus unserer Sicht ein falsches Signal angesichts einer immer weiterwachsenden Zahl grenzüberschreitender Straftaten, nicht nur im Bereich der Internetkriminalität, sondern auch im Bereich des organisierten Verbrechens.

Auch unter Berücksichtigung, dass es mit der Richtlinie 2006/24/EG bereits ein europäisches Regelungsinstrument gab, sollte eine europäische Herangehensweise aus unserer Sicht nicht aufgegeben werden.

Mit Blick auf ein mögliches europäisches Instrument ist zu beachten, dass die Entscheidungen des Europäischen Gerichtshofs das Primärrecht, also die Interpretation der europäischen

Grundrechte, betreffen. Ein neues europäisches Regelungsinstrument zur Vorratsdatenspeicherung müsste sich daher an diesen Vorgaben und damit an der Grundrechte-Charta der EU messen lassen und mit dieser im Einklang stehen. Aus diesem Grunde befürworten wir die von der Kommission vorgeschlagene Herangehensweise, die sich an den von dem Gerichtshof aufgestellten Kategorien orientiert. Dies bedeutet gleichzeitig, dass Öffnungsklauseln im Bereich des Sekundärrechts (wie der E-Privacy-Verordnung) aus deutscher Sicht die von dem Gerichtshof aufgezeigte Rechtslage nicht zu ändern vermögen. Deutschland hatte sich bereits im Rahmen der Verhandlungen zur E-Privacy-Verordnung im Februar 2021 gegen eine (Mit-)Regelung der Vorratsdatenspeicherung in der E-Privacy-Verordnung ausgesprochen. Eine solche Mitregelung der Vorratsdatenspeicherung in einem anderen Sekundärrechtsakt lehnen wir weiterhin ab.

Grundsätzlich denkbar erschiene schließlich ein „gemischter“ Ansatz, nur bestimmte Aspekte in einem europäischen Rechtsinstrument zu regeln. Im Fokus sollte indes eine möglichst einheitliche Regelung stehen.

II. Zu den von der Kommission vorgeschlagenen Regelungsansätzen im Einzelnen

- Allgemeine Speicherung von Verkehrs- und Standortdaten für Zwecke der nationalen Sicherheit - Ansatz 3a

In light of the delineation of national and EU competences, what are Member States' views on a legislative initiative that would harmonise certain criteria relating to the retention of traffic and location data and related access conditions for national security purposes, for situations that involve private actors (for storage, transmission and providing access to data to relevant competent authorities)?

Mit den Urteilen vom 6. Oktober 2020 (verbundene Rechtssachen C-511/18, C-512/18 und C-520/18 „Quadrature du Net u.a.“ und C-623/17, „Privacy International“) hat der Europäische Gerichtshof entschieden, dass eine nationale Regelung, die es einer staatlichen Stelle gestattet, den Betreibern elektronischer Kommunikationsdienste vorzuschreiben, zur Wahrung der nationalen Sicherheit den Sicherheits- und Nachrichtendiensten Verkehrs- und Standortdaten zu übermitteln, in den Geltungsbereich der Richtlinie 2002/58 fällt. Gleichzeitig hat der Gerichtshof klargestellt, dass eine allgemeine und unterschiedslose Speicherung von Verkehrs- und Standortdaten für einen eng begrenzten Zeitraum in Fällen einer als real und aktuell oder vorhersehbar einzustufenden ernststen Bedrohung für die nationale Sicherheit zulässig ist.

Hinsichtlich der Erstreckung eines europäischen Regelungsinstruments auf den Bereich der nationalen Sicherheit haben wir auch unter Berücksichtigung der Ausführungen des Europäischen Gerichtshofs in den genannten Entscheidungen mit Blick auf Artikel 4 Absatz 2 EUV Vorbehalte, da wir die nationale Sicherheit weiterhin im alleinigen Zuständigkeitsbereich der Mitgliedstaaten verorten. Sollte man sich indes für ein europäisches Regelungsinstrument in dem Bereich entscheiden, teilen wir die Einschätzung der Kommission, dass die in dem Papier dargelegten Kriterien Voraussetzungen für eine entsprechende Speicherung sein müssten.

