Europäisches Parlament
2014-2019

Ausschuss für bürgerliche Freiheiten, Justiz und Inneres

1.4.2019

6. ARBEITSDOKUMENT (B)

zu dem Vorschlag für eine Verordnung über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen (2018/0108(COD)) – Garantien und Rechtsbehelfe

Ausschuss für bürgerliche Freiheiten, Justiz und Inneres

Berichterstatterin: Birgit Sippel

Mitverfasser: Romeo Franz

II. Ex-ante-Garantien

Nachdem der Vorschlag bereits im Hinblick auf die Benachrichtigung der betroffenen Person untersucht wurde, werden in diesem Arbeitsdokument die Garantien behandelt, die vor der Erhebung von Daten und deren Übermittlung an den Anordnungsstaat bereitgestellt werden müssen (sogenannte Ex-ante-Garantien).

Da die vorherige Authentifizierung der Europäischen Herausgabe- bzw. Sicherungsanordnung durch den Diensteanbieter (durch die sichergestellt wird, dass die Herausgabe- bzw. Sicherungsanordnung tatsächlich von einer zuständigen Justizbehörde ausgestellt wurde) bereits ausführlich im dritten Arbeitsdokument behandelt wurde[1], geht es im vorliegenden Dokument in erster Linie um Ex-ante-Garantien im Zusammenhang mit Dritten und dem Vollstreckungsverfahren.

1. Betroffene Dritte[2]

Selbst bei einem gezielten Einsatz der Europäischen Herausgabeanordnung lässt es sich kaum vermeiden, dass nebenbei Daten von Personen erhoben werden, mit denen die eigentlich anvisierte Person, also der Verdächtige bzw. Beschuldigte, kommuniziert hat. Dabei können manche Daten für die Ermittlungen unerheblich sein. Daher müssen nicht nur die Sicherung, Herausgabe und Weitergabe von Daten von betroffenen Personen, sondern auch von Daten Dritter (auch im Hinblick auf die Sicherheit der Daten) strengen Vorschriften unterliegen, durch die die vollständige Achtung der Grundrechte und Datenschutzgrundsätze sichergestellt wird. Jedoch wurden Fragen im Zusammenhang mit der Vorratsspeicherung, Weitergabe und Sicherheit der erhobenen Daten bislang nicht hinreichend berücksichtigt und es wurde auch nicht angemessen darauf eingegangen. Zwar besteht grundlegende Einigkeit darüber, dass Daten hinreichend gegen Hackerangriffe und andere Bedrohungen geschützt werden müssen, doch es werden eindeutige Vorschriften und Verfahren dazu benötigt, wie lange die gesammelten Daten gespeichert und an wen und für welche Zwecke sie weitergegeben werden dürfen, bevor die Daten erhoben und an den Anordnungsstaat übermittelt werden.

2. Benachrichtigung und Reaktionsmöglichkeit der Behörden im Vollstreckungsstaat

Ein anderer wichtiger Aspekt in Bezug auf Ex-ante-Garantien betrifft die stärkere Einbeziehung der Behörden des Vollstreckungsstaats, einschließlich einer umfassenden Benachrichtigung über den Erlass einer Europäische Herausgabe- oder Sicherungsanordnung und der Möglichkeit einer aussagekräftigen Reaktion oder sogar einer vorherigen Zustimmung. Dieser Aspekt wurde bereits in einigen der vorhergehenden Arbeitsdokumente hervorgehoben. Im Vorschlag für eine Verordnung ist derzeit kein derartiges automatisches Reaktionsrecht der Vollstreckungsbehörde vorgesehen. Zwar ist in Artikel 14 Absatz 4 Buchstabe f und Absatz 5 Buchstabe f festgelegt, dass ein Diensteanbieter einer Europäischen Herausgabe- oder Sicherungsanordnung nicht nachkommen muss, wenn diese „offenkundig

[1] Siehe auch die Stellungnahme Nr. 28/2018 der Bundesrechtsanwaltskammer, in der auch darauf hingewiesen wird, dass den Diensteanbietern in Anlehnung an Artikel 5 der EEA-Richtlinie mehr Informationen übermittelt werden müssen.

