Referentenentwurf E-Evidence[1]

- Informationspapier -

Welchem Zweck dient der Referentenentwurf?

Der Referentenentwurf schafft die organisatorischen Voraussetzungen für die grenzüberschreitende Erhebung elektronischer Beweismittel innerhalb der Europäischen Union. Zudem trifft er Zuständigkeits- und Rechtschutzregelungen für die auf EU-Ebene neu geschaffenen Instrumente der Europäischen Sicherungsanordnung und der Europäischen Herausgabeanordnung.

Mit diesen Regelungen dient der Entwurf der Umsetzung einer EU-Richtlinie[2] sowie der Durchführung einer EU-Verordnung[3]. Die beiden Dossiers wurden in den Gremien der Europäischen Union unter dem Schlagwort „E-Evidence“ verhandelt. Die EU-Verordnung mit begleitender EU-Richtlinie reagiert auf die stark zunehmende Bedeutung digitaler Medien bei der Anbahnung und Ausführung krimineller Handlungen. So werden etwa Eigentumsdelikte immer häufiger mittels elektronischer Kommunikationsmittel vorbereitet, indem bspw. Tatobjekte über das Internet ausgespäht oder Verabredungen über Messengerdienste getroffen werden. Auch der Handel mit Betäubungsmitteln wird zunehmend über Messengerdienste koordiniert. Im internationalen Kontext stellt dies die Strafverfolgungsbehörden vor besondere Herausforderungen. Denn zum einen ist schwierig zu bestimmen, wo sich die relevanten Daten befinden, zum anderen erweisen sich die klassischen Methoden der Ermittlungszusammenarbeit angesichts der Volatilität im digitalen Raum oftmals als zu schwerfällig. Rechtshilfeersuchen beanspruchen in der Regel mehrere Monate – insbesondere in die USA, wo die überwiegende Zahl der Diensteanbieter ihren Sitz haben (z. B. Meta, Microsoft, Apple, Google). In dieser Zeit können relevante Daten längst gelöscht oder veraltet sein. Hinzu kommt, dass die Diensteanbieter die Daten in der Regel dezentral und flexibel nach wirtschaftlichen Kriterien speichern, weswegen diese ständig „wandern“ können, im Extremfall etwa zehntelsekündlich. Ländergrenzen oder reale Anknüpfungspunkte spielen damit keine Rolle; die Welt wird zum einheitlichen digitalen Raum. Welche Daten sich zu welchem Zeitpunkt wo befinden, kann letztlich nur der jeweilige Diensteanbieter selbst beantworten.

Welche Regelungen sehen EU-Verordnung und EU-Richtlinie im Wesentlichen vor?

Die neuen Vorschriften ermöglichen es Strafverfolgungsbehörden, elektronische Beweismittel direkt von Diensteanbietern in anderen Mitgliedstaaten anzufordern (sog. „Herausgabeanordnungen") oder die Aufbewahrung von Daten für bis zu 60 Tage zu verlangen, damit relevante Daten nicht gelöscht werden oder verloren gehen (sog. „Sicherungsanordnungen"). Die Beantwortung einer Herausgabeanordnung muss binnen 10 Tagen, in Notfällen binnen acht Stunden, erfolgen.

Diensteanbieter aus Drittstaaten müssen in der EU Empfangsbevollmächtigte (sog. „Adressaten“) benennen, an die sich die Strafverfolgungsbehörden wenden können, um die Herausgabe oder Sicherung der Daten zu verlangen.

---

1 Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2023/1544 und zur Durchführung der Verordnung (EU) 2023/1543 über die grenzüberschreitende Sicherung und Herausgabe elektronischer Beweismittel im Strafverfahren innerhalb der Europäischen Union.

2 Richtlinie (EU) 2023/1544 des Europäischen Parlaments und des Rates vom 12. Juli 2023 zur Festlegung einheitlicher Regeln für die Benennung von benannten Niederlassungen und die Bestellung von Vertretern zu Zwecken der Erhebung elektronischer Beweismittel in Strafverfahren; im Folgenden: Verordnung.

3 Verordnung (EU) 2023/1543 des Europäischen Parlaments und des Rates vom 12. Juli 2023 über Europäische Herausgabeanordnungen und Europäische Sicherungsanordnungen für elektronische Beweismittel in Strafverfahren und für die Vollstreckung von Freiheitsstrafen nach Strafverfahren; im Folgenden: Richtlinie.

Wie soll dies im deutschen Recht umgesetzt werden?

Der durch die Verordnung und Richtlinie geschaffene E-Evidence-Mechanismus soll durch ein neues Stammgesetz[4] in die deutsche Rechtsordnung implementiert werden.

Wie unterscheidet sich der E-Evidence-Mechanismus von dem bisherigen Verfahren?

