Europäisches Parlament
2014-2019

Ausschuss für bürgerliche Freiheiten, Justiz und Inneres

1.4.2019

6. ARBEITSDOKUMENT (C)

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 SippelKo-Autor: Romeo Franz

III. Ex-post-Garantien

1. Wirksame Rechtsbehelfe (Artikel 17)

Im Arbeitsdokument wurde bereits darauf hingewiesen, dass Nutzerinformationen sehr wahrscheinlich erst in einem sehr späten Stadium der Untersuchung vorliegen. Daher ist es sehr zweifelhaft, ob die betroffene Person in einem so späten Stadium der Untersuchung tatsächlich noch um wirksame Rechtsbehelfe ersuchen kann. Da dies erneut Anlass zu ernsthaften Bedenken hinsichtlich der Grundsätze der Waffengleichheit und des kontradiktorischen Verfahrens als Teil des Rechts auf ein faires Verfahren (Artikel 6 EMRK) gibt, wird in diesem Teil des Arbeitsdokuments näher auf Artikel 17 der vorgeschlagenen Verordnung eingegangen, in dem es um „wirksame Rechtsbehelfe“ geht.

In Artikel 17 Absatz 1 der vorgeschlagenen Verordnung über elektronische Beweismittel wird dem Verdächtigen oder Beschuldigten das „Recht [eingeräumt], während des Strafverfahrens, für das die Anordnung erlassen wurde, wirksame Rechtsbehelfe gegen die Europäische Herausgabeanordnung einzulegen“.[1] Dies gilt nicht für Sicherungsanordnungen. In Artikel 17 Absatz 2 heißt es weiter: „Handelt es sich bei der Person, deren Daten eingeholt wurden, nicht um einen Verdächtigen oder Beschuldigten in einem Strafverfahren, für das die Anordnung erlassen wurde, so hat der Betreffende [...] das Recht, im Anordnungsstaat wirksame Rechtsbehelfe gegen die Europäische Herausgabeanordnung einzulegen.“ „Ein solches Recht auf Einlegung eines wirksamen Rechtsbehelfs wird vor einem Gericht des Anordnungsstaats nach dessen nationalem Recht ausgeübt und beinhaltet die Möglichkeit, die Rechtmäßigkeit der Maßnahme, einschließlich ihrer Notwendigkeit und Verhältnismäßigkeit, anzufechten.“ (siehe Artikel 17 Absatz 3)

Demnach sieht der Vorschlag weder für den Verdächtigen bzw. Beschuldigten noch für die beteiligten Dritten das Recht auf Einlegung eines wirksamen Rechtsbehelfs bei Sicherungsanordnungen vor. Wie bereits erwähnt, weiß die betroffene Person in Fällen, in denen auf eine Sicherungsanordnung keine Herausgabeanordnung folgt, nicht, dass ihre Daten gesichert wurden und hat somit keinerlei Zugang zu Rechtsbehelfen.

Eine weitere Frage betrifft den Ort, an dem ein Rechtsbehelf eingelegt werden kann. Da der Vorschlag vorsieht, dass Rechtsbehelfe für Verdächtige und Beschuldigte nur während des Strafverfahrens im Anordnungsstaat (Artikel 17 Absatz 1) und Rechtsbehelfe für Dritte (Artikel 17 Absatz 2) nur im Anordnungsstaat nach Maßgabe seines nationalen Rechts eingelegt werden können, ist es zweifelhaft, ob die betroffene Person tatsächlich einen solchen Rechtsbehelf einlegen kann. Im Gegensatz dazu ist es im Hinblick auf den grenzübergreifenden Charakter des vorgeschlagenen Instruments für elektronische Beweismittel sehr wahrscheinlich, dass die Wirksamkeit des Rechtsbehelfs durch die räumliche Entfernung zum Anordnungsstaat, potenzielle Sprachprobleme, mangelnde Kenntnis des jeweils anderen Rechtssystems sowie finanzielle Schwierigkeiten beim Einlegen von Rechtsbehelfen in einem anderen Mitgliedstaat offensichtlich beeinträchtigt wird.[2] Es

[1] Es wird erklärt, dass dieses Recht unbeschadet der nach der Richtlinie (EU) 2016/680 und der Verordnung (EU) 2016/679 verfügbaren Rechtsbehelfe besteht.

