Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Justiz- und Polizeidepartement EJPD

Bundesamt für Justiz BJ

24. Oktober 2023

Bericht zur e-Evidence-Vorlage der EU

BJ-D-FFB23401/87

Inhaltsverzeichnis

1 Ausgangslage

Das digitale Zeitalter verändert nicht nur verschiedenste Aspekte unseres Lebens, sondern auch die Methoden, derer sich Kriminelle bei ihren Machenschaften bedienen. Für eine effiziente Strafverfolgung ist daher unerlässlich, dass sich die Strafverfolgungsbehörden und andere an der Verbrechensbekämpfung beteiligte Behörden diesen neuen Entwicklungen anpassen. Dazu gehört auch, die **adäquaten rechtlichen Grundlagen** für eine erfolgreiche Verbrechensbekämpfung zu schaffen.

Um den mit der Digitalisierung einhergehenden Herausforderungen für die Verbrechensbekämpfung zu begegnen, entstanden und entstehen auf internationaler Ebene verschiedene neue Instrumente. So wurde am 17. November 2021 das Zweite Zusatzprotokoll zum Übereinkommen des Europarates über Computerkriminalität betreffend die verstärkte Zusammenarbeit und Weitergabe von elektronischem Beweismaterial verabschiedet und im Rahmen der Vereinten Nationen wird über ein Übereinkommen zur Cyberkriminalität verhandelt. Parallel dazu entwickeln auch die Staaten ihr Recht weiter: Die USA verabschiedeten im November 2018 den **Clarifying Lawful Overseas Use of Data Act (CLOUD Act)**, der im Rahmen von Strafverfahren zu einem erleichterten Zugriff auch auf im Ausland gelagerte Daten führen soll. Aufgrund der praktischen Bedeutung des CLOUD Act hat das BJ diesen aus Sicht des Schweizer Rechts beurteilt und am 17. September 2021 einen Bericht dazu veröffentlicht (Bericht zum US CLOUD Act (Cloud-Gesetz) nachfolgend: Bericht CLOUD Act).

Angesichts dieser Entwicklungen steht auch die Europäische Union (EU) nicht still und erarbeitete eine neue Regelung für elektronische Beweismittel, das sogenannte **e-Evidence-Paket**. Das e-Evidence Paket geht zurück auf die Terroranschläge in Brüssel im Jahr 2016. Zwei Tage nach den Anschlägen forderten die europäischen Justiz- und Innenminister einen besseren Zugang zu elektronischen Beweismitteln. Auch der Rat der Europäischen Union äusserte in der Folge, dass ein wirksamer Zugang zu elektronischen Beweismitteln für die Bekämpfung von schwerer Kriminalität und Terrorismus von wesentlicher Bedeutung ist. Am 17. April 2018 präsentierte die Kommission ihren Vorschlag für eine e-Evidence Richtlinie und Verordnung.

Am 13. Juni 2023 verabschiedete das Europäische Parlament das Gesetzespaket zur e-Evidence, der Rat der Europäischen Union stimmte seinerseits am 27. Juni 2023 dem Gesetzespaket zu. Das e-Evidence-Paket wurde schliesslich **am 28. Juli 2023 formell verabschiedet**. Ziel des Gesetzespakets ist es, einen kohärenten EU-Rahmen für den Umgang mit elektronischen Beweismitteln zu schaffen und deren Erhebung zu beschleunigen. Die neuen Vorschriften ermöglichen es den Strafverfolgungsbehörden der EU-Mitgliedstaaten insbesondere, Beweismittel direkt von digitalen Diensteanbietern (service provider) in anderen Mitgliedstaaten anzufordern (so genannte "Herausgabeanordnungen") oder die Aufbewahrung von Daten für einen Zeitraum von bis zu 60 Tagen zu verlangen, damit relevante Daten nicht zerstört werden oder verloren gehen ("Datenspeicherungsanordnungen"). Dadurch wird ein alternativer Mechanismus zum bisher geltenden Rechtshilfeweg geschaffen.

Die neuen Regelungen dürften auch grosse Auswirkungen auf die Schweiz haben, da hier ansässige service provider, die ihre Dienste in der EU anbieten, unter bestimmten Voraussetzungen unter die Regelungen fallen werden. Zu denken ist hier beispielsweise an Kommunikationsdienste wie Threema oder Protonmail. Die Regelungen könnten aber darüber hinaus noch weitere von Schweizer Firmen angebotene digitale Dienstleistungen treffen.

Ergänzend zum CLOUD Act-Bericht erläutert der vorliegende Bericht den Inhalt des EU e-Evidence-Pakets, nimmt einen Rechtsvergleich vor und beleuchtet die Folgen und Herausforderungen für die Schweiz sowie die Unterschiede zum US Cloud Act. Zum Schluss zeigt der Bericht mögliche Handlungsoptionen für die Schweiz auf.

2 Inhalt des EU e-Evidence Pakets

2.1 Übersicht

Das EU e-Evidence Paket besteht aus einer Richtlinie, welche die wichtigsten Grundsätze der Vorlage festlegt, und aus einer Verordnung mit detaillierten Bestimmungen.

Die **Richtlinie**[1] verpflichtet digitale Dienstleister, die in der EU bestimmte Dienstleistungen anbieten, dazu, eine Niederlassung in der EU zu etablieren oder einen gesetzlichen Vertreter zu benennen, an den die Behörden der Mitgliedstaaten ihre Herausgabe- und Datenspeicherungsanordnungen richten können.

Die **Verordnung**[2] schafft die Europäische Herausgabeanordnung sowie die Europäische Sicherungsanordnung. Sie regelt damit die Voraussetzungen, unter denen digitale Dienstleanbieter in der EU entweder eine Niederlassung haben oder einen gesetzlichen Vertreter ernennen müssen und unter denen die zuständigen (Strafverfolgungs-)Behörden eines EU-Mitgliedstaates im Rahmen eines Strafverfahrens einen solchen service provider direkt zur Herausgabe oder Aufbewahrung von Daten auffordern können.

Die Verordnung findet keine Anwendung auf Verfahren, die eröffnet wurden, um einem anderen EU-Mitgliedstaat oder einem Drittstaat Rechtshilfe zu gewähren.

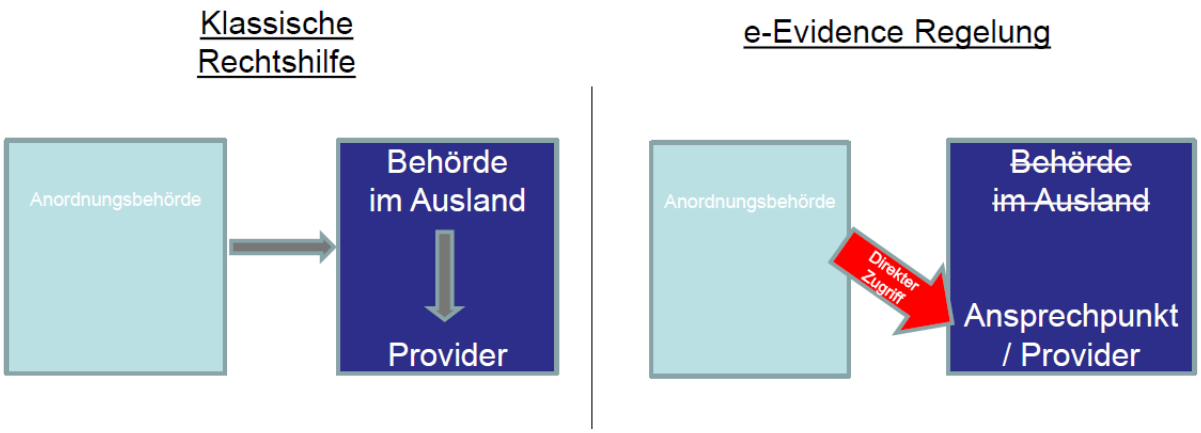

Abb.: Das Funktionieren von e-Evidence im Vergleich mit dem klassischen Rechtshilfeverfahren

2.2 Rechtsgrundlage in der EU

Wie erwähnt, besteht das e-Evidence-Paket aus zwei verschiedenen Instrumenten, einer Verordnung und einer Richtlinie. Diese beiden Instrumente ergänzen einander zwar, sie basieren aber nicht auf denselben primärrechtlichen Grundlagen.

Die Richtlinie beruht auf den Artikeln 53 und 63 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV). Diese beiden Artikel befinden sich unter dem Titel IV des AEUV

[1] 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, Abl. L 191/181.

[2] 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, Abl. L 191/118.

über die Freizügigkeit und den freien Dienstleistungs- und Kapitalverkehr. Die Verordnung hingegen stützt sich auf Artikel 82 Absatz 1 AEUV über die gegenseitige Anerkennung von Urteilen und die Stärkung der justiziellen Zusammenarbeit in Strafsachen. Artikel 82 befindet sich unter dem Titel V des AEUV, der den Raum der Freiheit, der Sicherheit und des Rechts regelt.

Auch wenn die unterschiedlichen primärrechtlichen Grundlagen auf den ersten Blick unbedeutend erscheinen, haben diese in der Praxis Konsequenzen, denn sowohl Dänemark wie auch Irland haben sich für ein Opt-out betreffend den Titel V des AEUV entschieden. Während Dänemark ein vollständiges Opt-out hat und sich nicht an Rechtsakten, die auf der Grundlage dieses Titels angenommen werden, beteiligt, handelt es sich bei Irland um ein teilweises Opt-out. Das heisst, dass sich Irland bei Bedarf an bestimmten Initiativen im Bereich des Raums der Freiheit, der Sicherheit und des Rechts beteiligen kann.

Für das e-Evidence-Paket bedeutet dies, dass sowohl Dänemark als auch Irland zwar die Richtlinie des Pakets umsetzen müssen, nicht aber die Verordnung. Im Gegensatz zu Dänemark besteht für Irland aber die Möglichkeit, die Verordnung umzusetzen, wenn es das will. Die Verordnung übernimmt jedoch mehrere EU-Instrumente, die sich auf den Titel V abstützen und die Irland nicht übernommen hat. Eine Umsetzung der Verordnung könnte sich für Irland daher als kompliziert erweisen.[3]

2.3 Anwendungsbereich

2.3.1 Diensteanbieter

Als erstes stellt sich die Frage, welche Diensteanbieter überhaupt vom Gesetzespaket betroffen sind.

Die Verordnung enthält zunächst eine sehr allgemein gehaltene Voraussetzung, wonach darunter **jede natürliche oder juristische Person** fällt, die eine **von der Verordnung umfasste Dienstleistung in der EU** erbringt. Dienstleistungen, die ausschliesslich ausserhalb der Union angeboten werden, fallen nicht in den Anwendungsbereich der Verordnung, selbst wenn der betreffende Dienstleister eine Niederlassung in der EU hat. Welche Dienstleister also von der Verordnung betroffen sind, hängt demnach ab von den Leistungen, welche diese anbieten.

2.3.2 Erfasste Dienstleistungen

Es stellt sich die Frage, **welche Dienstleistungen** konkret von der Verordnung umfasst sind. Diese werden in Artikel 3 Absatz 3 der Verordnung aufgezählt. Es handelt sich um die Leistungen der folgenden Dienste:

2.3.2.1 Elektronische Kommunikationsdienste

Die Verordnung verweist hier auf die Definition in Artikel 2 Absatz 4 der EU-Richtlinie 2018/1972 über den europäischen Kodex für elektronische Kommunikation. Gemäss dieser Richtlinie sind „elektronische Kommunikationsdienste“ gewöhnlich gegen Entgelt über elektronische Kommunikationsnetze erbrachte Dienste, die folgende Dienste umfassen:

- Internetzugangsdienste, also Dienste, die Zugang zum Internet bieten (in der Schweiz wären dies z. B. **Swisscom, UPC-Sunrise** etc.);

[3] Dennoch scheint sich Irland für ein opt-in entschieden zu haben, siehe hinten Ziff. 3.

- interpersonelle Kommunikationsdienste, worunter gemäss Artikel 2 Absatz 5 der Richtlinie 2018/1972 ein gewöhnlich gegen Entgelt erbrachter Dienst zu verstehen ist, der einen direkten Informationsaustausch zwischen einer endlichen Zahl von Personen ermöglicht, wobei die Empfänger von den Personen bestimmt werden, die die Kommunikation veranlassen oder daran beteiligt sind (in der Schweiz wären dies z. B. **Protonmail oder Threema**);
- Dienste, die ganz oder überwiegend in der Übertragung von Signalen bestehen, wie Übertragungsdienste, die für die Maschine-Maschine-Kommunikation und für den Rundfunk genutzt werden (z. B. **Anbieter von Blogs, Videoabrufdiensten oder Sozialen Netzwerken**).

2.3.2.2 Domainnamen-Services und IP Nummerierungsdienste

Hierunter fallen IP-Adressanbieter, Dienste, die Domainregistrierungen anbieten sowie Anbieter, die Proxy-Dienste im Zusammenhang mit Domainnamen anbieten (in der Schweiz wären das z.B. **Switch, ProtonVPN** etc.).

2.3.2.3 Andere Dienste, die es ihren Nutzenden ermöglichen, miteinander zu kommunizieren oder die Daten über ihre Nutzenden verarbeiten oder speichern können

Hier verweist die Verordnung auf die Umschreibung in Artikel 1 Absatz 1 litera b der EU-Richtlinie 2015/1535, wonach unter „Dienst“ eine Dienstleistung der Informationsgesellschaft, d. h. jede in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleistung zu verstehen ist.[4]

Diese doch eher komplizierte und nicht leicht zu fassende Umschreibung wird durch Beispiele in Anhang I derselben Richtlinie verständlicher. Demnach fallen **nicht** unter die Dienste gemäss Artikel 1 Absatz 1 litera b:

- Dienste, bei deren Erbringung der Erbringer und der Empfänger gleichzeitig physisch anwesend sind, selbst wenn dabei elektronische Geräte benutzt werden (Untersuchung oder Behandlung in einer Arztpraxis mithilfe elektronischer Geräte, aber in Anwesenheit des Patienten/der Patientin; Konsultation eines elektronischen Katalogs in einem Geschäft in Anwesenheit des Kunden/der Kundin; Buchung eines Flugtickets über ein Computernetz, wenn sie in einem Reisebüro in Anwesenheit des Kunden/der Kundin vorgenommen wird) **(e contrario wären erfasst: Online-Shops, Anbieter von online-Buchungen von Flugtickets etc.)**;
- Bereitstellung elektronischer Spiele in einer Spielhalle in Anwesenheit der benutzenden Person **(e contrario wären erfasst: Anbieter von online-Spielen)**;
- Dienste, die zwar mit elektronischen Geräten, aber in materieller Form erbracht werden (Geldausgabe- oder Fahrkartenautomaten, Zugang zu gebührenpflichtigen Strassennetzen, Parkplätzen usw., auch wenn elektronische Geräte bei der Ein- und/oder Ausfahrt den Zugang kontrollieren und/oder die korrekte Gebührenentrichtung gewährleisten) (e contrario wären erfasst: **Parking-Apps, SBB-App etc.**);
- Offline-Dienste (Vertrieb von CD-ROMs oder Software auf Disketten) **(e contrario wären erfasst: Online-Dienste)**;
- Dienste, die nicht über elektronische Verarbeitungs- und Speicherungssysteme erbracht werden (Sprachtelefondienste; Telefax-/Telexdienste; über Sprachtelefon oder Telefax erbrachte Dienste; medizinische Beratung per Telefon/Telefax; anwaltliche Beratung per Telefon/Telefax; Direktmarketing per Telefon/Telefax) **(e**

[4] „Im Fernabsatz erbrachte Dienstleistung“ bezeichnet eine Dienstleistung, die ohne gleichzeitige physische Anwesenheit der Vertragsparteien erbracht wird; „elektronisch erbrachte Dienstleistung“ eine Dienstleistung, die mittels Geräten für die elektronische Verarbeitung von Daten am Ausgangspunkt gesendet und am Endpunkt empfangen wird und die vollständig über Draht, Funk, auf optischem oder anderem elektromagnetischem Wege gesendet, weitergeleitet und empfangen wird; „auf individuellen Abruf eines Empfängers erbrachte Dienstleistung“ eine Dienstleistung, die durch die Übertragung von Daten auf individuelle Anforderung erbracht wird.

contrario wären erfasst: Online-Beratungen in den entsprechenden Bereichen);
- Dienste, die nicht auf individuellen Abruf eines Empfängers, sondern gleichzeitig für eine unbegrenzte Zahl von einzelnen Empfängern erbracht werden (Punkt-zu-Mehrpunkt-Übertragung) (Fernsehdienste (einschliesslich zeitversetzter Video-Abruf; Hörfunkdienste; Teletext (über Fernsehsignal)) **(e contrario wären erfasst, Anbieter die auf den individuellen Abruf abzielen, z.B. online-Zeitungen oder podcasts etc.).**

Des Weiteren präzisiert die Verordnung in Artikel 3 Absatz 4, was unter **«Dienstleistung in der EU erbringen / anbieten»** zu verstehen ist: Der Diensteanbieter muss es einer natürlichen oder juristischen Person in einem Mitgliedstaat ermöglichen, die in Absatz 3 genannten Dienste zu nutzen und eine wesentliche Verbindung **(substantial connection)** zu einem Mitgliedstaat haben. Eine solche liegt dann vor, wenn der Diensteanbieter:

- eine Niederlassung in der EU hat; oder
- eine erhebliche Anzahl Nutzende in einem oder mehreren Mitgliedstaaten hat; oder
- seine Tätigkeiten auf einen oder mehrere Mitgliedstaaten ausrichtet (z. B. durch das Verwenden einer Sprache oder Währung, die in diesem Mitgliedstaat normalerweise verwendet wird oder der Möglichkeit, bei ihm Güter oder Dienstleistungen zu bestellen). Die Ausrichtung von Tätigkeiten auf einen Mitgliedstaat kann sich auch aus der Verfügbarkeit einer App in dem betreffenden nationalen App-Store, aus der Bereitstellung lokaler Werbung oder Werbung in der in diesem Mitgliedstaat allgemein verwendeten Sprache oder aus der Abwicklung von Kundenbeziehungen, etwa durch die Bereitstellung eines Kundendienstes in der in diesem Mitgliedstaat allgemein verwendeten Sprache, ergeben.[5]

Die blosse Zugänglichkeit innerhalb der EU auf eine Webseite des Diensteanbieters oder das Veröffentlichen einer blossen E-Mailadresse oder anderer Kontaktdaten des Diensteanbieters genügen für sich alleine hingegen nicht, um von einer Ausrichtung der Tätigkeiten zu sprechen.[6]

→ Erbringt ein Anbieter einen Dienst im Sinne von Artikel 3 Absatz 3 und besteht eine substantial connection zur EU, so muss der Diensteanbieter entweder eine Niederlassung in der EU haben oder, wenn er keine solche hat, einen gesetzlichen Vertreter benennen.

2.3.3 Betroffene Daten

Das EU e-Evidence-Paket umfasst nur Daten, die sich auf die in der Union angebotenen Dienstleistungen beziehen. Beziehen sich die Daten auf eine solche in der Union angebotene Dienstleistung, so spielt deren Standort keine Rolle (sie können sich also auch ausserhalb der EU befinden).

[5] siehe Vorb. (30) der Verordnung

[6] Siehe Vorb. (29) der Verordnung.

2.3.3.1 Teilnehmer-, Verkehrs- und Inhaltsdaten

Erfasst sind Teilnehmerdaten[7], Daten, die einzig der Identifizierung des Nutzers dienen[8], Verkehrsdaten (Randdaten)[9] und Inhaltsdaten[10] (Art. 3 Abs. 9-12 der Verordnung). Nicht möglich ist hingegen die Echtzeitüberwachung, d. h. beispielsweise das Abhören des Telefons in Echtzeit.

2.3.3.2 Privilegierte Daten

Die Verordnung enthält zudem eine explizite Regelung zu Daten, die nach dem Recht des anordnenden Staates durch das Berufsgeheimnis geschützt sind (siehe Art. 5 Abs. 9 f. der Verordnung). Werden diese Daten von einem Diensteanbieter als Teil einer Infrastruktur, die «privilegierten Berufsangehörigen» (Berufsangehörigen, die unter das Berufsgeheimnis fallen) in ihrer beruflichen Eigenschaft zur Verfügung gestellt wird,[11] gespeichert oder anderweitig verarbeitet, kann eine Herausgabeanordnung zur Erlangung von Verkehrs- oder Inhaltsdaten nur erlassen werden, wenn:

- der oder die privilegierte Berufsangehörige im Anordnungsstaat wohnt;
- die Kontaktaufnahme mit dem oder der Berufsangehörigen den Ermittlungen abträglich sein könnte; oder
- nach dem anwendbaren Recht auf die Privilegien verzichtet wurde.

