Marksteine der Bundesgerichtspraxis zur strafprozessualen Überwachung des digitalen Fernmeldeverkehrs

Probleme der grenzüberschreitenden Strafverfolgung bei Delikten über soziale Netzwerke und den mobilen Internetverkehr

Marc Forster

Inhaltsübersicht

I. Überwachung digitaler sozialer Netzwerke

1. Problematik der grenzüberschreitenden Strafverfolgung von Cybercrime

Am 1. Januar 2012 ist das Internationale Übereinkommen vom 23. November 2001 über die *Cyberkriminalität* (CCC)[1] für die Schweiz in Kraft getreten. Neben den meisten europäischen Staaten (sowie unter anderen Kanada, Australien und Japan) haben

[1] SR 0.311.43.

auch die Vereinigten Staaten von Amerika das Übereinkommen ratifiziert. Es ist für die USA seit 1. Januar 2007 in Kraft. In der Präambel zum CCC weisen die Mitgliedstaaten des Europarates und die übrigen Vertragsstaaten des Übereinkommens unter anderem darauf hin, dass zur wirksamen Bekämpfung der Computerkriminalität eine verstärkte, zügige und gut funktionierende *internationale Zusammenarbeit* in *Strafsachen* nötig sei. Zweck des Übereinkommens ist es (laut Art. 39 Abs. 1 CCC), die zwischen den Vertragsparteien bestehenden zwei- oder mehrseitigen Verträge oder Übereinkünfte in diesem Sinne zu *ergänzen*.[2]

Die Vertragsstaaten des Übereinkommens mussten feststellen, dass die modernen Kommunikations- und Datenverarbeitungstechnologien eine *Herausforderung* für die Bekämpfung der Computer- und Internetkriminalität darstellen. Elektronische Daten werden (unabhängig vom Herkunfts- oder Aufbewahrungsort) *innert Sekunden* an beliebige Empfänger auf der ganzen Welt versandt oder an eine Vielzahl von Personen und Einrichtungen verbreitet. In Computersystemen gespeicherte Informationen können für einen bestimmten oder unbestimmten Personenkreis zugänglich gemacht, gezielt gesucht und entsprechend heruntergeladen werden. Staatsgrenzen bilden für den Informationsfluss im Internetzeitalter *keine Hindernisse* mehr, und die neuen Technologien führen in steigendem Masse dazu, dass die *Aktivitäts*- und die *Erfolgsorte* von deliktischem Verhalten geographisch *weit auseinander* liegen können. Da der Anwendungsbereich der staatlichen (insbesondere strafprozessualen) Gesetzgebungen demgegenüber vom *Territorialitätsgrundsatz* begrenzt wird,[3] muss

[2] Insbesondere das Europäische Übereinkommen vom 20. April 1959 über die Rechtshilfe in Strafsachen (EUeR, SR 0.351.1) oder (im Verhältnis zwischen der Schweiz und den USA) der Staatsvertrag vom 25. Mai 1973 zwischen der Schweizerischen Eidgenossenschaft und den Vereinigten Staaten von Amerika über gegenseitige Rechtshilfe in Strafsachen (RVUS, SR 0.351.933.6). Am 28. Januar 2003 wurde ein *Zusatzprotokoll* zum CCC abgeschlossen, welches *rassistische* und *fremdenfeindliche Handlungen* über *Computersysteme* zum Gegenstand hat (ETS Nr. 189). Dieses Zusatzprotokoll wurde von der Schweiz am 9. Oktober 2003 unterzeichnet. Es trat am 1. März 2006 (nach den ersten fünf Ratifikationen) für diverse Vertragsstaaten in Kraft. Die Schweiz hat das Zusatzprotokoll zum Cybercrime-Übereinkommen bisher noch nicht ratifiziert. Die USA haben es nicht unterzeichnet. Das CCC ist auch auf die internationale Verfolgung von *Rassismus* anwendbar; das *Zusatzprotokoll* verpflichtet die Vertragsstaaten aber darüber hinaus noch zu spezifischen *materiellstrafrechtlichen* Regelungen gegen Rassismus (vgl. Niggli Marcel A., Rassendiskriminierung und Internet, in: Christian Schwarzenegger/Oliver Arter/Florian S. Jörg [Hrsg.], Internet-Recht und Strafrecht, Bern 2005, S. 299 ff., 323 ff.). Ob die *USA* das Zusatzprotokoll unterzeichnen werden, ist *unsicher*, da nach US-Recht der Meinungsäusserungsfreiheit ein *sehr hoher* Stellenwert zukommt (vgl. Baltisser Annina, Datenbeschädigung und Malware im Schweizer Strafrecht – Der Tatbestand des Art. 144bis StGB im Vergleich mit den Vorgaben der Cybercrime Convention und der deutschen Regelung, Diss., Zürich 2013, S. 148).

