Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Justiz- und Polizeidepartement EJPD

Bundesamt für Justiz BJ

Konsultationspapier

Datum:	28. Februar 2024
An:	Interessierte Kreise inner- und ausserhalb der Bundesverwaltung
Kopie an:	--

Aktenzeichen: 432.5-2695/4/1

Handlungsoptionen der Schweiz im Bereich e-Evidence

1 Ausgangslage

Als Folge der Globalisierung spielt die zwischenstaatliche Zusammenarbeit in Strafsachen eine immer wichtigere Rolle. Die fortschreitende Digitalisierung generell und im vorliegenden Kontext insbesondere die grenzüberschreitende Erhebung und Übergabe elektronischer Beweismittel stellt diese Zusammenarbeit dabei vor Herausforderungen verschiedener Art: Digitale Daten sind flüchtig und die herkömmliche Strafrechtshilfe ist daher oft zu langsam, um diese über Landesgrenzen hinweg rechtzeitig sicherzustellen. Daten sind zudem immer weniger territorial geprägt, sie sind vermehrt in Daten-Clouds irgendwo auf der Welt gespeichert. Das bringt die Frage mit sich, wer sich und von wo aus Zugriff auf diese verschaffen kann und darf. Die staatliche Souveränität vermag den tatsächlichen Möglichkeiten nur noch beschränkt Grenzen zu setzen. Auch das in der transnationalen Strafverfolgung geltende Prinzip der Territorialität gerät ins Wanken. Statt sich der territorialitäts- und souveränitätsorientierten Strafrechtshilfe zu bedienen, beginnen die Strafverfolgungsbehörden auf direktere Zusammenarbeitsformen zu setzen, mitunter auf eine direkte Beteiligung Privater an Strafverfahren im Ausland.

Die Schweiz ist mit der Frage konfrontiert, wie sie mit den diversen internationalen Entwicklungen im Bereich des grenzüberschreitenden Zugriffs auf elektronische Beweismittel im Rahmen von Strafverfahren Schritt halten will. Besonders relevant sind die USA und die EU als Hauptpartnerinnen der Schweiz in diesem Bereich.

Im März 2018 verabschiedeten die USA den **C**larifying **L**awful **O**verseas **U**se of **D**ata Act (nachfolgend CLOUD Act). Die EU hat im Sommer 2023 ihr e-Evidence-Paket verabschiedet.

Bundesamt für Justiz BJ
Christian Sager, Dr. iur., LL.M.
Bundesrain 20
3003 Bern
Tel. +41 58 462 43 67
christian.sager@bj.admin.ch
www.bj.admin.ch

Beide Gesetzgebungsprojekte hat das Bundesamt für Justiz in Berichten ***(vgl. Beilagen)*** analysiert.[1]

2 Ziel der Konsultation

Basierend auf der in den beiden genannten Berichten vorgenommenen Analyse soll die vorliegende Notiz die Handlungsoptionen der Schweiz im Bereich des grenzüberschreitenden Zugriffs auf elektronische Beweismittel im Rahmen von Strafverfahren aufzeigen. Die Optionen lassen sich grob in die drei Kategorien «Passivität», «eigenständige Lösung» und «Verhandlungslösung» unterteilen. Zu diesen Optionen und möglichen Untervarianten möchte das BJ mit dem vorliegenden Papier gezielt eine interessierte Öffentlichkeit (Strafverfolgung, Diensteanbieter, relevante Verbände sowie digitalisierungspolitische Akteure) befragen, um ein möglichst klares Bild zum weiteren Vorgehen zu erhalten.

3 Handlungsoptionen der Schweiz

3.1 Passivität – Wait and See

Die erste Option besteht darin, dass sich die Schweiz passiv verhält und keinerlei rechtliche Anpassungen oder gesetzgeberische Schritte vornimmt.