[2] Für den Zugang zu Daten Dritter, die keine Verdächtigen sind, gelten besonders strenge Voraussetzungen. So kann auf solche Daten nur in Ausnahmefällen zugegriffen werden, also z. B. wenn wesentliche Interessen der nationalen Sicherheit, der Verteidigung oder der öffentlichen Sicherheit gewahrt werden müssen.

gegen die Charta verstößt oder offensichtlich missbräuchlich ist“; dabei wird jedoch vorausgesetzt, dass der Diensteanbieter der Europäischen Herausgabe- oder Sicherungsanordnung nicht Folge geleistet hat. Nur in diesem Fall käme den Behörden des Vollstreckungsstaats eine aktive Rolle zu.

Um sicherzustellen, dass der gegenwärtigen Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte (EGMR) und den Verpflichtungen der Mitgliedstaaten entsprochen wird, scheint eine stärkere Einbeziehung des Vollstreckungsstaats jedoch die einzige sinnvolle Lösung zu sein.[3] Bestimmungen zu möglichen Benachrichtigungen und Reaktionen könnten sich an Artikel 31 der EEA-Richtlinie und den in Artikel 11 der EEA-Richtlinie aufgeführten Gründen für die Versagung der Anerkennung orientieren und an die unterschiedlichen Datenkategorien angepasst werden.

In Bezug auf Teilnehmer- und Zugangsdaten könnte es für eine solche stärkere Einbeziehung des Vollstreckungsstaats erforderlich sein, dass die Europäische Herausgabe- oder Sicherungsanordnung zum gleichen Zeitpunkt automatisch an den Diensteanbieter und die zuständige Behörde des Vollstreckungsstaats übermittelt wird und die Behörde des Vollstreckungsstaats innerhalb einer bestimmten Frist aus einem der in Artikel 11 der EEA-Richtlinie genannten Gründe für die Versagung der Anerkennung Einwände gegen die Europäische Herausgabe- oder Sicherungsanordnung geltend machen könnte.[4] Demzufolge würde nicht verlangt, dass die Behörden des Vollstreckungsstaats eine Europäische Herausgabe- oder Sicherungsanordnung bestätigen müssen, sondern lediglich dem Vollstreckungsstaat das Recht eingeräumt, einer Anordnung zur Herausgabe oder Sicherung von Teilnehmer- und Zugangsdaten zu widersprechen.

Was sensiblere Daten, also Transaktions- und Inhaltsdaten, anbelangt, könnten für eine stärkere Einbeziehung des Vollstreckungsstaats strengere Voraussetzungen nötig sein, z. B. das Vorliegen einer befürwortenden Entscheidung und somit einer Bestätigung des Staats, in dem die Europäische Herausgabe- oder Sicherungsanordnung vollstreckt werden soll, bevor die Daten herausgegeben oder gesichert werden.[5]

Was den Wortlaut der Grundrechtsklausel anbelangt, sollte nicht die äußerst vage Formulierung aus dem Vorschlag der Kommission („offenkundig gegen die Charta der Grundrechte der Europäischen Union verstößt“), sondern die Definition aus Artikel 11 Absatz 1 Buchstabe f der EEA-Richtlinie („berechtigte Gründe für die Annahme bestehen, dass die Vollstreckung einer in der EEA angegebenen Ermittlungsmaßnahme mit den Verpflichtungen des Vollstreckungsstaats nach Artikel 6 EUV und der Charta unvereinbar wäre“) verwendet werden.

Für eine Übernahme des Wortlauts der EEA-Richtlinie spricht nicht zuletzt, dass damit der derzeitige Flickenteppich aus Klauseln überwunden werden kann, der aus unterschiedlichen EU-Rechtsinstrumenten zur gegenseitigen Anerkennung und der Rechtsprechung des

[3] Siehe drittes Arbeitsdokument.

[4] Zur Anwendung von Artikel 11 der EEA-Richtlinie siehe auch die Stellungnahme des Rates der europäischen Anwaltsverbände vom 19. Oktober 2010 zum Vorschlag der Kommission.

