

**89. Konferenz der Justizministerinnen und Justizminister der Länder
am 6. und 7. Juni 2018 in Eisenach**

Beschlussvorschlag

**TOP... Strafverfolgung und Datenschutz – Vorschläge der Kommission zur
Verbesserung des grenzüberschreitenden Zugangs zu elektronischen
Beweismitteln in Strafsachen („E-Evidence“)**

Berichterstattung: Hamburg

1. Die Justizministerinnen und Justizminister haben sich mit den am 17. April 2018 veröffentlichten Vorschlägen der Kommission für eine Verordnung zur Einführung einer Europäischen „Production Order“ und einer Europäischen „Preservation Order“ in Bezug auf elektronische Beweismittel in Strafsachen (COM[2018] 225 final) sowie für eine Richtlinie zur Benennung gesetzlicher Vertreter zum Zwecke der Beweismittelgewinnung in Strafverfahren (COM[2018] 226 final) befasst.
2. Sie stimmen angesichts der fortschreitenden Digitalisierung und Vernetzung darin überein, dass der grenzüberschreitenden Sicherung und Erhebung von elektronischen Beweismitteln für die Gewährleistung einer effektiven Strafverfolgung eine erhebliche Bedeutung zukommt. Hierzu steht im Verhältnis zu den EU-Mitgliedstaaten mit der Europäischen Ermittlungsanordnung bereits jetzt ein grundsätzlich geeignetes Rechtsinstrument bereit.
3. Die Justizministerinnen und Justizminister betonen zugleich, dass bei der Einführung weiterer grenzüberschreitender Ermittlungsinstrumente, die dem nachvollziehbaren Ziel der Verfahrensbeschleunigung dienen sollen, ein grundrechtskonformer Umgang mit digitalen Beweismitteln und die Beibehaltung des bestehenden Datenschutzniveaus sicherzustellen sind. Daher müssen sowohl der Erlass entsprechender Anordnungen im Inland als auch die grenzüberschreitende Datenherausgabe durch inländische Diensteanbieter an das Ausland zumindest denselben strafprozessualen Voraussetzungen genügen wie eine rein inländische Datenherausgabe.
4. In diesem Zusammenhang erscheint es aus Sicht der Justizministerinnen und Justizminister bedenklich, dass nach dem jetzigen Regelungsvorschlag keine grundsätzliche Unterrichtung der zuständigen Behörden des Mitgliedstaates, in dem der adressierte Diensteanbieter seinen Sitz oder gesetzlichen Vertreter hat, im Sinne einer „Notifikationslösung“ vorgesehen ist. So besteht nur in Ausnahmefällen die Möglichkeit des Widerspruchs, falls die Sicherung oder Erhebung der elektronischen Beweismittel in einem vergleichbaren innerstaatlichen Fall nicht zulässig wäre oder sonstige übergeordnete rechtsstaatliche Grundsätze der Datenherausgabe entgegenstehen.
5. Die Justizministerinnen und Justizminister weisen zudem darauf hin, dass bei einem Abrücken von bestehenden Rechtshilfegrundsätzen wie der grundsätzlichen Einbindung der zuständigen ausländischen Behörden im Verhältnis zu Drittstaaten die Gefahr besteht, dass dort vergleichbare Regelungen geschaffen werden, die ohne Rücksicht auf das

hiesige Schutzniveau und ohne etwaige Abwehrmechanismen einen direkten Zugriff der ausländischen Strafverfolgungsbehörden auf in der EU gespeicherte Daten erlauben.

6. Sie bitten daher die Bundesregierung, sich auf internationaler und insbesondere auf EU-Ebene auch weiterhin für die Wahrung des geltenden Grundrechts- und Datenschutzniveaus einzusetzen und die Länder in den anstehenden Diskussions- und Entscheidungsprozess zu den vorgelegten Legislativvorschlägen der Kommission eng einzubinden.

Begründung

Die nunmehr veröffentlichten Legislativvorschläge der Kommission beziehen sich nur auf einen Teilbereich der Handlungsfelder, die Gegenstand der Diskussion im Rahmen der im Vorfeld zum Thema „E-Evidence“ durchgeführten Expertenkonsultationen waren. Konstellationen, in denen Strafverfolgungsbehörden der Mitgliedstaaten im Zuge einer Ermittlungsmaßnahme – insbesondere einer Durchsuchung – ohne Beteiligung eines Providers bzw. dessen technische Unterstützung direkt auf Daten zugreifen können, die in anderen Mitglied- oder Drittstaaten etwa in einer sogenannten „Cloud“ gespeichert sind, werden von den jetzigen Vorschlägen nicht erfasst.

Die beabsichtigten Ermittlungsinstrumente der direkt an die Diensteanbieter zu adressierenden Europäischen „Production Order“ oder „Preservation Order“ sollen die aktuell vorhandenen Rechtshilfeinstrumente und hier insbesondere die Europäische Ermittlungsanordnung (EEA) um einen schnellere Verfahrensweise ergänzen. Dieses grundsätzlich nachvollziehbare, möglicherweise aber ohne Evaluation der EEA auch verfrühte Anliegen darf allerdings nicht dazu führen, dass bestehende grund- und datenschutzrechtliche Standards abgesenkt werden. In diesem Zusammenhang hat die Bundesregierung in der Vergangenheit zu Recht darauf hingewiesen, dass zur Wahrung des geltenden Grundrechtsschutzniveaus die grenzüberschreitende Datenherausgabe durch inländische Diensteanbieter zumindest denselben strafprozessualen Voraussetzungen genügen müsste wie rein inländische Datenherausgaben (vgl. BT-Drs. 19/1493, Antwort auf Frage 3).

