Rat der
Europäischen Union

Brüssel, den 23. November 2015
(OR. en)

14369/15

JAI 895
COPEN 319
DROIPEN 150
CYBER 110

VERMERK

Absender:	Vorsitz
Empfänger:	Ausschuss der Ständigen Vertreter/Rat
Nr. Vordok.:	13689/15
Betr.:	Effektive Strafjustiz im digitalen Zeitalter – Bestimmung des Bedarfs – Sachstand

1. Die Bewertung der Bedrohungslage im Bereich der organisierten Kriminalität im Internet (iOCTA) von 2015[1] kommt zu dem Schluss, dass die Cyberkriminalität aggressiver und provokativer wird und die unterschiedlichsten kriminellen Aktivitäten, einschließlich herkömmlicher Straftaten, die digitale Spuren hinterlassen, umfasst. Dieses gegen Einzelpersonen und Unternehmen gerichtete Vorgehen ist kennzeichnend für den Wandel im Profil der Cyberkriminellen, was auch auf eine Beteiligung der organisierten Kriminalität und auf zunehmende psychologische Auswirkungen der Cyberkriminalität auf die Opfer schließen lässt.

2. Neue technologische Entwicklungen und Innovationen stellen besondere Herausforderungen für die Durchführung effektiver Ermittlungen dar und nötigen das Strafverfolgungssystem immer mehr, seine Instrumente und Vorgehensweisen entsprechend anzupassen. Von besonderer Bedeutung ist dies bei Terrorismusbekämpfungs- und Antiradikalisierungsmaßnahmen: Die Kommunikationskanäle des Internets und die zahlreichen sozialen Medien, einschließlich verschlüsselungsbasierter Technologien, werden weithin für terroristische Zwecke genutzt.

[1] Dok. 12728/15.

3. In einem sich so rasant entwickelnden technologischen Umfeld werden elektronische Daten bei Strafverfahren immer wichtiger. Diese Daten stellen elektronische Beweismittel dar. Allerdings ist es immer noch schwierig, zulässige elektronische Beweismittel zu erheben und im Verfahren zu verwenden sowie eine rechtskräftige Verurteilung der Straftäter zu erwirken. In Anbetracht dessen muss das den zuständigen Behörden zur Verfügung stehende rechtliche und praktische Instrumentarium an der Notwendigkeit einer effektiven Strafjustiz im digitalen Zeitalter gemessen werden.

4. Im Anschluss an die Beratungen im CATS vom 10. November 2015 werden in der Anlage des vorliegenden Dokuments eine Reihe möglicher Arbeitsbereiche beschrieben, die die Justizminister im Hinblick auf Vorgaben für das weitere Vorgehen zur Bewältigung der Herausforderungen bei der Erhebung und Verwendung elektronischer Beweismittel in Strafverfahren prüfen sollten.

Die Minister werden ersucht, anzugeben, welches der in diesem Dokument behandelten Themen prioritär behandelt werden sollte.

Diese lassen sich wie folgt zusammenfassen:

- Probleme aufgrund des Verlusts von Daten im digitalen Umfeld, die die Effektivität der Strafverfolgung beeinträchtigen können, einschließlich der Auswirkungen, die ein effektives System zur Vorratsdatenspeicherung in dieser Hinsicht haben könnte,
- die Probleme der zuständigen Behörden bei der Anwendung der herkömmlichen Regeln für die Rechtshilfe, insbesondere hinsichtlich der zur Bearbeitung eines Rechtshilfeersuchens zu erfüllenden formalen Auflagen oder der Schnelligkeit des Verfahrens, sowie die potenzielle Wirkung einer optimalen Verwendung der Europäischen Ermittlungsanordnung bei in der EU angesiedelten Fällen,
- Notwendigkeit, den Rahmen für die Zusammenarbeit mit ausländischen Diensteanbietern zu optimieren, wenn die derzeitige Praxis der zuständigen Behörden, sich mit direkten Ersuchen an sie zu wenden, in Anbetracht zunehmender Bedenken hinsichtlich der Grundrechte und Verfahrensgarantien überprüft werden muss,
- rechtliche Folgen des Standorts größerer digitaler Infrastrukturen und der entsprechenden Eigentumsverhältnisse und insbesondere die Intensivierung des diesbezüglichen Dialogs mit den US-Behörden,