Hat die anordnende Behörde Grund zur Annahme, dass die ersuchten Verkehrs- oder Inhaltsdaten durch im Recht des ausführenden Staates garantierte Immunitäten oder Privilegien oder durch die Presse- oder Meinungsäusserungsfreiheit geschützt sind, so kann sie dies vor Erlass einer Herausgabeanordnung mit dem ausführenden Staat klären.

2.4 Herausgabe und Speicherung der Daten: Die Herausgabeanordnung (European Production Order; EPOC) und die Datenspeicherungsanordnung (Preservation Order, EPOC PR)

2.4.1 Herausgabeanordnung (Art. 5 der Verordnung)

Mittels der Herausgabeanordnung kann die zuständige Behörde eines Mitgliedstaates die unter das e-Evidence-Paket fallenden Daten direkt von einem Diensteanbieter in einem anderen Mitgliedstaat herausverlangen.

Die Herausgabeanordnung muss **notwendig und verhältnismässig** sein. Die Herausgabe kann nur dann angeordnet werden, wenn sie unter denselben Bedingungen in einem ähnlichen innerstaatlichen Fall auch angeordnet werden könnte (Art. 5 Abs. 2 der Verordnung).

Des Weiteren ist die Herausgabeanordnung nur für **Straftaten mit einem bestimmten Strafmass** zulässig, wobei die Höhe des verlangten Strafmasses von der Art der herausverlangten Daten abhängt:

---

[7] Teilnehmerdaten umfassen einerseits Daten, die auf die Identität des Abonnenten oder Kunden schliessen lassen wie der Name, das Geburtsdatum, die Adresse, Rechnungs- und Zahlungsdaten, Telefonnummer oder E-Mailadresse und andererseits Daten über die Art und Dauer der Dienstleistung.

[8] Dazu gehören IP Adressen und wo notwendig, die entsprechenden Quellports und Zeitstempel, d. h. Datum und Uhrzeit.

[9] Zu den Verkehrsdaten gehören z. B. die Quelle und das Ziel einer Nachricht oder einer anderen Art von Interaktion, der Standort des Geräts, das Datum, die Uhrzeit, die Dauer, die Grösse, der Weg, das Format, das verwendete Protokoll und die Art der Komprimierung sowie andere Metadaten und Daten der elektronischen Kommunikation, die keine Teilnehmerdaten sind und sich auf den Beginn und die Beendigung einer Benutzerzugriffssitzung auf einen Dienst beziehen, wie z. B. das Datum und die Uhrzeit der Nutzung, die Anmeldung beim Dienst und die Abmeldung vom Dienst.

[10] Inhaltsdaten sind alle Daten in einem digitalen Format, wie Text, Sprache, Videos, Bilder und Ton, mit Ausnahme von Teilnehmerdaten oder Verkehrsdaten.

[11] Zu denken wäre hier beispielsweise an ein digitales Geschäftsverwaltungssystem einer Anwaltskanzlei.

- Teilnehmerdaten und Daten, die einzig der Identifizierung dienen, können für alle Straftaten herausverlangt werden sowie für die Vollstreckung von Freiheitsstrafen oder freiheitsentziehenden Massnahmen von mindestens 4 Monaten;
- Verkehrs- und Inhaltsdaten können herausverlangt werden für Straftaten, die im anordnenden Staat mit einer Freiheitsstrafe mit einer Höchststrafe von mindestens 3 Jahren belegt sind, für bestimmte in separaten Richtlinien festgelegte Straftaten (Betrug und Fälschung von Zahlungsmitteln, sexueller Missbrauch und Ausbeutung von Kindern sowie Kinderpornografie, Angriffe auf Informationssysteme) sowie für die Vollstreckung von Freiheitsstrafen oder freiheitsentziehenden Massnahmen von mindestens 4 Monaten.

2.4.2 Datenspeicherungsanordnung (Art. 6 der Verordnung)

Mit der Datenspeicherungsanordnung kann die zuständige Behörde eines Mitgliedstaates einen Diensteanbieter in einem anderen Mitgliedstaat zur Aufbewahrung bestimmter Daten für einen bestimmten Zeitraum verpflichten.

Die Datenspeicherungsanordnung muss **notwendig und verhältnismässig** sein, um die Entfernung, Löschung oder Veränderung von Daten zu verhindern im Hinblick auf ein zukünftiges Rechtshilfeersuchen, eine Europäische Ermittlungsanordnung[12] oder eine Europäische Herausgabeanordnung.

Die Datenspeicherung kann für alle Straftaten angeordnet werden, vorausgesetzt, dass sie unter denselben Bedingungen in ähnlichen innerstaatlichen Fällen angeordnet werden könnte, sowie für die Vollstreckung von Freiheitsstrafen oder freiheitsentziehenden Massnahmen von mindestens 4 Monaten.

2.4.3 Anordnende Behörde (issuing authority)

Die Verordnung regelt auch, welche Behörden der Mitgliedstaaten Daten anfordern können, d. h. eine Herausgabe- oder Datenspeicherungsanordnung erlassen und dem Diensteanbieter direkt zustellen können.

Welche Behörde des anordnenden Staates **(issuing State)** direkt die Herausgabe verlangen kann, hängt von der Art der Daten ab (Art. 4 der Verordnung):

Teilnehmerdaten können von einer Richterin oder einem Richter, vom Gericht, von einem Untersuchungsrichter oder einer Untersuchungsrichterin, von der zuständigen Staatsanwältin oder dem zuständigen Staatsanwalt herausverlangt werden. Zudem kann jede andere Behörde, die gemäss dem Recht des anordnenden Staates zuständig ist, solche Daten herausverlangen, wenn die Anordnung durch eine Richterin, einen Untersuchungsrichter, eine Staatsanwältin oder ein Gericht validiert wurde.

Bei den Verkehrs- und Inhaltsdaten ist die Herausgabe eingeschränkter. Eine solche kann von einer Richterin oder einem Richter, von einem Gericht oder einem Untersuchungsrichter oder eine Untersuchungsrichterin herausverlangt werden sowie von jeder anderen Behörde, die gemäss dem Recht des anordnenden Staates zuständig ist, sofern die Anordnung von einer Richterin oder einem Richter, einem Gericht oder einer Untersuchungsrichterin oder einem Untersuchungsrichter überprüft und genehmigt wurde (Validierung). Im Gegensatz zu Teilnehmerdaten können also Verkehrs- und Inhaltsdaten nicht durch einen Staatsanwalt / eine Staatsanwältin selbständig herausverlangt werden. Die Staatsanwaltschaft könnte aber

[12] Die Europäische Ermittlungsanordnung ist eine gerichtliche Entscheidung, die von einer Justizbehörde eines EU-Mitgliedstaats zur Durchführung einer oder mehrerer Ermittlungsmassnahmen zur Erlangung von Beweisen in einem anderen Mitgliedstaat erlassen wird.

einen entsprechenden Antrag stellen (vgl. Art. 4 Abs. 2 lit. b der Verordnung), der dann durch eine richterliche Behörde genehmigt werden müsste.

Bei der Datenspeicherung wird die Unterscheidung nach Art der Daten nicht getroffen: Eine Datenspeicherung kann für alle Daten von einem Richter oder einer Richterin, einem Gericht, einem Untersuchungsrichter oder einer Untersuchungsrichterin, von einer Staatsanwältin oder Staatsanwalt oder jeder nach dem nationalen Recht des anordnenden Staates zuständigen Behörde angeordnet werden. Wird sie von einer nach dem nationalen Recht zuständigen Behörde angeordnet, so muss ein Gericht, ein Richter oder eine Richterin, ein Untersuchungsrichter oder eine Untersuchungsrichterin oder ein Staatsanwalt oder eine Staatsanwältin die Anordnung für gültig erklären (Validierung).

2.4.4 Adressaten der Anordnung

Adressaten der Herausgabeanordnung sind die Diensteanbieter. Im Grundsatz gilt, dass die Herausgabeanordnung an den Diensteanbieter zu richten ist, der als Verantwortlicher (controller) handelt (Art. 5 Abs. 6 der Verordnung). Wer Verantwortlicher über die Daten ist, ist in der EU-Datenschutzgrundverordnung (DSGVO) Art. 4 Abs. 7 geregelt:[13]

> *"Verantwortlicher" (controller) ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden;*

Ausnahmsweise kann die Herausgabeanordnung direkt an den Diensteanbieter gerichtet werden, der die Daten im Auftrag des controllers speichert oder anderweitig verarbeitet (Auftragsverarbeiter (processor))[14], wenn der controller trotz angemessener Bemühungen der anordnenden Behörde nicht ermittelt werden kann oder dessen Adressierung die Ermittlungen gefährden könnte. In diesem Fall hat der processor den controller über die Herausgabe der Daten zu informieren, es sei denn, die anordnende Behörde hat den processor ersucht, den controller nicht zu informieren, um das betreffende Strafverfahren nicht zu behindern (Art. 5 Abs. 7 der Verordnung).[15]

Artikel 5 Absatz 8 der Verordnung enthält zudem eine wichtige Einschränkung in Bezug auf Daten, die von einem Diensteanbieter für eine Behörde gespeichert oder anderweitig verarbeitet werden. Für solche Daten kann eine Herausgabeanordnung nur dann erlassen werden, wenn die Behörde im anordnenden Staat ansässig ist.

Sowohl die Herausgabe- wie auch die Datenspeicherungsanordnung sind direkt an die bezeichnete Niederlassung oder den ernannten gesetzlichen Vertreter des Diensteanbieters zu richten. Reagieren diese nicht, so kann die Herausgabeanordnung in Notfällen auch an eine andere Niederlassung oder einen anderen gesetzlichen Vertreter des Diensteanbieters in der EU gerichtet werden. Zugleich ist in gewissen Fällen auch der ausführende Staat zu informieren (siehe 1.4.5).

---

[13] Die Erwägungen und Bestimmungen in der Verordnung verweisen, wo einschlägig, direkt auf Bestimmungen der DSGVO sowie der Datenschutz-Richtlinie, welche in diesen Fällen anwendbar sind.

[14] Gemäss Art. 4 Abs. 8 der EU-Datenschutz-Grundverordnung ist der „Auftragsverarbeiter" (processor) eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

[15] In diesem Bereich geht die e-evidence Verordnung der DSGVO vor, welche eine Informationspflicht des processors an den controller vorschreibt.

2.4.5 Notifizierung des ausführenden Staates *(executing State)*

Jeder Mitgliedstaat kann eine oder mehrere Zentralstellen benennen, die für die administrative Übermittlung von Zertifikaten, Anordnungen oder Notifizierungen, den Erhalt von Daten und Notifizierungen sowie die Übermittlung offizieller Korrespondenz zuständig ist.

Verlangt die anordnende Behörde die Herausgabe von Verkehrs- oder Inhaltsdaten, so hat sie die zuständige Behörde des ausführenden Staates (executing state = Staat, in welchem der Diensteanbieter niedergelassen ist oder seinen gesetzlichen Vertreter ernannt hat) darüber zu notifizieren, indem sie die Herausgabeanordnung zeitgleich dieser Behörde zustellt (Art. 8 Abs. 1 der Verordnung). Die Notifizierung entfällt in gewissen Fällen, namentlich wenn der anordnende Staat hinreichende Gründe für die Annahme hat, dass die Straftat im anordnenden Staat begangen wurde, wird oder werden könnte und die Person, um deren Daten ersucht wird, im anordnenden Staat wohnt («Wohnsitzkriterium»).

Die ausführende Behörde kann die Anordnung innerhalb von 10 Tagen und in Notfällen innerhalb von 96 Stunden (siehe unten) überprüfen (Art. 12 der Verordnung). Die möglichen Ablehnungsgründe sind in der Verordnung abschliessend geregelt (vgl. dazu 2.4.6.). Erhebt die ausführende Behörde keine Einwände, so hat der Diensteanbieter die Daten herauszugeben, d. h. es ist keine aktive Genehmigung des ausführenden Staates erforderlich (vgl. dazu 2.4.7.).

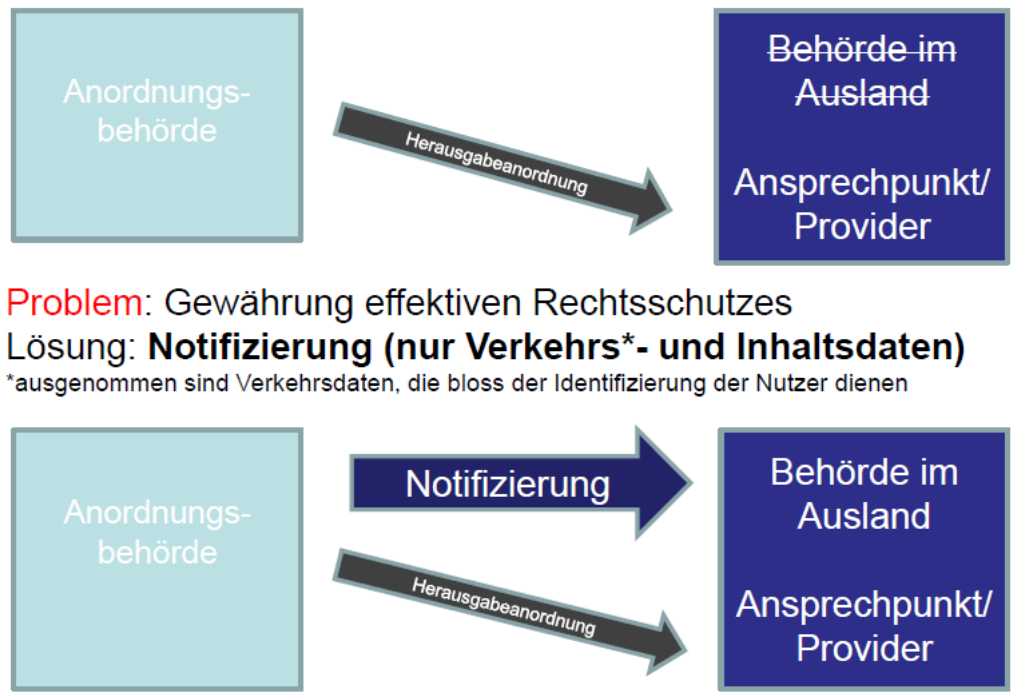

Abb.: Einbezug des Vollstreckungsstaates mittels sog. Notifizierung

Die Notifizierungspflicht ist stark eingeschränkt. So gilt sie gar nicht für Datenspeicherungsanordnungen und nicht für die Herausgabe von Teilnehmerdaten sowie Verkehrsdaten, die alleine der Identifikation des Nutzenden dienen. Letzteres kann insbesondere dann gravierende Konsequenzen haben, wenn die Anordnung auf die Identität von journalistischen Quellen oder Whistleblowern abzielt. In diesem Fall obliegt es alleine dem Diensteanbieter, eine Verletzung der Presse- oder Meinungsäusserungsfreiheit geltend zu machen, da der ausführende Staat gar nicht informiert wird (vgl. 2.4.6). Macht der Diensteanbieter eine solche Verletzung nicht geltend, kann es mitunter zur Herausgabe von Daten kommen, die auf dem heute zu beschreitenden Rechtshilfeweg wegen dieser Verletzung nicht herausgegeben wür-

den. Auch das «Wohnsitzkriterium» ist als problematisch einzustufen, da diese Beurteilung alleine im Ermessen der Strafverfolgungsbehörden des anordnenden Staates liegt, die schliesslich ein beachtliches Interesse an der Vermeidung der Notifizierung haben, um zu vermeiden, dass der ausführende Staat Ablehnungsgründe geltend macht. Gar nicht vorgesehen ist zudem die Notifizierung des Staates, in welchem die betroffene Person ihren Sitz oder Wohnsitz hat. Dies ist insbesondere dann problematisch, wo weder die anordnenden noch die ausführenden Behörden Kenntnis über mögliche Immunitäten gemäss dem Recht des Drittstaates haben, in welchem die betroffene Person ihren Wohnsitz hat.[16]

2.4.6 Ablehnungsgründe

Die Verordnung enthält sowohl für den Adressaten einer Anordnung wie auch für den ausführenden Staat (d. h. dessen notifizierte Zentralstelle) Ablehnungsgründe, die gegen eine Herausgabe- oder Datenspeicherungsanordnung geltend gemacht werden können.

So kann der Adressat einer Anordnung (Diensteanbieter) geltend machen, dass die Anordnung gegen Immunitäten, Privilegien oder die Presse- oder Meinungsäusserungsfreiheit gemäss dem Recht des ausführenden Staates verstösst. Liegt eine solche Rüge vor, hat die anordnende Behörde darüber zu befinden, ob die Anordnung zurückgezogen, angepasst oder aufrecht erhalten bleibt (Art. 10 Abs. 5 und Art. 11 Abs. 4 der Verordnung).

Zugleich kann der ausführende Staat – also die notifizierte Zentralstelle – eine Anordnung dann ablehnen, wenn (Art. 12 Abs. 1 der Verordnung):

- die Daten durch in seinem Recht garantierte Immunitäten oder Privilegien oder durch die Presse- oder Meinungsäusserungsfreiheit geschützt sind;
- in Ausnahmefällen auf der Grundlage konkreter und objektiver Anhaltspunkte stichhaltige Gründe für die Annahme bestehen, dass die Vollstreckung der Anordnung unter Berücksichtigung der besonderen Umständen des Falles eine offenkundige Verletzung eines einschlägigen grundlegenden Rechts, wie es in Artikel 6 des Vertrages über die Europäische Union (EUV)[17] und der Charta der Grundrechte der Europäischen Union (EU-Charta) festgelegt ist, zur Folge hätte;
- die Ausführung der Anordnung gegen das *ne bis in idem*-Prinzip verstösst oder
- keine doppelte Strafbarkeit vorliegt, d. h. der der Anordnung zugrunde liegende Sachverhalt im ausführenden Staat nicht strafbar ist, es sei denn es handle sich um eine Straftat, die unter den in Anhang IV aufgeführten Kategorien von Straftaten aufgeführt und im anordnenden Staat mit einer Freiheitsstrafe oder einer freiheitsentziehenden Massnahme mit einem Höchststrafmass von mindestens drei Jahren bedroht ist.

Gemäss der Einschätzung von NGOs könnte die Tatsache, dass der Ablehnungsgrund der Menschenrechte auf Ausnahmesituationen und einschlägige, fundamentale Rechte eingeschränkt ist, dazu führen, dass Personen, die in Staaten wohnen, in denen Herausforderungen im Bereich der Rechtstaatlichkeit bestehen, besonders beeinträchtigt werden. Denn diese können sich nicht länger dadurch schützen, indem sie bewusst einen Diensteanbieter in einem anderen Staat nutzen. Zu denken ist dabei beispielsweise an Menschenrechtsaktivistinnen und -aktivisten.[18]

---

[16] Siehe dazu Kritik der NGO European Digital Rights (EDRi), e-Evidence compromise blows a hole in fundamental rights safeguards, verfügbar unter: https://edri.org/our-work/e-evidence-compromise-blows-a-hole-in-fundamental-rights-safeguards/

[17] Art. 6 EUV sieht unter anderem vor, dass die Grundrechte, wie sie in der EMRK gewährleistet sind und wie sie sich aus den gemeinsamen Verfassungsüberlieferungen der Mitgliedstaaten ergeben, als allgemeine Grundsätze Teil des Unionsrechts sind.

[18] Siehe dazu Kritik der NGO European Digital Rights (EDRi), e-Evidence compromise blows a hole in fundamental rights safeguards, verfügbar unter: https://edri.org/our-work/e-evidence-compromise-blows-a-hole-in-fundamental-rights-safeguards/

2.4.7 Ausführung

Ist gemäss Artikel 8 der Verordnung die Notifikation der ausführenden Behörde erforderlich und hat diese innerhalb der vorgesehenen Frist (siehe 2.4.5) keine Einwände gegen die Herausgabe erhoben, so hat der Diensteanbieter die ersuchten Daten am Ende der 10 Tage direkt an die zuständige anordnende Behörde oder der in der Anordnung angegebenen Strafverfolgungsbehörden herauszugeben (Art. 10 Abs. 2 der Verordnung). Bestätigt die ausführende Behörde bereits vor Ablauf der 10 Tage, dass sie keinen Ablehnungsgrund geltend machen wird, muss der Diensteanbieter so bald wie möglich, jedoch spätestens nach Ablauf der 10 Tage, tätig werden. Ist eine Notifikation der ausführenden Behörde nicht notwendig, so hat der Diensteanbieter die Daten innerhalb von 10 Tagen direkt der anordnenden Behörde oder der in der Anordnung genannten Strafverfolgungsbehörde herauszugeben (Art. 10 Abs. 3 der Verordnung).