[2] Siehe auch Meijers-Ausschuss, CM 1809, 18. Juli 2018, wo es heißt: „*Im Rahmen des vorgeschlagenen Mechanismus ist es sehr wahrscheinlich, dass eine Situation eintritt, in der die betroffene Person – unabhängig davon, ob es sich dabei um einen Verdächtigen handelt oder nicht – in einem anderen Mitgliedstaat wohnt als dem Anordnungsstaat oder dem Staat, in dem der rechtliche Vertreter des Dienstleisters niedergelassen ist oder*

stellt sich daher die Frage, ob Nutzer nicht auch die Möglichkeit haben sollten, die Rechtmäßigkeit vor den Gerichten ihres Mitgliedstaats (oder zumindest im Vollstreckungsmitgliedstaat, wo die Befugnisse ausgeübt wurden) anzufechten.[3]

Darüber hinaus werden in dem Vorschlag keine Rechtsbehelfe genannt, sodass es den Mitgliedstaaten überlassen bleibt, im Rahmen des nationalen Rechts die Folgen eines Verstoßes gegen die Verfahrensvorschriften bei der Beschaffung elektronischer Daten zu bestimmen. Mit Blick auf frühere Instrumente zur gegenseitigen Anerkennung auf EU-Ebene, wie etwa die EEA-Richtlinie oder auch die Richtlinien über Verfahrensgarantien, muss eingeräumt werden, dass es sich um ein allgemeines Problem handelt. Bislang fehlt in diesen Richtlinien über Verfahrensrechte und in der EEA-Richtlinie ein eindeutiger Verweis auf einen einheitlichen Rechtsbehelf oder es wird darin nur sehr vage auf beispielsweise die Verteidigungsrechte und die Fairness des Verfahrens Bezug genommen.[4]

2. Die Frage der Zulässigkeit von Daten als Beweismittel

Empirisch gesehen scheint aus der Sicht der betroffenen Person der einzig wirksame Rechtsbehelf das Recht zu sein, die Zulässigkeit der zusammengetragenen Beweismittel anzufechten.[5] Dies könnte auch dazu beitragen, rechtswidrige Strafverfolgungspraktiken, d. h. einen Missbrauch des Instruments für elektronische Beweismittel, zu verhindern. Die angesprochene Problematik bezieht sich auf die Frage der Zulässigkeit von Beweismitteln im Zusammenhang mit der Ausschlussvorschrift.[6] Derzeit unterscheiden sich die Ansätze der EU-Mitgliedstaaten in Bezug auf die beiden genannten Konzepte deutlich voneinander und reichen von einem vollständigen Fehlen von Zulässigkeitsvorschriften bis hin zu sehr

---

in dem der Dienstleister seinen Sitz hat. Würde dies nicht zu Unsicherheiten im Rahmen des Besitzstands im Bereich der Grundrechte oder zu sonstigen Unsicherheiten bezüglich der Frage, in welchem Land der Einzelne eine Beschwerde einreichen kann, führen? ... Der Meijers-Ausschuss schlägt daher vor, ernsthaft die Möglichkeit in Betracht zu ziehen, Einzelpersonen ausdrücklich die Klageerhebung vor einem Gericht in ihrem Wohnsitzstaat zu gestatten."

[3] Vergleiche mit den Artikeln 50 und 52 der Richtlinie 2016/680 („Datenschutzrichtlinie für Strafverfolgungsbehörden" – Recht auf Einreichung einer Beschwerde bei einer einzigen von der betroffenen Person auszuwählenden Aufsichtsbehörde und Weiterleitung der Beschwerde durch diese an die zuständige Aufsichtsbehörde).