[3] Vgl dazu Charlet François/Boquet Cédric, De l'application de la LSCPT aux fournissseurs de services de VoIP, Jusletter vom 10. November 2014, Rz. 37; Donatsch Andreas/Heimgartner Stefan/

die Strafverfolgung im Bereich des Cybercrime dringend über *adäquate Instrumente* des *internationalen Strafrechts* unterstützt werden.[4]

Die international vereinheitlichten und spezifizierten Instrumente des Cybercrime-Übereinkommens versuchen insbesondere den Umständen Rechnung zu tragen, dass förmliche *Rechtshilfeverfahren* sich regelmässig *aufwändig, kompliziert* und *langwierig* gestalten und diverse Staaten keine oder nur eine relativ kurze *«Vorratsdatenspeicherung»* in Bezug auf die rückwirkende Erhebung von Randdaten des elektronischen Fernmeldeverkehrs kennen,[5] weshalb der *Ablauf* der gesetzlichen *Überwachungsfrist* droht, noch bevor über ein hängiges Rechtshilfegesuch entschieden werden konnte.[6] Das Übereinkommen sieht diesbezüglich *spezifische Instrumente* vor, darunter die vorsorgliche *umgehende Sicherung* gespeicherter Computerdaten im Hinblick auf ein

---

Simonek Madeleine, Internationale Rechtshilfe, Zürich 2011, S. 4, 34 f.; Dyens Alexandre, Territorialité et ubiquité en droit pénal international suisse, Diss. Lausanne, Basel 2014, S. 19 f.; Gless Sabine, Internationales Strafrecht, Basel 2011, Rz. 258; Heimgartner Stefan, Die internationale Dimension von Internetstraffällen – Strafhoheit und internationale Rechtshilfe in Strafsachen, in: Christian Schwarzenegger/Oliver Arter/Florian S. Jörg (Hrsg.), Internet-Recht und Strafrecht, Bern 2005, S. 117 ff., 120 ff., 135; Morscher Lukas, Aktuelle Entwicklungen im Technologie- und Kommunikationsrecht, ZBJV 147 (2011), S. 177 ff., 214 f.; Ryser Dominic, «Computer Forensics», eine neue Herausforderung für das Strafprozessrecht, in: Christian Schwarzenegger/Oliver Arter/Florian S. Jörg (Hrsg.), Internet-Recht und Strafrecht, Bern 2005, S. 553 ff., 575 f.; Schweingruber Sandra, Cybercrime-Strafverfolgung im Konflikt mit dem Territorialitätsprinzip, Jusletter vom 10. November 2014, Rz. 4; Seitz Nicolai, Strafverfolgungsmassnahmen im Internet, Diss., Köln 2004, S. 366 f.; Unseld Lea, Internationale Rechtshilfe im Steuerrecht, Diss., Zürich 2011, S. 6 f.; Zimmermann Robert, La coopération judiciaire internationale en matière pénale, 4. Aufl. Bern 2014, Rz. 568; Botschaft zum Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) vom 27. Februar 2013 (nachfolgend Botschaft BÜPF), BBl 2013 2683 ff., 2689, 2708, 2742 unten; BGer 1B_344/2014 vom 14. Januar 2015, E. 5.3.