In Notfällen hat der Diensteanbieter die Daten unverzüglich zu übermitteln, spätestens jedoch innerhalb von 8 Stunden nach Erhalt der Herausgabeanordnung (Art. 10 Abs. 4 der Verordnung). In denjenigen Fällen, in denen die ausführende Behörde notifiziert werden muss (also bei Verkehrs- und Inhaltsdaten), kann diese innerhalb von 96 Stunden nach Erhalt der Notifizierung die anordnende Behörde und den Adressaten über ihre Einwände oder Bedingungen zur Verwendung der Daten informieren. Wurden die Daten bereits herausgegeben, sind sie entsprechend zu löschen oder deren Nutzung entsprechend einzuschränken. Problematisch scheint hier insbesondere, dass die Herausgabe der Daten bereits stattgefunden hat, obschon sich deren Herausgabe im Nachhinein als unzulässig erweist.

Kann der Diensteanbieter der Herausgabe oder Datenspeicherung nicht nachkommen, weil die Anordnung unvollständig ist, grobe Fehler oder nicht genügend Informationen zur Ausführung enthält oder es ihm aufgrund von Umständen, die er nicht zu vertreten hat, faktisch unmöglich ist, so hat er unverzüglich die anordnende Behörde zu informieren (Art. 10 Abs. 6 und 7 und Art. 11 Abs. 5 und 6 der Verordnung), allenfalls auch die ausführende Behörde, falls eine Notifikation gemäss Artikel 8 der Verordnung an diese erfolgt ist.

Die Datenspeicherungsanordnung verfällt automatisch nach 60 Tagen, es sei denn, die anordnende Behörde bestätigt, dass eine Herausgabeanordnung ausgestellt wurde (Art. 11 der Verordnung). Innerhalb der 60 Tage kann die anordnende Behörde die Sicherung um 30 Tage verlängern.

2.4.8 Information der Nutzerin oder des Nutzers

Die anordnende Behörde hat die betroffene Person unverzüglich über die Datenherausgabe zu informieren (Art. 13 der Verordnung). Im Anhang I, Abschnitt H ist zudem explizit festgehalten, dass es dem Diensteanbieter untersagt ist, die Person, um deren Daten ersucht wird, zu informieren und es allein der anordnenden Behörde obliegt, diese Person unverzüglich über die Datenherausgabe zu unterrichte. Die anordnende Behörde kann die Information der Person, um deren Daten ersucht wird, nach Massgabe des innerstaatlichen Rechts des anordnenden Staates verzögern, einschränken oder unterlassen, soweit und solange die Voraussetzungen von Artikel 13 Absatz 3 der EU-Datenschutzrichtlinie[19] erfüllt sind. Die anordnende Behörde hat die Gründe für die Verzögerung, Einschränkungen oder Unterlassung in

[19] Siehe Art. 13 Abs. 3: Die Mitgliedstaaten können Gesetzgebungsmassnahmen erlassen, nach denen die Unterrichtung der betroffenen Person [...] soweit und so lange aufgeschoben, eingeschränkt oder unterlassen werden kann, wie diese Massnahme in einer demokratischen Gesellschaft erforderlich und verhältnismässig ist und sofern den Grundrechten und den berechtigten Interessen der betroffenen natürlichen Person Rechnung getragen wird: a) zur Gewährleistung, dass behördliche oder gerichtliche Untersuchungen, Ermittlungen oder Verfahren nicht behindert werden, b) zur Gewährleistung, dass die Verhütung, Aufdeckung, Ermittlung oder Verfolgung von Straftaten oder die Strafvollstreckung nicht beeinträchtigt werden, c) zum Schutz der öffentlichen Sicherheit, d) zum Schutz der nationalen Sicherheit, e) zum Schutz der Rechte und Freiheiten anderer.

der Akte aufzuführen und eine kurze Begründung in die Herausgabeanordnung aufzunehmen.

Wie die betroffene Person informiert wird, wenn sie sich nicht auf dem Territorium der anordnenden Behörde befindet, ist in der Verordnung nicht explizit geregelt. Aufgrund des Wortlauts von Artikel 13, der nur die anordnende Behörde anspricht, ist davon auszugehen, dass die Information in jedem Fall durch die anordnende Behörde geschieht, unabhängig davon, wo die Person ihren Wohnsitz hat (kann auch in einem Drittstaat sein). Verlangt beispielsweise eine deutsche Behörde von einem französischen service provider Daten von einer Person, die in Frankreich ihren Wohnsitz hat, so hat die deutsche Behörde diese Person zu informieren.

2.4.9 Sanktionen und Vollstreckung

2.4.9.1 Sanktionen

Die Mitgliedstaaten haben die finanziellen Sanktionen für die Diensteanbieter festzulegen für Verstösse gegen Artikel 10 (Ausführung der Herausgabeanordnung), Artikel 11 (Ausführung der Datenspeicherungsanordnung) sowie Artikel 13 Absatz 4 (Vertraulichkeit, Geheimhaltung, Integrität). Die vorgesehenen finanziellen Sanktionen müssen wirksam, verhältnismässig und abschreckend sein und können bis zu 2% des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahrs des Diensteanbieters betragen (Art. 15 Abs. 1 der Verordnung).

Die Diensteanbieter können nicht für Schäden haftbar gemacht werden, die ihren Nutzenden oder Dritten ausschliesslich durch die Einhaltung der Herausgabe- oder Datenspeicherungsanordnung in gutem Glauben entstehen (Art. 15 Abs. 2 der Verordnung).

2.4.9.2 Vollstreckung

Kommt der Diensteanbieter ohne Angabe von Gründen einer Herausgabeanordnung innerhalb der Frist oder einer Datenspeicherungsanordnung nicht nach und hat die ausführende Behörde ebenfalls keine der in Artikel 12 genannten Verweigerungsgründe geltend gemacht, so kann die anordnende Behörde die ausführende Behörde um Vollstreckung der Herausgabe- oder Datenspeicherungsanordnung ersuchen (Art. 16 Abs. 1 Verordnung).

Die ausführende Behörde hat unverzüglich über die Anerkennung des Vollstreckungsbeschlusses zu entscheiden, spätestens jedoch nach fünf Arbeitstage nach Eingang des Beschlusses (Art. 16 Abs. 2 Verordnung).

Die ausführende Behörde fordert den Diensteanbieter auf, seinen Verpflichtungen nachzukommen und informiert ihn zugleich über:

- die Möglichkeit, gegen die Vollstreckung der betreffenden Anordnung unter Berufung auf einen in der Verordnung genannten Ablehnungsgrund (siehe 2.4.6) Einspruch zu erheben. Macht der Anbieter von dieser Möglichkeit Gebrauch, so hat die ausführende Behörde darüber zu entscheiden, ob die Herausgabe- oder Datenspeicherungsanordnung auf Grundlage der vom Diensteanbieter bereitgestellten Informationen zu vollstrecken ist oder nicht. Die ausführende Behörde kann dazu auch zusätzliche Informationen von der anordnenden Behörde einholen;
- die Sanktionen / Bussen, die im Falle einer Nichteinhaltung verhängt werden;
- die Frist für die Einhaltung oder den Einspruch.

Die Vollstreckung einer Herausgabe- oder Datenspeicherungsanordnung kann von der ausführenden Behörde in bestimmten in der Verordnung abschliessend geregelten Fälle verweigert werden, wenn:

- die Herausgabe oder Datenspeicherung nicht durch die zuständige Behörde angeordnet oder validiert wurde;
- die Herausgabe oder Datenspeicherung nicht für eine in der Verordnung vorgesehene Straftat angeordnet wurde;
- der Diensteanbieter der Herausgabe- oder Datenspeicherungsanordnung nicht nachkommen konnte wegen Gründen, die er nicht zu verantworten hat oder weil die Anordnung gravierende Fehler aufweist;
- die Herausgabeanordnung keine Daten betrifft, die von oder im Auftrag des Diensteanbieters zum Zeitpunkt des Erhalts der Anordnung gespeichert sind;
- die Dienstleistung nicht von dieser Verordnung erfasst ist;
- die angeforderten Daten durch Immunitäten oder Privilegien geschützt sind, wie sie nach dem Recht des ausführenden Staates gewährt werden, oder die angeforderten Daten von der Beschränkung der strafrechtlichen Verantwortlichkeit erfasst sind, die sich auf die Presse- oder Meinungsäusserungsfreiheit in anderen Medien beziehen, welche die Ausführung oder Vollstreckung der Herausgabeanordnung verhindern;
- in Ausnahmesituationen, wenn auf der Grundlage der in der Herausgabeanordnung enthaltenen Informationen ersichtlich ist, dass stichhaltige Gründe für die Annahme bestehen, dass die Vollstreckung der Anordnung unter den besonderen Umständen des Falles eine offensichtliche Verletzung eines einschlägigen Grundrechts gemäss Artikel 6 EUV und der EU-Charta bedeuten würde.

Die ausführende Behörde hat die anordnende Behörde sowie den Diensteanbieter unverzüglich über ihren Entscheid zu informieren. Erlangt die ausführende Behörde die mit der Herausgabeanordnung ersuchten Daten vom Diensteanbieter, so hat sie diese der anordnenden Behörde unverzüglich zu übermitteln.

Kommt ein Diensteanbieter seinen Verpflichtungen aus der Herausgabe- oder Datenspeicherungsanordnung nicht nach, obschon deren Vollstreckbarkeit von der ausführenden Behörde bestätigt wurde, auferlegt ihm die ausführende Behörde eine Busse im Sinne von Artikel 15 der Verordnung.

2.4.10 Gegenläufige rechtliche Verpflichtungen

Ist ein Diensteanbieter der Ansicht, dass die Datenherausgabe einer Verpflichtung gemäss dem anwendbaren Recht eines Drittstaates widerspricht, hat er der anordnenden sowie der ausführenden Behörde innerhalb von 10 Tagen nach Erhalt der Herausgabeanordnung eine begründete Verweigerung zuzustellen. Die Weigerung kann nicht darauf gestützt werden, dass im anwendbaren Recht des Drittstaates keine ähnlichen Bedingungen oder Verfahren für den Erlass einer Herausgabeanordnung bestehen oder alleine darauf, dass die Daten in einem Drittstaat gespeichert sind (Art. 17 Abs. 1 f. der Verordnung).

Hält die anordnende Behörde trotz der begründeten Weigerung an der Anordnung fest, entscheidet das zuständige Gericht im anordnenden Staat. Dieses hat zunächst zu beurteilen, ob eine Pflichtenkollision besteht, indem es untersucht, ob das Recht des Drittstaates überhaupt auf die spezifischen Umstände des Falls anwendbar ist und falls dem so ist, ob das Recht des Drittstaates die Bekanntgabe der betreffenden Daten im konkreten Fall verbietet. Befindet das Gericht, dass kein relevanter Konflikt besteht, bleibt die Anordnung bestehen. Kommt es zum Schluss, dass das Recht des Drittstaates die Herausgabe der betreffenden

Daten verbietet, entscheidet das Gericht, ob die Anordnung aufrechtzuerhalten oder aufzuheben ist. Die Kriterien für diese Beurteilung sind in der Verordnung detailliert aufgeführt (Art. 17 Abs. 6 der Verordnung).

Hier kann zumindest in Frage gestellt werden, inwiefern das Gericht im anordnenden Staat tatsächlich als «neutrale» Instanz betrachtet werden kann, wenn es die Interessen der eigenen anordnenden Behörde gegen die Interessen des Drittstaates abzuwägen hat.

2.5 Rechtsschutz

Der Rechtsschutz ist in Artikel 18 der Verordnung geregelt. Dieser sieht vor, dass der Person, um deren Daten ersucht wird, ein Recht auf wirksame Rechtsbehelfe gegen die Herausgabeanordnung zustehen muss. Handelt es sich bei dieser Person um eine verdächtigte oder beschuldigte Person, so stehen ihr die wirksamen Rechtsbehelfe während des Strafverfahrens zu, in welchem die Daten verwendet werden.

Das Recht auf wirksame Rechtsbehelfe gilt unbeschadet des Rechts, Rechtsbehelfe gemäss der EU-Datenschutzverordnung (DSGVO) einzulegen.

Das Recht auf einen wirksamen Rechtsbehelf ist vor einem Gericht des Anordnungsstaats nach dessen innerstaatlichem Recht geltend zu machen. Dabei kann die Rechtmässigkeit der Massnahme angefochten werden, einschliesslich ihrer Notwendigkeit und Verhältnismässigkeit, unbeschadet der Garantien der Grundrechte im Vollstreckungsstaat.

Wird die Person, um deren Daten um Herausgabe ersucht wird, gemäss Artikel 13 Absatz 1 der Verordnung vom anordnenden Staat über die Herausgabe informiert, hat der anordnende Staat sie auch rechtzeitig über die ihr nach seinem innerstaatlichen Recht bestehenden Möglichkeiten zur Einlegung von Rechtsbehelfen zu informieren. Der anordnende Staat hat dafür zu sorgen, dass diese wirksam ausgeübt werden können.

Zur Einlegung von Rechtsbehelfen gelten dieselben Fristen oder sonstigen Bedingungen wie in vergleichbaren innerstaatlichen Verfahren. Dabei muss gewährleistet sein, dass die betroffene Person ihr Recht auf einen Rechtsbehelf wirksam ausüben kann.

Unabhängig der innerstaatlichen Verfahrensvorschriften haben der anordnende Staat und jeder andere Mitgliedstaat, dem elektronische Beweismittel nach dieser Verordnung übermittelt wurden, sicherzustellen, dass die Verteidigungsrechte und die Fairness des Verfahrens bei der Würdigung der durch die Herausgabeanordnung erlangten Beweismittel gewahrt bleiben.

2.6 Dezentralisiertes IT-System

Das e-Evidence Paket sieht die Errichtung eines dezentralisierten IT-Systems vor, das die sichere elektronische Kommunikation und den Datenaustausch zwischen den zuständigen Behörden und den Diensteanbietern oder nur zwischen den zuständigen Behörden gewährleistet.

Die bezeichnete Niederlassung oder der gesetzliche Vertreter des Diensteanbieters müssen Zugriff auf das dezentralisierte IT System via das jeweilige nationale IT System haben, um Herausgabeanordnungen und Datenspeicherungsanordnungen zu empfangen, die ersuchten Daten zu übermitteln und mit der zuständigen Behörden zu kommunizieren.

Die Kosten für die Errichtung, den Betrieb und die Wartung der dezentralen Zugangspunkte des IT-Systems tragen dabei die jeweiligen Mitgliedstaaten. Zudem trägt jeder Mitgliedstaat die Kosten für die Errichtung und Anpassung seiner nationalen IT-Systeme, um diese kompatibel zu machen.

2.7 Umsetzungsfrist

Die Umsetzungsfrist des e-Evidence-Pakets beträgt 36 Monate und begann mit der Publikation im Amtsblatt der Europäischen Union am 28. Juli 2023 zu laufen.[20]

3 Rechtsvergleichung

Das e-Evidence-Paket wird nicht nur Auswirkungen auf die Schweiz haben wird, sondern auch auf andere Staaten, deren Diensteanbieter in der EU bestimmte Dienste anbieten. Die Schweiz hat daher mit verschiedenen Staaten Kontakt aufgenommen, um sich über deren Position zu den neuen EU-Regeln auszutauschen. Die meisten dieser Staaten haben das neue Gesetzespaket jedoch noch nicht eingehend analysiert.

Das **Vereinigte Königreich** hat mit den USA ein Exekutivabkommen auf der Grundlage des US CLOUD Act geschlossen. Aufgrund seines Austritts aus der EU, ist das Vereinigte Königreich nicht Teil der e-Evidence-Regelung. Zu seiner Positionierung gegenüber dem e-Evidence-Paket hat das Vereinigte Königreich aber noch keine Überlegungen angestellt. Es erscheint aufgrund des Anschlusses UKs an das System des US CLOUD Act aber eher unwahrscheinlich, dass sich UK vertieft für die EU-Regelung interessiert.

Island und **Norwegen**, zwei Staaten, die sich insofern in einer ähnlichen Lage befinden wie die Schweiz, als dass sie ebenfalls nicht EU-Mitgliedstaaten sind, aber als Schengen-Staaten über eine starke Zusammenarbeit mit der EU in den relevanten Bereichen verfügen, scheinen ebenfalls noch nicht mit der Analyse des e-Evidence-Pakets und der internationalen Zusammenarbeit in Strafsachen im Bereich der elektronischen Beweisführung begonnen zu haben. Im Gegensatz zu Norwegen und der Schweiz hat Island das Zweite Zusatzprotokoll (ZP II) zum Übereinkommen über Cyberkriminalität unterzeichnet.

Des Weiteren stand die Schweiz im Austausch mit **Dänemark**. Dänemark ist zwar Mitglied der EU, es verfügt jedoch über ein Opt-out in Bezug auf den Raum der Freiheit, der Sicherheit und des Rechts. Dies bedeutet, dass es Verordnungen, die sich auf diesen Zuständigkeitsbereich stützen, nicht umsetzt. Wie erwähnt stützt sich nur die e-Evidence-Verordnung auf den Raum der Freiheit, der Sicherheit und des Rechts, nicht aber die e-Evidence-Richtlinie. Dies hat zur Folge, dass Dänemark verpflichtet ist, die Richtlinie umzusetzen, nicht aber die Verordnung. Die Richtlinie sieht jedoch hauptsächlich vor, dass die Staaten, die sich nicht an der Verordnung beteiligen, die notwendigen Schritte unternehmen müssen, damit die in ihrem Hoheitsgebiet niedergelassenen Diensteanbieter einen gesetzlichen Vertreter in der EU ernennen. Dänemark evaluiert zurzeit, wie es die Richtlinie ohne die Verordnung umsetzen kann.

Etwas anders gelagert ist die Situation für **Irland**, da es über ein flexibles Opt-out verfügt. Dies erlaubt es Irland, selbst zu entscheiden, an welchen Gesetzgebungsprojekten es sich im Bereich der Freiheit, der Sicherheit und des Rechts beteiligen möchte. Aufgrund der grossen Anzahl von auf seinem Hoheitsgebiet ansässigen Dienstleistern hat Irland ein besonderes Interesse daran, sich am e-Evidence-Paket zu beteiligen, um zu verhindern, dass die Dienste-

[20] ABl. L 191/118 vom 28. Juli 2023.

anbieter einen Vertreter in einem anderen EU-Mitgliedstaat benennen müssen. Gleichzeitig verweist die Verordnung jedoch auf bestimmte Instrumente, die Irland nicht übernommen hat.

Irland hat bereits kurz nach dem Brexit und während der Verhandlungen über das e-Evidence-Paket angedeutet, dass es sich daran beteiligen werde. So ist Irland derzeit daran, sein innerstaatliches Recht anzupassen, damit auf der Grundlage des e-Evidence-Pakets erlassene Herausgabe- und Datenspeicherungsanordnungen direkt an in Irland ansässige Diensteanbieter gerichtet werden können. Auch wenn Irland nicht alle Instrumente übernommen hat, auf denen die Bestimmungen der e-Evidence-Verordnung teilweise beruhen (wie z. B. die Europäische Ermittlungsanordnung), hofft der Staat die Verordnung umsetzen zu können. Durch die Anpassung seines innerstaatlichen Rechts strebt Irland eine Umsetzung der Richtlinie sofort bei deren Inkrafttreten an.

Schliesslich verhandeln die **USA** und die EU bereits seit mehreren Jahren über ein Abkommen, das den Zugang zu elektronischen Beweismitteln zwischen den beiden Entitäten regeln würde. Während die Medien und das DOJ in den USA hauptsächlich von einem *Executive Agreement* sprechen, deuten die der Schweiz vorliegenden Informationen eher darauf hin, dass die beiden Entitäten über ein unabhängiges internationales Abkommen verhandeln, das eine Brücke zwischen dem US-amerikanischen und dem europäischen System schlagen soll. Nachdem die Verhandlungen 2020 aufgrund von COVID 19 und den Diskussionen über das e-Evidence-Paket in der EU auf Eis gelegt wurden, wurden sie nun wieder aufgenommen. Es scheint sich dabei in erster Linie um ein Instrument zu handeln, mit dem vermieden werden soll, dass die Diensteanbieter widersprüchlichen Verpflichtungen unterliegen, da sie de facto sowohl dem CLOUD Act als auch dem e-Evidence-Paket unterworfen wären.

4 Auswirkungen auf die Schweiz

Das e-Evidence-Paket wird zwar hauptsächlich Auswirkungen auf die EU-Mitgliedstaaten oder zumindest auf diejenigen Mitgliedstaaten haben, die an dem Paket beteiligt sind, aber aufgrund der territorialen Nähe der Schweiz zur EU und der engen Beziehungen der Schweiz zu den EU-Mitgliedstaaten dürfte es auch Auswirkungen auf die Schweiz haben. Die Auswirkungen werden hauptsächlich in der Schweiz ansässige Diensteanbieter betreffen, zum Teil jedoch weitere Auswirkungen haben.