- spezielle Probleme aufgrund des Cloud-Computings, die oft als "Standortverlust" bezeichnet werden, und die sich daraus ergebenden Folgen für die anwendbaren Gerichtsstandsregeln sowie die mögliche Erwägung eines grenzüberschreitenden Zugriffs auf Daten in Fällen, in denen der Standort der Daten unbekannt ist,

- Komplexität aufgrund der unterschiedlichen Regeln und Normen für die Zulässigkeit elektronischer Beweismittel vor den zuständigen einzelstaatlichen Gerichten,

- Erfordernis einer Abwägung jeder Maßnahme oder Initiative zur Steigerung der Effektivität der Strafverfahren im digitalen Zeitalter gegen die Auflagen der Grundrechtecharta der EU und die Normen der EMRK in der Auslegung durch den Europäischen Menschenrechtsgerichtshof.

ANLAGE

Probleme bei der Erhebung elektronischer Beweismittel und ihrer Verwendung in Strafverfahren

1. Mit der effektiven Erhebung, Übermittlung und Zulässigkeit elektronischer Beweismittel[2] in Strafverfahren sind unter strafrechtlichen Gesichtspunkten erhebliche Probleme verbunden. Bestätigt wurde dies in den ersten Länderberichten, die im Rahmen der *Siebten Runde der gegenseitigen Begutachtungen in Bezug auf die praktische Umsetzung und Durchführung der europäischen Maßnahmen zur Verhütung und Bekämpfung der Cyberkriminalität* ausgearbeitet wurden, und in verschiedenen Beratungen über Fragen im Zusammenhang mit elektronischen Beweismitteln, so etwa in der informellen COSI/CATS-Sitzung vom 22./23.Juli 2014 und in einem Workshop über Rechtshilfe im digitalen Zeitalter, der am 15. Oktober 2015 vom Vorsitz zusammen mit der Universität von Luxemburg veranstaltet wurde.
2. Am 19. Oktober und 11. November 2015 hat die Gruppe der Freunde des Vorsitzes (Fragen des Cyberraums) – wie in der Liste der prioritären Maßnahmen für die Durchführung der erneuerten Strategie der inneren Sicherheit der EU vorgesehen – die (rechtlichen) Lücken bei der Bekämpfung der Cyberkriminalität erörtert, um umfassende Vorgehensweisen, mit denen die derzeitigen Hindernisse für Ermittlungen in Cyberstraftaten überwunden und der Kommission konkrete Beiträge zu möglichen neuen Rechtsinstrumenten vorgelegt werden sollen, herauszuarbeiten, das Bewusstsein zu schärfen und bewährte Vorgehensweisen auszutauschen[3].
3. Das vorliegende Dokument schließt an diese Beratungen an und stützt sich auf Beiträge von Eurojust, die auf entsprechende Fallarbeit zurückgehen, die Abschlussberichte seines Workshops über Cyberkriminalität vom 19./20. November 2015 und seine taktische Sitzung über Cyberkriminalität vom 1. Juli 2015. Als Quellen für dieses Dokument dienten außerdem eine Reihe von Themenberichten des Ausschusses des Übereinkommens über Computerkriminalität des Europarates (T-CY)[4], die von Europol/dem Europäischen Zentrum zur Bekämpfung der Cyberkriminalität erstellte iOCTA 2015, die Ergebnisse des obengenannten Workshops des Vorsitzes über Rechtshilfe im digitalen Zeitalter sowie die kürzlich vom EP-Ausschuss für bürgerliche Freiheiten, Justiz und Inneres (LIBE) in Auftrag gegebene Studie über die Herausforderungen der Strafverfolgung bei der Cyberkriminalität[5]. Auch die in der Sitzung des CATS vom 10. November 2015 vorgebrachten Bemerkungen der Mitgliedstaaten sind berücksichtigt.

---

2 Für die Zwecke dieses Dokuments bezieht sich der Begriff "elektronische Beweismittel" auf alle elektronischen Daten im Zusammenhang mit einer Straftat, die im Laufe eines Strafverfahrens von Bedeutung sein können. Die Erhebung, Weitergabe und Verwendung von Daten zu reinen Störungs- oder Präventionszwecken fällt daher nicht darunter.