In diesem Zusammenhang weisen wir darauf hin, dass der Bereich der nationalen Sicherheit im deutschen Recht derzeit von der Vorratsdatenspeicherung ausgenommen ist.

- Gezielte Speicherung von Verkehrs- und Standortdaten zur Bekämpfung schwerer Straftaten und zur Verhütung ernster Bedrohungen der öffentlichen Sicherheit - Ansatz 3b

- What are the legal challenges for Member States and the technical challenges for providers to comply with a targeted retention obligation and how could they be overcome? Please be as specific and concrete as possible in your responses.*

- What is the 'objective evidence' (in the case of persons) and what are the 'objective and non-discriminatory factors' (in the case of geographical areas) or other objective criteria that Member States could consider in drawing up a targeted retention framework?*

- Do Member States consider there is merit in revisiting the 'data matrix' exercise initiated by Europol in 2018 to try to find ways to devise a targeted retention system that fulfils the Court's requirements?*

- Do Member States consider there is merit in devising a targeted retention system by developing criteria to limit the means of communication or the number or type of electronic communications service providers subject to retention obligations (e.g. based on size, geographical coverage, number of subscribers, cross-border presence)?*

- Can Member States share their views of what serious threats to public security entails?*

Das von dem Europäischen Gerichtshof entwickelte Instrument der gezielten Speicherung, also Speicherpflichten, die sich auf einen bestimmten Personenkreis oder ein bestimmtes geographisches Gebiet beschränken, ist keine gleich effektive Alternative zu einer allgemeinen Vorratsdatenspeicherung.

In aller Regel ist den Strafverfolgungsbehörden im Vorfeld – d. h. vor Bestehen eines konkreten Tat- bzw. Gefahrenverdachts – nicht bekannt, wann, wo und durch wen Straftaten begangen werden. Sowohl die für nichtig erklärte Richtlinie 2006/24/EG als auch die jeweiligen nationalen Regelungen zur allgemeinen Vorratsdatenspeicherung beruhen gerade auf dem Umstand, dass sich nicht voraussagen lässt, welche Verkehrsdaten welcher Personen aus welchem Gebiet und in welchem Zeitraum zur Bekämpfung der schweren Kriminalität benötigt werden. Schwere Straftaten werden nicht nur in bestimmten geographischen Räumen begangen und sie finden oftmals im privaten Umfeld statt. Zudem findet die entscheidende Kommunikation oftmals gerade dort nicht statt, wo sich die Straftat ereignet oder sich eine Gefahr verwirklicht. Gerade im Bereich organisierter Kriminalität ist die Auswertung des Kommunikationsverhaltens im Vorfeld einer Tat von entscheidender Bedeutung für die Bewertung von Tatbeiträgen. Gleichzeitig ist eine auf einen geographischen Bereich beschränkte Speicherung angesichts der Mobilität von Tatverdächtigen wenig gewinnbringend.

In rechtlicher Hinsicht stellt sich das zudem das Problem, wie eine solche gezielte Speicherung erfolgen kann, ohne dass damit die Diskriminierung bestimmter Personengruppen einhergeht. Dies gilt sowohl für die gezielte Speicherung der Daten einer bestimmten Person selbst als auch für die Bildung spezifischer geographischer Gebiete.

Ein mögliches Kriterium für eine (in die Zukunft gerichtete) personenbezogene Speicherung in Einzelfällen könnte aus unserer Sicht allenfalls bejaht werden, wenn aufgrund konkreter Hinweise und Erkenntnisse der begründete Verdacht besteht, dass eine Person eine Straftat von auch im Einzelfall erheblicher Bedeutung, begangen, zu begehen versucht oder eine Straftat vorbereitet hat bzw. wenn im Bereich der Terrorismusbekämpfung von einer Person eine erhebliche Gefahr für die öffentliche oder nationale Sicherheit ausgeht. Eine rechtskräftige Vorstrafe allein dürfte demgegenüber aus hiesiger Sicht kein anwendbares Kriterium darstellen, da dies unweigerlich zu einer Vorverurteilung führen würde.