[5] Dieses Problem wird auch durch die Einführung des neuen Artikels 7a in der allgemeinen Ausrichtung des Rates nicht gelöst, der für Inhaltsdaten eine Benachrichtigung vorsieht, wenn eine Person aus dem Vollstreckungsstaat betroffen ist. Dem Vollstreckungsstaat wird darin keine ausdrückliche Befugnis eingeräumt, eine ablehnende (Reaktion innerhalb einer bestimmten Frist) oder befürwortende Haltung (Zustimmung) zum Ausdruck zu bringen. Der Anordnungsstaat wird eventuellen Bedenken nur (in sehr wenigen Fällen) Rechnung tragen. Siehe auch die Empfehlungen des Rates der europäischen Anwaltsverbände vom 28. Februar 2019 zu elektronischen Beweismitteln.

Europäischen Gerichtshofs resultiert.[6] Auch wenn im Laufe der Zeit deutlich geworden ist, dass eine eindeutige Grundrechtsklausel für die Einhaltung der Grundrechtsverpflichtungen von wesentlicher Bedeutung ist, wurden in der Praxis in allen Instrumenten zur gegenseitigen Anerkennung unterschiedliche Klauseln verwendet, wobei damit teilweise die klare Absicht verfolgt wurde, sie einzuschränken oder ihre Anwendung unmöglich zu machen.[7] Es ist also eine Grundrechtsklausel erforderlich, die so weit gefasst ist, dass ein Richter damit erforderlichenfalls arbeiten kann (Richter sind zum Schutz der Grundrechte verpflichtet), und die auf alle Rechte (nicht nur auf einen Katalog von Rechten)[8] und Artikel 6 EUV[9] Bezug nimmt. Nur so kann in Zukunft vermieden werden, dass diesbezügliche Streitigkeiten Gerichten vorgelegt werden und es zu Spannungen im Zusammenhang mit den Grundrechten kommt.[10]

3. Benachrichtigung des *betroffenen* Staates

Gemäß dem im Vorschlag der Kommission verfolgten Ansatz hätten die Behörden des Anordnungsstaats unmittelbare rechtliche Befugnisse gegenüber Diensteanbietern (und somit in Bezug auf Daten von Bürgern), wobei die betroffene Person nur eingeschränkt oder spät benachrichtigt würde. Somit hätte die betroffene Person keine effektive Möglichkeit, die Rechtmäßigkeit, Verhältnismäßigkeit oder Notwendigkeit der Anordnung vor einem ihr zugänglichen Gericht in ihrem Wohnsitzstaat anzufechten. Dieser Umstand wirkt sich unmittelbar auf das Recht auf ein faires Verfahren und die Verteidigungsrechte aus. Der

[6] Siehe z. B.: Artikel 1 Absatz 3 des Rahmenbeschlusses 2002/584/JI über den Europäischen Haftbefehl, der nur eine pauschale Bezugnahme enthält, und die ausdrücklichen Klauseln, die in einigen Mitgliedstaaten bei dessen Umsetzung verwendet wurden; Artikel 20 Absatz 3 des Rahmenbeschlusses 2005/214/JI vom 24. Februar 2005 über die Anwendung des Grundsatzes der gegenseitigen Anerkennung von Geldstrafen und Geldbußen; Artikel 11 Absatz 1 Buchstabe f der EEA-Richtlinie; Artikel 8 Absatz 1 Buchstabe f und Artikel 19 Absatz 1 Buchstabe h der Verordnung (EU) 2018/1805 über die gegenseitige Anerkennung von Sicherstellungs- und Einziehungsentscheidungen, die verbundenen Rechtssachen C-404/15 und C-659/15 PPU, *Aranyosi und Căldăraru*, und die Rechtssache C-216/18 PPU, *Minister for Justice and Equality / LM*.

[7] Zum Beispiel durch die Verwendung des Ausdrucks „eklatante Rechtsverweigerung“ („flagrant denial of justice“) (ein vom EGMR entwickeltes Konzept, das vor allem im Zusammenhang mit der Auslieferung an Drittstaaten verwendet wird), der vom Europäischen Parlament in den Verhandlungen über die EEA-Richtlinie wegen seiner umfangreichen Einschränkungen ausdrücklich zurückgewiesen wurde.