3 Dok. 12612/15.

4 http://www.coe.int/en/web/cybercrime/t-cy-reports

5 Studie des EP-Ausschusses für bürgerliche Freiheiten, Justiz und Inneres (2015) "The law enforcement challenges of cybercrime: are we really playing catch-up?", PE 536.471

1. Datenvorratsspeicherung und Datenverlust

4. In der Richtlinie 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation) sind spezielle Regeln für die Verarbeitung personenbezogener Daten, aber auch das Recht auf Vertraulichkeit der Kommunikation (Artikel 5) und die Pflicht der Betreiber niedergelegt, Verkehrsdaten zu löschen, sobald sie für die Übertragung einer Nachricht nicht mehr benötigt werden, außer wenn sie unter bestimmten Bedingungen zum Zweck der Gebührenabrechnung und der Bezahlung von Zusammenschaltungen verarbeitet werden. Nach deren Artikel 15 Absatz 1[6] ist es unter bestimmten Bedingungen zulässig, die in dieser Richtlinie niedergelegten Rechte und Pflichten für eine Reihe spezieller Zwecke zu beschränken, zu denen auch "*die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten*" gehört. Somit wird die Einführung nationaler Maßnahmen zur Vorratsdatenspeicherung unter bestimmten Bedingungen ermöglicht. Mit der Richtlinie 2006/24/EG (Vorratsdatenspeicherungsrichtlinie) sollten diese Regeln harmonisiert werden, damit gewährleistet ist, dass die Daten insbesondere für die Ermittlung, Feststellung und Verfolgung schwerer Straftaten zur Verfügung stehen.

5. Naturgemäß sind elektronische Beweismittel kurzlebig. Dazu kommt, dass Straftäter aufgrund der zunehmenden privaten Nutzung des Live-Streaming, der Verschlüsselung, des Entstehens des Darknet und der Anonymisierung der Strafverfolgung entscheidende Beweismittel vollkommen entziehen können. Somit können entscheidende elektronische Beweismittel verlorengehen, wenn den zuständigen Behörden keine geeigneten Mittel zur Verfügung stehen, um effektiv zu reagieren. Eine effektive Vorratsdatenspeicherungsregelung könnte sich in dieser Hinsicht als nützlich erweisen.

---

6 Artikel 15 Absatz 1 der Richtlinie 2002/58/EG lautet:
"Die Mitgliedstaaten können Rechtsvorschriften erlassen, die die Rechte und Pflichten gemäß Artikel 5, Artikel 6, Artikel 8 Absätze 1, 2, 3 und 4 sowie Artikel 9 dieser Richtlinie beschränken, sofern eine solche Beschränkung gemäß Artikel 13 Absatz 1 der Richtlinie 95/46/EG für die nationale Sicherheit (d.h. die Sicherheit des Staates), die Landesverteidigung, die öffentliche Sicherheit sowie die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig ist. Zu diesem Zwecke können die Mitgliedstaaten unter anderem durch Rechtsvorschriften vorsehen, dass Daten aus den in diesem Absatz aufgeführten Gründen während einer begrenzten Zeit aufbewahrt werden. Alle in diesem Absatz genannten Maßnahmen müssen den allgemeinen Grundsätzen des Gemeinschaftsrechts einschließlich den in Artikel 6 Absätze 1 und 2 des Vertrags über die Europäische Union niedergelegten Grundsätzen entsprechen."

6. In seiner Analyse des Rechtsrahmens der EU-Mitgliedstaaten und der derzeitigen Probleme bei der Vorratsdatenspeicherung vom 26. Oktober 2015[7] erläutert Eurojust, dass die derzeitige EU-weite Fragmentierung des Rechtsrahmens für die Vorratsdatenspeicherung infolge der Nichtigerklärung der Richtlinie 2006/24/EG (Vorratsdatenspeicherungsrichtlinie) durch das Urteil des Gerichtshofs der Europäischen Union (EuGH) vom 8. April 2014 die Effektivität der strafrechtlichen Ermittlungen und der Strafverfolgung auf nationaler Ebene beeinträchtigt, insbesondere was die Zuverlässigkeit und die Zulässigkeit von Beweismitteln vor Gericht sowie die grenzüberschreitende justizielle Zusammenarbeit zwischen den Mitgliedstaaten und weltweit anbelangt.