Darüber hinaus ist eine gezielte Speicherung technisch kaum umsetzbar. So ist allein die konkrete Bestimmung, welche Funkzellen in einem bestimmten Gebiet genutzt werden, für die Provider nach dem derzeitigen Stand der Technik nicht möglich, da je nach Auslastung des Netzes bzw. Standort einer Person auch andere Funkzellen genutzt werden können. Zudem müsste sichergestellt sein, dass eine Speicherung ab dem Moment endet, indem ein Gerät einen bestimmten geographischen Standort verlässt bzw. von Neuem beginnt, wenn das Gerät wieder in den Bereich eintritt.

Unter Berücksichtigung der bislang durch den Gerichtshof einzig in Betracht gezogenen Kriterien der personenbezogenen bzw. geographischen Speicherung, erscheint eine erneute Überprüfung der 2018 durch Europol erarbeiteten „Daten-Matrix“ nicht gewinnbringend.

Etwas anderes gilt jedoch dann, wenn man neben den Kriterien der personenbezogenen und geographischen Speicherung auch ein weiteres Kriterium anerkennt, das der Generalanwalt in seinem Schlussvortrag in der Rechtssache C-520/18 ins Spiel gebracht hat, nämlich eine Speicherung in Bezug auf die Kategorien der Daten. Insoweit messen wir die Entscheidung des Europäischen Gerichtshofs in dem deutschen Vorlageverfahren besondere Bedeutung zu, da in unserem nationalen Recht eine solche Beschränkung sowohl in Bezug auf die Datenkategorien als auch die Speicherdauer vorgenommen wird.

Bei der Entwicklung eines Systems gezielter Speicherung, das sich an den Kommunikationsmitteln bzw. der Größe der jeweiligen Provider orientiert, ist zu berücksichtigen, dass eine solche Beschränkung unweigerlich dazu führen würde, dass andere Mittel bzw. Provider durch Tatverdächtige genutzt werden würden, ohne dass sich an der Eingriffsintensität der übrigen Nutzer etwas ändern würde. Gleichzeitig wäre indes dafür Sorge zu tragen, dass gerade kleinere Unternehmen nicht über Gebühr belastet werden, so dass die jeweiligen Interessen in Ausgleich zu bringen sind.

- Umgehende Speicherung von Verkehrs- und Standortdaten zur Bekämpfung schwerer Straftaten und zur Verhütung ernsther Bedrohungen der öffentlichen Sicherheit (Quick-freeze) – Ansatz 3c

- *Given that a "quick freeze" provision can apply only if there is metadata available to "freeze", can Member States share any experience relating to the normal period of availability of metadata, absent a general retention obligation? Can Member States point to any ideas stemming from that experience that may be helpful in this context?*
- *Can Member States share any experience relating to the use of expedited retention in their current legislation?*
- *Which options do Member States see for operationalising this mechanism to meet its objective to support investigations into serious crime and protection of national security?*

Mit seiner Entscheidung in den verbundenen Rechtssachen C-511/18, C-512/18 und C-520/18 „Quadrature du Net u.a.“ vom 6. Oktober 2021 weist der Europäische Gerichtshof ferner auf

die Möglichkeit der umgehenden Speicherung von Daten hin und nimmt dabei auf das Übereinkommen des Europarats vom 23. November 2001 über Computerkriminalität (SEV Nr. 185, sogenannte Budapest Konvention) Bezug. Eine solche umgehende Speicherung ist nach der Entscheidung des Gerichtshofs zur Bekämpfung schwerer Kriminalität und zum Schutz der nationalen Sicherheit möglich, soweit diese in Umfang und Zeitraum auf das Notwendige beschränkt bleibt.