4 Vgl. Council of Europe, Explanatory Report to the Convention on Cybercrime (Explanatory Report CCC), *<http:conventions.coe.inttreatyenreportshtml185.htm>*, Ziff. 6; Botschaft über die Genehmigung und die Umsetzung des Übereinkommens des Europarates über die Cyberkriminalität vom 18. Juni 2010 (nachfolgend Botschaft CCC), BBl 2010 4697 ff., 4700, Ziff. 1.1; Baltisser (Fn. 2), S. 147 ff.; Heimgartner (Fn. 3), S. 142 ff.; Hilgendorf Eric, Tendenzen und Probleme einer Harmonisierung des Internetstrafrechts auf Europäischer Ebene, in: Christian Schwarzenegger/Oliver Arter/Florian S. Jörg (Hrsg.), Internet-Recht und Strafrecht, Bern 2005, S. 257 ff., 268 ff.; Schwarzenegger Christian, Die internationale Harmonisierung des Computer- und Internetstrafrechts durch die Convention on Cybercrime vom 23. November 2001, in: Andreas Donatsch/Marc Forster/Christian Schwarzenegger (Hrsg.), Strafrecht, Strafprozessrecht und Menschenrechte, Festschrift für Stefan Trechsel zum 65. Geburtstag, Zürich 2002, S. 305 ff.; Seitz (Fn. 3), S. 357 ff.; BGer 1B_344/2014 vom 14. Januar 2015, E. 5.4.

5 Vgl. Art. 273 Abs. 3 StPO; s.a. Art. 16 Abs. 2 CCC.

6 Vgl. Heimgartner (Fn. 3), S. 134 ff.; Schweingruber (Fn. 3), Rz. 5; Seitz (Fn. 3), S. 355 ff.; BGer 1B_344/2014 vom 14. Januar 2015, E. 5.5.

späteres Rechtshilfeersuchen,[7] die *umgehende Weitergabe* von *Verkehrsdaten* (Art. 1 Bst. d CCC), welche aufgrund eines vorsorglichen Ersuchens (nach Art. 29 CCC) gesichert wurden[8] sowie den direkten *grenzüberschreitenden Zugriff* in jenen Fällen, bei denen ein Berechtigter (etwa ein ausländischer Internet Service Provider) der Datenerhebung zugestimmt hat.[9]

2. Grundsatzurteil zu sozialen Netzwerken mit im Ausland gespeicherten Randdaten der Internet-Kommunikation («IP-History»)

Am 14. Januar 2015 fällte das Bundesgericht ein Grundsatzurteil, in welchem es die *rechtshilferechtlichen* und die *strafprozessualen* (ausnahmsweise auch grenzüberschreitenden) *Überwachungsmöglichkeiten* gemäss dem Internationalen Cybercrime-Übereinkommen voneinander abgrenzte. Im beurteilten Fall versuchten die Zürcher Strafverfolgungsbehörden, auf (in den USA gespeicherte) *Kommunikations-Randdaten* zuzugreifen. Um zu ermitteln, welche Personen (vermutlich von Anschlüssen in der Schweiz aus) inkriminierte *rassistische Nachrichten* (Postings) auf Webseiten eines weltweit verbreiteten «Social Network» platziert hatten (welches ein in den USA domiziliertes Unternehmen anbietet), verlangten die Schweizer Strafverfolger vom US-amerikanischen Internet Service Provider die Herausgabe der «*IP-Histories*» der beteiligten Kunden. Da die Voraussetzungen (von Art. 32 CCC) einer *grenzüberschreitenden* rückwirkenden Erhebung von Verkehrsdaten (Art. 1 Bst. d CCC) nicht erfüllt waren, wurden die Zürcher Strafverfolgungsbehörden jedoch auf den *Rechtshilfeweg* verwiesen.[10]

Ob und inwieweit (im Hinblick auf ein Rechtshilfersuchen) Gesuche der inländischen Strafverfolgungsbehörde um *vorsorgliche umgehende Sicherung*[11] zu bewilligen sind, und ob eine umgehende Weitergabe von *Verkehrsdaten* erfolgen kann, welche aufgrund des vorsorglichen Ersuchens gesichert wurden (Art. 30 CCC), hat nach den Bestimmungen des Cybercrime-Übereinkommens die zuständige Behörde des (nach Art. 29 CCC) *ersuchten Staates* zu entscheiden.[12] Damit die Schweizer Strafverfolgungsbehörden direkt («grenzüberschreitend») auf *nicht öffentlich zugängliche*[13]