7. Auf der Tagesordnung für die Ratstagung ist als gesonderter Punkt eine Diskussion der Minister speziell über den aktuellen Stand und die Auswirkungen des Vorratsdatenspeicherungsurteils des EuGH vom 8. April 2014 vorgesehen.

2. Das Verfahren der Rechtshilfe

8. Bei der Erhebung elektronischer Beweismittel spielt die Zeit grundsätzlich eine ausschlaggebende Rolle. Zügig abgewickelte Verfahren für die Sicherung und Erhebung elektronischer Beweismittel ist für die effektive Durchführung von Strafverfahren von wesentlicher Bedeutung. Da sich die elektronischen Daten sehr oft in einem ausländischen Rechtsraum befinden, müssen die zuständigen nationalen Behörden die vorhandenen Mittel für die internationale Zusammenarbeit in Anspruch nehmen, d.h. um Rechtshilfe ersuchen oder, bei EU-Mitgliedstaaten betreffende Verfahren, gegebenenfalls auf die bestehenden EU-Instrumente zur gegenseitigen Anerkennung für die justizielle Zusammenarbeit in Strafsachen zurückgreifen.

9. Die Richtlinie 2014/41/EU über die Europäische Ermittlungsanordnung (EEA) in Strafsachen[8] ist in dieser Hinsicht von besonderer Bedeutung. Sie wird ab dem 22. Mai 2017 das derzeitige fragmentierte EU-Recht über die Erhebung und Übermittlung von Beweismitteln zwischen EU-Mitgliedstaaten ersetzen, damit grenzüberschreitende Ermittlungen schneller und effizienter werden. Auch bei elektronischen Beweismitteln sollte diese Regelung innerhalb des Anwendungsbereichs der EEA in vollem Umfang genutzt werden.

---

[7] Dok. 13085/15.

[8] ABl. L 130 vom 1.5.2014, S. 1-36.

10. Häufig befinden sich elektronische Daten im Rechtsraum von Drittstaaten. In diesen Fällen sollte um Rechtshilfe ersucht werden. Die bestehenden Rechtshilferegelungen werden jedoch immer mehr als zu langsam und schwerfällig betrachtet, um den zeitlichen Zwängen gerecht zu werden. Somit stellt sich die Frage, wie die Rechtshilfeverfahren beschleunigt werden könnten, was in erster Linie durch eine Optimierung der vorhandenen Verfahren geschehen könnte. In dieser Hinsicht könnte in Erwägung gezogen werden, auch im Zusammenhang mit der EEA ein standardisiertes, vereinfachtes und möglicherweise elektronisch zu übermittelndes und zu empfangendes Antragsformular auszuarbeiten. Ferner könnte geprüft werden, ob die formalen Auflagen in den Rechtshilfeverfahren weiter differenziert werden könnten, je nachdem, um welche Daten – Teilnehmer-, Verkehrs- oder Inhaltsdaten – ersucht wird. In vielen Rechtsordnungen sind die Auflagen für Teilnehmerdaten tendenziell niedriger als für Verkehrsdaten, während die strengsten Regelungen für Inhaltsdaten gelten[9].

11. Es könnte ein gemeinsamer Standard für die Behandlung eines Zusammenarbeitsersuchens als "dringend" eingeführt werden. Außerdem ließen sich beschleunigte Verfahren für die Übermittlung von Beweismitteln unter bestimmten Bedingungen in Erwägung ziehen, wie sie für die Beweissicherung gemäß den einschlägigen Bestimmungen des Übereinkommens des Europarates über Computerkriminalität bereits besteht. Selbst wenn die Beweismittel gesichert sind, dürfte es beim derzeitigen Stand der Dinge generell lange dauern, bis sie im ersuchenden Land für das Strafverfahren zur Verfügung stehen.

12. Im Hinblick auf eine funktionierende Zusammenarbeit sollte eine frühzeitige Koordinierung und Beteiligung der Justizbehörden an den Strafverfahren in Erwägung gezogen werden. In dieser Hinsicht könnte ein weiterer Ausbau der 24/7-Kooperationsnetze, einschließlich derjenigen der Justizbehörden, sowie die Schaffung eines Netzes von mit Cyberkriminalität befassten Staatsanwälten in Erwägung gezogen werden. Dies wäre für die Förderung und Intensivierung der direkten Kontakte zwischen den Justizbehörden, auch für Rechtshilfeersuchen in der gesamten EU und weltweit, hilfreich. Diesbezüglich sollte auch die Rolle von Eurojust und Europol/des Europäischen Zentrums zur Bekämpfung der Cyberkriminalität in die Überlegungen einbezogen werden.

