



Monika Simmler, Prof. Dr. iur., Assistenzprofessorin für Strafrecht, Strafprozessrecht und Kriminologie an der Universität St. Gallen

## Gegenüberstellung des Schweizer Rechts und der E-Evidence-Gesetzgebung der EU – eine Auslegeordnung

### Inhaltsübersicht:

- I. Einleitung
- II. Zwangsmassnahmen betreffend E-Evidence
  - 1. Arten und Voraussetzungen
    - a) Europäische Herausgabe- und Sicherungsanordnung
    - b) System nach StPO und BÜPF
    - c) Diskrepanz zwischen Eingriffsintensität und Rechtsschutz
  - 2. Datenkategorien
    - a) Inhalts- und Verkehrsdaten
    - b) Teilnehmer- und Zugangsdaten
  - 3. Verpflichtete Diensteanbieter
- III. Würdigung

### I. Einleitung

Die Bedeutung elektronischer Beweismittel («E-Evidence») wächst kontinuierlich. Sie stehen oft unter der Kontrolle ausländischer Diensteanbieter. Das Territorialitätsprinzip steht einer direkten Erhebung von Beweismitteln im Ausland allerdings entgegen.<sup>1</sup> Für sie ist grundsätzlich der Rechtshilfeweg zu beschreiten. Das geht mit erheblichem Aufwand einher. In Kombination mit der Flüchtigkeit digitaler Beweismittel fordert die «Beweisverlagerung in die digitale Welt» die Behörden deshalb besonders heraus.<sup>2</sup>

Das Übereinkommen über die Cyberkriminalität («CCC»)<sup>3</sup> nimmt sich dieser Problematik an, indem es für öffentlich zugängliche Daten sowie bei einer Zustimmung des Berechtigten einen grenzüberschreitenden Zugriff auf E-Evidence zulässt. Da die Behörden dabei indes auf die freiwillige Mitwirkung der Anbieter angewiesen sind, wurden

weitere Lösungen sondiert. So soll das zweite Zusatzprotokoll zum CCC<sup>4</sup> grenzüberschreitende Zugriffe vereinfachen. Ähnliche Bestrebungen der EU resultierten in der E-Evidence-Verordnung («EE-VO»)<sup>5</sup> und E-Evidence-Richtlinie («EE-RL»)<sup>6</sup>. Sie ermächtigen Ermittlungsbehörden ab dem 18.8.2026,<sup>7</sup> die Sicherung oder Herausgabe von Daten gegenüber Diensteanbietern in anderen Mitgliedstaaten direkt und ohne Rechtshilfverfahren anzuordnen. Es werden zwei extraterritoriale Zwangsmassnahmen geschaffen, die Europäische Herausgabe- und Sicherungsanordnung.<sup>8</sup> Die EU verspricht sich mit dieser teilweisen Aufhebung des Territorialitätsprinzips eine Modernisierung der strafprozessualen Zusammenarbeit.<sup>9</sup>

Die neue Gesetzgebung der EU führt für die Schweiz zu einer paradoxen Situation: Schweizer Provider, die einen Dienst in der EU anbieten, müssen auf Anordnung eines EU-Mitgliedstaats Daten herausgeben, womit sie möglicherweise unerlaubte Handlungen für einen fremden Staat i.S.v. Art. 271 StGB vornehmen.<sup>10</sup> Während sich die EU ab 2026 so mittels unilateralen Akts Zugriff auf Daten Schweizer Anbieter einräumt, was die Souveränität der Schweiz berührt,<sup>11</sup> besteht zugleich jedoch kein Gegenrecht. Ein Anschluss an das EU-System ist deshalb zu prüfen.<sup>12</sup> Die Zeit drängt. Es handelt sich aber um komplexe Rechtsfragen, weshalb mögliche Reaktionen sorgsam zu evaluieren sind. Grundlage muss eine Gegenüberstellung der neuen EU-Regelung und dem in-

<sup>1</sup> BGE 141 IV 108, 121.

<sup>2</sup> GRAF, in: GRAF (Hrsg.), Onlinekommentar CCC, Art. 32 N 1 f.

<sup>3</sup> Vom 23.11.2001.

<sup>4</sup> Vom 12.5.2022. Die Schweiz hat das Protokoll bisher nicht unterzeichnet.

<sup>5</sup> Verordnung (EU) 2023/1543 v. 12.7.2023.

<sup>6</sup> Richtlinie (EU) 2023/1544 v. 12.7.2023.

<sup>7</sup> Art. 34 EE-VO.

<sup>8</sup> Art. 5 f. EE-VO.

<sup>9</sup> LUDWICZAK GLASSEY, Preuves électroniques: état de la situation en Suisse face à l'avancée majeure du droit européen, eucrim 2023, 204, 204.

<sup>10</sup> Dies eher verneinend LUDWICZAK GLASSEY, Preuves dans le nuage, accès transnational et souveraineté territoriale: un «troupe» impossible?, SJ 2024, 738, 751.

<sup>11</sup> Vgl. LUDWICZAK GLASSEY (Fn. 10), 751.

<sup>12</sup> Siehe deshalb Bundesamt für Justiz, Bericht zur e-Evidence-Vorlage der EU v. 24.10.2023.

nerstaatlichen Recht sein. Sie erlaubt in der Folge zu beurteilen, ob allfällige Diskrepanzen der Systeme hinnehmbar sind oder eine Harmonisierung angezeigt ist. Ihr widmet sich dieser Beitrag.

## II. Zwangsmassnahmen betreffend E-Evidence

### 1. Arten und Voraussetzungen

#### a) Europäische Herausgabe- und Sicherungsanordnung

Kern der EE-VO ist die Etablierung der Herausgabe- und Sicherungsanordnung. Mit Ersterer können bestimmte Daten direkt von Diensteanbietern in anderen Mitgliedstaaten angefordert werden (Art. 10 EE-VO). Mit der Sicherungsanordnung kann von ihnen die Aufbewahrung von Daten für einen Zeitraum von bis zu 60 Tagen verlangt werden (Art. 11 EE-VO). Die EE-VO legt den Rahmen dieser Zwangsmassnahmen fest. Die EE-RL verpflichtet die Diensteanbieter sodann, eine Niederlassung in der EU sicherzustellen oder einen Vertreter zu benennen (Art. 1 Abs. 1 EE-RL).