[7] «Expedited preservation of stored computer data», Art. 29 CCC; s. dazu Heimgartner (Fn. 3), S. 144 f.; Seitz (Fn. 3), 358.
[8] «Expedited disclosure of preserved traffic data».
[9] «Trans-border access to stored computer data with consent».
[10] Zur amtl. Publ. bestimmtes Urteil BGer 1B_344/2014 vom 14. Januar 2015, E. 5.
[11] Art. 29 CCC, «Expedited preservation request».
[12] BGer 1B_344/2014 vom 14. Januar 2015, E. 5.6–5.7.
[13] Art. 32 Bst. a CCC.

Verkehrsdaten (Kommunikations-Randdaten i.S.v. Art. 273 StPO) greifen könnten, müsste (nach Art. 32 Bst. b CCC) eine «rechtmässige und freiwillige *Zustimmung*» des Inhabers der Daten bzw. eines Herausgabeberechtigten erfolgt sein. Als Zustimmungsberechtigte kommen auch *ausländische* Personen und Gesellschaften in Frage, insbesondere *Internet Service Provider,* welche sich in ihren *Allgemeinen Nutzungsbedingungen* bzw. Datenverwendungsrichtlinien das Recht auf Datenweiterleitung an in- und ausländische Strafverfolgungsbehörden gegenüber ihren Kunden *ausbedungen* haben. Entgegen der Ansicht des Bundesrates bedarf es *keiner* Zustimmung «einer Person im *Inland*», welche rechtmässig befugt ist, die Daten «an eine inländische Strafverfolgungsbehörde weiterzuleiten».[14] Die «freiwillige Zustimmung» eines Berechtigten lag jedoch im beurteilten Fall nicht vor. Die streitige Randdatenerhebung (bzw. rückwirkende Überwachung) in den USA war deshalb auf dem förmlichen Rechtshilfeweg (Art. 31 CCC bzw. RVUS) zu beantragen.[15]

Was die Abfrage von ausländischen *Bestandesdaten* (vgl. dazu unten, Ziff. 3) des Internetverkehrs betrifft, ergibt sich aus Art. 18 Abs. 1 Bst. b CCC (über Art. 32 CCC hinaus) kein zusätzlicher Anspruch auf *grenzüberschreitende* Datenerhebung.[16] Für Gesuche um Herausgabe von Registrierungsdaten bei in den USA domizilierten Anbieterinnen ist das (von den US-amerikanischen Behörden anzuwendende) Amts- und

[14] BGer 1B_344/2014 vom 14. Januar 2015, E. 5.9–5.10; *anders* Botschaft CCC (Fn. 4), 4738. *Zutreffend* wäre, dass auch *inländische* Inhaber von E-Mail-Konten oder inländische Kunden von sozialen Netzwerken direkt ihre freiwillige Zustimmung zur Datenherausgabe geben könnten (Heimgartner [Fn. 3], S. 146; Seitz [Fn. 3], S. 371). In solchen Fällen braucht es keine *zusätzliche* Zustimmung der ausländischer Providerfirma (oder eines anderen Verwalters der Daten). Inländische Nutzer von Internetangeboten wissen denn auch oft gar nicht, *in welchem Land* ihre Daten gespeichert werden. Zwei auf Internetanschlüssen in der Schweiz miteinander kommunizierende User von digitalen Netzwerken und Nachrichtendiensten sind sich z.B. selten bewusst, dass ihre Daten im Ausland (oft in den USA) gespeichert werden (Seitz [Fn. 3], S. 356). Die verunglückte Formulierung in der Botschaft geht über eine solche (zutreffende) Aussage allerdings hinaus, und im vorliegenden Fall lag gerade *keine Zustimmung* von *inländischen Kunden* der US-Providerfirma vor. Diese sollten durch die Verkehrsdatenerhebung in den USA erst *identifiziert* werden. Art. 32 Bst. b CCC ist im Übrigen auch auf den Fall anwendbar, dass im *Inland* agierende *Töchter* oder *Partner* ausländischer Provider angewiesen werden, Daten auszuliefern, die *im Ausland* (bei der Muttergesellschaft) gespeichert werden (Seitz [Fn. 3], S. 371). Wenn ausländische Provider hingegen Schweizer Tochtergesellschaften oder Partner haben, die in der *Schweiz* Daten speichern (sogenannte «Server Farms»), ist diesbezüglich *schweizerisches* Landesrecht (StPO/BÜPF) anwendbar (Morscher [Fn. 3], S. 214 f.).