---

9 Siehe Diskussionspapier des T-CY "Criminal justice access to data in the cloud: challenges", Mai 2015
(T-CY(2015)10), S. 7
https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680304b59

3. Direkte Ersuchen und Zusammenarbeit mit ausländischen Diensteanbietern

13. Für die Bekämpfung der Cyberkriminalität ist die Zusammenarbeit mit der Privatwirtschaft von ausschlaggebender Bedeutung. Allerdings gibt es für eine derartige Zusammenarbeit keinen gemeinsamen Rechtsrahmen. Dies kommt besonders zum Tragen, wenn es um den Zugang zu Daten ausländischer Diensteanbieter geht.

14. Um den Unzulänglichkeiten des derzeitigen Rechtshilfeverfahrens bei der Erhebung elektronischer Beweismittel abzuhelfen, greifen die zuständigen Behörden auf andere Methoden der Gewinnung elektronischer Beweismittel zurück, indem sie sich beispielsweise direkt an ausländische Diensteanbieter wenden. In derartigen Fällen kann es Diensteanbietern nach dem innerstaatlichen Recht gestattet sein, (ausländischen) Strafverfolgungsbehörden Daten, die keine Inhaltsdaten sind, freiwillig offenzulegen. Dies ist jedoch nicht in allen Staaten der Fall. Andererseits sind Diensteanbieter nicht immer zur Zusammenarbeit bereit, selbst wenn diese nach innerstaatlichem Recht zulässig ist. Außerdem ist nicht in allen Mitgliedstaaten zulässig, eine innerstaatliche Vorlageanordnung an eine privatrechtliche juristische Person im Ausland zu richten. Ebenso ist es möglich, dass selbst ein durch eine freiwillige Auskunftserteilung erlangtes elektronisches Beweismittel vor dem Gericht des ersuchenden Staates nicht zulässig ist, weil es außerhalb des Rechtshilferahmens erlangt wurde. Wie im Workshop des Vorsitzes über Rechtshilfe im digitalen Zeitalter vom 15. Oktober aufgezeigt wurde, dürfte ein derartiges Verfahren generell wohl auf eine Art Rechtshilfe "ohne Hilfe" hinauslaufen, was Bedenken hinsichtlich der Grundrechte und der Verfahrensgarantien hervorrufen dürfte.

15. Andererseits könnten ausländische Diensteanbieter, die direkt angesprochen werden, in die Lage geraten, dass aus verschiedenen Staaten widerstreitende Ersuchen an sie gerichtet werden, aber auch widerstreitende Auflagen für den Schutz der Privatsphäre und Verfahrensgarantien für sie gelten, wenn sie in mehreren Rechtsräumen tätig sind. Beispielsweise können Diensteanbieter durch die Offenlegung von Daten gegenüber den Behörden des einen Staates gegen die Datenschutzbestimmungen eines anderen Staates verstoßen.

16. In Anbetracht dessen müssen eindeutige Bedingungen für einen tragfähigen Rahmen der Zusammenarbeit zwischen den privaten Akteuren und den Behörden hinsichtlich der Erhebung elektronischer Beweismittel festgelegt werden, und zwar auf der Grundlage der uneingeschränkten Achtung der Verfahrensgarantien für Verdächtige und Beschuldigte in Strafverfahren und im Einklang mit dem Schutz personenbezogener Daten.

4. Rechtliche Folgen des Standorts der digitalen Infrastruktur und des Eigentums an dieser Infrastruktur

17. Da sich die nationalen Rechtsvorschriften des Vollstreckungsstaats auf die internationale Zusammenarbeit auswirken können, ist es von ausschlaggebender Bedeutung, den Dialog mit Ländern zu intensivieren, die hinsichtlich des Betriebs wichtiger digitaler Infrastruktur und der entsprechenden Eigentumsverhältnisse eine zentrale Rolle spielen.