Die deutsche Rechtsordnung kennt kein „Quick-freeze“-Verfahren, da unsere nationale Regelung zur Vorratsdatenspeicherung weitgehender ist, so dass kein Umsetzungsbedarf in Bezug auf die Budapest Konvention gesehen wurde. Vor diesem Hintergrund können wir zu Erfahrungen bei der Umsetzung keine Stellung nehmen. Das „Quick-freeze“-Verfahren stellt jedoch aus unserer Sicht keine mit der Vorratsdatenspeicherung vergleichbar effektive Aufklärungsmöglichkeit dar, da eine Speicherung immer erst im Einzelfall und erst zu dem Zeitpunkt angeordnet wird, zu dem dazu wegen eines bestimmten Tatverdachts konkreter Anlass besteht. Die Daten aus der Zeit vor der Anordnung ihrer Speicherung können damit nur erfasst werden, wenn und soweit sie bei den Betreibern bspw. zu Abrechnungszwecken noch vorhanden sind, was – ohne dass eine Pflicht zur Speicherung vorliegt und angesichts der steigenden Zahl von Flatrate-Tarifen – immer seltener der Fall ist. Bei der Aufklärung von Straftaten, deren Begehung nicht vorhergesehen werden kann, spielt indes die Aufklärung der Ereignisse, die sich vor der Tatbegehung ereignet haben, die größte Rolle, um kriminelle Netzwerke bzw. Strukturen zu ermitteln.

- Allgemeine Speicherung von IP-Adressen zur Bekämpfung schwerer Straftaten und zur Verhütung ernster Bedrohungen der öffentlichen Sicherheit – Ansatz 3d

- Do Member States see the benefits of this approach? Do they see any drawbacks in this approach e.g. that the IP address of the destination of a communication is not retained? Is there a lawful way to overcome this limitation?

- Are there other technical identifiers that could, in line with the jurisprudence, be captured in such legislation for example time stamps and source-port numbers to allow for identification of individuals where IP addresses are shared across multiple users, as may be the case e.g. in mobile communications?

- What cybercrimes are not currently covered by the notion of 'serious crime' in Member States' legislation?

In der Entscheidung in den verbundenen Rechtssachen C-511/18, C-512/18 und C-520/18 „Quadrature du Net u.a.“ hat sich der Europäische Gerichtshof darüber hinaus das erste Mal zu der anlasslosen Speicherung von IP-Adressen verhalten und dabei betont, dass IP-Adressen einen geringeren Sensibilitätsgrad als übrige Verkehrsdaten aufweisen, sofern im Bereich von E-Mail und Internettelefonie nur die IP-Adressen der Kommunikationsquelle gespeichert werden und nicht die des Adressaten einer Kommunikation. Der Gerichtshof begründet dies damit, dass sich diesen Adressen als solchen keine Information über die Dritten entnehmen lassen, mit denen die Person, von der die Kommunikation ausging, in Kontakt stand.

Der Gerichtshof erkennt damit an, dass IP-Adressen, die von den Telekommunikationsdiensten für eigene Zwecke häufig nicht oder nur für sehr kurze Zeit gespeichert werden, in vielen Fällen den einzigen Ermittlungsansatz darstellen, wenn Straftaten im Internet begangen werden und damit die einzige Spur sind, die verfolgt werden kann, um einen Beschuldigten zu ermitteln. Dies gilt insbesondere bei Straftaten im Bereich der Kinderpornografie. Neben dem Schutz der nationalen Sicherheit vermögen nach der Rechtsprechung des Gerichtshofs nur die Bekämpfung schwerer Kriminalität und die Verhütung schwerer Bedrohungen der öffentlichen Sicherheit diesen Eingriff zu rechtfertigen.

Im deutschen Recht wird zwischen schweren und besonders schweren Straftaten unterschieden. Nach derzeitiger Rechtslage setzt ist die Vorratsdatenspeicherung nach § 100g Absatz 2 StPO das Vorliegen einer besonders schweren Straftat voraus und sieht dabei einen abschließenden Straftatenkatalog vor, der indes nicht sämtliche Fälle der Computerkriminalität umfasst. Nicht unter die besonders schweren Straftaten fallen beispielsweise die Tatbestände des Ausspähens und Abfangens von Daten bzw. Vorbereitungshandlungen hierzu wie auch die Datenhehlerei (§§ 202a bis 202d des Strafgesetzbuchs), aber auch der Computerbetrug (§ 263a des Strafgesetzbuchs), der jedoch als schwere Straftat eingeordnet wird.