[4] Die Verordnung über elektronische Beweismittel geht in Artikel 18 noch einen Schritt weiter, was die Gewährleistung von Immunitäten und Vorrechten sowie der grundlegenden Interessen des Vollstreckungsstaats betrifft, jedoch nur in Bezug auf Transaktions- oder Inhaltsdaten. Bei der Prüfung der Relevanz und der Zulässigkeit der betreffenden Beweismittel während des Strafverfahrens, für das die Anordnung erlassen wurde, stellt jedoch nur das Gericht des Anordnungsstaats sicher, dass diese Gründe genauso berücksichtigt werden, als wären sie im nationalem Recht vorgesehen. In Anbetracht der unterschiedlichen Systeme könnten sich die Folgen erheblich unterscheiden und nicht die gleichen wie im Vollstreckungsstaat sein. In der allgemeinen Ausrichtung des Rates wurde Artikel 18 gestrichen.

[5] Siehe zum Vergleich beispielsweise die Urteile des Obersten Gerichtshofs der Vereinigten Staaten in der Rechtssache Wolf/Colorado, 338 U.S. 25 (1949), in der zugunsten eines in den Bundesstaaten divergierenden Sanktionssystems entschieden wurde, und in der Rechtssache Mapp/Ohio, 367 U.S. 643 (1961), in der das erste Urteil aufgehoben und die Ausschlussvorschrift als gemeinsamer wirksamer Rechtsbehelf in allen Bundesstaaten eingeführt wurde, um Verstöße gegen den vierten Zusatzartikel zur Verfassung über das Verbot rechtswidriger Durchsuchungen und Beschlagnahmen zu verhindern. Siehe auch Fair Trials International, Consultation paper on e-evidence, Februar 2019, S. 4: *„Die Prüfung der Rechtmäßigkeit der Erhebung von Beweismitteln durch die Strafverfolgungsbehörden erfolgt im Rahmen des Strafverfahrens (oder kurz davor, nach dem die Beweismittel zusammengetragen wurden). Dies ermöglicht es Beschuldigten, die Zulässigkeit von Beweismitteln anzufechten, auf die sich der Staat stützt, um eine Verurteilung zu erwirken. Beschuldigten muss das Recht eingeräumt*

strengen Zulässigkeits- und Ausschlussvorschriften.[7] Nach Ansicht von Fachleuten variieren die Vorschriften in Bezug auf ihre Anwendung sogar von Gericht zu Gericht und von Richter zu Richter sehr stark. Und auch auf EU-Ebene gibt es keinen klaren Rechtsrahmen für die Zulässigkeit von Beweismitteln, was die Anwendung des Grundsatzes der gegenseitigen Anerkennung erschwert. Die einzige gemeinsame Grundlage ergibt sich aus der Rechtsprechung des EGMR, in deren Rahmen klare Regeln für Verstöße gegen Artikel 3 EMRK (Verbot von Folter und unmenschlicher oder erniedrigender Behandlung) festgelegt wurden.[8] Was jedoch das Recht auf ein faires Verfahren (siehe Artikel 6 EMRK, einschließlich des Rechts auf Aussageverweigerung, des Rechts auf einen Rechtsanwalt, des Recht auf Verteidigung usw.[9]) oder das Recht auf Privatsphäre (siehe Artikel 8 EMRK) betrifft, sind die Vorschriften deutlich weniger klar und beziehen sich nur auf den Grundsatz der Fairness des gesamten Verfahrens bei Verletzungen der genannten Rechte. Selbst die einschlägige Rechtsprechung zu Artikel 8 EMRK (im Zusammenhang mit der Zulässigkeit und dem fairen Prozess in Artikel 6 EMRK) des EGMR beruht auf vagen Kriterien, die weit unter denen der derzeit in mehreren Mitgliedstaaten geltenden Normen liegen.[10]

Daher muss im Rahmen des neuen Verfahrens festgelegt werden, welche Rechtsbehelfe anwendbar sind, wenn elektronische Beweismittel rechtswidrig beschafft wurden. Um zu verhindern, dass Strafverfolgungsbehörden rechtswidrig beschaffte Beweismittel in Anspruch nehmen können (z. B. wenn es nur aufgrund der rechtswidrig beschafften Beweismittel zu einer Verurteilung kommt), muss im Rahmen der vorgeschlagenen neuen Instrumente eine Überprüfung der Art und Weise, in der die Beweismittel gesammelt wurden, ermöglicht werden. Zu diesem Zweck muss die den elektronischen Daten zugrunde liegende Quelle gegenüber dem überprüfenden Gericht und der Verteidigung offengelegt werden, damit beurteilt werden kann, ob die elektronischen Daten rechtmäßig erhoben wurden, und damit ermittelt werden kann, wie sich entlastende Beweismittel beschaffen lassen. Wurde nachgewiesen, dass Beweismittel rechtswidrig beschafft wurden, müssen neue Vorschriften