18. Dies gilt insbesondere für die Zusammenarbeit mit den USA. In der Studie des LIBE-Ausschusses von 2015 über die Herausforderungen der Strafverfolgung bei der Cyberkriminalität wird ausgeführt, dass US-amerikanischen und in den USA niedergelassenen Unternehmen hinsichtlich des Funktionierens des Internets eine Führungsrolle zukommt. Somit hat der US-amerikanische Rechtsrahmen einen erheblichen Einfluss auf die Strafverfolgung von Cyberkriminalität.[10] Über die unterschiedlichen Datenschutznormen hinaus wirkt sich dies unter rein strafrechtlichen Gesichtspunkten auf die Anforderungen an die rechtliche Begründung aus, denen in Rechtshilfeersuchen an die USA zu entsprechen ist, insbesondere wenn es um Ersuchen im Zusammenhang mit Inhaltsdaten geht.

19. Generell muss in allen Rechtshilfeersuchen erläutert werden, warum die zuständige Behörde ein legitimes Interesse an den Daten hat, um die sie ersucht. Nach US-amerikanischem Recht muss bei Ersuchen geprüft werden, ob ein sogenannter hinreichender Verdacht ('probable cause') besteht, wodurch höhere Anforderungen an die Begründung als beim Grund zu der Annahme ('reasonable suspicion') oder Ähnlichem gestellt werden. Die Begründung mit einem hinreichenden Verdacht beschränkt die zuständigen Behörden bei ihren Eingriffen auf das für bestimmte Ermittlungen unbedingt erforderliche Maß. Daher ist es sehr wahrscheinlich, dass ein Rechtshilfeersuchen von den US-amerikanischen Behörden zurückgewiesen wird, weil es die Begründungsanforderung des hinreichenden Verdachts nicht erfüllt. Sicherzustellen ist außerdem ein ausgewogenes Verhältnis zwischen den Möglichkeiten der US-amerikanischen und der ausländischen Behörden, Zugang zu "lokalen" US-amerikanischen Daten einerseits und zu anderen Arten von Daten andererseits zu erhalten. Diese Punkte sollten in einem ständigen Dialog zwischen der EU und den USA und auch im Rahmen der Überarbeitung des Rechtshilfeübereinkommens der EU zur Sprache gebracht werden.

---

10 Studie des LIBE-Ausschusses des EP (2015) "The law enforcement challenges of cybercrime: are we really playing catch-up?", PE 536.471, S. 46.

5. Standortverlust

20. Während der Zugang zu elektronischen Beweismitteln in ausländischen Rechtsräumen hauptsächlich im Rahmen der Rechtshilfe erfolgt, stellt die zunehmende Nutzung des Cloud-Computing und Web-gestützter Dienste für die zuständigen Behörden ein zusätzliches Problem dar, das als "Standortverlust" bezeichnet wird[11]. In diesem Fall wird das elektronische Beweismittel "irgendwo in der Cloud" gespeichert, entweder auf einem Server oder über mehrere Server verteilt oder es wird zwischen Servern mit wechselnden Standorten verschoben. Die betreffenden Daten befinden sich also physisch in ausländischen, unbekannten oder mehreren Rechtsräumen gleichzeitig oder werden zwischen diesen verschoben.

21. Grundsätzlich bestimmt der Standort die zuständige Behörde und das für die Ermittlungen geltende Recht, einschließlich des Umfangs etwaiger Zwangsmaßnahmen und der Verfahrensgarantien für Verdächtige oder Beschuldigte. Im Zusammenhang mit den obengenannten neuen technologischen Entwicklungen, bei denen die Daten den Standort wechseln, scheint das grundlegende Territorialitätsprinzip, das für die Begründung der gerichtlichen Zuständigkeit in Strafverfahren maßgeblich ist, an Bedeutung zu verlieren, was für die effektive Durchführung von Strafverfahren Probleme aufwirft.