[8] Einige Mitgliedstaaten wollten die Kategorien von Rechten, die unter einen solchen Grund fallen, einschränken, was die gegenseitige Anerkennung von Sicherstellungs- und Einziehungsentscheidungen betrifft. Das Europäische Parlament sprach sich nachdrücklich gegen eine Beschränkung auf lediglich bestimmte Rechte aus. Siehe auch die Stellungnahme des Europäischen Datenschutzausschusses (S. 19–20): *„Selbst der Grund, die Vollstreckung einer Anordnung mit der Begründung zu verweigern, dass sie gegen die Charta verstoßen würde, erscheint höher als die klassische Schwelle für eine Verletzung der Grundrechte des Betroffenen. Folglich sollte [...] der Verordnungsentwurf zumindest die klassische Mindestabweichung vorsehen, wonach beim Vorliegen substanzieller Gründe für die Annahme, dass die Vollstreckung einer [An]ordnung zu einer Verletzung eines Grundrechts der betreffenden Person führen würde und dass der Vollstreckungsstaat seine Verpflichtungen zum Schutz der [...] Grundrechte missachten würde, die Vollstreckung der [An]ordnung verweigert werden sollte.“*

[9] Es ist wichtig, auf Artikel 6 EUV zu verweisen, weil dort auf die drei Säulen des Grundrechtsschutzes Bezug genommen wird, nämlich auf die EMRK, die Charta und die gemeinsamen Verfassungsüberlieferungen. Durch einen solchen Verweis kann auch eine „Solange“-Kollision zwischen nationalen Verfassungen und dem Unionsrecht im Hinblick auf den Grundrechtsschutz vermieden werden.

[10] In den Mitgliedstaaten werden Instrumente zur gegenseitigen Anerkennung oft durch ein Sondergesetz umgesetzt. Es ergibt keinen Sinn und ist auch für Richter nicht praktikabel, wenn bei jedem Verfahren zur gegenseitigen Anerkennung eine andere (weiter oder enger gefasste) Grundrechtsklausel verwendet wird, z. B. eine Grundrechtsklausel für den Europäischen Haftbefehl, eine für Einziehungen und eine für Beweismittel. So gehen Richter nicht vor und sie beurteilen Fälle auch nicht auf diese Weise. Entweder sehen sie eine Grundrechtsgefährdung oder nicht.

Vorschlag der Kommission genügt daher nicht dem Kriterium der Lokalisierung der Zielperson, dem zufolge der Aufenthaltsort der betroffenen Person (neben dem Ort der Strafverfolgung) berücksichtigt werden sollte.[11]

Es kann u. a. sichergestellt werden, dass die Grundrechte der betroffenen Person, einschließlich Immunitäten und Vorrechten (bei Journalisten, Ärzten oder Anwälten), wirksam wahrgenommen werden können, indem ein Benachrichtigungsmechanismus eingeführt wird, durch den der Anordnungsstaat den betroffenen Staat unterrichtet oder um dessen Genehmigung ersucht, bevor er eine an den Vollstreckungsstaat und den Diensteanbieter gerichtete Anordnung erlässt. Dadurch würde der Schutz der Grundrechte den etablierten Standards der justiziellen Zusammenarbeit entsprechen, und der betroffene Staat könnte somit seinen Verpflichtungen hinsichtlich des Schutzes der Grundrechte nachkommen.

Dabei stellt sich jedoch die zentrale Frage, welcher Staat benachrichtigt werden soll: der Staat, in dem die Daten gespeichert sind, der Staat, in dem der rechtliche Vertreter des Diensteanbieters ernannt wurde, der Wohnsitzstaat der betroffenen Person[12] und/oder der Staat, dessen Staatsangehörigkeit diese besitzt?[13] Die Angelegenheit wird durch den in der parallelen Richtlinie eingeführten Begriff des Vertreters insoweit noch komplizierter, als sich der Vertreter an einem anderen Ort befinden kann als dem Ort, an dem der Anbieter seinen Sitz in der EU hat oder dem Ort, an dem die Daten in der EU gespeichert werden.[14] Theoretisch müssten also anscheinend an all diese Orte Benachrichtigungen übermittelt werden, damit die Verpflichtungen hinsichtlich des Schutzes der Grundrechte und des Datenschutzes gemäß dem Unionsrecht und der Europäischen Menschenrechtskonvention (EMRK) eingehalten werden. Um den erforderlichen Aufwand möglichst gering zu halten, könnte die Benennung eines Vertreters nur bei Anbietern aus Drittstaaten gefordert werden. Bei EU-Anbietern wäre es möglicherweise angebrachter, das derzeitige System zu verwenden, dem zufolge der Sitz des Anbieters bzw. der Ort der Daten grundsätzlich als Kontaktstelle dienen. In diesem Zusammenhang erscheint es problematisch, dass der Begriff des Vertreters (und alle damit verbundenen Aspekte im Zusammenhang mit Benachrichtigungen) in der allgemeinen Ausrichtung des Rates vom 8. März 2019[15] zur Richtlinie über elektronische Beweismittel anscheinend auf andere bestehende Instrumente wie etwa die EEA-Richtlinie ausgeweitet werden soll. Durch eine solche mögliche Ausweitung würde das derzeit geltende und etablierte System in Bezug auf EU-Anbieter infrage gestellt.[16]