[15] BGer 1B_344/2014 vom 14. Januar 2015, E. 5.11–5.12.

[16] BGer 1B_344/2014 vom 14. Januar 2015, E. 6.4; *a.M.* Schweingruber (Fn. 3), Rz. 25–28. In der Schweiz ansässige «Server Farms» von ausländischen Providern haben in der *Schweiz* gespeicherte Bestandesdaten hingegen (gestützt auf Art. 14 BÜPF) herauszugeben (BGer 1B_344/2014 vom 14. Januar 2015, E. 6.4).

Rechtshilferecht massgeblich. Ob allenfalls eine (rechtshilferechtliche) sogenannte *unaufgeforderte Übermittlung* von Bestandesdaten (ohne förmliches Rechtshilfeersuchen) durch die US-Behörden möglich und geboten wäre (Art. 26 CCC), hatte nicht das kantonale Zwangsmassnahmengericht (grenzübergreifend) zu entscheiden.[17]

3. Zur Abgrenzung zwischen Verkehrs- und Bestandesdaten im Internetverkehr

a) Definitionsgrundlagen

Die Erhebung von *Verbindungs-Randdaten* des Fernmeldeverkehrs (bzw. die Teilnehmeridentifikation im Sinne von Art. 273 Abs. 1 StPO) ist zu unterscheiden von der blossen *Bestandesdaten*-Auskunft (nach Art. 14 BÜPF) über registrierte Fernmeldeanschlüsse. Bei der Teilnehmeridentifikation (nach Art. 273 Abs. 1 Bst. a StPO) werden Teilnehmer an *konkreten Fernmeldeverbindungen* über einen gewissen Zeitraum hinweg identifiziert.[18] Das heisst, es werden *Verkehrsdaten* (keine Kommunikations*inhalte*) von Kommunikationen erhoben und gestützt darauf Anschlüsse und Teilnehmer identifiziert. Hier muss nach schweizerischem Recht der dringende Verdacht eines *Verbrechens* oder *Vergehens* (Art. 273 Abs. 1 StPO) vorliegen. Ausserdem muss die Verbindungsdaten-Erhebung *richterlich bewilligt* werden (Art. 273 Abs. 2 StPO).[19] Art. 1 Bst. d CCC definiert als *Verkehrsdaten* («Traffic data») im Sinne des Cybercrime-Übereinkommens «*alle Computerdaten* in Zusammenhang mit einer Kommunikation unter Nutzung eines Computersystems, die von einem Computersystem, das *Teil der Kommunikationskette* war, erzeugt wurden und aus denen der *Ursprung,* das *Ziel,* der *Leitweg,* die *Uhrzeit,* das *Datum,* der *Umfang* oder die *Dauer* der Kommunikation oder die *Art* des für die Kommunikation benutzten *Dienstes* hervorgeht». Bei blossen *Bestandesdaten*-Auskünften (nach Art. 14 Abs. 1 BÜPF) hingegen sind die Internet-Anschlüsse den Strafverfolgungsbehörden bereits *bekannt*,[20] und es wird den auskunftsberechtigten Behörden lediglich mitgeteilt, wer als Inhaber bzw. Rechnungsadressat dieses Anschlusses bei den Anbieterinnen *registriert* ist.[21] Es werden hier also lediglich Registierungsdaten mitgeteilt, aber keine Verbindungsdaten zu Kommuni-

[17] Zur amtl. Publ. bestimmtes Urteil BGer 1B_344/2014, E. 6.3, 6.5.

[18] «Verbindungen hat oder gehabt hat».