Die neuen Zwangsmassnahmen betreffen ausschliesslich die Herausgabe von im Zeitpunkt der Anordnung gespeicherten Daten (Art. 3 Ziff. 8 EE-VO), beziehen sich also auf eine *rückwirkende* Erhebung. Die Echtzeitüberwachung ist nicht vorgesehen. Während Anordnungen stets notwendig und verhältnismässig sein müssen und in vergleichbaren nationalen Fällen unter denselben Voraussetzungen eine ähnliche Anordnung erlassen werden können muss (Art. 5 Abs. 2 EE-VO), unterscheiden sich die weiteren Voraussetzungen je nach Massnahme und Datenkategorie. Die Herausgabe von Inhalts- und Verkehrsdaten kann nur bei Ermittlungen betreffend Straftaten mit einer Höchststrafe von mind. drei Jahren Freiheitsstrafe angeordnet werden oder aber bei katalogisierten Cyberstraftaten, Straftaten im Zusammenhang mit Terrorismus sowie Sexualstraftaten gegenüber Kindern (Art. 5 Abs. 4 EE-VO). Teilnehmer- und Zugangsdaten können bei allen Straftaten angefordert werden (Art. 5 Abs. 3 EE-VO). Dasselbe gilt für Sicherungsanordnungen (Art. 6 Abs. 3 EE-VO).

Die Herausgabe von Inhalts- und Verkehrsdaten erfordert eine gerichtliche Genehmigung (Art. 4 Abs. 2 EE-VO). Die Herausgabe von Teilnehmer- und Zugangsdaten sowie Sicherungsanordnungen fallen in die Kompetenz der Staatsanwaltschaften (Art. 4 Abs. 1 und Abs. 3 EE-VO).

Neu ist, dass nicht die Behörde eines anderen Staates, sondern der Vertreter des Diensteanbieters Adressat der Anordnung ist. Verpflichtet wird, wer es Personen in einem oder mehreren Mitgliedstaaten ermöglicht, seine Dienste in Anspruch zu nehmen (Art. 2 Ziff. 2 lit. b und Ziff. 3 lit. b EE-RL). Die blosser Zugänglichkeit reicht jedoch nicht aus. Es bedarf einer «wesentlichen Verbindung zur Union». Sie kann in einer Niederlassung oder faktisch bestehen, wenn der Anbieter eine erhebliche Anzahl von Nutzern in der EU hat oder seine Tätig-

keit auf den EU-Raum ausrichtet (z. B. indem die Anwendung im App-Store angeboten wird).<sup>13</sup>

#### b) System nach StPO und BÜPF

Das Schweizer Recht unterscheidet zwischen der Echtzeitüberwachung und der rückwirkenden Erhebung, wobei für verschiedene Datenkategorien andere Zwangsmassnahmen einschlägig sind. Die *Echtzeitüberwachung* des Post- und Fernmeldeverkehrs richtet sich nach Art. 269 StPO und kann sowohl Inhalts- als auch Randdaten betreffen. Sie findet kein Gegenstück in der E-Evidence-Gesetzgebung der EU. Die *rückwirkende Inhaltsdatenerhebung* – für die gemäss EE-VO die Herausgabebeanordnung zur Verfügung steht – ist nicht gesondert geregelt. Für sie ist auf die Art. 263 ff. StPO abzustellen.<sup>14</sup> Gemäss Art. 265 Abs. 1 StPO sind Inhaber verpflichtet, der Beschlagnahme unterliegende Gegenstände, Vermögenswerte und (*a maiore ad minus*) Daten<sup>15</sup> herauszugeben. Es bedarf keiner gerichtlichen Genehmigung. Der Rechtsschutz wird über die Siegelung gewährt (Art. 248 StPO).

Für die *rückwirkende Randdatenerhebung* besteht mit Art. 273 StPO eine Spezialregelung. Randdaten des Fernmeldeverkehrs i.S.v. Art. 8 lit. b BÜPF können herausverlangt werden, wobei das BÜPF-Instrumentarium zum Zug kommt. Die Randdatenerhebung ist nur für Vergehen und Verbrechen möglich und bedarf einer gerichtlichen Genehmigung (Art. 273 Abs. 1 und 2 StPO).

Das BÜPF erlaubt den Behörden sodann einen privilegierten Zugang zu *Bestandesdaten*. Sie gelten nicht als durch das Fernmeldegeheimnis geschützt und können nach Art. 21 BÜPF bei Anbietern herausverlangt werden.<sup>16</sup> Bei Straftaten, die über das Internet begangen wurden, können gemäss Art. 22 BÜPF ebenfalls Auskünfte eingeholt werden, welche die Identifikation der Täterschaft erlauben. Begehren zu Bestandesdaten erfolgen über den Dienst ÜPF und können von der Staatsanwaltschaft wie auch der Polizei gestellt werden (Art. 15 Abs. 1 BÜPF).

Eine Sicherungsanordnung kennt das Schweizer Recht nicht. Fernmeldedienste müssen jedoch sicherstellen, dass Rand- und Bestandesdaten während sechs Monaten gespeichert bleiben (Art. 21 Abs. 2, Art. 22 Abs. 2, Art. 26 Abs. 5 BÜPF). Zu beschlagnahmende Inhaltsdaten dürfen bei Verlustgefahr vorläufig sichergestellt werden (Art. 263 Abs. 3 StPO).

Das internationale Recht räumt den Schweizer Behörden bereits heute Möglichkeiten ein, grenzüberschreitend an E-Evidence zu gelangen. Gestützt auf das IRSG kann um die vorläufige Sicherung gefährdeter Beweismittel, die Überwachung des Post- und Fernmeldeverkehrs und die Übermittlung von Verkehrsdaten ersucht werden (Art. 18 ff. und 30 IRSG). Praxisrelevanter sind Ersuchen gestützt auf das CCC betreffend

<sup>13</sup> ErwGr 10 f. EE-RL; ErwGr 30 EE-VO.