---

werden, die Anforderung und Verwendung von Daten vor Gericht anzufechten und angemessene Rechtsbehelfe einzulegen, wenn elektronische Beweismittel rechtswidrig beschafft wurden. Um das Anfechtungsrecht ausüben zu können, muss es Beschuldigten möglich sein, Auskunft über die Quellen der elektronischen Beweismittel zu erhalten."

[6] Die beiden Konzepte sind miteinander verbunden, jedoch nicht identisch. Zulässigkeit bezieht sich auf die Frage, ob die Möglichkeit besteht, ein Urteil auf bestimmte Beweismittel zu stützen. Die Ausschlussvorschrift sieht zudem vor, dass der Richter, der im Strafverfahren urteilt, nicht mit unzulässigen Beweismitteln konfrontiert werden sollte, da ihn dies psychologisch beeinflussen könnte.

[7] Siehe beispielsweise S. C. Thaman, Exclusionary Rules in Comparative Law, 2012.

[8] Siehe z. B. EGMR, Gäfgen/Deutschland, Antrag Nr. 22978/05, Urteil vom 1. Juni 2010, und El Haski/Belgien, Antrag Nr. 649/08, Urteil vom 25. September 2012.

[9] Darüber hinaus sind die genannten EMRK-Standards wesentlich niedriger als die Verfassungs- und EU-Standards in den meisten Mitgliedstaaten. Beispielsweise ist das Recht auf Aussageverweigerung nach der Rechtsprechung des EGMR nur ein relatives Recht (siehe beispielsweise John Murray/Vereinigtes Königreich, Antrag Nr. 18731/91, Urteil vom 8. Februar 1996), aber ein absolutes Recht in der EU (siehe Richtlinie 343/2016 und einige nationale Verfassungen). Siehe zum Beispiel Bykov/Russland, Antrag Nr. 4378/02, Urteil vom 10. März 2009, im Hinblick auf Kriterien für die Bewertung der Fairness des Verfahrens aufgrund einer möglichen Verletzung des Rechts auf Aussageverweigerung.

[10] Siehe beispielsweise Rechtsprechung des EGMR, Malone /Vereinigtes Königreich, Antrag Nr. 8691/79, Urteil vom2. August 1984, Schenk/Schweiz, Antrag Nr. 10862/84, Urteil vom 12. Juli 1988, Kopp/Schweiz, Antrag Nr. 23224/94, Urteil vom 25. März 1998, Khan/Vereinigtes Königreich, Antrag Nr. 35394/97, Urteil vom 12. Mai 2000 usw.

über die Unzulässigkeit solcher Beweise eingeführt oder zumindest die nationalen Zulässigkeits-/Ausschlussvorschriften in einem gewissen Maße harmonisiert werden.[11]

3. Verbot der Weiterverarbeitung und Weitergabe von Beweismitteln

Es sollte ein Verbot der Nutzung der Beweismittel außerhalb des Untersuchungsverfahrens und insbesondere ein Verbot der Weitergabe von Daten an Ermittlungsbehörden, die nicht an dem Fall beteiligt sind, eingeführt werden. Die Übermittlung von Daten zu Zwecken der öffentlichen Sicherheit sollte klar geregelt sein. Das vorgeschlagene System ist ein Strafrechtssystem und sollte nicht für nachrichtendienstliche Zwecke genutzt werden, da in einigen Mitgliedstaaten die Tendenz besteht, die Grenze zwischen Strafverfolgung und nachrichtendienstlicher Arbeit zu verwischen. Des vorstehend genannten Verbots bedarf es für Fälle, in denen eine betroffene Person die Entscheidung erwirken konnte, dass eine Herausgabeanordnung rechtswidrig ausgestellt wurde (Artikel 17). Werden später als rechtswidrig befundene Daten weitergegeben, gestaltet es sich schwierig, ihre Löschung zu realisieren und zu kontrollieren.