Es bestehen schon Zweifel, ob Artikel 5 Absatz 2 des jetzigen Verordnungsentwurfs (VO-E) in ausreichendem Maße klargestellt, dass der Erlass einer „Production Order“ nur dann zulässig ist, wenn die Voraussetzungen einer vergleichbaren Beschlagnahme- und/oder Herausgabeanordnung nach der nationalen Prozessordnung (übertragen auf einen rein innerstaatlichen Sachverhalt) erfüllt sind. So stellt sich zum Beispiel die Frage, ob der in § 100j Absatz 3 Satz 1 StPO statuierte Richtervorbehalt von Artikel 4 Absatz 1 (a) VO-E verdrängt wird, nach dessen Regelung eine Europäische „Production Order“ im Hinblick auf Bestands- und Zugangsdaten auch vom zuständigen Staatsanwalt erlassen werden kann.

Ob diese Überlegungen im gleichen Maße auch für die „Preservation Order“ anzustellen sind, hinsichtlich derer eine mit Artikel 5 Absatz 2 des VO-E vergleichbare Regelung bisher fehlt, bedarf gegebenenfalls noch weiterer Erörterungen.

In jedem Fall sehen die bisherigen Überlegungen nur sehr eingeschränkte Schutzmechanismen vor, die sicherstellen könnten, dass die grenzüberschreitende

Datenherausgabe neben den Voraussetzungen des Rechts des ermittelnden Mitgliedstaates auch den Voraussetzungen des Rechts des Mitgliedstaates genügt, in dem der Diensteanbieter seinen Sitz hat.

Denn nur ausnahmsweise erfährt letztgenannter Mitgliedstaat von den Anordnungen, etwa wenn der betroffene Diensteanbieter europarechtliche Einwendungen gegen die „Production Order“ geltend macht (Artikel 9 Absatz 5 VO-E) oder einer Anordnung nicht nachkommt und daher eine Vollstreckung im Sinne von Artikel 14 VO-E erfolgen soll. Im Übrigen steht in diesen Fällen auch nur ein eingeschränkter Prüfungsmaßstab zur Verfügung, vgl. etwa Artikel 14 Absatz 2 VO-E.

Gleiches gilt, wenn gemäß Artikel 5 Absatz 7 oder Artikel 18 VO-E entweder im Vorwege die anordnende Stelle oder im weiteren strafrechtlichen Verfahren das Gericht – jeweils des Ausstellungsstaates (!) – überprüfen soll, ob die in Frage stehenden elektronischen Beweismittel gegebenenfalls nach dem Recht des anderen Mitgliedstaates unter einen besonderen Schutz (Immunitäten oder sonstige Vorrechte) fallen oder durch die Herausgabe dortige Sicherheits- oder Verteidigungsinteressen berührt sind. Zu diesem Zwecke können dann die zuständigen Stellen des anderen Mitgliedstaates konsultiert werden. Hier bestehen schon Zweifel, inwieweit die Strafverfolgungsbehörden und Gerichte des Ausstellungsstaates überhaupt aus eigener Anschauung beurteilen können, ob etwa Sicherheitsinteressen anderer Staaten der Erhebung oder Verwendung der erlangten Beweismittel entgegenstehen. Dies könnte ohnehin eine regelhafte Konsultation der zuständigen Stellen des anderen Mitgliedstaates notwendig machen.

In jedem Fall sollte es aber nicht allein der Einschätzung der Diensteanbieter oder der zuständigen Stellen bzw. Gerichte des Ausstellungsstaates überlassen bleiben, ob und wann der andere Mitgliedstaat über die Maßnahmen jedenfalls zu unterrichten ist, um diesem die Möglichkeit einzuräumen, innerhalb einer – kurzen – Frist der Datensicherung bzw. Datenherausgabe oder -verwertung zu widersprechen.

Soweit Diensteanbieter aus Drittstaaten – insbesondere aus den USA – mithilfe des Richtlinienvorschlages in den Anwendungsbereich der Verordnung einbezogen sind und so insgesamt der Speicherort der elektronischen Beweismittel irrelevant werden soll, verweist die Kommission auf die in den Artikeln 15 und 16 VO-E vorgesehenen Abhilfemöglichkeiten, die es den Diensteanbietern erlauben sollen, Einwendungen gegen die Datenherausgabe zu erheben, die sich aus dem Recht des Drittstaates ergeben. Zudem formuliert die Kommission die Erwartung, dass vergleichbare Regelungen in Drittstaaten ebenfalls dafür sorgen, dass das europäische Datenschutzniveau bei der Erhebung von Daten in der EU respektiert wird.

Abgesehen davon, ob die genannten Abhilfemöglichkeiten überhaupt als praktikabel anzusehen sind – auch hier hätte ein Gericht des Ausstellungsstaates, gegebenenfalls also ein deutsches Gericht das Datenschutzrecht eines anderen, in diesem Fall eines Nicht-EU-Staates zu prüfen – ist es tatsächlich unerlässlich, dass Ermittlungsbehörden aus Drittstaaten bei Datenerhebungen innerhalb der EU das hiesige Datenschutzrecht beachten müssen. Um dieser Erwartung Ausdruck zu verleihen, bedarf es aber internationaler Verhandlungen und Überzeugungsarbeit der Kommission und auch der Bundesregierung.