<sup>14</sup> Vgl. BGE 144 IV 74, 78 f.; BGE 143 IV 270, 274 f.

<sup>15</sup> Implizit BGE 143 IV 270, 274 f.

<sup>16</sup> HANSJAKOB, Überwachungsrecht der Schweiz, Zürich 2018, 235 und 440.

|                                                           | <i>E-Evidence-Gesetzgebung</i>                                                                                                                     | <i>Schweizer Recht</i>                                                                                              |
|-----------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| <i>Echtzeitüberwachung</i>                                | –                                                                                                                                                  | Art. 269 ff. StPO<br>– Straftaten: Katalogtaten<br>– Adressat: Anbieter gemäss BÜPF<br>– Kompetenz: Gericht         |
| <i>Rückwirkende Erhebung von Inhaltsdaten</i>             | Art. 4 Abs. 2 und Art. 5 Abs. 4 EE-VO<br>– Straftaten: Mindeststrafe 3 Jahre + Katalogtaten<br>– Adressat: Diensteanbieter<br>– Kompetenz: Gericht | Art. 263 ff. StPO<br>– Straftaten: Alle<br>– Adressat: Inhaber der Daten<br>– Kompetenz: Staatsanwaltschaft         |
| <i>Rückwirkende Erhebung von Verkehrs- bzw. Randdaten</i> | Art. 4 Abs. 2 und Art. 5 Abs. 4 EE-VO<br>– Straftaten: Mindeststrafe 3 Jahre + Katalogtaten<br>– Adressat: Diensteanbieter<br>– Kompetenz: Gericht | Art. 273 StPO<br>– Straftaten: Vergehen + Verbrechen<br>– Adressat: Diensteanbieter<br>– Kompetenz: Gericht         |
| <i>Rückwirkende Erhebung von Zugangsdaten</i>             | Art. 4 Abs. 1 und Art. 5 Abs. 3 EE-VO<br>– Straftaten: Alle<br>– Adressat: Diensteanbieter<br>– Kompetenz: Staatsanwaltschaft                      |                                                                                                                     |
| <i>Erhebung von Teilnehmer- bzw. Bestandesdaten</i>       | Art. 4 Abs. 1 und Art. 5 Abs. 3 EE-VO<br>– Straftaten: Alle<br>– Adressat: Diensteanbieter<br>– Kompetenz: Staatsanwaltschaft                      | Art. 21 f. BÜPF<br>– Straftaten: Alle<br>– Adressat: Diensteanbieter<br>– Kompetenz: Staatsanwaltschaft + Polizei   |
| <i>Sicherungsanordnungen</i>                              | Art. 4 Abs. 3 und Art. 6 EE-VO<br>– Straftaten: Alle<br>– Adressat: Diensteanbieter<br>– Kompetenz: Staatsanwaltschaft                             | – (Sicherstellung bei Gefahr nach Art. 263 Abs. 3 StPO und Vorratsdatenspeicherung bei Fernmeldediensten nach BÜPF) |

Tabelle 1: Zwangsmassnahmen nach E-Evidence-Gesetzgebung der EU und Schweizer Recht

Sicherung, Durchsuchung, Beschlagnahme oder Weitergabe gespeicherter Daten, die Echtzeitüberwachung sowie der direkte Zugriff bei freiwilliger Herausgabe (Art. 29 ff. CCC). Im Unterschied zum neuen EU-Recht sind diese Massnahmen an die innerstaatlichen Voraussetzungen gebunden und kollidieren nicht mit dem Schweizer Recht.

### c) Diskrepanz zwischen Eingriffsintensität und Rechtsschutz

Die gewichtigsten Unterschiede zwischen den Systemen (Tabelle 1) bestehen (1.) betreffend die *rückwirkende Inhaltsdatenerhebung*. Das EU-Recht kennt für sie mit dem Straftatenkatalog und dem gerichtlichen Genehmigungserfordernis höhere Hürden. Ein Anschluss an das EU-System bedeutete, dass die Behörden innerstaatlich weniger Restriktionen unterlägen als bei grenzüberschreitenden Zugriffen. Die *rückwirkende Randdatenerhebung* ist in der Schweiz (2.) für Vergehen und Verbrechen möglich, im EU-Recht schränkt der Straftatenkatalog den Anwendungsbereich deutlich weiter ein. Die *Sicherungsanordnung* ist (3.) dem Schweizer Recht nicht bekannt. Aufgrund der Vorratsdatenspeicherung und der Möglichkeit der vorläufigen Sicherstellung bei der Beschlagnahme besteht für sie kaum ein praktisches Bedürfnis. Das Sicherungsrecht wäre – ausser bei den sich bei abgeleiteten Kommunikationsdiensten befindlichen Randdaten – weniger einschneidend als die heute bereits bestehenden Instrumente.

Der Vergleich legt eine Ungereimtheit offen, die im Schweizer Recht unabhängig der EU-Gesetzgebung augenfällig ist. Die Herausgabe von Inhaltsdaten stellt einen schwereren Grundrechtseingriff dar als diejenige von Randdaten.<sup>17</sup> Da Erstere der Edition unterliegt, ist sie aber weniger voraussetzungsreich als die Randdatenerhebung nach Art. 273 StPO. Das lässt sich am Beispiel des E-Mail-Verkehrs illustrieren: Der Zugriff auf E-Mails während des Übermittlungsvorgangs gilt als Echtzeitüberwachung.<sup>18</sup> Gelesene oder zumindest zugestellte E-Mails unterliegen jedoch nicht mehr der Fernmeldeüberwachung.<sup>19</sup> Umstritten ist der Umgang mit automatisch synchronisierten, aber noch nicht zur Kenntnis genommenen E-Mails<sup>20</sup> oder mit solchen, die sich in der Cloud befinden<sup>21</sup>. Da es sich bei der Edition nicht um eine verdeckte Massnahme handelt, ist der Betroffene zu informieren.<sup>22</sup> Möchten Behörden, welchen Inhaltsdaten (z.B. Droh-E-Mails) vorliegen,

<sup>17</sup> BGE 144 I 126, 135.

<sup>18</sup> BGE 144 IV 74, 78 f.; BGE 143 IV 270, 275.