Der Vorteil dieser Lösung wäre, dass kein Gesetzgebungsaufwand entstünde. Diese Option ist aber aus verschiedenen Gründen als problematisch zu beurteilen. Wie erwähnt basiert das Schweizer System im Bereich der Erhebung elektronischer Beweismittel im Ausland ausschliesslich auf der klassischen Strafrechtshilfe, die relativ langsam und nicht auf elektronische Beweismittel zugeschnitten ist. Zugleich haben immer mehr Straftaten – auch herkömmliche wie z. B. ein Betrug – einen Cyber-Bezug. Bei vielen Betrugsformen erliegt das Opfer heute einer Täuschung im digitalen Raum: Das vermeintlich gute Geschäft auf der «Investment»-Webseite gibt es nicht oder die vermeintliche Online-Liebe erweist sich als Betrüger aus dem Ausland. Gemäss Schätzungen der Schweizer Strafverfolgungsbehörden haben rund zwei Drittel der schweizerischen Strafverfahren einen Bezug zu digitalen Daten, wobei diese Daten meist im Ausland liegen. Bleibt die Schweiz hier passiv, riskiert sie, dass eine erfolgreiche Rechtsdurchsetzung weiterhin schwierig bleibt.

Des Weiteren könnte es zu einem Rechtskonflikt kommen, wenn die EU-Regelungen zu e-Evidence anwendbar werden. Schweizer Diensteanbieter, die unter die Regelungen fallen und in der Folge in der EU einen gesetzlichen Vertreter ernennen müssen, wären dann verpflichtet, ihre Daten direkt, d. h. ausserhalb eines Rechtshilfeverfahrens, an die betreffende Strafverfolgungsbehörde des EU-Mitgliedstaates herauszugeben, auch wenn diese auf Servern in der Schweiz lagern. Aus Sicht des Schweizer Rechts würde der betreffende Diensteanbieter damit nach geltendem Recht vermutlich eine verbotene Handlung für einen fremden Staat gemäss Art. 271 StGB vornehmen.[2]

---

[1] Die Berichte sind im Internet publiziert, der Bericht zum US-CLOUD Act unter https://www.bj.admin.ch/bj/de/home/publiservice/publikationen/berichte-gutachten/2021-09-17.html, derjenige zur e-Evidence-Vorlage der EU unter https://www.bj.admin.ch/bj/de/home/publiservice/publikationen/berichte-gutachten/2023-10-24.html.

[2] Wenn ein in der Schweiz domizilierter Diensteanbieter gemäss e-Evidence-Regelung einen Sitz in einem EU-Staat errichten würde, dort eine Herausgabeanordnung eines EU-Mitgliedstaats erhielte und gestützt darauf Daten, die in der Schweiz liegen, herausgäbe, nähme er nach schweizerischem Verständnis eine Handlung vor, die dem Staat zukommt. Es käme zu einem Konflikt mit Art. 271 StGB – und der Diensteanbieter müsste jedes Mal um eine entsprechende Genehmigung des EJPD ersuchen, was kaum praktikabel wäre.

3.2 Eigenständige Lösung: Anpassung des nationalen Rechts

Die zweite Option besteht in einer eigenständigen Lösung der Schweiz, indem das nationale Recht an die e-Evidence-Regelung der EU angepasst wird. Dabei sind zwei Varianten denkbar:

3.2.1 Vermeidung von Rechtskonflikten

Um die angesprochenen Rechtskonflikte zu vermeiden, die sich durch die Einführung der neuen e-Evidence-Regelung ergeben, könnte die Schweiz ihr nationales Recht so anpassen, dass der ausländische Datenzugriff toleriert wird und der in der Schweiz ansässige Diensteanbieter sich nicht gemäss Art. 271 StGB strafbar macht.