- Allgemeine Speicherung der die Identität betreffenden Daten zur Bekämpfung von Kriminalität und Bedrohungen der öffentlichen Sicherheit generell, Ansatz 3e

- *Is retention of 'civil identity data' effective to fight crimes?*
- *What specific elements should be included in this data category?*

Der Begriff der „die Identität der Nutzer elektronischer Kommunikationsmittel betreffenden Daten“, der von dem Europäischen Gerichtshof sowohl in seiner Entscheidung vom 6. Oktober 2020 (verbundene Rechtssachen C-511/18, C-512/18 und C-520/18 „Quadrature du Net u.a.“) als auch vom 2. März 2021 (Rechtssache C-746/18, „Prokuratuur“) verwendet wird, ist nach

hiesiger Auffassung kein etablierter Begriff des EU-(Telekommunikations-)Rechts, so dass unsicher erscheint, welche Datenkategorien der Europäische Gerichtshof hiervon umfasst wissen will. Der Zugriff wird durch den Gerichtshof grundsätzlich nicht als schwer eingestuft, da diese Daten keine Informationen über die konkreten Kommunikationen und infolgedessen über das Privatleben eines Betroffenen liefern, wenn man von Kontaktdaten wie Adressen absieht.

Nach deutschem Verständnis dürften mit „die Identität der Nutzer elektronischer Kommunikationsmittel betreffenden Daten“ Bestandsdaten gemeint sein. Die Speicherung und der Zugriff auf diese Daten ist ein wichtiger Bestandteil zu Beginn eines Ermittlungsverfahrens, um einen noch unbekannten Täter zu identifizieren. Die Abfrage dieser Daten kann aber stets nur einen ersten Schritt zur Aufklärung eines Sachverhalts darstellen und ist für sich genommen nicht ausreichend.

Nach deutscher Rechtslage ist eine Bestandsdatenabfrage auch anhand einer dynamischen IP-Adresse möglich, obwohl die dynamische IP-Adresse selbst als Verkehrsdatum gilt. Dies bedeutet, dass die Strafverfolgungsbehörden mit einer ihnen bekannten IP-Adresse (z.B. auf einem beschlagnahmten Gerät festgestellt) an die Telekommunikationsdiensteanbieter herantreten und um die Beauskunftung der Bestandsdaten zu dem Nutzer, dem die IP-Adresse zu einem bestimmten Zeitpunkt zugeordnet war, bitten. Zur Zuordnung und damit zu Auskunftserteilung dürfen die Telekommunikationsdiensteanbieter auf alle vorliegenden Verkehrsdaten, auch die nach § 113b TKG gespeicherten Daten zurückgreifen. Die Verkehrsdaten werden aber ausschließlich zur Zuordnung herangezogen, aber nicht an die Strafverfolgungsbehörden herausgegeben. Diesen werden nur die jeweiligen Bestandsdaten übermittelt. Dies ist nach hiesigem Dafürhalten insbesondere im Bereich der Internetkriminalität auch von besonderer Bedeutung, um die Identität eines Tatverdächtigen zu ermitteln.

Die deutsche Rechtslage orientiert sich dabei an den Vorgaben des Bundesverfassungsgerichts, das mit Beschluss vom 27. Mai 2021 das erhöhte Eingriffsgewicht der Zuordnung einer dynamischen IP-Adresse hervorgehoben und klargestellt hat, dass die allgemeinen Befugnisse zur Übermittlung und zum Abruf von Bestandsdaten trotz ihres gemäßigten Eingriffsgewichts für die Gefahrenabwehr und die Tätigkeit der Nachrichtendienste grundsätzlich einer im Einzelfall vorliegenden konkreten Gefahr für ein Rechtsgut von besonderem Gewicht und für die Strafverfolgung eines Anfangsverdachts bedürfen.