<sup>19</sup> JOSITSCH/SCHMID, StPO Praxiskommentar, 4. Aufl., Zürich/St. Gallen 2023, Vor Art. 269–279 N 3.

<sup>20</sup> HENEGHAN/MELE/MÜLLER/WOHLERS, E-Mails als Beweismittel im Strafverfahren, AJP 2023, 1381, 1383 f.

<sup>21</sup> Die Anwendbarkeit von Art. 263 ff. StPO bejahend HANSJAKOB (Fn. 16), 93. Auch JEAN-RICHARD-DIT-BRESSEL, Die Mailbox – Ziel oder Weg?, ZStrR 125 (2007), 157, 171, und BGE 140 IV 181, 185 stellen auf die «Datenherrschaft» ab.

<sup>22</sup> JEAN-RICHARD-DIT-BRESSEL, in: NIGGLI/HEER/WIPRÄCHTIGER (Hrsg.), BSK StPO, 3. Aufl., Basel 2023, Art. 269 N 24.

Randdaten dieser Kommunikation erhalten, richtet sich die Herausgabe nach Art. 273 StPO. Sie kann verdeckt erfolgen, bedarf aber der gerichtlichen Genehmigung. Das EU-System sieht einen anderen Mechanismus vor: Die Herausgabe beider Datenkategorien kann offen oder verdeckt angeordnet werden (Art. 13 EE-VO), wird aber jedenfalls gerichtlich genehmigt. Damit verliert der Rechtsstreit um die Frage, wann E-Mails der Überwachung und wann der Edition unterliegen, an Bedeutung. Die Herausgaben gehen einheitlich vonstatten und bedürfen der gerichtlichen Überprüfung. Die Voraussetzungen stehen damit (mehr) in Einklang mit der Schwere des Eingriffs als im Schweizer System, wo die rückwirkende Randdatenerhebung voraussetzungsreicher ist als diejenige von Inhaltsdaten.

## 2. Datenkategorien

### a) Inhalts- und Verkehrsdaten

Das neue EU-Recht bezieht sich auf Inhalts-, Verkehrs- und Teilnehmerdaten, wobei die letzte Kategorie weiter in reguläre Teilnehmerdaten und besondere Zugangsdaten unterteilt wird. Das Schweizer Recht unterscheidet Inhalts-, Rand- und Bestandesdaten. Es stellt sich die Frage, wie sich diese Kategorien zueinander verhalten.

*Inhaltsdaten* beziehen sich auf den Informationsgehalt der Kommunikation.<sup>23</sup> Art. 3 Ziff. 12 EE-VO definiert sie als «Daten in einem digitalen Format wie Text, Sprache, Videos, Bilder und Tonaufzeichnungen, die nicht Teilnehmer- oder Verkehrsdaten sind». Dieses Verständnis deckt sich mit dem hiesigen.

*Randdaten* sind gemäss Art. 8 lit. b BÜPF «Daten, aus denen hervorgeht, mit wem, wann, wie lange und von wo aus die überwachte Person Verbindung hat oder gehabt hat, sowie die technischen Merkmale der entsprechenden Verbindung». Der Randdatenbegriff ist grundsätzlich deckungsgleich mit dem der *Verkehrsdaten*.<sup>24</sup> Nach schweizerischem Verständnis beziehen sich Randdaten immer auf eine (nicht öffentliche) Kommunikation. Interessant ist deshalb die Definition gemäss Art. 3 Ziff. 11 EE-VO. Verkehrsdaten sind demnach «Daten, die sich auf die Erbringung einer von einem Diensteanbieter angebotenen Dienstleistung beziehen, dazu dienen, Kontext- oder Zusatzinformationen über eine solche Dienstleistung zu liefern und von einem Informationssystem des Diensteanbieters generiert oder verarbeitet werden, beispielsweise Ursprung und Ziel einer Nachricht oder einer anderen Art von Interaktion, Daten über den Standort des Geräts, Datum, Uhrzeit, Dauer, Grösse, Route, Format, verwendetes Protokoll und Art der Kompression, sowie andere Metadaten der elektronischen Kommunikation und Daten, die keine Teilnehmerdaten sind, über den Beginn und die Beendigung der Nutzersitzung für einen Dienst, etwa das Datum und die Uhrzeit der Nutzung, die Anmeldung bei und die Abmeldung vom dem Dienst». Verkehrsdaten beziehen sich demzufolge nicht zwin-

gend auf eine Kommunikation i. S. d. Fernmeldegeheimnisses. Die EE-VO scheint davon auszugehen, dass sich Verkehrs- bzw. Randdaten auch auf einen Vorgang beziehen können, bei dem keine Kommunikation erfolgt.

Diese Differenz rückt einen Aspekt ins Zentrum, der *de lege lata* für Unklarheiten sorgt. Art. 269 ff. StPO und BÜPF widmen sich der Überwachung des Post- und Fernmeldeverkehrs. Im Vordergrund stehen Eingriffe in das Fernmeldegeheimnis, d. h. in das «Kommunikationsgeheimnis»<sup>25</sup>. Das Feld von Diensten, wie sie die EE-VO einbezieht, umfasst jedoch auch Anwendungen ohne direkten Kommunikationsbezug. Spannend ist in diesem Kontext etwa die Frage des Umgangs mit in der Cloud gespeicherten Daten. HANSJAKOB hält fest, dass bei Daten, die mittels Internetverbindung synchronisiert werden, die Regeln von Art. 269 ff. StPO einzuhalten sind.<sup>26</sup> Es ist aber fraglich, inwiefern sich diese auf sämtlichen Internetverkehr anwenden lassen, schützt doch das Fernmeldegeheimnis nur Kommunikationsvorgänge<sup>27</sup> und waren die Art. 269 ff. StPO gemäss Bundesgericht deshalb (zumindest zunächst) nur auf Fernmeldedienste anwendbar.<sup>28</sup> Daten in der Cloud haben i. d. R. keinen direkten Kommunikationsbezug. Ihre Edition stellt einen Eingriff in Art. 13 BV dar, betrifft aber allgemein die Privatsphäre und die informationelle Selbstbestimmung, nicht jedoch das Fernmeldegeheimnis. Darauf sind die den Art. 269 ff. StPO und dem BÜPF bekannten Datenkategorien nicht ausgerichtet. Die Aufnahme der abgeleiteten Kommunikationsdienste in den Kreis der Mitwirkungspflichtigen gemäss BÜPF verschaffte zwar etwas Abhilfe, vermag aber die Diskrepanz nicht zu überwinden, dass rückwirkend alle Arten von Inhaltsdaten via Beschlagnahme und Edition zugänglich sind, gleichzeitig Echtzeit- und Randdatenüberwachungen gemäss Art. 269 ff. StPO nicht auf nicht kommunikationsbezogene Internetdienstnutzungen zugeschnitten sind. Die Gesetzgebung der EU widmet sich den elektronischen Beweismitteln umfassender. Konsequenzen zeitigt dieser Umstand beim Begriff der Verkehrsdaten. Im Sinne der EE-VO zählen dazu z. B. Daten über den Standort eines Geräts oder dessen technischen Spezifikationen sowie allgemeine Informationen über Nutzersitzungen. Es geht folglich nicht bloss um den eine Kommunikation betreffenden «Verkehr».