---

[11] Siehe z. B. das Ratsdokument WK 3901/2017 zum belgischen Vorschlag für eine Vorgehensweise, in dem ausgeführt wird, dass dies neben dem Grund für die Strafverfolgung der relevanteste Anknüpfungspunkt sei, wobei der Begriff des „Orts der gewöhnlichen Nutzung des Dienstes durch die Zielperson“ vorgeschlagen wurde.

[12] Siehe zu dieser Möglichkeit z. B.: T. Christakis, CBDF, „Big divergence of opinions on e-evidence in the EU Council: A proposal in order to disentangle the notification knot“ (Große Meinungsverschiedenheiten im Rat beim Thema elektronische Beweismittel: Ein Vorschlag zur Lösung des Problems der Benachrichtigung).

[13] Ebd.

[14] Siehe Artikel 3 der vorgeschlagenen Richtlinie über die Bestellung von Vertretern zur Zwecken der Beweiserhebung in Strafverfahren („Der Vertreter muss in einem der Mitgliedstaaten, in denen der Diensteanbieter niedergelassen ist oder Dienste anbietet, ansässig oder niedergelassen sein.“). Ein solches System wäre bei Anbietern sinnvoll, die nicht in der EU ansässig sind, aber dort ihre Dienste anbieten. Was in der EU ansässige Anbieter anbelangt, würde durch die Verwendung eines solchen Systems jedoch von der derzeitigen Praxis und dem funktionierenden System der Zusammenarbeit abgewichen. Darauf wies der Deutsche Richterbund in seiner Stellungnahme Nr. 6/18 hin.

[15] Ratsdokument 6946/19.

[16] In Erwägung 8 der erwähnten allgemeinen Ausrichtung wird Folgendes festgestellt: *„Der Vertreter sollte als Zustellungsbevollmächtigter für inländische Anordnungen und Beschlüsse sowie für Anordnungen und*

Es muss jedoch nicht nur geklärt werden, an wen eine umfassende Benachrichtigung zu richten ist. Ein weiterer wichtiger Aspekt betrifft die möglichen Folgen einer solchen Benachrichtigung. Zumindest bei manchen Datenkategorien muss in Bezug auf solche Benachrichtigungen die Möglichkeit vorgesehen werden, – zumindest ablehnend – zu reagieren (bei einer ablehnenden Reaktion würden Maßnahmen in Anlehnung an Artikel 31 der EEA-Richtlinie in einer bestimmten Frist blockiert), damit den Zuständigkeiten des Vollstreckungsstaats im Rahmen des EMRK-Systems und dem sensiblen Charakter mancher Daten im Einklang mit der Rechtsprechung des Gerichtshofs Rechnung getragen wird (insbesondere im Hinblick auf die von der Kommission herangezogene sehr niedrige Schwelle, zum Beispiel, was den Handel mit Daten betrifft).[17]

4. Unterschiedliche Garantien für unterschiedliche Datenkategorien (Artikel 2)

Die Kommission hat in ihrem Vorschlag vier verschiedene Datenkategorien eingeführt: a) Teilnehmerdaten, b) Zugangsdaten, c) Transaktionsdaten und d) Inhaltsdaten. Gemäß dem Vorschlag gelten abhängig von der Kategorie der Daten, die von den zuständigen Behörden angefordert werden, unterschiedliche Anforderungen. Während Anordnungen für Teilnehmer- und Zugangsdaten nur von einem Staatsanwalt validiert werden müssen und der Zugriff auf solche Daten bei allen Straftaten erlaubt ist, kann auf Transaktions- und Inhaltsdaten nur zugegriffen werden, wenn die jeweilige Anordnung zuvor von einem Richter validiert wurde und die betreffende Straftat mit einem Höchststrafmaß von mindestens drei Jahren Haft geahndet wird oder zu den Straftaten zählt, zu denen im Rahmenbeschluss 2001/413/JI des Rates, in der Richtlinie 2011/93/EU und in der Richtlinie 2013/40/EU einheitliche Bestimmungen enthalten sind oder die in der Richtlinie (EU) 2017/541 als terroristische Straftaten aufgeführt sind.