Eine solche Lösung liesse sich technisch relativ einfach umsetzen. Es würde bloss eine «Erlaubnisnorm» geschaffen, welche es den Diensteanbietern gestattet, Herausgabeanordnungen von Staatsanwaltschaften aus der EU auch dann zu entsprechen, wenn die betroffenen Daten in der Schweiz lagern. Diese Lösung würde aber dazu führen, dass die Schweiz in ihrem Recht für die ausländischen Strafverfolgungsbehörden eine Möglichkeit vorsähe, die im Gegenzug für die schweizerischen Strafverfolgungsbehörden bei Datenzugriffen im Ausland nicht bestünde – nämlich der direkte Zugriff auf die Diensteanbieter. Damit würde der seitens der Schweizer Strafverfolgungsbehörden monierte dringende Handlungsbedarf ignoriert.

3.2.2 Zugang auf Daten auch für Schweizer Strafverfolgungsbehörden

Um diesem Problem zu begegnen, könnte die Schweiz eine Lösung entwickeln, die auch den schweizerischen Strafverfolgungsbehörden einen einfacheren Zugang zu Daten im Ausland mit Bezug zur Schweiz ermöglicht. Die Regelung wäre dabei analog zu derjenigen der EU auszugestalten, indem Diensteanbieter, die ihre Dienste in der Schweiz anbieten, einen gesetzlichen Vertreter in der Schweiz benennen oder eine Niederlassung in der Schweiz errichten müssten und so unter gewissen Voraussetzungen zur Auskunft oder Herausgabe von Daten verpflichten werden könnten. Dies hätte den Vorteil, dass die Schweiz ein System entwickeln könnte, das ihren eigenen Rechtsgrundsätzen entspricht und auf ihre Bedürfnisse zugeschnitten ist. Allerdings bieten Diensteanbieter aus der ganzen Welt ihre Dienste in der Schweiz an. Als kleines Land wäre es für die Schweiz wohl schwierig, all diese Diensteanbieter zur Ernennung einer gesetzlichen Vertretung oder zur Errichtung einer Niederlassung in der Schweiz mit entsprechenden Pflichten zu bewegen. Die Schweiz hat als Markt nicht die gleiche Attraktivität und Bedeutung wie die EU. Es ist unsicher, ob die Schweiz hier genügend Durchsetzungskraft hätte, um den Diensteanbietern autonom ein solches System aufzuzwingen. Insgesamt bliebe daher das Grundproblem der mangelnden grenzüberschreitenden Durchsetzbarkeit wohl bestehen.

3.3 Verhandlungslösung

Die dritte Option ist ein Anknüpfen an das eine und/oder andere internationale System. Im Gegensatz zum US CLOUD Act sieht das e-Evidence-Paket der EU eine solche Möglichkeit nicht ausdrücklich vor. Aufgrund der engen Verbindungen der Schweiz mit der EU im Bereich der justiziellen Zusammenarbeit und des Datenschutzes (insbesondere im Bereich der Schengener Zusammenarbeit), jedoch auch aufgrund der Personenfreizügigkeit (auf welche sich die e-Evidence Richtlinie abstützt) und des Zugangs zum Binnenmarkt, gerade auch im digitalen Bereich, erscheint es ratsam, den Blick dennoch primär auf die EU zu richten. Dabei könnte die Schweiz eine Lösung erarbeiten, die sich auf die e-Evidence-Gesetzgebung der EU abstützt. Wie erwähnt ist eine Beteiligung von Drittstaaten im e-Evidence-Paket zwar grundsätzlich nicht vorgesehen. Es erscheint aber zumindest als nicht ausgeschlossen, dass

die EU ihrerseits «Strafverfolgungslücken» mitten in ihrem geographischen Raum vermeiden möchte und auch Interesse an einer Anbindung der Schweiz hätte. Grundsätzlich wären vor diesem Hintergrund zwei Varianten denkbar:

3.3.1 Bilaterales Abkommen zur Übernahme der Richtline und Verordnung

Die Schweiz könnte mit der EU ein bilaterales Abkommen anstreben, das die Übernahme sowohl der Richtlinie wie auch der Verordnung des e-Evidence-Pakets vorsieht. Die Schweiz wäre dadurch an das ganze Paket gebunden und würde dieses innerstaatlich soweit erforderlich umsetzen. Zugleich bestünde hier Gegenseitigkeit, das heisst die EU-Mitgliedstaaten hätten gegenüber der Schweiz im Rahmen des e-Evidence-Pakets dieselben Verpflichtungen wie gegenüber den anderen am Paket beteiligten EU-Mitgliedstaaten.