Für Fälle, in denen die Untersuchung noch nicht abgeschlossen und das Verfahren noch unter Verschluss ist, müssen gesonderte Verfahren für die Beitreibung und Übertragung geschaffen werden. In diesem Zusammenhang sollten die Gerichte des Vollstreckungsmitgliedstaats entsprechende Entscheidungen über eine Weitergabe und Offenlegung treffen. Vor allem vor der Weitergabe der Daten an die Behörden von Drittstaaten ist eine gerichtliche Entscheidung im Vollstreckungsmitgliedstaat unerlässlich.[12]

4. Finanzieller Ausgleich und finanzielle Sanktionen

Darüber hinaus sollte geprüft werden, ob ein wirksamer Rechtsbehelf auch einen finanziellen Ausgleich für die betroffene Person umfassen könnte, wenn die Rechtsgrundlage dies hergibt. Mit einer solchen Ausgleichsregelung könnten auch Dritte, bei denen es sich nicht um Verdächtigte oder Beschuldigte handelt und bei denen die Frage der Zulässigkeit von Beweismitteln somit keine Rolle spielt, tatsächlich von einem wirksamen Rechtsbehelf profitieren. Um zu verhindern, dass die Strafverfolgungsbehörden Beweismittel rechtswidrig beschaffen, könnte es unabhängig von der Frage der Zulässigkeit sinnvoll sein, die Möglichkeit zu prüfen, auch Sanktionen für ausstellende Behörden vorzusehen, die Daten rechtswidrig angefordert haben (vgl. z.B. Art. 57 Polizei-Richtlinie), wenn die Rechtsgrundlage dies hergibt.

5. Rechtsbehelf für Diensteanbieter

Als private Unternehmen sind Diensteanbieter eher schlecht gerüstet und haben keinen Eigenanreiz, die Grundrechte ihrer Nutzer zu schützen. Daher dürfen und sollten

[11] Das Europäische Parlament verfolgte diesen Ansatz bereits im Rahmen seines internen Standpunkts zu Verhandlungen über bestimmte Aspekte der Unschuldsvermutung und schlug in diesem Zusammenhang eine strikte Nichtzulässigkeit im Falle eines Verstoßes gegen das Recht auf Aussageverweigerung (Gesetzgebungsverfahren zur Richtlinie 2016/343) vor.
[12] Deutscher Richterbund, ebd.

Diensteanbieter nicht in die Situation gebracht werden, dass sie im Hinblick auf den Grundrechtsschutz Behörden ersetzen müssen.

Die Interessenträger haben jedoch darauf hingewiesen, wie wichtig es ist, den Diensteanbietern die realistische Möglichkeit zu bieten, die Ausführung einer Herausgabe- oder Sicherungsanordnung abzulehnen, wenn sie hinreichende Gründe für die Annahme haben, dass eine solche Anordnung rechtswidrig ist.[13] In diesem Zusammenhang wurde die Frage gestellt, warum nur ein „offensichtlicher" Verstoß und nicht einfach „ein Verstoß" ein Ablehnungsgrund sein kann. Darüber hinaus würden Diensteanbieter ausreichend Zeit benötigen, um einen Antrag zu prüfen, und ihnen sollte nicht einseitig mit extrem kurzen Fristen und finanziellen Sanktionen gedroht werden.

IV. Wirksame Aufsicht und öffentliche Rechenschaftspflicht

1. Wirksame und systematische Aufsicht über die Anwendung der Maßnahmen

Mit einem fairen und verhältnismäßigen Einsatz der neuen Instrumente lässt sich das Vertrauen der Öffentlichkeit in die Strafrechtssysteme und Strafverfolgungsbehörden am ehesten gewährleisten. Damit Aufsichtsmechanismen wirksam sein können, muss sichergestellt sein, dass sie dem Risiko einer missbräuchlichen Anwendung vorbeugen und so dazu beitragen, den Ruf rechtmäßiger Strafverfolgungsmaßnahmen zu wahren und diejenigen zu schützen, die zu Opfern eines Missbrauchs der Instrumente werden könnten. Zu diesem Zweck sollten die für die grenzüberschreitende Herausgabe von Beweismitteln zuständigen Aufsichtsgremien im Rahmen einer angemessenen institutionellen Struktur (EEA-Modell, EDSA-Modell, GPKA-Modell oder gegebenenfalls nationale Modelle) einbezogen werden und echte Aufsichtsbefugnisse erhalten.