### b) Teilnehmer- und Zugangsdaten

Die Fokussierung der Art. 269 ff. StPO und des BÜPF auf das Fernmeldegeheimnis fordert auch beim Umgang mit IP-Adressen heraus. Neben den Inhalts- und Randdaten besteht in der Schweiz die Kategorie der *Bestandesdaten*. Sie können nach

<sup>23</sup> BOTTINELLI/WENGER, Onlinekommentar CCC (Fn. 2), Art. 34 N 5.

<sup>24</sup> So spricht die Botschaft zum BÜPF von «Verkehrsdaten, d. h. Randdaten», BBl 2013 2683, 2756.

<sup>25</sup> TSCHENTSCHER, Das Grundrecht auf Computerschutz, AJP 2008, 383, 390.

<sup>26</sup> HANSJAKOB (Fn. 16), 101.

<sup>27</sup> Z. B. BGE 144 I 126, 130.

<sup>28</sup> Für abgeleitete Internetdienste verneinen BGE 143 IV 21, 23 und BGE 143 IV 270, 277, die Anwendbarkeit von Art. 269 ff. StPO (vgl. auch BBl 2006 1085, 1250). Gestützt auf das totalrevidierte BÜPF würde es aber allenfalls zu einem anderen Schluss kommen.

Art. 21 BÜPF ediert werden. Als Informationen «über feststehende Abonnementsverhältnisse, die sich nicht auf einzelne Gespräche oder Sendungen beziehen»,<sup>29</sup> sind sie im Gegensatz zu den Randdaten also unabhängig von einem bestimmten Fernmeldeverkehr vorhanden.<sup>30</sup> Zu dieser Kategorie werden Adressierungselemente<sup>31</sup> gezählt (z.B. Zuordnung von Namen zu einem Anschluss) sowie Verträge oder der Personal Unblocking Key<sup>32,33</sup>. Gemäss HANSJAKOB handelt es sich bei IP-Adressen um Bestandesdaten, da es bei ihrer Erhebung darum gehe zu eruieren, wer die Adresse zu einem bekannten Zeitpunkt verwendet hat.<sup>34</sup> Eine Auskunft erfolge nach Art. 22 BÜPF, es gehe dort um Bestandesdaten, auch wenn sich Auskünfte über die Internetnutzung aufgrund der oft dynamischen Zuteilung der IP-Adressen einer Überwachung annäherten.<sup>35</sup> Anderer Ansicht war das Bundesgericht in BGer 6B\_656/2015. Auf Ersuchen gab ein Provider bekannt, über welche IP-Adressen auf das Konto zugegriffen wurde, von dem Droh-E-Mails verschickt wurden. Das Gericht klassifizierte sie als Randdaten, da sie die Kommunikation selbst betreffen.<sup>36</sup> Auch in BGE 141 IV 108 wird festgestellt, dass es sich bei einer IP-History um Randdaten handelt.<sup>37</sup> Gemäss HANSJAKOB überzeugt dies nicht, da die IP-History nicht darauf schliessen lasse, wer mit wem kommuniziert, sondern nur darauf, wer wann auf einen Dienst zugegriffen hat.<sup>38</sup>

Diese pauschalen Einordnungen von IP-Adressen rechtfertigen sich nicht, sind doch Konstellationen zu unterscheiden: Es kann (1.) der Behörde eine IP-Adresse bereits bekannt sein und darum gehen, beim Provider die zugehörigen Registrierungsdaten zu erhalten. Diesfalls handelt es sich auch gemäss Bundesgericht um eine Bestandesdatenabfrage.<sup>39</sup> Geht es um die Abfrage unveränderlich bei den Providern verfügbare Informationen zu bereits bekannten Zugängen, die für sich keine Rückschlüsse auf eine konkrete Fernmeldeverkehrsverbindung zulassen, ist diese Einordnung überzeugend. Davon abzugrenzen ist die (2.) Variante, bei der nur Internet-Kommunikationsaktivitäten bekannt sind. Zunächst ist diesfalls auszumachen, welche IP-Adressen der Internetaktivität zuzuweisen sind. In der Folge sind gestützt darauf die registrierten Kunden festzustellen. Es bedarf hier also vorweg der Eruierung der beteiligten Zugänge mittels IP-History. Dieser Schritt wird heute als Randdatenerhebung klassifiziert, was einleuchtet, sofern die IP-History tatsächlich einen Kommunikationsbezug aufweist. Das kann wohl behauptet werden, wenn – wie im angeführ-

ten Urteil – eruiert wird, über welche Anschlüsse zum Zeitpunkt eines E-Mail-Versandes ein Zugriff auf das Konto erfolgte. Strittig ist es dagegen, wenn allgemein festzustellen ist, welche IP-Adressen mit dem Aufrufen eines Dienstes in Verbindung gebracht werden können (z.B. bei Hinterlassen eines öffentlichen rassistischen Kommentars auf einer Webseite). Derartige Ermittlungsmassnahmen sind in der bestehenden Kategorisierung schwer einzuordnen. Sie betreffen keine Registrierungsdaten, sind aber auch nicht Randdaten, da ihre Erhebung nicht dazu dient, Teilnehmer oder Modalitäten einer spezifischen Kommunikation auszumachen. Es handelt sich um eine (3.) Variante. Sie legt die besondere Natur von IP-Adressen offen und zeigt, dass Auskünfte zu Internetaktivitäten nicht immer das Fernmeldegeheimnis betreffen.