4.1 Auswirkungen auf Diensteanbieter

Die in der Schweiz ansässigen Diensteanbieter, welche die vom e-Evidence-Paket erfassten Dienstleistungen auf dem europäischen Markt anbieten oder anbieten wollen (siehe 2.3.1) werden der e-Evidence-Regulierung der EU unterliegen.

Dies hat zur Folge, dass sie einerseits einen gesetzlichen Vertreter in einem EU-Mitgliedstaat ernennen müssen, sofern sie nicht ihre Niederlassung in die EU verlegen. Andererseits können die europäischen Strafverfolgungsbehörden ihre Herausgabe- und Datenspeicherungsanordnungen direkt an den gesetzlichen Vertreter eines in der Schweiz ansässigen Diensteanbieters in einem EU-Mitgliedstaat richten. Der Diensteanbieter muss diesen Anordnungen nachkommen, d. h. er muss die Daten, die von einer EU-Strafverfolgungsbehörde für ein Strafverfahren ausserhalb der Schweiz verlangt werden, herausgeben oder aufbewahren. Dadurch besteht die Gefahr, dass in der Schweiz gelagerte Daten ohne ein Rechtshilfeverfahren und der damit einhergehenden Garantien ins Ausland übermittelt werden.

Darüber hinaus kommt den in der Schweiz ansässigen Diensteanbietern die Aufgabe zu, eine allfällige Kollision bzw. Verletzung des Schweizer Rechts geltend zu machen. Macht der Diensteanbieter einen solchen Rechtskonflikt geltend, hat das Gericht im anordnenden

Staat darüber zu befinden. Folglich wird es den Diensteanbietern, also Privaten, obliegen, die Einhaltung von Schweizer Recht sicherzustellen und mögliche Rechtskonflikte zwischen den Verpflichtungen des Diensteanbieters nach Schweizer Recht und den Verpflichtungen aus dem e-Evidence-Paket zu vermeiden.

4.2 Weitere Auswirkungen

Die Schweiz und die EU haben seit vielen Jahren durch bilaterale Abkommen eine privilegierte Beziehung zueinander aufgebaut. Die internationale Zusammenarbeit in Strafsachen zwischen der Schweiz sowie der EU und ihren Mitgliedstaaten beruht auf den Instrumenten des Europarats und wird ergänzt durch die Assoziierung der Schweiz an das Schengen Abkommen[21] sowie das Betrugsbekämpfungsabkommen[22]. Das e-Evidence-Paket ist jedoch weder Teil der Schengener-Zusammenarbeit noch eines anderen bilateralen Abkommens zwischen der Schweiz und der EU. Abgesehen von den erwähnten Auswirkungen auf in der Schweiz ansässige Diensteanbieter, wird das e-Evidence-Paket daher bei seinem Inkrafttreten keine direkten Auswirkungen auf die Schweiz haben.

Um Kriminalität weiterhin effizient bekämpfen zu können, wird die Schweiz allerdings ihre Gesetzgebung in Bezug auf die Erhebung elektronischer Beweismittel anpassen müssen. Ein Alleingang der Schweiz ist kaum zielführend, denn eine rein nationale Gesetzgebung könnte keinen effektiven grenzüberschreitenden Zugang zu Daten als Beweismittel im Rahmen von Strafverfahren sicherstellen. Bei einem gesetzgeberischen Alleingang müsste die Schweiz vielmehr die Anwesenheit und die Kooperationsbereitschaft aller relevanten Diensteanbieter *in der Schweiz* erwirken können. Das scheint angesichts der geopolitischen Kräfteverhältnisse kaum realistisch. Daher wird die grenzüberschreitende Dimension des Datenzugriffs in der Praxis für die Schweiz sehr bedeutsam bleiben. Da die EU in vielen Bereichen ein wichtiger Partner der Schweiz ist, ist es unumgänglich, dass die Schweiz das e-Evidence-Paket und dessen Chancen und Risiken in ihre Überlegungen zur Neugestaltung der Erhebung elektronischer Beweismittel miteinbezieht.[23]

Des Weiteren wird mit dem e-Evidence-Paket auch ein Register der Diensteanbieter errichtet. Sollte ein solches Register, z.B. über Eurojust, verfügbar sein, wäre dies für die Schweizer Behörden nützlich, da sie wüssten, in welchem Staat die Diensteanbieter eine Niederlassung haben. Sie könnten folglich ihre Rechtshilfeersuchen direkt an den richtigen Staat richten.

5 Unterschiede zwischen dem e-Evidence-Paket und dem US Cloud Act

Der CLOUD Act und das e-Evidence-Paket der EU haben beide das Ziel, den Zugang zu elektronischen Beweismitteln zu erleichtern und so die grenzüberschreitende Kriminalität wirksamer zu bekämpfen. Im Folgenden werden die Unterschiede und Ähnlichkeiten der beiden Instrumente näher beleuchtet.

5.1 Territorialität und transnationaler Zugriff

Der erste Unterschied betrifft die Frage der Territorialität. Das e-Evidence-Paket der EU zielt auf alle Diensteanbieter ab, die ihre Dienste in der EU anbieten. Daher müssen Diensteanbieter, die ausserhalb der EU ansässig sind, einen gesetzlichen Vertreter in einem EU-Mitgliedstaat ernennen. Der CLOUD Act hingegen orientiert sich am engen Bezug, den ein

[21] Abkommen zwischen der Schweizerischen Eidgenossenschaft, der Europäischen Union und der Europäischen Gemeinschaft über die Assoziierung dieses Staates bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstands, SR 0.362.31.

[22] Abkommen über die Zusammenarbeit zwischen der Schweizerischen Eidgenossenschaft einerseits und der Europäischen Gemeinschaft und ihren Mitgliedstaaten andererseits zur Bekämpfung von Betrug und sonstigen rechtswidrigen Handlungen, die ihre finanziellen Interessen beinträchtigen, SR 0.351.926.8.

[23] Vgl. dazu die Überlegungen in Ziff. 6.

Diensteanbieter zu den USA haben muss. Wer in den USA angesiedelt ist oder eine US-Tochter oder Zweigniederlassung hat, ist erfasst. Unter gewissen Umständen auch bereits, wer seine Dienste mittels Werbung im US-Markt anpreist. Der CLOUD Act orientiert sich jedoch nicht am Kriterium der Präsenz in den USA und es wird auch nicht verlangt, dass die dem CLOUD Act unterstellten Diensteanbieter eine solche errichten. Die Diensteanbieter sind zur Herausgabe der Daten verpflichtet, die sich auf ihren Servern befinden, unabhängig davon, ob die Daten in den USA oder im Ausland gespeichert sind. So können Herausgabeanordnungen gemäss dem Cloud Act auch an die Schweizer Niederlassung eines in den USA ansässigen Diensteanbieter gestellt werden. Solche «extraterritorialen» Zugriffe auf Daten stellen für das amerikanische Rechtssystem kein Problem dar. Sie können jedoch zu Konflikten mit den Rechtssystemen derjenigen Staaten führen, auf deren Territorium sich die Daten befinden. Das EU-System hingegen «domestiziert» die Daten. Aufgrund der Anwesenheitspflicht der Diensteanbieter wird keine Anordnung in Gebiete ausserhalb der EU gesendet, sondern diese wird immer an den Hauptsitz oder den innerhalb in der EU ernannten Vertreter gerichtet. Dieser muss jedoch Zugang zu allen Daten des Unternehmens haben, unabhängig davon, wo diese gespeichert sind. Diensteanbieter, die von der EU-Verordnung betroffen sind, müssen alle Daten ihres Unternehmens übermitteln, unabhängig davon, wo diese gespeichert sind.

Beide Systeme sehen somit einen länderübergreifenden Zugriff auf die Daten vor und vereinfachen dadurch den grenzüberschreitenden Datenzugriff. Während das EU-System die Diensteanbieter dazu «zwingt», in der EU präsent zu sein, und den Zugriff auf alle Unternehmensdaten von der EU-Zentrale aus verlangt, basiert das US-System auf der Verbindung des Diensteanbieters mit den USA. Ein Diensteanbieter, der diese Verbindung zum US-amerikanischen Rechtssystem, wie es von den USA verstanden wird, hat, ist verpflichtet, alle seine Daten zu liefern, unabhängig davon, wo sie sich befinden.

Darüber hinaus sieht der CLOUD Act die Möglichkeit vor, *Executive Agreements* abzuschliessen, die es den US-Behörden ermöglichen, Anfragen an Diensteanbieter zu senden, die nicht auf US-Territorium ansässig sind, sich aber in den Staaten befinden, mit denen ein *Executive Agreement* geschlossen wurde, und umgekehrt.

5.2 Schutz personenbezogener Daten und Menschenrechtsschutz

Sowohl der US Cloud Act als auch das e-Evidence Paket enthalten Datenschutzbestimmungen. Die Bestimmungen des e-Evidence-Pakets müssen dabei den Datenschutzstandards der EU entsprechen, insbesondere der DSGVO. Die DSGVO ist für die Schweiz als Nicht-Mitgliedstaat der EU zwar nicht direkt anwendbar, da es sich nicht um eine Weiterentwicklung des Schengen-Besitzstands handelt. Die Schweiz hat jedoch ihr Datenschutzrecht revidiert, um den Entwicklungen auf internationaler und europäischer Ebene Rechnung zu tragen. Das totalrevidierte Datenschutzgesetz (DSG, SR 235.1) trat am 1. September 2023 in Kraft. Darüber hinaus gelten die Bestimmungen der DSGVO für Unternehmen in der Schweiz, die in den Anwendungsbereich der Verordnung fallen (Art. 3 DSGVO). Dies ist dann der Fall, wenn der Diensteanbieter in der EU niedergelassen ist oder, bei fehlender Niederlassung, wenn die Datenverarbeitung damit im Zusammenhang steht, betroffenen Personen in der EU Waren oder Dienstleistungen anzubieten oder deren in der EU erfolgendes Verhalten zu überwachen.

Die Schweiz verfügt über einen Angemessenheitsbeschluss der EU, der sie als Drittstaat mit einem angemessenen Datenschutzniveau anerkennt. So wird ein ungehinderter Datenaustausch ermöglicht. Die Schweiz kann davon ausgehen, dass die Anwendung des e-Evidence-Pakets die europäischen Datenschutzstandards erfüllen wird und diese Äquivalenz also nicht

gefährdet, da die betroffenen Unternehmen sowohl den europäischen als auch den schweizerischen Vorschriften unterliegen werden.

Im Gegensatz dazu unterscheiden sich die Datenschutzstandards des CLOUD Act von den Schweizer Standards. Der CLOUD Act Bericht kommt zum Schluss, dass die Datenverarbeitung im Rahmen eines Verfahrens, das auf dem CLOUD Act basiert, aufgrund mehrerer Elemente der DSGVO als problematisch eingestuft werden kann.[24]

Auch im Bereich der Menschenrechte bestehen zwischen dem Schweizer Recht und den e-Evidence-Bestimmungen grössere Parallelen als zum CLOUD Act. Die EU-Mitgliedstaaten sind alle Mitglieder des Europarats und unterstehen als solche der Europäischen Menschenrechtskonvention (EMRK). Die Umsetzung des e-Evidence-Pakets erfolgt daher in Übereinstimmung mit der EMRK, der auch die Schweiz angehört. Dazu gehört insbesondere die in Artikel 6 EMRK verankerte Rechtsweggarantie, wie sie auch Artikel 29*a* BV garantiert. So garantieren auch die e-Evidence-Bestimmungen für die von der Datenübertragung betroffene Person das Recht auf einen wirksamen Rechtsbehelf. Der US CLOUD Act sieht hingegen keine Möglichkeit für die betroffene Person vor, einen Richter oder eine Richterin anzurufen.

5.3 Verfahrensrechtliche Aspekte

Sowohl beim US CLOUD Act als auch beim e-Evidence-Paket werden Anordnungen von Behörden eines Staates direkt an einen Diensteanbieter in einem anderen Staat gerichtet. Die Behörden des Staates, in dem sich dieser Diensteanbieter befindet, müssen zur Datenerhebung grundsätzlich nichts beitragen. Man könnte also von einer «Privatisierung der internationalen Rechtshilfe in Strafsachen» sprechen. Dieser Effekt wird im e-Evidence-Paket durch die Pflicht zur Notifizierung abgeschwächt. So hat die anordnende Behörde bei der Herausgabe von Verkehrs- und Inhaltsdaten sowohl den Diensteanbieter als auch die zuständige Behörde in dem Staat, in dem der Diensteanbieter niedergelassen ist oder seinen gesetzlichen Vertreter ernannt hat, über die Anordnung zu informieren (siehe 2.4.5).

Dieser Mechanismus ist im US CLOUD Act oder im *Executive Agreement* zwischen den USA und dem Vereinigten Königreich nicht vorgesehen. Der Staat, in dessen Hoheitsgebiet sich der Diensteanbieter befindet, erhält keine Kenntnis von den Anfragen, die bei den sich in seinem Hoheitsgebiet befindenden Anbietern eingehen. Dies gilt selbst dann, wenn ein *Executive Agreement* abgeschlossen wurde.

Ein weiterer wichtiger Aspekt, den es zu erwähnen gilt, ist die Anwendung von Zwang oder die Durchsetzung von Anordnungen. Der US CLOUD Act sieht vor, dass die Strafverfolgungsbehörden auf dem Gebiet eines anderen Staates keinen Zwang anwenden dürfen. Wenn sich also ein Diensteanbieter in einem Staat, der mit den USA ein *Executive Agreement* eingegangen ist, weigert, die Daten zu übermitteln, müssen die US-Behörden die Daten durch internationale Rechtshilfe in Strafsachen beschaffen. Das e-Evidence-Paket sieht vor, dass die Anordnung in diesem Fall ohne Rechtshilfeverfahren direkt mit den Mechanismen in der e-Evidence-Verordnung durchgesetzt wird. So kann eine anordnende Behörde in einem EU-Mitgliedstaat unter Einhaltung der in der Verordnung vorgesehenen Verfahren (siehe 1.4.9) eine finanzielle Sanktion gegen einen Diensteanbieter erwirken, der sich in einem anderen EU-Mitgliedstaat befindet.

Das e-Evidence-Paket führt ein zentrales Register der Niederlassungen und gesetzlichen Vertreter von Diensteanbietern ein, die in der EU eine unter die Verordnung fallende Dienst-

[24] BJ, Bericht zum US Cloud Act, S. 24 ff.

leistung anbieten. Dank diesem Register können die Strafverfolgungsbehörden ihre Anfragen schnell an die zuständige Stelle richten. Ein solches Register ist vom US CLOUD Act nicht vorgesehen.

Bezüglich der Datenverschlüsselung sind sowohl der CLOUD Act als auch das e-Evidence-Paket neutral. Denn keines dieser Instrumente sieht vor, dass die Diensteanbieter die ihnen vorliegenden Daten vor dem Versand entschlüsseln müssen, was für die Strafverfolgungsbehörden in der Praxis einige Komplikationen mit sich bringen dürfte.

5.4 Öffnung gegenüber anderen Staaten

Der US CLOUD Act sieht für Staaten, die dies wünschen und aus Sicht der USA einen gewissen rechtstaatlichen Standard erfüllen, die Möglichkeit vor, ein *Executive Agreement* mit den USA abzuschliessen. Dadurch können die Behörden anderer Staaten Anordnungen direkt an US-Diensteanbieter richten und umgekehrt. Angesichts der zunehmenden Globalisierung wird ein solches offenes System zu einer schnelleren internationalen Zusammenarbeit und damit zu einer besseren Bekämpfung der Kriminalität insgesamt führen.

Im e-Evidence-Paket ist keine Möglichkeit der Assoziierung für Drittstaaten vorgesehen. Im Gegenteil: Da es auf mehreren EU-Rechtsakten beruht, darunter Mechanismen zur Vereinfachung der Rechtshilfe wie die Europäische Ermittlungsanordnung, scheint es für einen Drittstaat schwierig zu sein, sich diesem System auf bilateralem Weg anzuschliessen.

5.5 Rechtskonflikte

Beide Systeme sehen Regeln für mögliche Rechtskonflikte vor. Unter dem US CLOUD Act sind diese jedoch sehr begrenzt. Nur der Diensteanbieter selbst – nicht aber der Staat in welchem der Anbieter seinen Sitz hat – kann sich auf einen solchen Rechtskonflikt berufen, und auch nur unter der Voraussetzung, dass ein *Executive Agreement* abgeschlossen wurde. Der Entscheid, ob ein Rechtskonflikt vorliegt oder nicht, obliegt dabei dem Staat, der die Daten anfordert.

Auch unter dem e-Evidence-System der EU ist es primär Sache des Diensteanbieters, einen Rechtskonflikt mit dem Recht eines Drittstaates oder mit dem Recht des Staates, in welchem der Diensteanbieter seine Niederlassung errichtet oder einen gesetzlichen Vertreter ernannt hat, geltend zu machen.[25] Der Diensteanbieter hat über seine Ablehnung zugleich aber auch die zuständige Behörde des Staates zu informieren, in welchem er seine Niederlassung errichtet oder einen gesetzlichen Vertreter ernannt hat. Wie beim US CLOUD Act ist es auch hier der Staat, der die Informationen anfordert, der darüber entscheidet, ob ein solcher Rechtskonflikt vorliegt oder nicht. Macht der Diensteanbieter einen der eingeschränkten Ablehnungsgründe gemäss dem Recht des Staates, in welchem er sich befindet, geltend, so entscheidet die anordnende Behörde (siehe 2.4.6), bei Geltendmachung einer Kollision mit dem Recht eines Drittstaates, obliegt der Entscheid dem zuständigen Gericht im anordnenden Staat (siehe 2.4.10).

Im Gegensatz zum US Cloud Act hat der anordnende Staat aber in bestimmten Fällen den Staat, in welchem der Diensteanbieter seine Niederlassung errichtet oder seinen gesetzlichen Vertreter ernannt hat, über die Anordnung zu notifizieren. Letzterer hat dann die Möglichkeit,

[25] Wobei in Bezug auf das Recht des Staates, in welchem der Diensteanbieter seine Niederlassung errichtet oder einen gesetzlichen Vertreter ernannt hat, die Ablehnung auf im Recht dieses Staates geschützte Immunitäten, Privilegien und die Presse- oder Meinungsäusserungsfreiheit beschränkt ist.

die Anordnung bei Vorliegen einer der in der Verordnung abschliessend genannten Verweigerungsgründe abzulehnen (siehe 2.4.6).[26]

6 Fazit

Die e-Evidence-Regeln der EU stellen einen wichtigen Schritt im Bereich des grenzüberschreitenden Zugriffs auf Daten als Beweismittel im Rahmen von Strafverfahren auf dem europäischen Kontinent dar. Durch die Festlegung klarer Regeln sowohl für die Präsenz von Diensteanbietern in der EU als auch für europäische Herausgabe- und Datenspeicherungsanordnungen stärkt die EU die internationale Zusammenarbeit in Strafsachen und berücksichtigt dabei – zumindest bis zu einem gewissen Grad – die grundlegenden Rechte der Personen, gegen die sich solche Verfahren richten, sowie den Schutz ihrer Daten. Die neuen Regeln dürften bei der Bekämpfung der grenzüberschreitenden Kriminalität eine entscheidende Rolle spielen.