Bisher müssen sich Strafverfolgungsbehörden für die Herausgabe von elektronischen Beweismitteln, die ein Diensteanbieter mit Sitz im Ausland gespeichert hat, im Wege eines „klassischen" Rechtshilfeersuchens bzw. einer Europäischen Ermittlungsanordnung an den Sitzstaat wenden. Das Ersuchen bzw. die Anordnung richtet sich dabei nicht an den Diensteanbieter direkt, sondern an die zuständige Behörde des Sitzstaates. Diese prüft das Rechtshilfeersuchen und leitet es an den Diensteanbieter weiter. Die Herausgabe der Daten läuft ebenfalls über den behördlichen Kanal. Dieser Prozess ist zeit- und ressourcenintensiv.

Der E-Evidence-Mechanismus bricht dies auf, indem er über die neuen Instrumente der Europäischen Herausgabeanordnung und der Europäischen Sicherungsanordnung einen Direktzugriff auf die Diensteanbieter ermöglicht. Diese haben mindestens einen Empfangsbevollmächtigten in der EU einzurichten (siehe dazu unten), der Anordnungen entgegennimmt und innerhalb kurzer Fristen (maximal zehn Tage, in Eilfällen maximal acht Stunden) die Datenherausgabe veranlasst. Die Behörden des Sitzstaates werden in diese Abläufe nicht mehr operativ eingebunden. Sie üben jedoch eine Kontrollfunktion bei der Anforderung von Verkehrs- und Inhaltsdaten aus. In bestimmten Konstellationen können sie hier binnen einer zehntägigen Frist die Datenübermittlung verhindern.

Für welche Fälle gilt der E-Evidence-Mechanismus? Ist er in diesen Fällen zwingend zu nutzen?

Der Mechanismus gilt für Herausgabe- oder Sicherungsanordnungen von Strafverfolgungsbehörden, bei denen sie elektronische Beweismittel in grenzüberschreitenden Fällen innerhalb der EU direkt bei den betroffenen Diensteanbietern sichern und einholen können.

Elektronische Beweismittel können weiterhin auch im Wege der Europäischen Ermittlungsanordnung oder des Europäischen Übereinkommens über die Rechtshilfe in Strafsachen eingeholt werden.

Was sind elektronische Beweismittel?

Elektronische Beweismittel im Sinne der Vorschriften sind alle digitalen Teilnehmer-, Verkehrs- oder Inhaltsdaten, die bei der Ermittlung und Verfolgung von Straftaten verwendet werden. Das sind konkret:

- Teilnehmerdaten: Daten zur Identität der betroffenen Person, etwa Name, Geburtsdatum, Anschrift und andere Kontaktdaten sowie Daten zu der Art und Dauer der Dienstleistung;
- Verkehrsdaten: Daten zur Erbringung der angebotenen Dienstleistung, beispielsweise Ursprung und Ziel einer Nachricht, der Standort eines Gerätes, das Format oder das verwendete Protokoll sowie andere Metadaten der Kommunikation über und Nutzung des Dienstes;
- Inhaltsdaten: alle anderen in einem digitalen Format verfügbaren Daten, wie Texte, Videos und Bilder.

Wer sind Diensteanbieter?

4 Gesetz über Europäische Herausgabe- und Sicherungsanordnungen zu elektronischen Beweismitteln (Elektronische-Beweismittel-Umsetzungs- und Durchführungsgesetz – EBewMG).

Der Begriff der Diensteanbieter ist weit definiert und umfasst sowohl natürliche als auch juristische Personen, die eine der folgenden Kategorien von Dienstleistungen anbieten: Elektronische Kommunikationsdienste, bestimmte Dienste der Informationsgesellschaft sowie Internetdomännamen- und IP-Nummerierungsdienste. In die erste Kategorie fallen Übertragungsdienste und Internetzugangsdienste (z. B. Telekom, Vodafone etc.); Kennzeichen der Anbieter ist, dass sie die Interaktion zwischen Nutzern erleichtern. Zur zweiten Kategorie gehören sowohl Unternehmen, die ihre Dienste über Onlineportale bereitstellen (Amazon, E-Bay, Google, Zalando, Meta, usw.), als auch Anbieter von z. B. Cloud- und Hostingdiensten. Auch umfasst sind Gaming-Anbieter, sofern ihre Dienste eine Kommunikationsfunktion beinhalten.

Unter welchen Voraussetzungen kann eine Sicherungsanordnung erlassen werden?

Die Sicherung von Daten kann für alle bei den Diensteanbietern gespeicherten Daten, also Teilnehmer-, Verkehrs- und Inhaltsdaten, durch die Staatsanwaltschaft angeordnet werden. Die Ermittlungsbehörde des Staates, der eine Anordnung erlassen möchte, hat die Verhältnismäßigkeit der Maßnahme zu prüfen. Weitere Voraussetzung für die Anordnung ist, dass eine ähnliche Anordnung in einem vergleichbaren nationalen Fall unter denselben Voraussetzungen ergehen könnte. Maßstab werden hier die geplanten Regelungen zu Quick Freeze sein.