Bei diesem Vorgehen würde sich aber die Frage stellen, ob eine solche vollständige Einbindung aus Schweizer Sicht politisch wünschbar und rechtlich ohne die gleichzeitige Übernahme weiterer EU-Rechtsakte, die eine Verbindung zu e-Evidence haben, überhaupt möglich wäre.

3.3.2 Bilaterales Abkommen zur Übernahme der Richtlinie

Die Richtlinie des e-Evidence-Pakets stützt sich auf Bestimmungen über die Freizügigkeit und den freien Dienstleistungs- und Kapitalverkehr des Vertrags über die Arbeitsweise der Europäischen Union (AEUV), die Verordnung hingegen auf den Titel V des AEUV, der den Raum der Freiheit, der Sicherheit und des Rechts regelt. In der Praxis hat dies insbesondere eine Bedeutung für Dänemark, das sich für ein vollständiges Opt-out betreffend den Titel V des AEUV entschieden hat und sich folglich nicht an Rechtsakten beteiligt, die auf der Grundlage von Titel V angenommen werden. Dies führt dazu, dass Dänemark die e-Evidence-Verordnung nicht anwenden kann.[3] Dänemark wird aber die Richtlinie übernehmen müssen und muss folglich eine innerstaatliche Grundlage schaffen, um diese umzusetzen.

Es stellt sich die Frage, ob die Schweiz evtl. – analog dem Beispiel von Dänemark – eine Lösung erarbeiten könnte, die sich einerseits auf die e-Evidence Richtlinie abstützt und andererseits auf einer nationalen Gesetzgebung der Schweiz beruht, die den «Unterbau» dazu darstellen und die e-Evidence Verordnung ersetzen würde. Diese Lösung bietet sich u. U. an, da sich die Richtlinie wie erwähnt auf die Freizügigkeit abstützt – ein Bereich, in welchem die Schweiz mittels sektoriellen Abkommen mit der EU verbunden ist.[4] Evtl. könnte die Übernahme der Richtlinie in die Form einer Zusatzvereinbarung zu einem bestehenden Abkommen mit der EU gekleidet werden. Aber auch hier darf das Kriterium der Gegenseitigkeit nicht aus den Augen gelassen werden. Ziel der zu treffenden Vereinbarung müsste sein, dass ein Diensteanbieter seinen Sitz auch in der Schweiz errichten könnte und an diesem Sitz in der Schweiz Sicherungs- und Herausgabeanordnungen von Staatsanwaltschaften in der EU entgegennehmen darf. Gleichzeitig müssten es die EU und ihre Mitgliedstaaten jedoch tolerieren, dass die schweizerischen Staatsanwaltschaften ihrerseits Herausgabeanordnungen an die Sitze von Dienstanbietern in der EU richten und die Diensteanbieter diesen entsprechen dürften.

Gelänge ein grundsätzlicher Anschluss an die e-Evidence Gesetzgebung der EU, so hätte das zur Folge, dass Datenzugriffe auch auf Daten bei Diensteanbietern von ausserhalb der

[3] Im Gegensatz dazu verfügt Irland über ein flexibles Opt-out in Bezug auf den Titel V des AEUV, d. h. Irland kann sich bei Bedarf an bestimmten Initiativen im Bereich des Raums der Freiheit, der Sicherheit und des Rechts beteiligen. Gemäss Informationen des BJ hat Irland - insbesondere aus wirtschaftlichen Gründen - ein grosses Interesse daran, die e-Evidence-Verordnung zu übernehmen und umzusetzen.