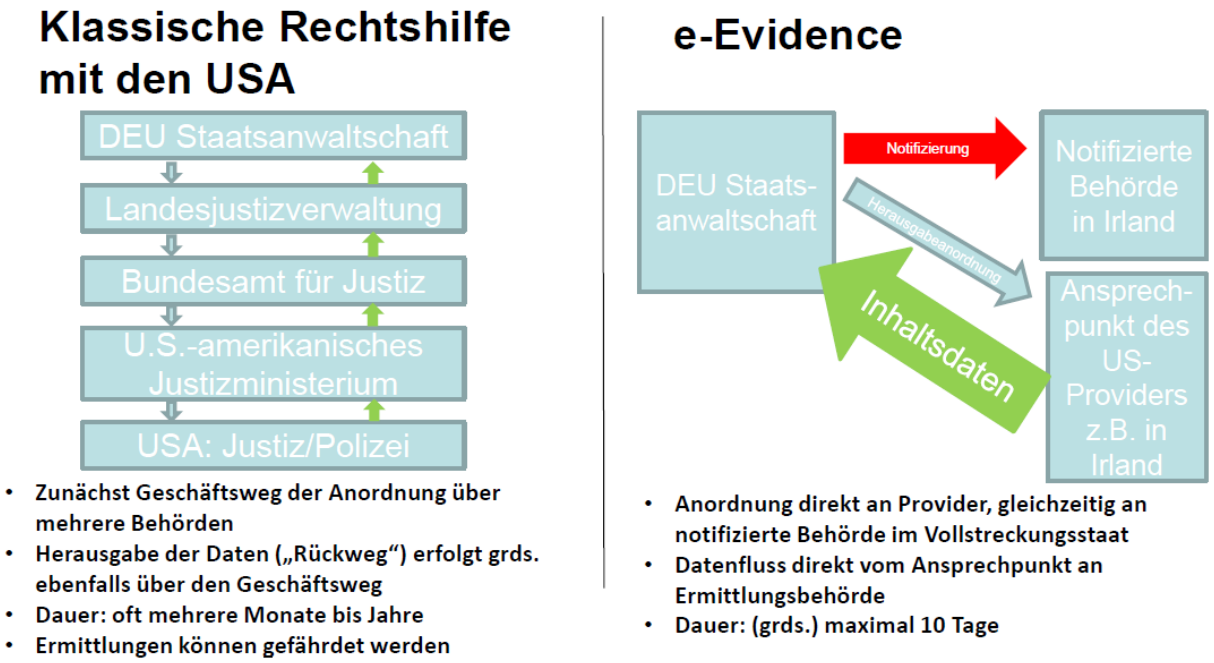

Abb.: Datenzugriff seitens einer deutschen Staatsanwaltschaft bei US-Provider unter e-Evidence-Regelung und unter klassischem Rechthilfeverfahren (Quelle: BMJ Deutschland)

Angesichts der Entwicklung in den Systemen ihrer wichtigsten Partner muss sich auch die Schweiz mit dem Thema e-Evidence auseinandersetzen. Das Schweizer Recht basiert derzeit ausschliesslich auf der Rechtshilfe, die relativ langsam und nicht auf elektronische Beweismittel zugeschnitten ist. Ein Alleingang der Schweiz scheint jedoch nicht zielführend. Elektronische Beweismittel stellen das Konzept der Territorialität in Frage und werden in verschiedenen Staaten von Unternehmen gespeichert, die nicht alle dem Schweizer Recht unterstehen. Vor diesem Hintergrund scheint eine einseitige Schweizer Lösung schwer vorstellbar. Die Schweiz muss in der Lage sein, mit anderen Staaten zusammenzuarbeiten. Zum gegenwärtigen Zeitpunkt scheinen verschiedene Handlungsoptionen zu bestehen:

- Die erste Option besteht darin, nichts zu tun. Wie ausgeführt, handelt es sich hier um einen Bereich, der sich schnell entwickelt und immer häufiger Auswirkungen auf Strafverfahren hat. Nichts zu tun, würde eine Lücke schaffen, die Kriminelle ausnutzen

[26] Die Ablehnungsgründe umfassen dabei aber nicht das ganze Recht des ausführenden Staates, sondern sind beschränkt auf Immunitäten, Privilegien, die Presse- oder Meinungsäusserungsfreiheit, offenkundige Verletzungen eines einschlägigen Grundrechts gemäss der EU-Charta oder Art. 6 EUV, Verstoss gegen das ne bis in idem-Prinzip sowie die fehlende doppelte Strafbarkeit.

könnten. Ausserdem könnte es zu einem Rechtskonflikt (vgl. insb. Art. 271 StGB)[27] kommen, wenn die EU-Regelung zu e-Evidence in Kraft tritt.

- Das zweite Szenario wäre eine Anpassung des nationalen Rechts, um eine eigenständige Lösung zu entwickeln. Bei näherer Betrachtung lässt sich dieses Szenario in zwei Untervarianten unterteilen:

    - Zum einen könnte die Schweiz versuchen, einzig Rechtskonflikte zu vermeiden, die sich mit der e-Evidence-Regelung der EU ergäben. Sie würde ihr nationales Recht so anpassen, dass der ausländische Datenzugriff toleriert wird. Das wäre zwar technisch relativ einfach, hierbei würde die Schweiz den ausländischen Behörden allerdings etwas ermöglichen, ohne für ihre Behörden das entsprechende Gegenrecht zu erlangen.
    - Andererseits könnte die Schweiz versuchen, eine eigenständige Lösung zu entwickeln, die den Schweizer Behörden einen grösseren Zugang zu Daten mit Bezug zur Schweiz ermöglicht. 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 schwierig, all diese Diensteanbieter zur Ernennung einer gesetzlichen Vertretung oder der Errichtung einer Niederlassung in der Schweiz zu bewegen.

- Das dritte Szenario wäre ein Anknüpfen an das eine und/oder andere System. Wie erwähnt, sieht das e-Evidence-Paket eine solche Möglichkeit nicht ausdrücklich vor, der US CLOUD Act hingegen schon. Die EU und die USA verhandeln jedoch über ein Abkommen, um die internationale Zusammenarbeit im Bereich der elektronischen Beweismittel zu erleichtern. Die Schweiz könnte versuchen, ihr nationales Recht unter Berücksichtigung der beiden Systeme – und allenfalls der «Konfliktlösung» zwischen den beiden Akteuren EU und USA – autonom anzupassen. Diese Gesetzesrevision könnte die Möglichkeit vorsehen, mittels Staatsverträgen Brücken zu anderen Rechtssystemen zu bauen.
  Aufgrund der dargelegten 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 nicht nur auf die USA, sondern auch auf die EU und die schweizerischen Nachbarstaaten zu richten. Es stellt sich daher gar die Frage, ob die Schweiz evtl. eine Lösung erarbeiten könnte, welche sich auf die e-Evidence-Gesetzgebung der EU abstützt.

In jedem Fall muss die Schweiz handeln und dies rasch. 36 Monate nach dem 28. Juli 2023, also am 28. Juli 2026, wird die neue e-Evidence-Gesetzgebung in Kraft treten. Ab diesem Datum besteht, wenn keine Lösung gefunden werden konnte, 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 ihren Strafverfolgungsbehörden die Möglichkeit bietet, mit anderen Staaten oder zumindest mit Anbietern, die sich auf dem Territorium anderer Staaten befinden, zusammenarbeiten zu können.

[27] Wenn ein in der Schweiz domizilierter Diensteanbieter gemäss e-Evidence-Regelung einen Ansprechpunkt in einem EU-Staat errichtete, dort EU-Herausgabeanordnungen erhielte und gestützt auf diese 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.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de justice et police DFJP

Office fédéral de la justice OFJ

24 octobre 2023

Rapport sur le projet e-evidence de l'UE

BJ-D-FFB23401/87

Table des matières

1 Contexte

L'ère du numérique ne transforme pas seulement les différents aspects de nos existences, mais également les méthodes auxquelles ont recours les criminels dans le cadre de leurs activités. Ainsi, afin d'assurer l'efficacité de la poursuite pénale, il est indispensable que les autorités compétentes en la matière de même que les autres organismes qui participent à la lutte contre le crime s'adaptent à ces nouveaux développements. Cela comprend également l'adoption de **bases légales adéquates** pour une lutte efficace contre le crime.

Pour accompagner les défis inhérents à la révolution numérique sur le plan de la lutte contre le crime, de nouveaux instruments ont été et sont en train d'être négociés au niveau international. Ainsi, le Deuxième Protocole additionnel à la convention du Conseil de l'Europe sur la cybercriminalité a été adopté le 17 novembre 2021 afin de renforcer la coopération et de faciliter la transmission de preuves électroniques. En outre, une convention sur la cybercriminalité est en cours de négociation dans le cadre des Nations Unies. En parallèle, les États développent également leur législation en la matière : en novembre 2018, les États-Unis ont adopté le **Clarifying Lawful Overseas Use of Data Act (CLOUD Act)**, qui a pour but de permettre aux autorités de poursuite pénale d'accéder plus facilement aux données stockées à l'étranger. En raison de l'importance pratique du CLOUD Act, l'OFJ l'a examiné à la lumière du droit suisse et a publié le 17 septembre 2021 un rapport consacré à ce thème (rapport sur le US CLOUD Act (loi Cloud) ci-après : rapport CLOUD Act).

Face à ces développements, l'Union européenne (UE) n'est pas en reste et a adopté une nouvelle réglementation sur les preuves électroniques, appelé **paquet e-evidence**. Celui-ci s'inscrit dans le contexte des attentats de Bruxelles de 2016 : deux jours après les attentats, les ministres de la justice et de l'intérieur des États membres de l'UE ont exigé un meilleur accès aux preuves électroniques. Suite à cela, le Conseil de l'UE avait souligné à son tour le rôle essentiel revêtu par un accès efficace aux preuves électroniques afin de mieux lutter contre la criminalité grave et le terrorisme. Le 17 avril 2018, la Commission a présenté sa proposition de directive et de règlement en matière de preuves électroniques.

Le 13 juin 2023, le Parlement européen a adopté le paquet législatif e-evidence, qui a ensuite été approuvé par le Conseil de l'UE le 27 juin 2023, puis **publié au Journal officiel de l'UE le 28 juillet 2023**. Son but est de créer un cadre législatif cohérent dans le droit de l'UE afin de régler l'accès aux preuves électroniques et d'accélérer leur obtention. La nouvelle réglementation permet en particulier aux autorités de poursuite pénale des États membres de l'UE d'adresser directement leurs demandes de preuves aux fournisseurs de services dans d'autres États membres (« injonctions de production ») ou d'exiger la conservation de données pendant une période allant jusqu'à 60 jours afin d'éviter que les données concernées ne soient détruites ou perdues (« injonctions de conservation »). Elle crée ainsi un mécanisme alternatif à la procédure d'entraide judiciaire toujours applicable aujourd'hui.

La nouvelle réglementation pourrait également avoir des effets importants pour la Suisse, car les fournisseurs de services qui y sont établis et fournissent leurs services dans l'UE seront soumis en présence de certaines conditions aux nouveaux textes de loi. On pense par exemple aux services de communication comme Threema ou Protonmail. Toutefois, ces règles pourraient concerner également d'autres services numériques proposés par les entreprises suisses.

En complément au rapport CLOUD Act, le présent rapport vise à expliquer le contenu du paquet e-evidence de l'UE, à analyser les aspects de droit comparé et à mettre en évidence les conséquences et défis pour la Suisse de même que les différences par rapport au CLOUD Act américain. Enfin, le rapport explore les options qui s'offrent à la Suisse pour agir en la matière.

2 Contenu du paquet e-evidence

2.1 Condensé

Le paquet e-evidence se compose d'une directive, qui expose les principes essentiels du projet, et d'un règlement qui contient des dispositions détaillées.

La **directive**[1] oblige les fournisseurs qui proposent certains services numériques dans l'UE à désigner un établissement ou un représentant légal sur le territoire de l'UE auxquels les autorités des États membres peuvent adresser leurs injonctions de production et de conservation.

Le **règlement**[2] institue l'injonction européenne de production et l'injonction européenne de conservation. Il définit les conditions de l'obligation des fournisseurs de services qui proposent des services dans l'UE d'avoir un établissement sur le territoire de l'UE ou d'y désigner un représentant légal. Il règle en outre les conditions auxquelles les autorités (de poursuite pénale) compétentes d'un État membre de l'UE peuvent ordonner directement aux fournisseurs de services de produire ou de conserver des données.

Le règlement n'est pas applicable aux procédures engagées en vue de fournir une entraide judiciaire à un autre État membre de l'UE ou à un État tiers.

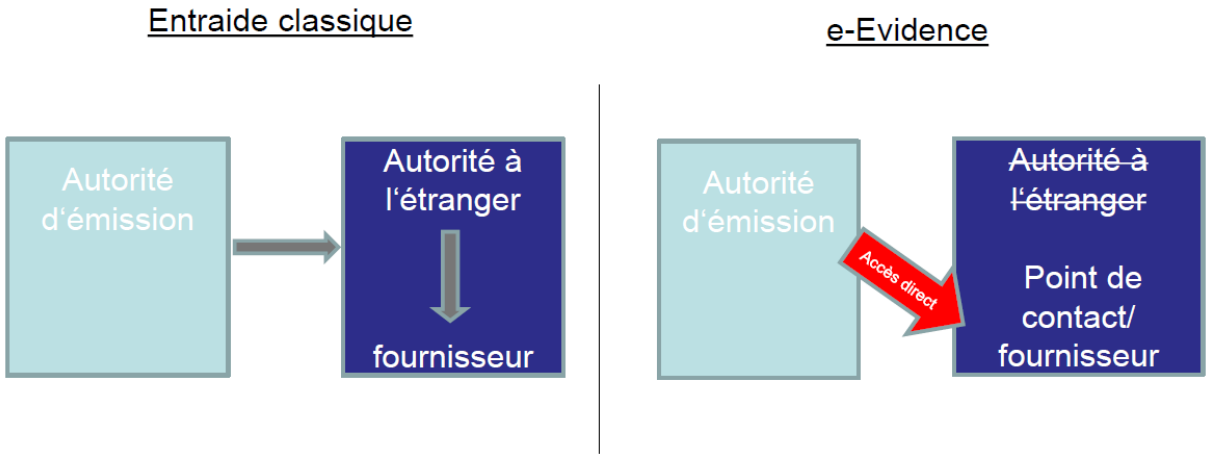

Illustration : fonctionnement du système e-evidence en comparaison avec la procédure classique d'entraide judiciaire

2.2 Bases légales au sein de l'UE

Comme mentionné, le paquet e-evidence repose sur deux instruments différents, un règlement et une directive. Bien que ces deux instruments se complètent, ils ne reposent toutefois pas sur les mêmes bases légales sur le plan du droit primaire.

La directive se fonde sur les art. 53 et 63 du traité sur le fonctionnement de l'Union européenne (TFUE). Ces deux articles figurent au titre IV du TFUE qui traite de la libre circulation des personnes, des services et des capitaux. En revanche, le règlement se base sur l'art. 82, par. 1 TFUE relatif à la reconnaissance mutuelle des jugements et au renforcement de la coopération

[1] DIRECTIVE (UE) 2023/1544 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 12 juillet 2023 établissant des règles harmonisées concernant la désignation d'établissements désignés et de représentants légaux aux fins de l'obtention de preuves électroniques dans le cadre des procédures pénales, JO L 191/181

[2] RÈGLEMENT (UE) 2023/1543 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 12 juillet 2023 relatif aux injonctions européennes de production et aux injonctions européennes de conservation concernant les preuves électroniques dans le cadre des procédures pénales et aux fins de l'exécution de peines privatives de liberté prononcées à l'issue d'une procédure pénale, JO L 191/118

judiciaire en matière pénale. Cet article figure au titre V du TFUE, qui traite de l'espace de liberté, de sécurité et de justice.

Bien que cette différence de base légale primaire puisse sembler anodine au premier abord, elle a des conséquences en pratique, car le Danemark et l'Irlande ont décidé de ne pas participer au titre V du TFUE. Alors que le Danemark a une option de retrait complète et ne prend part à aucun des instruments adoptés sur la base de ce titre, l'Irlande a une option de retrait partielle, ce qui signifie qu'elle peut au besoin participer à certaines initiatives de l'espace de liberté, de sécurité et de justice.

Pour le paquet e-evidence, cela signifie que le Danemark et l'Irlande doivent tous deux mettre en œuvre la directive mais non le règlement, et que contrairement au Danemark, l'Irlande a la possibilité de mettre en œuvre le règlement si elle le souhaite. Cependant, le règlement reprend plusieurs instruments de l'UE qui reposent sur le titre V, auxquels l'Irlande n'est pas forcément partie, raison pour laquelle une mise en œuvre du règlement e-evidence par cet État pourrait s'avérer compliquée en pratique[3].

2.3 Champ d'application

2.3.1 Fournisseurs de services

En premier lieu se pose la question des fournisseurs de services précisément visés par le paquet législatif.

Le règlement prévoit d'abord une condition de nature très générale selon laquelle on entend par fournisseur de services **toute personne physique ou morale qui fournit une ou plusieurs des catégories de services visés par le règlement**. Les services proposés exclusivement en dehors de l'UE n'entrent pas dans le champ d'application du règlement, même lorsque le fournisseur concerné possède un établissement dans l'UE. La question des fournisseurs concernés par le règlement dépend donc du type de prestations proposées par ceux-ci.

2.3.2 Services concernés

Ensuite se pose la question **des services** concernés concrètement par le règlement. Ceux-ci sont énumérés à l'art. 3, par. 3 du règlement. Il s'agit des services faisant partie des catégories suivantes.

2.3.2.1 Services de communications électroniques

Le règlement renvoie la définition fournie à l'art. 2, par. 4 de la directive (UE) 2018/1972 établissant le code des communications électroniques européen. Aux termes de cette directive, « est un service de communications électroniques », le service fourni normalement contre rémunération via des réseaux de communications électroniques qui comprend les types de services suivants :

- les services d'accès à Internet (en Suisse, par exemple **Swisscom, UPC-Sunrise**, etc.) ;
- les services de communications interpersonnelles, ce par quoi il y a lieu de comprendre, conformément à l'art. 2, par. 5 de la directive (UE) 2018/1972, un service normalement fourni contre rémunération qui permet l'échange direct d'informations entre un nombre fini de personnes, par lequel les personnes qui

[3] L'Irlande semble avoir décidé d'appliquer le règlement, voir le ch. 3 ci-dessous.

amorcent la communication ou y participent en déterminent le ou les destinataires (en Suisse, par exemple **Prontonmail ou Threema**) ;
- les services consistant entièrement ou principalement en la transmission de signaux tels que les services de transmission utilisés pour la fourniture de services de machine à machine et pour la radiodiffusion (par ex. **fournisseurs de blogs, services de vidéo à la demande ou réseaux sociaux**).

2.3.2.2 Services d'attribution de noms de domaine et de numérotation IP

Cela comprend les fournisseurs d'adresses IP, les services du bureau d'enregistrement de noms de domaine, ainsi que les fournisseurs qui proposent des services de proxy en lien avec des noms de domaine (en Suisse, par exemple **Switch, ProtonVPN**, etc.).

2.3.2.3 Autres services qui permettent à leurs utilisateurs de communiquer entre eux ou de stocker ou de traiter d'une autre manière des données pour le compte des utilisateurs auxquels le service est fourni

Sur ce point, le règlement renvoie à la description figurant à l'art. 1, par. 1, let. b de la directive UE 2015/1535, selon lequel le terme « service » désigne tout service de la société de l'information, c'est-à-dire tout service presté normalement contre rémunération, à distance, par voie électronique et à la demande individuelle d'un destinataire de services[4].

Cette description quelque peu compliquée et difficile à comprendre est illustrée par des exemples à l'annexe I de ladite directive qui la rendent plus compréhensible. Selon cette annexe, les services suivants **ne sont pas couverts** par la liste figurant à l'art. 1, par. 1, let. b :

- services prestés en présence physique du prestataire et du destinataire, même s'ils impliquent l'utilisation de dispositifs électroniques (examen ou traitement dans un cabinet de médecin au moyen d'équipements électroniques, mais en présence physique du patient ; consultation d'un catalogue électronique dans un magasin en présence physique du client ; réservation d'un billet d'avion via un réseau d'ordinateurs dans une agence de voyage en présence physique du client) **(a contrario, les services suivants couverts seraient : les magasins en ligne, fournisseurs de réservations en ligne de billets d'avion, etc.) ;**
- mise à disposition de jeux électroniques dans une galerie en présence physique de l'utilisateur **(a contrario, les services couverts seraient : les fournisseurs de jeux en ligne) ;**
- services dont le contenu est matériel même s'ils impliquent l'utilisation de dispositifs électroniques (distribution automatique de billets de banque ou de billets de train ; accès aux réseaux routiers, parkings payants, etc., même si à l'entrée et/ou à la sortie des dispositifs électroniques interviennent pour contrôler l'accès et/ou assurer le paiement correct **(a contrario, les services couverts seraient : les applications de parkings, application CFF, etc.) ;**
- services « off-line » (distribution de CD-ROM ou de logiciels sur disquette) **(a contrario, les services couverts seraient : les services en ligne) ;**
- services qui ne sont pas fournis au moyen de systèmes électroniques de stockage et de traitement de données (services de téléphonie vocale ; services de télécopieur/télex ; services prestés par téléphonie vocale ou télécopieur ; consultation d'un médecin par téléphone/télécopieur ; consultation d'un avocat par téléphone/télécopieur ; marketing direct par téléphone/télécopieur) **(a contrario, les services couverts seraient : les conseils fournis en ligne dans les domaines concernés) ;**

[4] Le terme « service presté à distance » désigne un service fourni sans que les parties soient simultanément présentes ; le terme « service presté par voie électronique » désigne un service envoyé à l'origine et reçu à destination au moyen d'équipements électroniques de traitement et de stockage de données, et qui est entièrement transmis, acheminé et reçu par fils, par radio, par moyens optiques ou par d'autres moyens électromagnétiques ; le terme « service presté à la demande individuelle d'un destinataire de services » désigne un service fourni par transmission de données sur demande individuelle.