[19] Zum Begriff der *Verkehrsdaten* (Verbindungs-Randdaten) s. Art. 13 Abs. 1 Bst. d und Art. 15 Abs. 1–4 BÜPF (dazu Hansjakob Thomas, in: Andreas Donatsch/Thomas Hansjakob/Viktor Lieber [Hrsg.], Kommentar zur Schweizerischen Strafprozessordnung [StPO], 2. Aufl. Zürich 2014, Art. 273 Rz. 1–10; Seitz [Fn. 3], S. 147 ff.; BGE 137 IV 340).

[20] «Bestimmte Fernmeldeanschlüsse».

[21] Vgl. Hansjakob (Fn. 19), Art. 273 Rz. 7; Seitz (Fn. 3), S. 72 ff. Zur *Bestandesdaten*-Definition des Cybercrime-Übereinkommens s. Art. 18 Abs. 3 CCC.

kationen erhoben. Blosse Auskünfte über bekannte Anschlüsse (nach Art. 14 Abs. 1 BÜPF) werden daher nicht nur zu Strafverfolgungszwecken an die Staatsanwaltschaft erteilt, sondern auch an die Polizei zur Erfüllung polizeilicher Aufgaben.[22] Eine richterliche Bewilligung ist hier nicht erforderlich.[23] Eine Bestandesdatenerhebung kann (nötigenfalls) über eine Editionsverfügung erfolgen (Art. 265 StPO). Bei Straftaten, die über das *Internet* begangen werden, sind die (dem schweizerischen Recht unterworfenen[24]) Dienstanbieterinnen verpflichtet, der Polizei und der Staatsanwaltschaft alle Angaben zu machen, die eine Identifikation des Urhebers ermöglichen.[25] Bei Erhebungen gemäss Art. 14 Abs. 4 BÜPF wird allerdings nur abgeklärt, wer einen *bestimmten Internet-Anschluss benützt* hat. Entsprechende Bestandesdaten müssen zehn Jahre rückwirkend ediert werden. Randdatenerhebungen nach Art. 273 StPO liegen demgegenüber vor, wenn eruiert werden soll, «wer wann mit wem» über das Internet «kommuniziert» hat.[26]

b) Abgrenzungsschwierigkeiten in der Praxis

In mehreren Urteilen[27] hat das Bundesgericht *Abgrenzungsschwierigkeiten* zwischen der Randdaten- und Bestandesdatenerhebung im Internetverkehr festgestellt. In BGE 139 IV 98 hat es Art. 14 Abs. 4 BÜPF für anwendbar erklärt[28] in einem Fall, bei dem der Staatsanwaltschaft ein Internetanschluss (mit einer sogenannten «statischen» IP-Adresse) *bereits bekannt* war. Die Staatsanwaltschaft verlangte rückwirkend die Bekanntgabe der *Identität* jener Teilnehmer, die während knapp zwei Monaten (2. Juni bis 20. Juli 2011) diesen Anschluss benutzt hatten. Das Urteil wurde in der Lehre teilweise kritisiert. Zwar sei es im Ergebnis durchaus richtig. Das Bundesgericht

---

[22] Art. 14 Abs. 2 Bst. a–b BÜPF.

[23] Vgl. Hansjakob Thomas, Wichtige Entwicklungen der Bundesgerichtspraxis zu Überwachungen des Post- und Fernmeldeverkehrs, forum poenale 2013, S. 173 ff., 176 f.; zur amtl. Publ. bestimmtes Urteil BGer 1B_344/2014 vom 14. Januar 2015, E. 6.2.

[24] Als Konsequenz des *Territorialitätsgrundsatzes* (s. oben, Ziff. 1) sind in der Schweiz ansässige Tochter- oder Partnergesellschaften von ausländischen Providerfirmen, die *in der Schweiz Daten speichern* (sogenannte «Server Farms»), dem schweizerischen Recht (StPO/BÜPF) unterworfen (vgl. Morscher [Fn. 3], S. 214 f.; BGer 1B_344/2014 vom 14. Januar 2015, E. 6.2).

[25] Art. 14 Abs. 4 i.V.m. Art. 1 Abs. 1–2 BÜPF sowie Art. 24*b* und Art. 27 VÜPF.

[26] Hansjakob (Fn. 19), Art. 273 Rz. 8.