2. Transparenz und Rechenschaftspflicht

In Artikel 19 der vorgeschlagenen Verordnung wird auf das Thema „Überwachung und Berichterstattung" verwiesen. Dabei werden konkrete Verpflichtungen der Kommission und der Mitgliedstaaten festgelegt, um die Erträge, Ergebnisse und Auswirkungen der vorgeschlagenen Verordnung zu überwachen und eine Vielzahl an Daten zu erheben. Eine solche Bestimmung stellt einen Mehrwert dar.

Statistiken sind ein neu auftretendes Problem im Bereich des EU-Strafrechts, da sich die Mitgliedstaaten in Legislativverhandlungen verglichen mit dem Europäischen Parlament und der Kommission oftmals für eine geringere Anzahl statistischer Daten aussprechen.[14] Diese Daten sind jedoch von wesentlicher Bedeutung, um unter anderem potenziellen Problemen mit übertriebenen und unbegründeten Anordnungen entgegenzuwirken und das Funktionieren der bestehenden Instrumente zu bewerten. Folglich sollten die Mitgliedstaaten nicht nur statistische Daten erheben und der Kommission übermitteln (wie in Artikel 19 Absatz 2

[13] Positionspapier EDRi.

[14] Vergleiche beispielsweise die ursprünglichen Vorschläge der Kommission und die endgültigen Rechtsakte in Artikel 11 der Richtlinie 2014/42/EU über die Sicherstellung und Einziehung von Tatwerkzeugen und Erträgen aus Straftaten in der Europäischen Union sowie in Artikel 35 der Verordnung (EU) 2018/1805 über die gegenseitige Anerkennung von Sicherstellungs- und Einziehungsentscheidungen.

vorgesehen), sondern auch veröffentlichen. Darüber hinaus scheint es notwendig, Artikel 19 Absatz 2 auch auf ausführlichere Informationen auszuweiten:

– Anzahl der ausgestellten Sicherungsanordnungen und Angabe, für welche anderen Mitgliedstaaten Sicherungsanordnungen ausgestellt wurden,

– Angabe der Art der Straftaten, für die Sicherungsanordnungen ausgestellt wurden,

– Zahl der Verurteilungen in Fällen, in denen von Sicherungsanordnungen Gebrauch gemacht wurde.

V. Einschränkungen von Garantien und das so genannte „Recht auf Sicherheit“

In ihrer Folgenabschätzung zum Vorschlag zu elektronischen Beweismitteln, aber auch in anderen Vorschlägen seit dem Inkrafttreten der Charta der Grundrechte der Europäischen Union stellt die Kommission fest, dass auf der Grundlage von Artikel 6 der Charta ein „Recht auf Sicherheit“ besteht und dass ein solches Recht, wie es scheint, gegen andere individuelle Rechte und Garantien abzuwägen ist.[15]

Dieser Argumentation ist jedoch vehement zu widersprechen, da ein Verweis auf Artikel 6 der Charta irreführend und falsch ist. Weder gemäß der EMRK noch nach der Charta gibt es ein rechtlich anerkanntes „Recht auf Sicherheit“. Entgegen der Auffassung der Kommission sieht der vorstehend genannte Artikel das Recht auf Freiheit und das Recht auf Sicherheit nicht als zwei separate Rechte vor, die gegeneinander abgewogen werden müssen. Artikel 6 der Charta ist lediglich ein Abbild von Artikel 5 EMRK (mit genau demselben Titel), in dem eindeutig das Recht auf Schutz gegen rechtswidrige Inhaftierungen durch den Staat benannt wird. Demnach gibt es kein getrenntes rechtlich anerkanntes Recht auf Sicherheit.[16] Zwar handelt es sich bei Sicherheit um ein grundlegendes menschliches Bedürfnis[17],es ist aber weder nach der EMRK noch nach der Charta ein rechtlich anerkanntes Grundrecht.