- services non fournis à la demande individuelle d'un destinataire de services, mais par l'envoi de données sans appel individuel et destinés à la réception simultanée d'un nombre illimité de destinataires (transmission « point à multi-point ») (services de radiodiffusion télévisuelle (y compris la quasi-vidéo à la demande) ; services de radiodiffusion sonore ; télétexte (télévisuel)) **(a contrario, les services couverts seraient : les services fournis à la demande individuelle, par ex. les journaux en ligne ou les podcasts).**

Par ailleurs, l'art. 3, par. 4 précise ce qu'il faut comprendre par **« proposer / fournir des services dans l'Union »** : le fournisseur de services doit permettre aux personnes physiques ou morales dans un État membre d'utiliser les services **énumérés au par. 3)** et avoir un lien substantiel, fondé sur des critères factuels spécifiques, avec un État membre. Un tel lien substantiel est réputé exister :

- lorsque le fournisseur de services dispose d'un établissement dans l'UE ; ou
- lorsqu'il existe un nombre significatif d'utilisateurs dans un ou plusieurs États membres ; ou
- lorsqu'il existe un ciblage des activités sur un ou plusieurs États membres (par ex. du fait de l'usage d'une langue ou d'une devise généralement utilisée dans cet État membre ou du fait de la possibilité de commander chez lui des biens ou des services). Le ciblage des activités sur un État membre pourrait également être constaté sur la base de la disponibilité d'une application dans la boutique d'applications nationale correspondante, de la diffusion de publicité locale ou de publicité dans la langue généralement utilisée dans cet État membre, ou de la gestion des relations avec la clientèle, comme la fourniture d'un service à la clientèle dans la langue généralement utilisée dans cet État membre[5].

Par contre, la seule accessibilité dans l'UE d'un site Internet d'un fournisseur de services ou la publication d'une simple adresse e-mail ou d'autres données de contact du fournisseur de services ne suffisent pas à elles seules pour déterminer si un fournisseur de services propose des services dans l'Union[6].

→ Lorsqu'un fournisseur propose un service couvert par l'art. 3, par. 3 et qu'il existe un lien substantiel avec l'UE, il doit soit avoir un établissement dans l'UE, soit y désigner un représentant légal.

2.3.3 Données concernées

Le paquet e-evidence couvre uniquement les données qui concernent des services proposés dans l'UE. Si tel est le cas, l'emplacement des données ne joue aucun rôle (elles peuvent également se situer en dehors du territoire de l'UE).

2.3.3.1 Données relatives aux abonnés, au trafic et au contenu

Sont concernées les données relatives aux abonnés[7], les données demandées à la seule fin d'identifier l'utilisateur[8], les données relatives au trafic (données secondaires)[9] et les données

[5] Cf. considérant (30) du préambule du règlement.

[6] Cf. considérant (29) du préambule du règlement.

[7] Les données relatives aux abonnés recouvrent d'une part toutes les données qui permettent de déterminer l'identité d'un abonné ou d'un client, telles que le nom, la date de naissance, l'adresse, les données de facturation et de paiement, le numéro de téléphone ou l'adresse électronique fournis, et d'autre part les données relatives au type de service et à sa durée.

[8] Elles comprennent les adresses IP et, si nécessaire, les ports sources et les horodatages correspondants, à savoir la date et l'heure.

[9] Les données relatives au trafic recouvrent par exemple la source et la destination d'un message ou d'un autre type d'interaction, l'emplacement du dispositif, la date, l'heure, la durée, la taille, le routage, le format, le protocole utilisé et le type de compression, et d'autres métadonnées de communications électroniques et des données, autres que les données relatives aux abonnés, relatives au début et à la fin d'une session d'accès d'un utilisateur à un service, telles que la date et l'heure d'utilisation, la connexion et la déconnexion du service.

relatives au contenu[10] (art. 3, par. 9 à 12 du règlement). En revanche, la surveillance en temps réel, à savoir par exemple l'écoute téléphonique en temps réel, n'est pas possible.

2.3.3.2 Données protégées par le secret professionnel, par des immunités ou par des privilèges

Le règlement contient en outre des dispositions expressément consacrées aux données qui sont protégées par le secret professionnel, en vertu du droit de l'État d'émission (cf. art. 5, par. 9 s. du règlement). Lorsque ces données sont stockées ou traitées d'une autre manière par un fournisseur de services en tant que partie d'une infrastructure fournie à des professionnels soumis au secret professionnel, dans le cadre de leur activité professionnelle[11], une injonction européenne de production visant à obtenir des données relatives au trafic ou des données relatives au contenu ne peut être émise que :

- lorsque le professionnel soumis au secret professionnel réside dans l'État d'émission ;
- lorsque le fait de s'adresser à ce professionnel soumis au secret professionnel pourrait nuire à l'enquête ; ou
- lorsque le secret professionnel a été levé conformément au droit applicable.

Si l'autorité d'émission a des raisons de croire que les données relatives au trafic ou les données relatives au contenu demandées sont protégées par des immunités ou des privilèges accordés, en vertu du droit de l'État chargé de la mise en œuvre, ou qu'elles sont protégées, en vertu de la liberté de la presse ou de la liberté d'expression, elle peut demander des éclaircissements à l'État chargé de la mise en œuvre avant d'émettre l'injonction européenne de production.

2.4 Production et stockage des données : l'injonction européenne de production et l'injonction européenne de conservation

2.4.1 Injonction européenne de production (art. 5 du règlement)

L'injonction européenne de production permet à l'autorité compétente d'un État membre de demander directement à des fournisseurs de services établis ou représentés dans un autre État membre la production de données qui relèvent du champ d'application du paquet e-evidence.

L'injonction européenne de production doit être **nécessaire et proportionnée**. De plus, elle ne peut être émise que si une injonction similaire aurait pu être émise dans les mêmes conditions dans le cadre d'une procédure nationale similaire (art. 5, par. 2 du règlement).

En outre, une injonction de production est admise uniquement pour des **infractions pénales passibles d'une certaine quotité de peine**, étant précisé que cette quotité dépend du type de données :

- les données relatives aux abonnés et les données demandées à la seule fin d'identifier l'utilisateur peuvent être demandées pour toutes les infractions pénales ainsi que pour l'exécution d'une peine ou d'une mesure de sûreté privatives de liberté d'au moins quatre mois ;
- les données relatives au trafic et au contenu peuvent être demandées pour les infractions pénales punissables dans l'État d'émission d'une peine privative de liberté d'une durée d'au moins trois ans, pour certaines infractions énumérées dans des directives séparées (fraude et contrefaçon de moyens de paiement, abus

[10] Les données relatives au contenu recouvrent toutes les données dans un format numérique telles que du texte, de la voix, des vidéos, des images et du son, autres que les données relatives aux abonnés ou les données relatives au trafic.

[11] On pense par exemple au système de gestion électronique des dossiers d'une étude d'avocats.

sexuels et exploitation sexuelle d'enfants, pédopornographie, atteintes à des systèmes d'information) et pour l'exécution d'une peine ou d'une mesure de sûreté privatives de liberté d'au moins quatre mois.

2.4.2 Injonction européenne de conservation (art. 6 du règlement)

L'injonction européenne de conservation permet à l'autorité compétente d'un État membre d'obliger un fournisseur de services établi ou représenté dans un autre État membre de conserver des données spécifiques pendant une certaine période.

Elle doit être **nécessaire et proportionnée** afin d'empêcher le retrait, la suppression ou la modification de données en vue d'une demande d'entraide judiciaire, d'une décision d'enquête européenne[12] ou d'une injonction européenne de production.

Elle peut être est émise pour toutes les infractions pénales lorsqu'elle aurait pu être émise dans les mêmes conditions dans le cadre d'une procédure nationale similaire, et pour l'exécution d'une peine ou d'une mesure de sûreté privatives de liberté d'au moins quatre mois.

2.4.3 Autorité d'émission

Le règlement détermine également les autorités des États membres autorisées à demander des données, à savoir à émettre une injonction européenne de production ou de conservation et à l'adresser directement au fournisseur de services.

L'autorité de l'État d'émission qui peut exiger directement la production des données dépend du type de données concernées (art. 4 du règlement).

Les *données relatives aux abonnés* peuvent être demandées par un juge, une juridiction, un juge d'instruction ou un procureur compétents dans l'affaire concernée. En outre, toute autre autorité compétente désignée par son droit national comme compétente pour ordonner la collecte de telles données, conformément au droit national, peut demander la production de ces données, lorsque l'injonction est validée par un juge, une juridiction, un juge d'instruction ou un procureur dans l'État d'émission.

La production des *données relatives au trafic et au contenu* est plus restreinte. Elle peut être demandée par un juge, une juridiction ou un juge d'instruction compétents dans l'affaire concernée, ou par toute autre autorité compétente en vertu du droit de l'État d'émission, à condition que l'injonction ait été examinée et approuvée (validation) par un juge, une juridiction ou un juge d'instruction. Contrairement aux données relatives aux abonnés, les données relatives au trafic et au contenu ne peuvent pas être demandées par un procureur de manière autonome. Le Ministère public pourrait toutefois formuler une proposition en ce sens (cf. art. 4, par. 2, let. b du règlement) qui devrait ensuite être approuvée par une autorité judiciaire.

S'agissant de la conservation des données, une distinction est opérée en fonction du type de données : la conservation des données peut être demandée par un juge, une juridiction, un juge d'instruction ou un procureur ou par toute autre autorité compétente définie par l'État d'émission, conformément au droit national. Dans ce cas, un juge, une juridiction, un juge d'instruction ou un procureur doit déclarer l'injonction valable (validation).

[12] La décision d'enquête européenne est une décision judiciaire émise par une autorité judiciaire d'un État membre de l'UE qui vise à faire exécuter des mesures d'enquête en vue de recueillir des preuves en matière pénale dans un autre État membre.

2.4.4 Destinataires des injonctions

Les destinataires des injonctions de production sont les fournisseurs de services. Le principe est que l'injonction de production est adressée directement au fournisseur de services agissant en qualité de responsable du traitement (art. 5, par. 6 du règlement). La qualité de responsable du traitement est définie à l'art. 4, par. 7 du règlement général sur la protection des données de l'UE (RGPD)[13] :

> *Le « responsable du traitement » est la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement ; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre.*

L'injonction de production peut, à titre exceptionnel, être adressée directement au fournisseur de services qui stocke ou traite d'une autre manière les données pour le compte du responsable du traitement (sous-traitant)[14], lorsque le responsable du traitement ne peut pas être identifié malgré des efforts raisonnables de la part de l'autorité d'émission ou lorsque le fait de s'adresser à lui pourrait nuire à l'enquête. Dans ce cas, le sous-traitant est tenu d'informer le responsable du traitement de la production des données, sauf si l'autorité d'émission lui a demandé de s'en abstenir, afin de ne pas entraver la procédure pénale concernée (art. 5, par. 7 du règlement)[15].

L'art. 5, par. 8 du règlement contient en outre une limitation importante concernant les données qui sont stockées ou traitées d'une autre manière par un fournisseur de services pour une autorité publique. Pour ce type de données, une injonction de production ne peut être émise que si l'autorité publique est située dans l'État d'émission.

Tant les injonctions de production que les injonctions de conservation doivent être adressées directement à l'établissement ou au représentant légal désigné par le fournisseur de services concerné. Lorsque l'établissement ou le représentant légal désigné ne réagit pas, l'injonction de production peut être adressée dans les cas d'urgence à tout autre établissement ou représentant légal du fournisseur de services dans l'UE. Dans certains cas, l'État chargé de la mise en œuvre doit également être informé (cf. ch. 1.4.5).

2.4.5 Notification à l'État chargé de la mise en œuvre

Chaque État membre peut désigner une ou plusieurs autorités centrales compétentes pour la transmission administrative de certificats, d'injonctions ou de notifications, pour la réception de données et de notifications et pour la transmission de correspondance officielle.

Lorsque l'autorité d'émission requiert la production de données relatives au trafic ou au contenu, elle est tenue d'adresser une notification à l'autorité compétente de l'État chargé de la mise en œuvre (c'est-à-dire de l'État dans lequel le fournisseur de services est établi ou dans lequel il a désigné son représentant légal), en lui transmettant dans le même temps l'injonction de production (art. 8, par. 1 du règlement). Dans certains cas, une telle notification n'est pas nécessaire, notamment lorsque l'État d'émission a des motifs raisonnables de croire que l'infraction a été commise, est en train d'être commise ou est susceptible d'être commise sur

[13] Les considérants et dispositions du règlement renvoient directement aux dispositions pertinentes du RGPD et de la directive relative à la protection des données à caractère personnel.

[14] Aux termes de l'art. 4, par. 8, du RGPD, le « sous-traitant » est la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement.

[15] Dans ce domaine, le règlement e-evidence l'emporte sur le RGPD, qui prévoit un devoir d'information du responsable du traitement envers le sous-traitant.

son territoire, et que la personne dont les données sont demandées y est domiciliée (« critère du domicile »).

L'autorité chargée de la mise en œuvre dispose ensuite d'un délai de dix jours pour évaluer l'injonction et, en cas d'urgence, de 96 heures au plus (art. 12 du règlement ; cf. ci-dessous). Les motifs de refus sont énumérés de manière exhaustive dans le règlement (cf. ch. 2.4.6.). Lorsque l'autorité chargée de la mise en œuvre ne soulève aucune objection, le fournisseur de services est tenu de produire les données, ce qui signifie qu'une approbation active de la part de l'État chargé de la mise en œuvre n'est pas nécessaire (cf. ch. 2.4.7.).

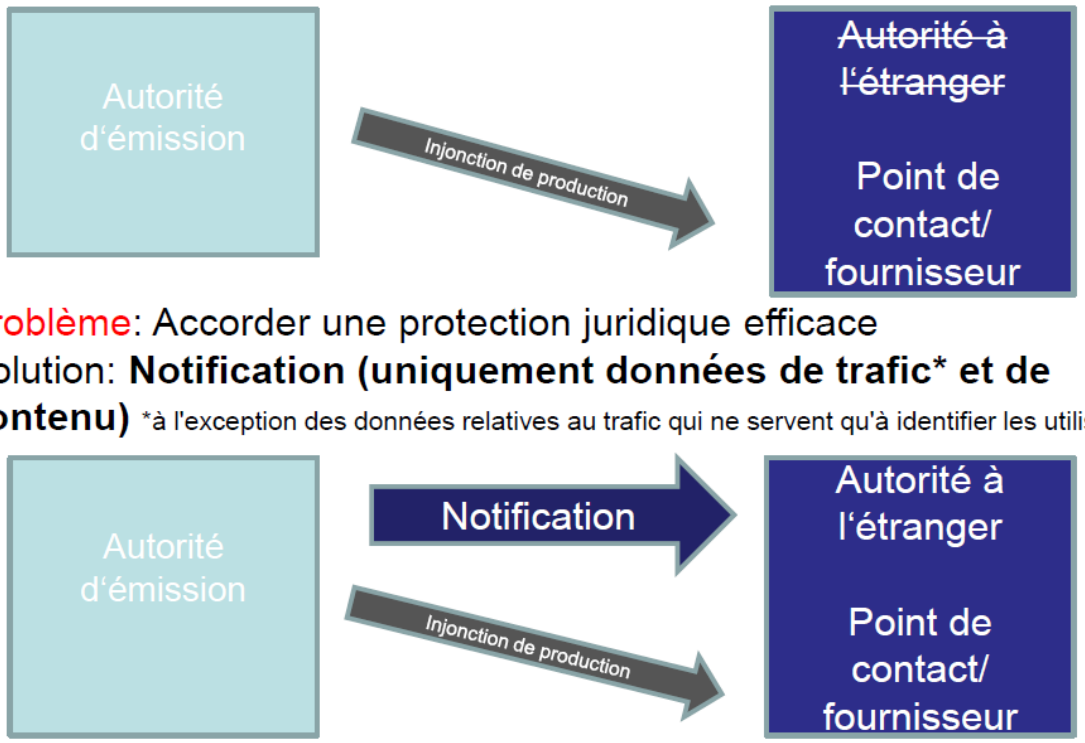

Illustration : implication de l'État chargé de l'exécution au moyen d'une « notification »

L'obligation de notifier a des limites strictes. Elle ne s'applique pas aux injonctions de conservation, ni aux injonctions de production de données relatives aux abonnés ou au trafic qui servent uniquement à identifier l'utilisateur. Cela peut avoir des conséquences graves si l'injonction vise l'identification de sources journalistiques ou de lanceurs d'alerte. Il incombe le cas échéant au fournisseur de services de faire valoir une violation de la liberté de la presse ou de la liberté d'expression, car l'État chargé de la mise en œuvre n'est pas informé (cf. ch. 2.4.6). Si le fournisseur de services n'invoque pas une telle violation, il peut arriver que des données soient produites alors qu'elles ne l'auraient pas été en raison de cette violation par la voie de la procédure d'entraide judiciaire. Le « critère du domicile » est également problématique, car son examen est laissé au seul pouvoir d'appréciation des autorités de poursuite pénale de l'État d'émission, qui ont finalement un intérêt significatif à ce que la notification n'ait pas lieu pour éviter que l'État, chargé de la mise en œuvre, n'invoque des motifs de refus. En outre, le règlement ne prévoit pas le cas de la notification à l'État dans lequel la personne concernée a son siège ou son domicile. Cela peut s'avérer problématique, en particulier lorsque ni l'autorité d'émission, ni l'autorité chargée de la mise en œuvre n'ont connaissance d'éventuelles immunités prévues par le droit de l'État tiers dans lequel est domiciliée la personne concernée[16].

[16] Voir à ce sujet l'avis critique de l'ONG European Digital Rights (EDRi), e-Evidence compromise blows a hole in fundamental rights safeguards, disponible sous : https://edri.org/our-work/e-evidence-compromise-blows-a-hole-in-fundamental-rights-safeguards/

2.4.6 Motifs de refus

Le règlement énumère plusieurs motifs de refus qui peuvent être invoqués à l'encontre d'une injonction de production ou de conservation tant par les destinataires d'une injonction que par l'État chargé de la mise en œuvre (à savoir son autorité centrale compétente pour recevoir les notifications).

Le destinataire d'une injonction (fournisseur de services) peut faire valoir que l'injonction enfreint des immunités, des privilèges, la liberté de la presse ou la liberté d'expression conformément au droit de l'État chargé de la mise en œuvre. En présence d'un tel grief, l'autorité d'émission doit décider s'il y a lieu de retirer, d'adapter ou de maintenir l'injonction (art. 10, par. 5 et art. 11, par. 4 du règlement).

Dans le même temps, l'État chargé de la mise en œuvre – à savoir l'autorité centrale chargée de recevoir les notifications – peut refuser une injonction (art. 12, par. 1 du règlement) :

- lorsque les données demandées sont protégées par des immunités ou des privilèges ou par la garantie de la liberté de la presse ou de la liberté d'expression, en vertu de son droit national ;
- dans des cas exceptionnels, lorsqu'il existe des motifs sérieux de croire, sur la base d'éléments précis et objectifs, que l'exécution de l'injonction entraînerait, en tenant compte des circonstances particulières de l'espèce, une violation manifeste d'un droit fondamental pertinent énoncé à l'art. 6 du traité sur l'Union européenne (TUE)[17] et dans la Charte des droits fondamentaux de l'Union européenne (Charte de l'UE) ;
- lorsque l'exécution de l'injonction serait contraire au principe *ne bis in idem*, ou
- lorsqu'il n'existe pas de double incrimination, à savoir que les faits pour lesquels l'injonction a été émise ne constituent pas une infraction au titre du droit de l'État chargé de la mise en œuvre, à moins qu'ils ne concernent une infraction figurant dans les catégories d'infractions énumérées à l'annexe IV, si ces faits sont passibles dans l'État d'émission d'une peine ou d'une mesure de sûreté privatives de liberté d'une durée maximale d'au moins trois ans.

Selon les ONG, le fait que le motif de refus inhérent aux droits humains soit limité à des situations exceptionnelles de violation des droits fondamentaux pourrait avoir pour effet de désavantager particulièrement les personnes qui résident dans des États, qui connaissent des défis sur le plan de l'État de droit, car ces personnes ne seraient plus en mesure de se protéger en recourant volontairement à un fournisseur de services établi dans un autre État. On pense par exemple aux militants des droits humains[18].

2.4.7 Exécution

Lorsqu'une notification à l'autorité chargée de la mise en œuvre au sens de l'art. 8 du règlement est nécessaire et que cette autorité n'a pas émis d'objections contre la production dans le délai prévu (cf. ch. 2.4.5), le fournisseur de services est tenu de transmettre les données demandées à la fin d'une période de dix jours directement à l'autorité d'émission compétente ou aux autorités de poursuite pénale indiquées dans l'injonction (art. 10, par. 2 du règlement). Lorsque l'autorité chargée de la mise en œuvre confirme avant même l'expiration du délai de dix jours qu'elle n'invoquera aucun motif de refus, le fournisseur de services est tenu d'agir dès que possible après cette confirmation et au plus tard à l'expiration de ce délai de dix jours. Lorsqu'une notification à l'autorité chargée de la mise en œuvre n'est pas nécessaire, le

[17] L'art. 6 TUE dispose notamment que les droits fondamentaux tels qu'ils sont garantis par la CEDH et tels qu'ils résultent des traditions constitutionnelles communes aux États membres font partie du droit de l'Union en tant que principes généraux.