Im Zusammenhang mit den neuen Datenkategorien treten zwei Probleme auf: 1) Die Definitionen überschneiden sich teilweise (siehe die Definitionen für Zugangs- und Transaktionsdaten), und es besteht die Gefahr, dass die Strafverfolgungsbehörden an der rechtmäßigen Anwendung der Instrumente gehindert werden. 2) Die Unterteilung entspricht

---

Beschlüsse auf der Grundlage von Rechtsakten der Union fungieren, die [...] in den Geltungsbereich von Titel V Kapitel 4 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) [...] fallen und der Beweiserhebung in Strafsachen dienen, einschließlich wenn diese Anordnungen und Beschlüsse in Form von Bescheinigungen übermittelt werden. Dazu gehören sowohl Rechtsakte, die die unmittelbare Zustellung von Anordnungen an den Diensteanbieter oder seinen Vertreter in Fällen mit grenzüberschreitendem Bezug zulassen, wie die [Verordnung über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen (im Folgenden „Verordnung")[6]], als auch andere Rechtsakte [...] zur justiziellen Zusammenarbeit, die zwischen den Mitgliedstaaten anwendbar sind, insbesondere die, die in Geltungsbereich von Titel V Kapitel 4 fallen, wie die Richtlinie über die Europäische Ermittlungsanordnung[7] und das Rechtshilfeübereinkommen von 2000[8]. Die Inanspruchnahme von Vertretern sollte im Einklang mit den Verfahren erfolgen, die in den für das Gerichtsverfahren geltenden Rechtsakten und Rechtsvorschriften vorgesehen sind. Die zuständigen Behörden des Mitgliedstaats, in dem der Vertreter ansässig oder niedergelassen ist, sollten gemäß der Rolle tätig werden, die ihnen in dem betreffenden Rechtsakt zugewiesen wurde, sofern ihre Einbeziehung vorgesehen ist."

[17] Der Europäische Datenschutzausschuss (EDSA) kritisierte die „simple" Argumentationsweise der Kommission in Fällen der Vorratsdatenspeicherung, bei denen die Kommission alles als erlaubt ansieht, was vom Gerichtshof nicht ausdrücklich geregelt bzw. verboten wurde. Stellungnahme 23/2018 des EDSA (S. 16): *„Insbesondere bedauert der EDSA, dass die niedrigste Schwelle, die den Strafverfolgungsbehörden die Möglichkeit einräumt, den Zugang zu Teilnehmer- und Zugangsdaten für jede Straftat zu beantragen, auf einem Umkehrschluss [aus] der Rechtsprechung des EuGH [...] beruht [...] ."* Siehe dazu auch die Stellungnahme Nr. 6/18 des Deutschen Richterbunds und die Stellungnahme der European Criminal Bar Association, in der eine aussagekräftige Benachrichtigung gefordert wird, auf die innerhalb einer bestimmten Frist reagiert werden kann.

nicht den Definitionen von Datenkategorien in bestehenden europäischen Rechtsvorschriften[18] im Bereich des Datenschutzes und der Privatsphäre bei der elektronischen Kommunikation sowie in internationalen Verträgen[19], weswegen die Gefahr besteht, dass es zu Diskrepanzen und Widersprüchen mit der Rechtsprechung des Gerichtshofs der Europäischen Union und des EGMR kommt.[20]

[18] Artikel 10 Absatz 2 Buchstabe e der EEA-Richtlinie 2014/41/EU, Artikel 4 Absatz 3 Buchstabe c des Vorschlags für eine Verordnung über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (COM(2017)0010).
[19] Übereinkommen des Europarates über Computerkriminalität.
[20] Mehr dazu im zweiten Arbeitsdokument zum Anwendungsbereich, insbesondere in Bezug auf dynamische IP-Adressen.