Unter welchen Voraussetzungen kann eine Herausgabeanordnung erlassen werden?

Es ist danach zu unterscheiden, ob sich die Herausgabeanordnung auf Teilnehmerdaten oder solche Verkehrsdaten, die lediglich der Identifizierung dienen, richtet oder aber ob sie sich auf Inhalts- sowie sonstige Verkehrsdaten bezieht. Da die erstgenannten Datenkategorien als weniger sensibel betrachtet werden, können diese unter denselben Voraussetzungen wie eine Sicherungsanordnung erlassen werden.

Bei einer Anforderung, die die zweite Kategorie Daten betrifft, müssen diese Voraussetzungen ebenso erfüllt werden. Zusätzlich gilt Folgendes: Sie können nur bei Straftaten, die im Anordnungsstaat mit einer Freiheitsstrafe im Höchstmaß von mindestens drei Jahren geahndet werden, oder bei bestimmten Straftaten in Verbindung mit Cyberkriminalität, Kinderpornografie, Fälschung im Zusammenhang mit unbaren Zahlungsmitteln oder Terrorismus angefordert werden und die Anforderung muss durch ein Gericht oder einen Richter/eine Richterin erfolgen.

Zudem ist in diesen Fällen in der Regel eine Behörde im Zielstaat im Wege der „Unterrichtung“ (Notifizierung) einzubeziehen.

Wie werden besonders sensible Daten, etwa aus einer Behörde oder von Berufsgeheimnisträgern, wie etwa Rechtsanwälten oder Ärzten, geschützt?

Sind Daten betroffen, die ein Diensteanbieter für eine Behörde vorhält, darf eine Herausgabeanordnung nur dann ergehen, wenn sich die betroffene Behörde im Anordnungsstaat befindet. Damit soll verhindert werden, dass die Ermittlungsbehörden eines Mitgliedstaats per Herausgabeanordnung auf die (bei Diensteanbietern gespeicherten) Daten von Behörden anderer Mitgliedstaaten zugreifen. Befindet sich die Behörde im Anordnungsstaat, gilt keine Einschränkung.

Für Fälle, in denen ein Diensteanbieter vom Berufsgeheimnis geschützte Daten im Rahmen einer Infrastruktur speichert oder anderweitig verarbeitet, enthält die Verordnung ebenfalls eine gesonderte Vorschrift mit restriktiven Erhebungsvoraussetzungen, soweit Inhalts- und Verkehrsdaten betroffen sind. Für allgemeine Daten von Berufsgeheimnisträgern (die also nicht in einer speziellen Infrastruktur belegen sind), gilt: Sie werden im Rahmen der „Unterrichtung“ bei Abfrage von (bestimmten) Verkehrs- und Inhaltsdaten geschützt. Die notifizierte Behörde prüft dann das Vorliegen von Ablehnungsgründen, zu denen auch „Immunitäten und Vorrechte“ zählen.

Was sind Empfangsbevollmächtigte?

Für die Entgegennahme der Herausgabe- oder Sicherungsanordnungen haben die Diensteanbieter Empfangsbevollmächtigte (sog. „Adressaten“) in der EU vorzuhalten. Der Adressat muss in einem Mitgliedstaat eingerichtet werden, der sich am E-Evidence-Mechanismus beteiligt und in dem die Dienste tatsächlich angeboten werden. Der Adressat ist entweder eine Niederlassung in der EU oder – wenn ein Diensteanbieter keine Niederlassung hat – ein sogenannter Vertreter.

Was ist, wenn ein Diensteanbieter seinen Pflichten nicht nachkommt?

Wenn ein Diensteanbieter einer an ihn gerichteten Anordnung nicht nachkommt, ist ein Vollstreckungsverfahren vorgesehen. Hier hat der Diensteanbieter die Möglichkeit, auf Basis eines Katalogs von Gründen Einwände gegen die Ausführung der Herausgabe- oder Sicherungsanordnung zu erheben. Zu diesen Gründen zählen, neben formalen Aspekten wie Unzuständigkeit der Anordnungsbehörde, auch Immunitäten und Vorrechte sowie die Pressefreiheit.

Verletzt der Diensteanbieter die ihn aus der Verordnung treffenden Pflichten, so sind gegen ihn Sanktionen zu verhängen.

Wer kontrolliert, ob die Diensteanbieter ihren Pflichten nachkommen?

Das Bundesamt für Justiz überwacht als zentrale Behörde die Erfüllung der Pflichten, die sich für die Diensteanbieter ergeben. Dies betrifft zum einen die Einrichtung von Adressaten, zum anderen die Zusammenarbeit der Anbieter mit den zuständigen Behörden. Das Bundesamt für Justiz ist dabei nicht zur Vollstreckung im Einzelfall berufen, schreitet jedoch ein, wenn ein Diensteanbieter sich systematisch unkooperativ zeigt.