[18] Voir à ce sujet l'avis critique de l'ONG European Digital Rights (EDRi), e-Evidence compromise blows a hole in fundamental rights safeguards, disponible sous : https://edri.org/our-work/e-evidence-compromise-blows-a-hole-in-fundamental-rights-safeguards/

fournisseur de services est tenu de transmettre les données directement à l'autorité d'émission ou aux autorités de poursuite pénale indiquées dans un délai de dix jours (art. 10, par. 3, du règlement).

En cas d'urgence, le fournisseur de services est tenu de transmettre les données demandées sans retard injustifié, au plus tard dans les huit heures suivant la réception de l'injonction de production (art. 10, par. 4, du règlement). Dans les cas où une notification à l'autorité chargée de la mise en œuvre est nécessaire (à savoir en présence de données relatives au trafic et au contenu), celle-ci peut notifier à l'autorité d'émission et au destinataire, au plus tard dans les 96 heures suivant la réception de la notification, ses objections ou les conditions auxquelles elle entend soumettre l'utilisation des données. Si les données ont déjà été produites, l'autorité d'émission doit les effacer ou restreindre d'une autre manière leur utilisation. Le point problématique est que la production des données a déjà eu lieu alors qu'il s'avère *a posteriori* qu'elle n'était pas autorisée.

Lorsque le fournisseur de services ne peut pas s'acquitter de la production ou de la conservation des données parce que l'injonction est incomplète, contient des erreurs manifestes ou ne contient pas suffisamment d'informations pour être exécutée, ou en raison d'une impossibilité de fait due à des circonstances qui ne lui sont pas imputables, il est tenu d'en informer sans délai l'autorité d'émission (art. 10, par. 6 et 7, et 11, par. 5 et 6, du règlement) ; si l'injonction a été notifiée à l'autorité chargée de la mise en œuvre en vertu de l'art. 8 du règlement, il doit aussi informer cette dernière.

L'injonction de conservation des données prend fin automatiquement après soixante jours, à moins que l'autorité d'émission ne confirme qu'une injonction de production ultérieure a été émise (art. 11 du règlement). Au cours de cette période de soixante jours, l'autorité d'émission peut prolonger la durée de la conservation de trente jours.

2.4.8 Information de l'utilisateur

L'autorité d'émission est tenue d'informer la personne concernée, sans retard injustifié, au sujet de la production de données (art. 13 du règlement). De plus, la section H de l'annexe I du règlement prévoit l'interdiction expresse pour le fournisseur de données d'informer la personne dont les données sont demandées, et dispose qu'il incombe à la seule autorité d'émission d'informer cette personne concernant la production des données. L'autorité d'émission peut, conformément au droit national de l'État d'émission, retarder ou limiter l'information de la personne dont les données sont demandées, ou ne pas informer cette personne, dans la mesure où, et aussi longtemps que, les conditions de l'art. 13, par. 3 de la directive de l'UE sur la protection des données[19] sont remplies. Dans ce cas, l'autorité d'émission indique dans le dossier les raisons du retard, de la limitation de l'information ou de la non-information et ajoute une brève justification dans l'injonction de production.

Le règlement ne règle pas expressément la manière dont la personne concernée doit être informée lorsqu'elle ne se trouve pas sur le territoire de l'autorité d'émission. Sur la base du texte de l'art. 13, qui mentionne uniquement l'autorité d'émission, il y a lieu de présumer que l'information est transmise en tous les cas par l'autorité d'émission, indépendamment du lieu de domicile de la personne concernée (qui peut être situé dans un État tiers). Par exemple, si une autorité allemande demande à un fournisseur de services français des données

[19] Voir l'art. 13, par. 3 : les États membres peuvent adopter des mesures législatives visant à retarder ou limiter la fourniture des informations à la personne concernée [...], ou à ne pas fournir ces informations, dès lors et aussi longtemps qu'une mesure de cette nature constitue une mesure nécessaire et proportionnée dans une société démocratique, en tenant dûment compte des droits fondamentaux et des intérêts légitimes de la personne physique concernée pour : a) éviter de gêner des enquêtes, des recherches ou des procédures officielles ou judiciaires ; b) éviter de nuire à la prévention ou à la détection d'infractions pénales, aux enquêtes, aux poursuites en la matière ou à l'exécution de sanctions pénales ; c) protéger la sécurité publique ; d) protéger la sécurité nationale ; e) protéger les droits et libertés d'autrui.

concernant une personne qui est domiciliée en France, c'est l'autorité allemande qui doit informer cette personne.

2.4.9 Sanctions et mise en œuvre

2.4.9.1 Sanctions

Les États membres doivent déterminer les sanctions pécuniaires applicables aux fournisseurs de services en cas de violations des art. 10 (exécution d'une injonction de production), 11 (exécution d'une injonction de conservation) et 13, par. 4 (confidentialité, secret et intégrité). Les sanctions pécuniaires prévues doivent être effectives, proportionnées et dissuasives et peuvent aller jusqu'à 2 % du chiffre d'affaires annuel mondial total du fournisseur de services pour l'exercice précédent (art. 15, par. 1 du règlement).

Les fournisseurs de services ne peuvent pas être tenus responsables du préjudice causé à leurs utilisateurs ou à des tiers qui résulte exclusivement du respect de bonne foi d'une injonction de production ou de conservation (art. 15, par. 2, du règlement).

2.4.9.2 Mise en œuvre

Lorsque le fournisseur de services ne respecte pas une injonction de production ou de conservation dans les délais impartis sans indication de motifs et que l'autorité de mise en œuvre n'a invoqué aucun des motifs de refus énumérés à l'art. 12, l'autorité d'émission peut demander à l'autorité chargée de la mise en œuvre de mettre en œuvre l'injonction de production ou de conservation (art. 16, par. 1 du règlement).

L'autorité chargée de la mise en œuvre doit statuer sans délai sur la reconnaissance de la décision de mise en œuvre, au plus tard dans un délai de cinq jours suivant la réception de la décision (art. 16, par. 2 du règlement).

L'autorité chargée de la mise en œuvre enjoint au fournisseur de services d'honorer ses obligations et l'informe dans le même temps :

- de la possibilité de former opposition contre l'exécution de l'injonction concernée en invoquant l'un des motifs de refus mentionnés dans l'injonction (cf. ch. 2.4.6). Si le fournisseur de services fait usage de cette possibilité, l'autorité chargée de la mise en œuvre doit décider sur la base des informations du fournisseur de services d'exécuter ou non l'injonction de production ou de conservation. Pour ce faire, elle peut demander des informations supplémentaires à l'autorité d'émission ;
- des sanctions / amendes applicables en cas de non-respect ;
- du délai pour se conformer à l'injonction ou formuler une objection.

La mise en œuvre d'une injonction de production ou de conservation peut être refusée par l'autorité chargée de la mise en œuvre dans un certain nombre de cas réglés de manière exhaustive dans le règlement, à savoir :

- lorsque l'injonction européenne de production n'a pas été émise ou validée par une autorité d'émission prévue à l'art. 4 ;
- lorsqu'elle n'a pas été émise pour une infraction prévue dans le règlement ;
- lorsque le fournisseur de services n'a pas pu se conformer à une injonction de production ou de conservation pour des motifs qui ne lui sont pas imputables ou parce que l'injonction contient des erreurs graves ;
- lorsque l'injonction de production ne concerne pas des données stockées par le fournisseur de services ou pour son compte au moment de la réception de l'injonction ;
- lorsque le service n'entre pas dans le champ d'application du règlement ;

- lorsque les données demandées sont protégées par des immunités ou des privilèges accordés, en vertu du droit de l'État chargé de la mise en œuvre, ou qu'elles sont couvertes par des règles relatives à la limitation de la responsabilité pénale, liées à la liberté de la presse ou à la liberté d'expression dans d'autres médias, qui empêchent l'exécution ou la mise en œuvre de l'injonction de production ;
- dans des situations exceptionnelles, lorsque sur la base des seules informations contenues dans l'injonction, il est évident qu'il existe des motifs sérieux de croire, sur la base d'éléments de preuve précis et objectifs, que l'exécution de l'injonction européenne de production entraînerait, dans les circonstances particulières de l'espèce, une violation manifeste d'un droit fondamental pertinent énoncé à l'art. 6 TUE et dans la Charte de l'UE.

L'autorité chargée de la mise en œuvre doit informer immédiatement l'autorité d'émission et le fournisseur de services de sa décision. Si l'autorité chargée de la mise en œuvre obtient du destinataire les données demandées dans l'injonction européenne de production, elle doit transmettre ces données sans délai à l'autorité d'émission.

Lorsqu'un fournisseur de services ne respecte pas les obligations, qui lui incombent conformément à une injonction de production ou de conservation dont le caractère exécutoire a été confirmé par l'autorité chargée de la mise en œuvre, cette autorité lui impose une sanction pécuniaire conformément à l'art. 15 du règlement.

2.4.10 Obligations juridiques contradictoires

Lorsqu'un fournisseur de services considère que la production des données demandées est en conflit avec une obligation découlant du droit applicable d'un pays tiers, il est tenu d'informer l'autorité d'émission et l'autorité chargée de la mise en œuvre des motifs pour lesquels il refuse l'exécution de l'injonction de production, dans un délai de dix jours à compter de la réception de celle-ci. Le refus ne peut se fonder sur le fait que le droit applicable de l'État tiers concerné ne contient pas de conditions ou de procédures similaires pour l'émission d'une injonction de production ni sur le seul fait que les données sont stockées dans un État tiers (art. 17, par. 1 s. du règlement).

Lorsque l'autorité d'émission entend maintenir l'injonction malgré le refus motivé, le tribunal compétent de l'État d'émission tranche le conflit. Il doit évaluer dans un premier temps s'il existe un conflit d'obligations, en examinant si le droit de l'État tiers est applicable aux circonstances spécifiques du cas d'espèce et, le cas échéant, si le droit de l'État tiers proscrit la communication des données concernées dans le cas concret. Si le tribunal constate qu'il n'existe pas de conflit au sens indiqué ci-dessus, il maintient l'injonction. Si en revanche, il parvient à la conclusion que le droit de l'État tiers proscrit la production des données concernées, il décide s'il y lieu de maintenir ou de lever l'injonction. Les critères sur lesquels doit se fonder cette évaluation sont énumérés en détail dans le règlement (art. 17, par. 6 du règlement).

Sur ce point, on peut à tout le moins se demander dans quelle mesure le tribunal de l'État d'émission peut effectivement être considéré comme une instance « neutre », lorsqu'il est amené à évaluer les intérêts de sa propre autorité d'émission au regard des intérêts d'un État tiers.

2.5 Voies de droit

Les voies de droit sont réglées à l'art. 18 du règlement, qui prévoit que la personne dont les données sont demandées a droit à des recours effectifs contre l'injonction de production. Si

cette personne est une personne suspecte ou prévenue, elle a droit à des recours effectifs pendant la procédure pénale dans le cadre de laquelle les données sont utilisées.

Le droit à des recours effectifs existe sans préjudice du droit de recours prévu par le RGPD.

Il doit être exercé devant un tribunal de l'État d'émission conformément au droit de cet État. Il comprend la possibilité de contester la légalité de la mesure, y compris sa nécessité et sa proportionnalité, sans préjudice des garanties des droits fondamentaux dans l'État chargé de la mise en œuvre.

Si la personne dont les données sont demandées est informée par l'État d'émission de la production de données, conformément à l'art. 13, par. 1 du règlement, cet État doit l'informer, également en temps utile, sur les possibilités de former un recours prévu par le droit national.

L'État d'émission est tenu de veiller à ce que ces recours puissent être effectivement exercés (art. 18, par. 3 du règlement). La formation de recours est régie par les délais et autres conditions applicables dans le cadre de procédures nationales similaires. À cet égard, il y a lieu de garantir que la personne concernée puisse exercer ces recours de manière effective.

Indépendamment des règles de procédure nationales, l'État d'émission et tout autre État membre auquel des preuves électroniques ont été transmises, en vertu du règlement, doivent garantir que les droits de la défense et l'équité de la procédure sont respectés lors de l'évaluation des preuves obtenues au moyen de l'injonction de production.

2.6 Système informatique décentralisé

Le paquet e-evidence prévoit la création d'un système informatique décentralisé destiné à garantir la fiabilité de la communication électronique et de l'échange de données entre les autorités compétentes et les fournisseurs de services ou uniquement entre les autorités compétentes.

Les établissements ou les représentants légaux désignés par les fournisseurs de services doivent avoir accès au système informatique décentralisé par l'intermédiaire de leurs systèmes informatiques nationaux respectifs afin de recevoir les injonctions de production et de conservation, de transmettre les données demandées et de communiquer avec les autorités compétentes.

Les coûts inhérents à l'installation, à l'exploitation et à la maintenance des points d'accès décentralisés du système informatique sont à la charge des États membres concernés. De plus, chaque État membre prend en charge les coûts relatifs à l'établissement et à l'adaptation de ses systèmes informatiques nationaux, afin de les rendre compatibles entre eux.

2.7 Délai de mise en œuvre

Le délai de mise en œuvre du paquet e-evidence est de 36 mois et a commencé à courir le 28 juillet 2023 au moment de la publication au Journal officiel de l'Union européenne[20].

3 Droit comparé

Le paquet e-evidence n'aura pas seulement des conséquences sur la Suisse, mais également sur d'autres États dont les fournisseurs de services exercent leur activité dans l'UE. C'est pourquoi la Suisse a pris contact avec plusieurs États afin d'échanger concernant leur position

[20] JO L 191 du 28 juillet 2023, p. 118

relative aux nouvelles règles de l'UE. Toutefois, la plupart de ces États n'ont pas encore procédé à une analyse détaillée du nouveau paquet législatif.

Le **Royaume-Uni** a conclu un *executive agreement* avec les États-Unis sur la base du CLOUD Act. En raison de son départ de l'UE, le Royaume-Uni ne sera pas tenu par la réglementation e-evidence. Il n'a pas encore pris position concernant le paquet e-evidence. Au vu de son adhésion au système du CLOUD Act américain, il semble peu probable que le pays s'intéresse de manière approfondie à la réglementation européenne.

L'**Islande** et la **Norvège**, deux États qui sont dans une situation similaire à celle de la Suisse, en ce sens qu'ils ne sont pas non plus membres de l'UE mais ont développé une forte coopération avec cette dernière en tant qu'États Schengen dans les domaines concernés, ne semblent pas non plus avoir entamé d'analyse au sujet du paquet e-evidence et de la coopération pénale internationale dans le domaine des preuves électroniques. Contrairement à la Norvège et à la Suisse, l'Islande a signé le Deuxième Protocole additionnel à la convention sur la cybercriminalité.

La Suisse a également eu des échanges avec le **Danemark**. Bien qu'il soit membre de l'UE, il dispose d'une option de retrait en ce qui concerne l'espace de liberté, de sécurité et de justice, ce qui signifie qu'il ne met pas en œuvre les règlements fondés sur ce domaine de compétences de l'UE. Comme mentionné plus haut, alors que le règlement est basé sur l'espace de liberté, de sécurité et de justice, ce n'est pas le cas de la directive e-evidence, raison pour laquelle le Danemark doit mettre en œuvre la directive mais pas le règlement. Cependant, la directive prévoit en substance que les États qui ne participent pas au règlement doivent prendre les mesures nécessaires pour que les fournisseurs de services établis sur leur territoire nomment un représentant légal dans l'UE. Le Danemark est actuellement en train d'analyser la manière de mettre en œuvre la directive sans le règlement.

La situation de l'**Irlande** est différente puisqu'elle dispose d'une option de retrait flexible, qui lui permet de décider de manière autonome à quels projets législatifs elle souhaite participer dans le domaine de l'espace de liberté, de sécurité et de justice. En raison du grand nombre de fournisseurs de services établis sur son territoire, l'Irlande a un intérêt particulier à participer au paquet e-evidence afin d'éviter que ces fournisseurs de services ne soient contraints de désigner un représentant dans un autre État membre de l'UE. Cependant, le règlement renvoie à certains instruments auxquels l'Irlande n'a pas adhéré.

L'Irlande a indiqué peu après le Brexit, alors que les négociations du paquet e-evidence étaient en cours, qu'elle entendait participer à cette initiative. Aussi est-elle en train de modifier son droit national afin que les injonctions européennes de production et de conservation prises sur la base du paquet e-evidence puissent être adressées directement aux fournisseurs de services établis en Irlande. Elle espère pouvoir mettre en œuvre le règlement même si elle n'a pas repris tous les instruments sur lesquels se fondent ses dispositions (par exemple, la décision d'enquête européenne). En modifiant son droit national, elle vise une mise en œuvre de la directive dès son entrée en vigueur.

Enfin, les **États-Unis** et l'UE négocient, depuis plusieurs années, un accord qui règlerait l'accès aux preuves électroniques entre les deux entités. Si les médias et le *Departement of justice* américain parlent principalement d'un *executive agreement*, les informations en possession de la Suisse semblent plutôt indiquer que les deux entités négocient un accord international indépendant qui permettrait de créer un pont entre le système américain et le système européen. Après une période de gel des négociations en 2020 en raison d'une part de la pandémie et d'autre part des délibérations relatives au paquet e-evidence dans l'UE, les

discussions ont maintenant repris. Il semble que l'instrument en cours de négociation ait pour but d'éviter que les fournisseurs de service soient soumis à des obligations contradictoires puisqu'ils seraient assujettis dans les faits tant au CLOUD Act qu'au projet e-evidence.

4 Conséquences pour la Suisse

S'il est vrai que le paquet e-evidence aura principalement des conséquences pour les États membres de l'UE, ou en tout cas pour ceux qui y participent, il devrait avoir également des répercussions sur la Suisse, non seulement au vu de sa proximité territoriale avec l'UE, mais également en raison des liens étroits qu'elle entretient avec les États de l'UE. Ces répercussions concerneront principalement les fournisseurs de services établis en Suisse, mais pas uniquement.

4.1 Conséquences pour les fournisseurs de services

Les fournisseurs de services établis en Suisse qui proposent ou souhaitent proposer sur le marché européen des services couverts par le paquet e-evidence (cf. ch. 2.3.1), seront soumis à la réglementation de l'UE.

Il en résulte d'une part qu'ils devront désigner un représentant légal dans un État membre de l'UE, dans la mesure où ils n'y transfèrent pas leur établissement, et d'autre part, que les autorités européennes de poursuite pénale pourront adresser directement leurs injonctions de production et de conservation à ce représentant. Le fournisseur de services devra se conformer à ces injonctions, ce qui signifie qu'il devra produire ou conserver les données demandées par une autorité de poursuite pénale de l'UE en vue d'une procédure pénale en dehors de la Suisse. Cela entraîne le risque que des données stockées en Suisse soient transmises à l'étranger sans recours à l'entraide pénale internationale et aux garanties de procédure qu'elle offre.

De plus, il incombera aux fournisseurs de services établis en Suisse d'invoquer d'éventuels conflits de lois ou violations du droit suisse. Lorsqu'un fournisseur de services invoquera un tel conflit de lois, le tribunal de l'État d'émission devra statuer à ce sujet. Partant, il reviendra aux fournisseurs de services, et donc à des entités privées, de veiller au respect du droit suisse et d'éviter d'éventuels conflits de lois entre les obligations du fournisseur de services conformément au droit suisse et celles issues du paquet e-evidence.

4.2 Autres conséquences

La Suisse et l'UE ont développé depuis de nombreuses années des relations privilégiées fondées sur les accords bilatéraux. La coopération internationale en matière pénale entre la Suisse et l'UE et ses États membres se fonde sur les instruments du Conseil de l'Europe et est complétée par l'association de la Suisse à l'accord de Schengen[21] et à l'accord sur la lutte contre la fraude[22]. Le paquet e-evidence ne fait pas partie de la coopération Schengen ni d'un autre accord bilatéral entre la Suisse et l'UE. C'est pourquoi, outre les effets mentionnés ci-dessus pour les fournisseurs de services établis en Suisse, le paquet e-evidence n'aura pas de conséquences directes pour la Suisse lors de son entrée en vigueur.