Die EU-Gesetzgebung nimmt sich dem Problem an, indem sie eine neue Datenkategorie einführt. Auch die EE-VO kennt reguläre *Teilnehmerdaten*. In diese Kategorie fallen «alle Daten, die bei einem Diensteanbieter über die Teilnahme an seinen Diensten vorliegen» und entweder die Identität eines Teilnehmers oder Kunden oder die Art der Dienstleistung und ihre Dauer betreffen (Art. 3 Ziff. 9 EE-VO). Es handelt sich um «Bestandesdaten im weiteren Sinne», da sie nicht nur Daten betreffend Kommunikationsdiensten anvisieren. Neben diese Teilnehmerdaten stellt die EE-VO «ausschliesslich zum Zweck der Identifizierung des Nutzers angeforderte Daten» ab. Dabei handelt es sich um «IP-Adressen und, falls notwendig, die relevanten Quellports und Zeitstempel, nämlich Daten und Uhrzeit, oder die technischen Äquivalente dieser Kennungen und die damit zusammenhängenden Informationen, sofern sie von Strafverfolgungs- oder Justizbehörden ausschliesslich zum Zweck der Identifizierung des Nutzers in einer bestimmten strafrechtlichen Ermittlung angefordert werden» (Art. 3 Ziff. 10 EE-VO). Im Wesentlichen geht es um IP-Histories und Logfiles. Es kann von *Zugangsdaten* gesprochen werden, «die allein genommen den Nutzer nicht identifizieren, aber als erster Schritt für eine Identifizierung unbedingt notwendig sind».<sup>40</sup> Die EE-VO unterscheidet demzufolge zwischen IP-Adressen, die nicht ausschliesslich zum Zweck der Identifizierung genutzt werden, so z.B. um Informationen zu erlangen, die eher allgemein in die Persönlichkeitssphäre der Betroffenen eingreifen. Sie sind wie Verkehrsdaten zu behandeln. Bei IP-Adressen, die nur der Identifikation dienen, also eben sog. Zugangsdaten, rechtfertigt sich jedoch eine privilegierte Behandlung wie bei Teilnehmerdaten.<sup>41</sup> Die EE-VO führt folglich eine Differenzierung zwischen eigentlichen «Daten der allgemeinen Internetüberwachung» und «Daten der blossen Anschlussidentifikation» ein, wie sie das Schweizer Recht nicht kennt.

<sup>29</sup> JEAN-RICHARD-DIT-BRESSEL, BSK StPO (Fn. 22), Art. 273 N 7.

<sup>30</sup> HANSJAKOB (Fn. 16), 236.

<sup>31</sup> Vgl. Art. 3 lit. f FMG.

<sup>32</sup> BGE 141 IV 423, 429.

<sup>33</sup> JEAN-RICHARD-DIT-BRESSEL, BSK StPO (Fn. 22), Art. 273 N 7; HANSJAKOB (Fn. 16), 89 und 441; ähnlich Art. 18 Abs. 3 CCC.

<sup>34</sup> HANSJAKOB (Fn. 16), 260 f.

<sup>35</sup> HANSJAKOB (Fn. 16), 446.

<sup>36</sup> BGer, Urteil v. 16.12.2016, 6B\_656/2015, E. 1.4.1 f.

<sup>37</sup> BGE 141 IV 108, 120.

<sup>38</sup> HANSJAKOB (Fn. 16), 447.

<sup>39</sup> BGE 141 IV 108, 120.

<sup>40</sup> Europäische Kommission, Häufig gestellte Fragen: Neue EU-Vorschriften für die Beschaffung von elektronischem Beweismaterial v. 17.4.2018.

<sup>41</sup> ErwGr 33 EE-VO.

### 3. Verpflichtete Diensteanbieter

Das EU-Gesetzgebungspaket unterscheidet drei Kategorien von Diensteanbietern. Zur (1.) Kategorie zählen *elektronische Kommunikationsdienste*. Sie umfasst einer früher erlassenen Richtlinie über den europäischen Kodex für die elektronische Kommunikation («EK-RL»)<sup>42</sup> zufolge Internetzugangsdienste, interpersonelle Kommunikationsdienste und Übertragungsdienste, die für die Maschine-Maschine-Kommunikation und für den Rundfunk genutzt werden.<sup>43</sup> Neben einer (2.) Kategorie von *Internetdomännennamen- und IP-Nummerierungsdiensten* verpflichtet die EE-VO (3.) *andere Dienste der Informationsgesellschaft*. Dazu zählen Dienste, «die es ihren Nutzern ermöglichen, miteinander zu kommunizieren, oder es ermöglichen, für Nutzer, für welche die Dienstleistung erbracht wird, Daten zu speichern oder auf sonstige Weise zu verarbeiten, sofern die Speicherung von Daten ein bestimmender Bestandteil der für den Nutzer erbrachten Dienste ist» (Art. 2 Ziff. 1 EE-RL; Art. 3 Ziff. 3 EE-VO). Als Beispiel angeführt werden Online-Marktplätze sowie Hosting- und Cloud-Computing-Dienste. Diese Services betreffen nicht zwingend die Kommunikation,<sup>44</sup> verfügen aber über E-Evidence von Interesse. Die Abgrenzung der Kategorie ist anspruchsvoll. Finanzdienstleistungen werden ausgeschlossen. Fraglich bleibt aber z.B., ob Streaming-Plattformen wie YouTube oder Spotify darunterfallen. Sie sind keine elektronischen Kommunikationsdienste,<sup>45</sup> könnten aber andere Dienste der Informationsgesellschaft darstellen. Die Speicherung von Daten ist bei ihnen zwar kein «bestimmender Bestandteil», allerdings verfügen sie über Interaktions- und Kommentarfunktionen, d.h., sie ermöglichen als Nebenprodukt Kommunikation. Online-Videospiele werden aufgrund ihrer Chat-Funktion unter den Begriff subsumiert.<sup>46</sup> Der Gesetzgeber wollte Plattformen verpflichten, die einen Informationsaustausch zulassen,<sup>47</sup> auch wenn die Mehrwegkommunikation eine blosse «Annexfunktion» darstellt.<sup>48</sup> Der Gesetzestext bezieht die Einschränkung des «bestimmenden Bestandteils» ferner nur auf die Variante der Speicherfunktion. Diese Argumente sprechen für eine weite Auslegung der Kategorie der «anderen Dienste der Informationsgesellschaft».