Nach der EMRK enthalten bestimmte Artikel nur das Konzept positiver Verpflichtungen der Vertragsparteien, zum Beispiel Artikel 2 (das Recht auf Leben) [18]oder Artikel 3 (das Verbot von Folter und unmenschlicher oder erniedrigender Behandlung)[19], wobei die Vertragsparteien der Konvention in bestimmten Fällen für die Verletzung dieser positiven Verpflichtungen verantwortlich sein können. Solche Verpflichtungen stellen jedoch keinesfalls eine Art „Schattenrecht auf Sicherheit“ dar. Darüber hinaus heißt es in Artikel 52 Absatz 3 der Charta: „So weit diese Charta Rechte enthält, die den durch die Europäische Konvention zum Schutze der Menschenrechte und Grundfreiheiten garantierten Rechten entsprechen, haben sie die gleiche Bedeutung und Tragweite, wie sie ihnen in der genannten Konvention verliehen wird. Diese Bestimmung steht dem nicht entgegen, dass das Recht der Union einen weiter gehenden Schutz gewährt.“ Folglich dürfen die Rechte und Garantien nicht unter das Niveau der Charta fallen. Der Hinweis der Kommission auf das künstliche, nicht existente „Recht auf Sicherheit“ wird jedoch in dem Vorschlag verwendet, um ein ausgewogenes Verhältnis zwischen diesen Rechten und Garantien auf einem anderen und möglicherweise niedrigeren Niveau als dem der EMRK zu schaffen.

---

[15] Bei elektronischen Beweismitteln steht dies im Zusammenhang mit der Opferproblematik. In anderen Dokumenten der Kommission scheint es sich dabei jedoch um ein eigenständiges Recht zu handeln. Siehe beispielsweise die Arbeitsunterlage der Kommissionsdienststellen zur Folgenabschätzung als Begleitunterlage zu dem Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln und zur Ersetzung des Rahmenbeschlusses 2001/413/JI des Rates.

[16] Dies wurde von der Agentur der Europäischen Union für Grundrechte und von dem EU-Netz unabhängiger Sachverständiger für Grundrechte klar benannt („*Während der Ausarbeitung von Artikel 6 der Charta im Konvent führte der Begriff „Sicherheit“ wiederholt zu kontroversen Diskussionen, und einige Mitglieder schlugen vor, ihn einfach zu streichen, da er in einigen EU-Mitgliedstaaten wie Frankreich, Italien oder Deutschland unterschiedlich ausgelegt werden könnte. Der Konvent entschied jedoch, den Begriff im Sinne der restriktiven Auslegung der Straßburger Rechtsprechung gemäß Artikel 5 EMRK beizubehalten.*“).

[17] Siehe A. Maslow, Motivation and Personality, 1954.

[18] Siehe etwa Urteil des EGMR vom 28. Oktober 1998 in der Rechtssache Osman/Vereinigtes Königreich, Antrag Nr. 23452/94.

[19] Siehe etwa Urteil des EGMR vom 10. Mai 2001 in der Rechtssache Z. und andere/Vereinigtes Königreich, Antrag Nr. 29292/95.

Eine Klarstellung in dieser Frage ist wichtig, da es den Anschein hat, dass durch die Verwendung dieses rechtlich nicht existierenden Begriffs unter anderem durch die Kommission das Gleichgewicht von Rechten und Garantien (als Derivat individueller Rechte, wie etwa des Rechts auf einen wirksamen Rechtsbehelf, Zugang zu einem Gericht, ein faires Verfahren, Einschränkungen der Privatsphäre, Recht auf Unterrichtung über Gebühren, Gleichheit oder Verfügungsgrundsatz usw.) im Vergleich zu den Normen der EMRK beeinträchtigt wurde.[20]

Fazit

– Ex-ante-Rechtsbehelfe müssen strenge Voraussetzungen für die Ausgabe von Sicherungsanordnungen umfassen, wie z.B. einen bestimmten erreichten Standard für die Beschaffung von Beweismitteln und ein bestimmtes, ordnungsgemäß bewertetes Verhältnismäßigkeitsniveau, wobei auch der Diensteanbieter in der Lage sein sollte, eine entsprechende Prüfung durchzuführen.