22. In manchen Fällen könnte die rechtmäßige Suche innerhalb des im Hoheitsgebiet der strafrechtlichen Ermittlungen angesiedelten ursprünglichen Systems auf ein vernetztes Informationssystem im Ausland ausgedehnt werden, ohne dass dies bemerkt wird; dies gilt auch für Fälle, in denen unklar ist, in welchem Hoheitsgebiet das Informationssystem seinen Standort hat. Dies kann in der Praxis zu einem grenzüberschreitenden Zugriff auf in einem ausländischen Rechtsraum befindlichen Daten "ohne Zustimmung" führen, was über die vorhandenen rechtlichen Möglichkeiten (z.B. Artikel 32 Buchstabe b des "Budapester Übereinkommens über Computerkriminalität" des Europarates) hinausgeht. Die Behandlung und Nutzung der so gewonnenen Daten richtet sich nach dem nationalen Recht und unterliegt folglich bei den Verfahrensgarantien unterschiedlichen Standards.

---

11 Siehe Bericht der Gruppe des Europarates über grenzüberschreitenden Zugang vom 6. Dezember 2012 über den grenzüberschreitenden Zugang und die gerichtliche Zuständigkeit und die entsprechenden Optionen, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/T-CY/TCY2013/TCYreports/TCY_2012_3_transborder_rep_V31public_7Dec12.pdf

23. Der "Standortverlust" kann zu widerstreitenden Strafverfolgungsanträgen oder zu Parallelermittlungen führen, wodurch wiederum deutlich wird, dass die Justizbehörden frühzeitig einbezogen werden müssen, aber auch, dass die Regeln für die Feststellung der gerichtlichen Zuständigkeit überarbeitet und für Fälle, in denen der Standort der Daten unbekannt ist, Alternativen zum Rechtshilfeverfahren – wie grenzüberschreitender Zugang zu Daten für Zwecke der Strafverfolgung – geprüft werden müssen.

6. Zulässigkeit elektronischer Beweismittel

24. Eurojust weist darauf hin, dass die Justizbehörden nach einzelstaatlichem Recht möglicherweise gehalten sind, die Rechtmäßigkeit der Beweiserhebung anhand der gesetzlich vorgeschriebenen Kriterien umfassend zu bewerten, damit die Beweismittel vor Gericht zulässig sind; anders liegt der Fall in Rechtssystemen, die auf dem Vertrauensprinzip beruhen und in denen alle Beweismittel vorgelegt und vom Richter nach freiem Ermessen bewertet werden. Diese Auflagen müssen bei der Erhebung und Weitergabe elektronischer Beweismittel berücksichtigt werden. Daraus kann sich für die zuständigen Behörden beispielsweise die Notwendigkeit ergeben, Beweismittel entsprechend den Auflagen eines ausländischen Rechtssystems zu sichern und zu erheben.

25. Für eine korrekte Auslegung elektronischer Beweismittel in Strafverfahren können Fachkenntnisse erforderlich sein, die bei den Staatsanwaltschaften oder Gerichten vielleicht nicht in ausreichendem Maße vorhanden sind. Außerdem bedarf die ordnungsgemäße Vorlage elektronischer Beweismittel in einem Gerichtsverfahren wohl einer kriminaltechnischen Sensibilisierung innerhalb des Justizwesens, die vielleicht nicht immer vorausgesetzt werden kann.

26. Für diese Sensibilisierung wären Informationsaustausch, Austausch bewährter Vorgehensweisen und gezielte Schulungen in Betracht zu ziehen.

7. Abwägung gegen Grundrechte und Rechtsstaatlichkeit

27. effektive Verfahrens- und Datenschutzgarantien sowie die uneingeschränkte Wahrung der Rechtsstaatlichkeit bilden die gemeinsame Grundlage, auf der alle politischen Initiativen und praktischen Lösungen für eine effektivere Durchführung von Strafverfahren beruhen sollten.

28. Daher sollte zwischen den Erfordernissen der Strafjustiz in Verfahren im Zusammenhang mit Cyberkriminalität und den etablierten Grundrechtsprinzipien regelmäßig eine sorgfältige Abwägung vorgenommen werden. Das ist keine leichte Aufgabe. Diese Problematik ist bei den Arbeiten des Europarates im Zusammenhang mit dem Zusatzprotokoll über den grenzüberschreitenden Zugang zu Daten deutlich geworden. Sie wird auch in etlichen neueren Urteilen des Gerichtshofs aufgezeigt, in denen dieser dem Gesetzgeber die klare Vorgabe erteilt, diese Arbeiten voranzubringen und regelmäßig an den Grundrechten und dem Legalitätsgebot zu messen.