Bei der Echtzeit-, Randdaten- und Bestandesdatenerhebung sind in der Schweiz gestützt auf das BÜPF nur bestimmte Anbieter mitwirkungspflichtig. Bei der Schaffung des aBÜPF standen Dienstleistungen im Vordergrund, die dem Post- und dem Fernmeldegesetz unterstehen. Bereits 1998 wurde zwar fest-

gestellt, dass auch «Internet-Provider einen Fernmeldedienst an[bieten]».<sup>49</sup> Fokussiert wurden aber Eingriffe in das Post- und Fernmeldegeheimnis, weshalb eine enge Verbindung des BÜPF mit den entsprechenden Grundrechtseingriffen besteht. Eingriffe in andere Teilgehalte von Art. 13 BV fallen dagegen z.B. unter Art. 280 ff. StPO. Der Fokus des BÜPF auf den Schutz vertraulicher Kommunikation schlägt sich in seinem Geltungsbereich nieder. Verpflichtet werden primär Post- und Fernmeldedienste. Mit der Totalrevision sollten darüber hinaus alle Dienste erfasst werden, «die Daten im Zusammenhang mit dem Post- und Fernmeldeverkehr besitzen».<sup>50</sup> Dazu gehören verschiedene Arten von Netz(zugangs)betreibern. Ferner wurden «Anbieterinnen von Diensten, die sich auf Fernmeldedienste stützen und eine Einweg- oder Mehrwegkommunikation ermöglichen», als «Anbieterinnen abgeleiteter Kommunikationsdienste» in den Katalog aufgenommen. Während die EU-Kategorien der Internetzugangsdienste sowie die interpersonellen Kommunikationsdienste demnach in den Anwendungsbereich des BÜPF fallen, ist fraglich, wie die anderen Dienste der Informationsgesellschaft zu werten sind. Dass die Definition der «abgeleiteten Kommunikationsdienste» die Einwegkommunikation umfasst und die Botschaft als Beispiel die Nutzung von Cloud-Diensten anführt,<sup>51</sup> spricht allerdings auch betreffend BÜPF für eine Entfernung vom Fokus auf das Fernmeldegeheimnis.

Während es unstrittig ist, dass Onlinedienste eine «fernmedietechnische Übertragung»<sup>52</sup> involvieren, beziehen sich Überwachungen des Fernmeldeverkehrs herkömmlich auf dem Fernmeldegeheimnis unterstehende Kommunikation. Wenn das Bundesgericht verneinte, dass Dienste wie Facebook gestützt auf Art. 269 ff. StPO überwacht werden können, da es sich bei ihnen nicht um Fernmeldedienste oder Zugangsprovider handelt,<sup>53</sup> zugleich dasselbe Gericht aber die IP-History-Edition bei einem E-Mail-Provider unter Art. 273 StPO subsumierte,<sup>54</sup> stellt sich die Frage, inwiefern BÜPF und StPO die heute massgeblichen Internetdienste einheitlich adressieren. Echtzeit- und Randdatenerhebungen gemäss StPO wären bei «anderen Diensten der Informationsgesellschaft» i.S.d. EE-VO allenfalls teilweise nicht möglich. Art. 263 ff. StPO kann gewisse Herausgabebegehren abdecken, was aber – wie festgehalten – zu Diskrepanzen beim Rechtsschutz führt. Eine Herausgabeanordnung betreffend eine IP-History gegenüber einer Plattform wie Facebook würde nach EU-Recht einen elektronischen Kommunikationsdienst betreffen, nach schweizerischem Recht wäre – je nach Einordnung – Art. 22 BÜPF, Art. 273 StPO oder auch Art. 263 ff. StPO anwendbar. Onlinedienste-Anbieter werden im EU-System gleichbehandelt wie Fernmeldedienste, während im Schweizer Recht Differenzen und Unklarheiten ver-

<sup>42</sup> Richtlinie (EU) 2018/1972 v. 11.12.2018.

<sup>43</sup> Art. 2 Ziff. 4, Ziff. 5 und ErwGr 10 EK-RL.

<sup>44</sup> ErwGr 14 EE-RL; ErwGr 27 EE-VO; vgl. auch Art. 1 lit. c CCC.

<sup>45</sup> BASAR, Die «E-Evidence-VO» tritt in Kraft – Update zu jurisPR-StrafR 5/2019, jurisPR-StrafR 14/2023, Anm. 1.

<sup>46</sup> WEISS/PRADEL, Zum Begriff des «Diensteanbieters» im Sinne der europäischen E-Evidence-Verordnung, Corporate Compliance Zeitschrift 4/2024, 102.

<sup>47</sup> BASAR (Fn. 45).

<sup>48</sup> REXIN, Diensteanbieter im Dienste von Ermittlungsbehörden, Computer & Recht 2024, 64, 65.

<sup>49</sup> BBl 1998 IV 4241, 4255 f.; vgl. auch BBl 2013 2683, 2704.

<sup>50</sup> HANSJAKOB (Fn. 16), 377.

<sup>51</sup> BBl 2013 2683, 2708.

<sup>52</sup> Siehe die Definition in Art. 3 lit. c FMG.

<sup>53</sup> BGE 143 IV 21, 23; 143 IV 270, 277.

<sup>54</sup> BGer, Urteil v. 16.12.2016, 6B\_656/2015; BGE 141 IV 108.

bleiben. Die EE-VO soll E-Evidence bei allen massgeblichen Diensten verfügbar machen. Auch die Kategorien des BÜPF erlauben eine weite Auslegung. Dessen Ratio ist aber auf Post- und Fernmeldedienste ausgerichtet und nicht auf die Überwachung von Internetaktivitäten im Allgemeinen.