– Damit die betroffene Person von allen verfügbaren Rechtsbehelfen Gebrauch machen kann, muss sie sich der Maßnahme sowie des Umstands bewusst sein, dass ihre Daten herausgegeben/gesichert wurden, um das Recht auf Verteidigung und auf ein faires Verfahren zu gewährleisten. Daher muss zumindest im Vollstreckungsstaat eine viel aussagekräftigere Benachrichtigung erfolgen, einschließlich einer Grundrechtsklausel auf der Grundlage des Beispiels der Europäischen Ermittlungsanordnung. Vertraulichkeit muss die Ausnahme sein – nicht die Regel – und muss strengen Bedingungen unterliegen.

– Was mögliche Verstöße gegen die in dieser Verordnung festgelegten Vorschriften betrifft, muss der Text auch den Zugang zu wirksamen Rechtsbehelfen vorsehen. Folglich bedarf es einheitlicherer Vorschriften über die im Anordnungsstaat verfügbaren Rechtsbehelfe und die Zulässigkeit rechtswidrig zusammengetragener Beweismittel sowie der Ausschlussvorschrift als Begleitmaßnahmen. Darüber hinaus könnten der Zugang zu Rechtsbehelfen in dem Land, in dem die Daten herausgegeben/gesichert wurden, oder in dem Mitgliedstaat, in dem der Verdächtige oder der Dritte wohnt, sowie Sanktionen gegen Behörden, die rechtswidrig Sicherungsanordnungen ausgeben, erforderlich sein, um für tatsächlich wirksame Rechtsbehelfe zu sorgen.

[20] Siehe auch EuGH, Rechtssache C-601/15, J. N./Staatssecretaris van Veiligheid en Justitie, Urteil vom 15. Februar 2016, Rn. 47 („ [...] ergibt sich aus den Erläuterungen zu Art. 6 der Charta [...] die Rechte aus Art. 6 der Charta den durch Art. 5 EMRK garantierten Rechten entsprechen [...]“). Leider hat der EuGH durch unklare Verweise in dem Gutachten 1/2015 und den Rechtssachen C-293/12 und C-594/12, Digital Rights Ireland und Seitlinger u. a., selbst für eine gewisse Verwirrung gesorgt. In Zukunft muss der EuGH in dieser Hinsicht sorgfältiger vorgehen, damit keine Missverständnisse entstehen, die sich negativ auf die Übereinstimmung der Charta mit den Mindestanforderungen der EMRK auswirken. Siehe auch X. Tracol, Gutachten 1/15 der Großen Kammer, Computer Law & Security Review 34 (2018) („ *Das Heranziehen von Artikel 6 der Charta durch die Große Kammer in diesem spezifischen Zusammenhang ist nicht nachvollziehbar und die Auswirkungen sind unklar.*“).

– Die Frage, ob sich der rechtliche Vertreter vom Ort der Niederlassung des Diensteanbieters entkoppeln lässt, muss noch eingehender untersucht werden, da dies erhebliche Auswirkungen auf den anderen zu notifizierenden Mitgliedstaat hätte. Es muss auch geklärt werden, ob ein solches System tatsächlich auch für in der EU niedergelassene Diensteanbieter notwendig ist (und nicht nur für in Drittländern niedergelassene Diensteanbieter), insbesondere im Hinblick auf bestehende Instrumente der Zusammenarbeit sowie die EMRK und den Rahmen der EU für Grundrechte und Datenschutz.

– Transparente und öffentliche Überwachung sowie die Erhebung von Statistiken müssen Teil des Systems sein.

– Nach Artikel 5 EMRK und 6 der Charta gibt es kein rechtlich anerkanntes „Recht auf Sicherheit“, und bei etwaigen Abwägungsprüfungen im Hinblick auf die Grundrechte darf kein Bezug auf ein solches nicht bestehendes Recht genommen werden.