Afin de pouvoir continuer à lutter efficacement contre la criminalité, la Suisse devra adapter sa législation en matière de preuves électroniques. La Suisse ne peut faire cavalier seul, car une législation purement nationale ne saurait garantir un accès transfrontalier effectif aux données

[21] Accord entre la Confédération suisse, l'Union européenne et la Communauté européenne sur l'association de la Confédération suisse à la mise en œuvre, à l'application et au développement de l'acquis de Schengen, RS 0.362.31

[22] Accord de coopération entre la Confédération suisse, d'une part, et la Communauté européenne et ses États membres, d'autre part, pour lutter contre la fraude et toute autre activité illégale portant atteinte à leurs intérêts financiers, RS 0.351.926.8

en tant que moyens de preuve dans le cadre de procédures pénales. Dans le cadre d'une action législative isolée, la Suisse devrait au contraire être en mesure d'obtenir la présence et la coopération de tous les fournisseurs de services concernés en Suisse. Au vu des rapports de force géopolitique, cela ne semble guère réaliste. C'est pourquoi la dimension transfrontalière de l'accès aux données restera très importante pour la Suisse dans la pratique. L'UE étant un partenaire important de la Suisse dans de nombreux domaines,, il est indispensable que la Suisse intègre le paquet e-evidence, ses opportunités et ses risques, dans ses réflexions sur la réorganisation de la collecte des preuves électroniques.[23].

Par ailleurs, le paquet e-evidence prévoit la mise en place d'un registre des fournisseurs de services. Si un tel registre venait à être disponible, par exemple par le biais d'Eurojust, il serait utile aux autorités suisses pour savoir dans quel État les fournisseurs de services ont un établissement. Elles pourraient adresser leurs demandes d'entraide directement au bon État.

5 Différences entre le paquet e-evidence et le US Cloud Act

Le CLOUD Act et le paquet e-evidence de l'UE poursuivent tous deux l'objectif de faciliter l'accès aux preuves électroniques et de lutter plus efficacement contre la criminalité transnationale. Les prochains paragraphes mettent en évidence les différences et similarités entre les deux instruments.

5.1 Territorialité et accès transnational

La première différence concerne la question de la territorialité. Le paquet e-evidence de l'UE vise tous les fournisseurs de services qui proposent leurs services dans l'UE, avec pour conséquence que les fournisseurs de services qui sont établis en dehors de l'UE devront y nommer un représentant légal. Le CLOUD Act se concentre quant à lui sur le lien étroit que doit avoir un fournisseur de services avec les États-Unis. Il s'applique aux fournisseurs de services établis sur le territoire américain ou qui y ont une filiale ou une succursale. Dans certains cas, il s'applique même à ceux qui font de la publicité pour leurs services sur le marché américain. Le CLOUD Act ne se fonde pas sur le critère de la présence aux États-Unis et n'exige pas non plus que les fournisseurs de services qui y sont soumis aient une telle présence sur le territoire américain. Les fournisseurs de services sont tenus de produire les données qui se trouvent sur leurs serveurs, indépendamment du fait que les données soient stockées aux États-Unis ou à l'étranger. Des injonctions de production en vertu du CLOUD Act peuvent notamment être adressées à un établissement suisse d'un fournisseur de services aux États-Unis. Si de tels accès « extraterritoriaux » aux données ne posent pas de problème dans le système juridique américain, ils peuvent cependant engendrer des conflits avec les systèmes juridiques des États où se trouvent les données. En revanche, le système de l'UE « domestique » les données. En raison de l'obligation de présence des fournisseurs de services, aucune injonction n'est jamais envoyée dans des territoires situés en dehors de l'UE, mais elle est toujours adressée au siège ou au représentant légal désigné dans l'UE. Toutefois, ce dernier doit également avoir accès à toutes les données de l'entreprise, indépendamment de l'endroit où elles sont stockées. Les fournisseurs de services qui sont concernés par le règlement de l'UE doivent transmettre toutes les données de leur entreprise, indépendamment du lieu où celles-ci sont stockées.

Les deux systèmes prévoient un accès transnational aux données, et simplifient l'accès transfrontalier aux données. Alors que le système de l'UE « oblige » les fournisseurs de services à être présents sur le territoire de l'UE et exige l'accès à toutes les données de l'entreprise depuis la centrale de l'UE, le système américain se base sur les liens des

[23] Voir les réflexions figurant au ch. 6.

fournisseurs de services avec les États-Unis. Un fournisseur de services qui a ce lien avec le système juridique américain, tel qu'il est compris par les États-Unis, est tenu de fournir toutes ses données, quel que soit l'endroit où elles se trouvent.

En outre, le CLOUD Act prévoit la possibilité de conclure des *executive agreements* qui permettent aux autorités américaines d'envoyer des demandes aux fournisseurs de services qui ne sont pas établis sur le territoire américain mais se trouvent dans des États avec lesquels un *executive agreement* a été conclu et vice et versa.

5.2 Protection des données à caractère personnel et des droits humains

Tant le CLOUD Act que le paquet e-evidence contiennent des dispositions relatives à la protection des données. Les dispositions du paquet e-evidence doivent respecter les standards de protection des données de l'UE, en particulier le RGPD. La Suisse n'étant pas membre de l'UE, le RGPD ne s'y applique pas directement puisqu'il ne s'agit pas d'un développement de l'acquis de Schengen. Toutefois, la Suisse a révisé sa législation en matière de protection des données afin de tenir compte de l'évolution intervenue dans ce domaine sur le plan international et européen. La nouvelle mouture de la loi sur la protection des données (LPD, RS 235.1) est entrée en vigueur le 1er septembre 2023. Les dispositions du RGPD s'appliquent à des entreprises en Suisse qui relèvent du champ d'application du règlement (art. 3 RGPD). C'est le cas lorsque le fournisseur de services est établi dans l'UE ou, à défaut d'établissement, lorsque le traitement des données s'inscrit dans le cadre de l'offre de biens ou de services dans l'UE à des personnes concernées ou du suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union.

La Suisse dispose d'une décision d'équivalence de l'UE qui la reconnaît comme un État tiers disposant d'un niveau adéquat de protection des données, ce qui permet un échange de données sans obstacle. Elle peut donc considérer que l'application du paquet e-evidence remplira les standards européens en la matière et ne compromettra pas cette équivalence, puisque les entreprises visées seront soumises tant aux règles européennes qu'aux règles suisses.

En revanche, les standards de protection des données prévus par le CLOUD Act diffèrent des standards suisses. Le rapport CLOUD Act parvient à la conclusion que le traitement des données effectué dans le cadre d'une procédure basée sur le CLOUD Act peut être qualifié de problématique à la lumière de plusieurs éléments du RGPD[24].

Sur le plan des droits humains, le droit suisse a davantage de points communs avec les dispositions en matière d'e-evidence qu'avec celles du CLOUD Act. Les États membres de l'UE sont tous membres du Conseil de l'Europe et sont soumis de ce fait à la Convention européenne des droits de l'homme (CEDH). Le paquet e-evidence sera appliqué en concordance avec cet instrument auquel la Suisse est également partie. Cela concerne en particulier la garantie de l'accès au juge consacrée à l'art. 6 CEDH et à l'art. 29*a* Cst. Les dispositions du paquet e-evidence garantissent également le droit à des recours effectifs à la personne concernée par le transfert des données. Le CLOUD Act ne prévoit pas la possibilité pour la personne concernée d'accéder à un juge.

5.3 Aspects procéduraux

Tant le CLOUD Act que le paquet e-evidence prévoient que les injonctions sont transmises directement par les autorités d'un État à un fournisseur de services dans un autre État. Les

[24] OFJ, rapport CLOUD Act, pp. 23 ss.

autorités de l'État dans lequel se trouve le fournisseur de services ne participent en principe pas à la collecte des données. On pourrait parler de « privatisation de l'entraide pénale internationale ». Dans le paquet e-evidence, cet effet est quelque peu nuancé par l'obligation de notification. Si la demande porte sur la production de données relatives au trafic ou au contenu, l'autorité d'émission est tenue d'informer de l'injonction tant le fournisseur de services que l'autorité compétente dans l'État dans lequel le fournisseur de services est établi ou a désigné un représentant légal (cf. ch. 2.4.5).

Ce mécanisme n'est pas prévu par le CLOUD Act ni par l'*executive agreement* conclu entre les USA et le Royaume-Uni. L'État sur le territoire duquel se trouve le fournisseur de services n'a aucune connaissance des demandes reçues par les fournisseurs qui se trouvent sur son territoire, et ce malgré l'*executive agreement*.

Un autre aspect important qu'il sied de mentionner est celui de l'utilisation de la contrainte ou de l'exécution des injonctions. Le CLOUD Act prévoit que les autorités de poursuite pénale ne peuvent utiliser aucune mesure de contrainte sur le territoire d'un autre État. Si un fournisseur de services d'un État ayant conclu un *executive agreement* avec les États-Unis refuse de transmettre les données demandées, les autorités américaines doivent passer par la voie de l'entraide pénale internationale pour obtenir ces données. Quant au paquet e-evidence, il prévoit que l'injonction est dans ce cas mise en œuvre au moyen des mécanismes prévus par le règlement sans passer par l'entraide judiciaire. Une autorité d'émission d'un État membre de l'UE peut, moyennant le respect des procédures prévues par le règlement (cf. ch. 1.4.9), prononcer une sanction financière à l'encontre d'un fournisseur de services qui se trouve sur le territoire d'un autre État membre de l'UE.

Le paquet e-evidence institue un registre central des établissements et représentants légaux des fournisseurs qui offrent dans l'UE des services entrant dans le champ d'application du règlement. Grâce à ce registre, les autorités de poursuite pénale sont en mesure d'adresser rapidement leurs demandes aux entités compétentes. Le CLOUD Act ne met pas en place ce type de registre.

Ni le CLOUD Act, ni le paquet e-evidence n'ont d'effet en matière de chiffrement des données. Aucun de ces instruments ne prévoit l'obligation pour les fournisseurs de données de décrypter les données en leur possession avant de les envoyer, ce qui pourrait engendrer quelques difficultés pratiques pour les autorités de poursuite pénale.

5.4 Ouverture à d'autres États

Le CLOUD Act prévoit la possibilité, pour les États qui le souhaitent et qui remplissent certains critères sur le plan de l'État de droit du point de vue des États-Unis, de conclure des *executive agreements* avec ces derniers, sur la base desquels les autorités d'autres États pourront faire parvenir des injonctions directement aux fournisseurs de services américains et vice et versa. Au vu de la mondialisation croissante, un tel système ouvert permettra d'accélérer la coopération internationale et de mieux lutter contre la criminalité de manière générale.

Le paquet e-evidence ne contient pas de possibilité d'ouverture à d'autres États, bien au contraire : étant donné qu'il repose sur plusieurs actes de l'UE, notamment sur des mécanismes visant à simplifier l'entraide comme la décision d'enquête européenne, il serait difficile pour un État tiers d'adhérer à ce système par la voie bilatérale.

5.5 Conflits de lois

Les deux systèmes prévoient des règles relatives à d'éventuels conflits de lois. Les règles prévues par le CLOUD Act sont toutefois très limitées : seul le fournisseur de services – et non l'État dans lequel il a son siège – est autorisé à invoquer un tel conflit de lois, et uniquement à la condition qu'un *executive agreement* ait été conclu. C'est l'État qui demande les données qui doit ensuite décider s'il existe ou non un conflit de lois dans le cas d'espèce.

Dans le cadre du système e-evidence, il revient également principalement au fournisseur de services d'invoquer un conflit de lois avec un État tiers ou l'État dans lequel il a installé son établissement ou a désigné un représentant légal[25]. Le fournisseur doit cependant également informer de son refus l'autorité compétente de l'État dans lequel il a installé son établissement ou désigné un représentant légal. Comme sous l'empire du CLOUD Act, c'est l'État qui demande les informations qui décide si l'on est ou non en présence d'un conflit de lois. Lorsque le fournisseur de services invoque l'un des motifs de refus limités conformément au droit de l'État dans lequel il se trouve, c'est l'autorité d'émission qui décide (cf. ch. 2.4.6) ; en cas d'invocation d'un conflit avec le droit d'un État tiers, la décision incombe au tribunal compétent de l'État d'émission (cf. ch. 2.4.10).

Contrairement au CLOUD Act américain, l'État d'émission doit dans certains cas adresser une notification concernant l'injonction à l'État dans lequel le fournisseur de services a installé son établissement ou désigné son représentant légal. Le fournisseur a ensuite la possibilité de refuser l'injonction en présence de l'un des motifs de refus énumérés de manière exhaustive dans le règlement (cf. ch. 2.4.6)[26].

6 Conclusion

Les règles e-evidence de l'UE représentent une avancée significative dans le domaine de l'accès transfrontalier aux données en tant que moyens de preuves dans le cadre de procédures pénales sur le continent européen. En établissant des règles claires, relatives tant à la présence des fournisseurs de services dans l'UE qu'aux injonctions européennes de production et de conservation, l'UE renforce la coopération internationale en matière pénale en tenant compte – au moins jusqu'à un certain point – des droits fondamentaux des personnes visées par de telles procédures et de la protection de leurs données. Ces nouvelles règles seront amenées à jouer un rôle crucial dans la lutte contre la criminalité transfrontalière.

[25] Étant précisé, en relation avec le droit de l'État dans lequel le fournisseur de services a installé son établissement ou désigné un représentant légal, que les motifs de refus sont limités aux immunités, privilèges et garanties de la liberté de la presse et d'expression prévus par le droit de cet État.

[26] Les motifs de refus ne couvrent pas l'intégralité du droit de l'État chargé de la mise en œuvre, mais sont limités aux immunités, privilèges, garanties de la liberté de la presse et de la liberté d'expression, violations manifestes d'un droit fondamental applicable conformément à la Charte de l'UE ou de l'art. 6 TUE, violation du principe ne bis in idem et absence de double incrimination.

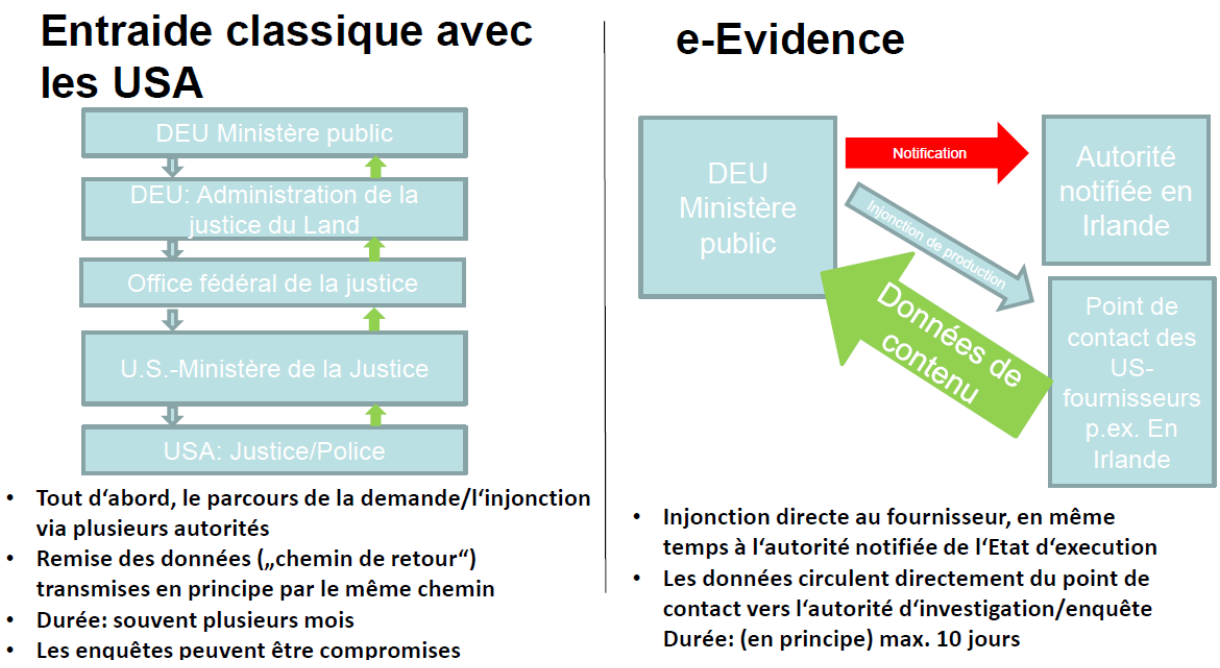

Illustration : accès aux données par un procureur allemand auprès d'un fournisseur de services américain conformément à la réglementation e-evidence et à la procédure d'entraide judiciaire classique (source : ministère allemand de la justice)

Compte tenu de l'évolution des régimes de ses principaux partenaires, la Suisse doit également se pencher sur le thème de l'e-evidence. Actuellement, le droit suisse se fonde uniquement sur l'entraide internationale en matière pénale, qui est relativement lente et n'est pas adaptée aux preuves électroniques. Il ne paraît pas judicieux de faire cavalier seul. Les preuves électroniques remettent en cause le concept de territorialité et sont stockées dans différents États par des entreprises qui ne sont pas toutes soumises au droit suisse. Dans ce contexte, une solution suisse unilatérale semble difficilement envisageable. La Suisse doit être en mesure de coopérer avec d'autres États. À ce stade, plusieurs options sont envisageables.

- La première consiste à ne rien faire. Comme indiqué, il s'agit d'un domaine qui évolue rapidement et qui a de plus en plus souvent des incidences sur les procédures pénales. Ne rien faire aurait pour effet de créer une lacune dont les criminels pourraient se servir. En outre, un conflit de lois serait susceptible de survenir (cf. en particulier l'art. 271 CP)[27] lors de l'entrée en vigueur de la réglementation de l'UE en matière d'e-evidence.

- Le deuxième scénario serait de modifier le droit suisse afin de développer une solution autonome. En y regardant de plus près, ce scénario se décompose en deux options :

  - d'une part, la Suisse pourrait simplement essayer d'éviter les conflits de lois qui découleraient de la réglementation e-evidence. Elle pourrait adapter son droit national de sorte que l'accès étranger aux données soit toléré. Cela serait relativement simple à réaliser sur le plan technique, mais elle accorderait un droit aux autorités étrangères sans recevoir de contrepartie ;
  - d'autre part, la Suisse pourrait essayer de développer une solution autonome qui permettrait d'étendre l'accès des autorités suisses aux données qui ont un lien avec la Suisse. Cela aurait pour avantage qu'elle pourrait développer un droit qui serait conforme à ses propres principes juridiques et qui serait adapté à ses besoins. Cependant, des fournisseurs de services issus du monde entier offrent leurs services en Suisse. En tant que petit pays, il serait difficile pour

[27] Si un fournisseur de services domicilié en Suisse installait un point de contact dans un État de l'UE conformément à la réglementation e-evidence, y recevait des injonctions européennes de production et, sur cette base, produisait des données qui se trouvent en Suisse, il procéderait selon la conception suisse à des actes qui relèvent des pouvoirs publics. Il y aurait là un conflit avec l'art. 271 CP – et le fournisseur de services devrait à chaque fois requérir l'approbation du DFJP, ce qui est difficilement réalisable.

cette dernière d'amener tous ces fournisseurs de services à désigner un représentant légal sur son territoire ou d'y installer un établissement.

- Le troisième scénario pourrait consister en un rattachement à l'un ou l'autre des systèmes décrits ou aux deux. Le paquet e-evidence ne prévoit pas expressément une telle possibilité, contrairement au CLOUD Act. Cependant, l'UE et les États-Unis sont en train de négocier un accord visant à faciliter la coopération internationale dans le domaine des preuves électroniques. La Suisse pourrait tenter de modifier son droit national de manière autonome en tenant compte des deux systèmes et des solutions mises en place pour résoudre les conflits. Cette révision pourrait prévoir la possibilité de créer des ponts vers d'autres systèmes juridiques au moyen d'accords internationaux.
  Compte tenu des liens étroits existant entre la Suisse et l'UE dans les domaines de la coopération judiciaire et de la protection des données (en particulier dans le cadre de la coopération Schengen), eu égard également à la libre circulation des personnes (sur laquelle est fondée la directive e-evidence) et à l'accès au marché intérieur, également dans le domaine du numérique, il semble judicieux d'orienter les efforts non seulement sur les États-Unis, mais également sur l'UE et les États voisins de la Suisse. La question se pose même de savoir si la Suisse pourrait éventuellement élaborer une solution qui se fonde sur la législation e-evidence de l'UE.

Quoiqu'il en soit, la Suisse doit agir, et rapidement. La nouvelle législation e-evidence entrera en vigueur 36 mois après le 28 juillet 2023, à savoir le 28 juillet 2026. Si aucune solution ne devait être trouvée, il existe à partir de cette date le risque de conflit de lois avec le nouveau système de l'UE. Dans ce cadre, il y a lieu de garder à l'esprit que la Suisse ne doit pas mettre en danger ses accomplissements sur le plan de l'État de droit. Elle devrait toutefois viser en principe une solution qui permette à ses autorités de poursuite pénale de coopérer avec d'autres États, ou tout au moins avec des fournisseurs de services qui se trouvent sur le territoire d'autres États.