### III. Würdigung

Die Paradoxie, dass viele Schweizer Provider durch einen Akt der EU nächstes Jahr zur Datenherausgabe verpflichtet sein werden, was sie nicht nur Strafbarkeitsrisiken aussetzt, sondern die Souveränität der Schweiz beeinträchtigt, zugleich hiesige Behörden aber über kein Gegenrecht verfügen, setzt die Schweiz unter Zugzwang. Die Palette an rechtspolitischen Optionen ist breit. Kurzfristig können Provider mit einer Bewilligung i. S. v. Art. 271 Ziff. 1 StGB aus der Schusslinie genommen werden. Eine Lösung ist damit aber nicht gefunden. Längerfristig sind Gesetzgebungsprojekte unumgänglich.

Ist ein Anschluss an das EU-System politisch beabsichtigt, sei es gestützt auf einen Vertrag oder eine unilaterale extraterritoriale Verpflichtung, könnte eine punktuelle Harmonisierung angestrebt werden. Eine solche intendierte neben der Verankerung der vom EU-System vorgegebenen Mindestvorschriften vor allem zu verhindern, dass innerstaatliche und extraterritoriale Erhebungen von E-Evidence verschiedenen Systemen unterworfen sind, die – mit Blick etwas auf den Rechtsschutz oder betroffene Anbieter – einen unterschiedlichen Rechtsrahmen für die mit den Zwangsmassnahmen einhergehende Grundrechtseingriffe vorsehen. Die Harmonisierung müsste in erster Linie folgende Inkompatibilitäten adressieren: (1.) Mindestens die grenzüberschreitende Herausgabeanordnung betreffend Inhaltsdaten gegenüber Provider bedürfte einer gerichtlichen Genehmigung. (2.) Die Herausgabe von Zugangsdaten zu Identifikationszwecken wäre wie eine Bestandesdatenabfrage zu behandeln und nur die Edition einer IP-History zu anderen Zwecken stellte eine Randdatenerhebung dar. (3.) Der Geltungsbereich des BÜPF wäre zu überprüfen und ggf. auf weitere Dienste der Informationsgesellschaft auszuweiten, was sich wiederum auf das Verständnis des Randdaten- und Bestandesdatenbegriffs sowie die Anwendbarkeit von Art. 269 ff. StPO auswirken könnte.

Eine punktuelle Harmonisierung liesse womöglich eine Partizipation am EU-System zu, ohne dass innerstaatliches und internationales Recht (zu) offenkundige Diskrepanzen aufweisen würden. Allerdings blieben Ungereimtheiten ungelöst, die keineswegs nur im internationalen Verhältnis bestehen. Im Kern gehen sie darauf zurück, dass das Schweizer System auf die Überwachung des *Post- und Fernmeldeverkehrs*, nicht aber auf die Erlangung *elektronischer Beweismittel* ausgerichtet ist. Es geht um Fernmeldeverkehrs- und nicht um Internetüberwachung, um Eingriffe in das Fernmeldegeheimnis und nicht um andere Eingriffe in die Privat-

sphäre. E-Evidence betrifft aber oftmals Letztere, weshalb sich die Frage stellt, ob auch die Schweiz eine E-Evidence-Gesetzgebung braucht – umgesetzt als eigenes Gesetz oder als Revision von StPO und BÜPF. Sie müsste sich einem System verpflichten, bei dem einerseits Zwangsmassnahmen und Datenkategorien in Einklang mit der Schwere und Art des Grundrechtseingriffs stehen. Andererseits wären diejenigen Diensteanbieter zu adressieren, welche heute über die massgeblichen Daten verfügen. Selbstredend wäre dabei die Balance zwischen der hohen kriminalistischen Relevanz von E-Evidence und der nicht minder hohen Gefährdung der Freiheitsrechte der Überwachten zu finden. Dieses Spannungsfeld wird dem Gesetzgeber einiges abverlangen. Er sollte sich dennoch an die Arbeit machen. Die sich aufgrund der im Beitrag identifizierten Diskrepanzen aufdrängende Harmonisierung mit der EU-Regulierung ist als Chance zu begreifen, das System einer gesamthaften Überprüfung zu unterziehen.

---

**Stichwörter:** E-Evidence-Gesetzgebung, elektronische Beweismittel, Post- und Fernmeldeverkehr, Zwangsmassnahmen, Überwachung

**Mots-clés:** législation sur l'*e-evidence*, moyens électroniques de preuve, correspondance par poste et télécommunication, mesures de contrainte, surveillance

---

■ **Zusammenfassung:** Die E-Evidence-Gesetzgebung der EU erlaubt den grenzüberschreitenden Zugriff auf elektronische Beweismittel bei Diensteanbietern. Auch Schweizer Provider sind betroffen. Zugleich profitieren Schweizer Behörden nicht, womit Gesetzgebungsdruck entsteht. Die Diskrepanzen zwischen EU- und Schweizer Recht legen Schwachstellen des Überwachungsrechts offen. Sie sind primär dem Umstand geschuldet, dass StPO und BÜPF das Spektrum der im digitalen Zeitalter zentralen Eingriffe in Art. 13 BV unzureichend widerspiegeln. Eine Modernisierung bietet sich an.

**Résumé:** La législation de l'Union Européenne sur l'*e-evidence* permet l'accès transfrontalier aux moyens électroniques de preuve se trouvant chez les fournisseurs de services. Les fournisseurs d'accès suisses sont également concernés. En même temps, les autorités helvétiques ne tirent aucun profit du régime instauré; aussi la pression sur l'engagement de réformes législatives augmente-t-elle. Les divergences entre le droit européen et le droit suisse révèlent les points faibles de la réglementation en matière de surveillance. Elles sont principalement dues au fait que le code de procédure pénale suisse et la loi fédérale sur la surveillance de la correspondance par poste et télécommunication reflètent de manière insuffisante l'éventail des restrictions à l'art. 13 Cst. qui apparaissent comme centrales à l'ère du numérique. Une modernisation s'impose.