[4] Zwar umfasst das Freizügigkeitsabkommen zwischen der Schweiz und der EU sowie ihren Mitgliedstaaten (FZA, SR 0.142.112.681) nicht die volle Dienstleistungsfreiheit, aber immerhin Teilbereiche davon.

EU (also auch z. B. auf Daten von US-Diensteanbietern) nach dem System der e-Evidence erfolgen würden: Alle Diensteanbieter mit Zugang zum EU-Markt hätten dann nämlich in der EU – oder eben der Schweiz – einen Ansprechpunkt und über diesen würde der Datenzugriff für am EU-System beteiligte Staaten laufen.

Die EU und die USA verhandeln derzeit über ein Abkommen, um die Zusammenarbeit im Bereich der elektronischen Beweismittel zwischen den Systemen der e-Evidence und des CLOUD Act zu erleichtern. Gelänge der Schweiz ein Anschluss an das e-Evidence-System, könnte sie anschliessend versuchen, mit den USA ein ähnliches Abkommen zu verhandeln wie jenes, das zwischen der EU und den USA entsteht.[5]

4 Fazit aus Sicht BJ

Die neue e-Evidence-Gesetzgebung der EU wird am 28. Juli 2026 anwendbar. Bis dahin muss die Schweiz eine Lösung im Umgang mit der grenzüberschreitenden Erhebung elektronischer Beweismittel finden. Ansonsten besteht die Gefahr, dass es zu einem Rechtskonflikt mit dem neuen EU-System kommt. Einen solchen gilt es zu vermeiden. Dabei ist zu bedenken, dass die Schweiz ihre rechtsstaatlichen Errungenschaften nicht gefährden darf. Sie sollte jedoch grundsätzlich eine Lösung anstreben, die auch die Möglichkeiten ihrer Strafverfolgungsbehörden ausbaut, um mit anderen Staaten oder zumindest mit Diensteanbietern, die sich auf dem Territorium anderer Staaten befinden, zusammenarbeiten zu können.

5 Fragen

Gerne bitten wir Sie um Ihre Einschätzungen zu untenstehenden Fragen bis **Dienstag, 30. April 2024.**

Gerne können Sie Ihre Stellungnahme an Christian Sager (christian.sager@bj.admin.ch) und Nicola Hofer (nicola.hofer@bj.admin.ch) richten, die Ihnen auch bei Rückfragen gerne zur Verfügung stehen.

a. Teilen Sie die Auffassung des BJ, dass eine Rechtskollision mit der EU zu vermeiden ist und folglich dringender gesetzgeberischer Handlungsbedarf besteht?

b. Teilen Sie die Auffassung, dass eine Lösung nicht bloss auf die «Konfliktvermeidung» mit der EU beschränkt sein sollte, sondern sie sich darüber hinaus an den operativen Bedürfnissen der schweizerischen Strafverfolgungsbehörden zu orientieren hat?

c. Welche der vorgeschlagenen Handlungsoptionen würden Sie bevorzugen und warum? Sehen Sie allenfalls weitere Alternativen?

d. Weitere Überlegungen/Bemerkungen Ihrerseits?

Beilagen:
- Bericht des BJ zum US CLOUD Act vom 17. September 2021;
- Bericht des BJ zum e-Evidence-Paket der EU vom 24. Oktober 2023.

[5] Dabei wäre allerdings zu beachten, dass der Datenschutzstandard in den USA aus Schweizer Sicht derzeit nicht als angemessen anerkannt ist und ein Schweizer Dienstanbieter daher bei der Bekanntgabe von Personendaten an eine amerikanische Strafverfolgungsbehörde gegen schweizerisches Datenschutzrecht verstossen könnte. Jedoch ist davon auszugehen, dass entsprechende Datenschutzklauseln auch Gegenstand eines angesprochenen Abkommens zwischen der EU und den USA sein werden. Die Schweiz bedürfte jedenfalls solcher.