[27] Etwa BGE 139 IV 98 und zur amtl. Publ. bestimmtes Urteil BGer 1B_344/2014 vom 14. Januar 2015, E. 5.1, 6.2.

[28] Mit der Folge, dass jedenfalls die *sechsmonatige Frist* für rückwirkende Teilnehmeridentifikationen gestützt auf *Verbindungs-Randdaten* (Art. 273 Abs. 3 StPO) *nicht anwendbar* war.

habe jedoch die Randdaten- und Bestandesdatenerhebung miteinander «vermischt», welche das Gesetz «sauber» trenne.[29]

c) «Saubere» gesetzliche Abgrenzung?

Es fragt sich, ob die Abgrenzung zwischen Verbindungs-Randdaten und Bestandesdaten im Bereich des mobilen Internetverkehrs wirklich derart klar erscheint und für die Anwendungsschwierigkeiten primär die Gerichtspraxis verantwortlich zu machen ist:

Bei *Internetadressen* ist die Angabe eines registrierten Inhabers des Fernmelde-Anschlusses bzw. eines Rechnungsadressaten[30] schon aus technischen Gründen nicht ohne weiteres möglich, da der Internet Service Provider seinen Kunden in der Regel *für jede Session* eine *neue IP-Adresse* zuweist. Um den Teilnehmer zu *identifizieren,* muss der Provider somit zusätzlich alle zugewiesenen IP-Adressen abspeichern.[31] Wollen inländische Strafverfolger Kunden von *sozialen Netzwerken* (mit Internetanschlüssen im Inland, aber Randdatenspeicherung bei Providern im Ausland) gestützt auf Internetaktivitäten *identifizieren,* benötigen sie grundsätzlich[32] die «IP-History» des ausländischen Netzwerk-Providers.[33] Bei Straftaten, die über das Internet begangen werden, sind die dem schweizerischen Recht unterworfenen Dienstanbieterinnen zwar verpflichtet, der Polizei und der Staatsanwaltschaft «alle» (auch rückwirkenden) «Angaben» zu machen, die eine Identifikation des Urhebers ermöglichen.[34] Es stellen sich jedoch Abgrenzungsfragen, wenn der Internet-Anschluss den Strafverfolgungsbehörden nicht bereits bekannt ist und somit kein «typischer» Fall einer Bestandesdaten-Abfrage (im Sinne von Art. 14 Abs. 1 BÜPF) vorliegt. Falls bei Untersuchungen wegen Internetdelikten bereits eine E-Mail-Adresse bzw. ein Internetanschluss *be-*

[29] So Hansjakob (Fn. 23), S. 176 f. Zu den «praktisch häufigsten» Anwendungsfällen von Bestandesdatenerhebungen nach Art. 14 Abs. 4 BÜPF gehöre (laut Hansjakob [Fn. 23], S. 177) die Frage, «wer in einem Social Media eine bestimmte Mitteilung verfasst hat».

[30] Vgl. Art. 14 Abs. 1 i.V.m. Art. 13 Abs. 1 Bst. d BÜPF.

[31] Vgl. dazu Hansjakob (Fn. 23), S. 176; Métille Sylvain, Mesures techniques de surveillance et respect des droits fondamentaux, en particulier dans le cadre de l'instruction pénale et du renseignement, Diss. Neuchâtel, Basel 2011, S. 40 ff.; Seitz (Fn. 3), S. 9 ff.; Botschaft BÜPF (Fn. 3), 2702 Ziff. 1.4.16, 2732 f., 2736, 2742 f., 2746, 2769 f.

[32] Jedenfalls bei *mobilem verschlüsseltem* Internetverkehr.

[33] Vgl. zur amtl. Publ. bestimmtes Urteil BGer 1B_344/2014 vom 14. Januar 2015, E. 5.1–5.2 (dazu oben, Ziff. 2).

[34] Art. 14 Abs. 4 i.V.m. Art. 1 Abs. 1–2 BÜPF sowie Art. 24*b* und Art. 27 VÜPF; vgl. BGE 139 IV 98 E. 4.8 S. 101 f.; BGE 139 IV 195 E. 2.2 S. 197.

kannt ist, stellt die Ermittlung der betreffenden *Registrierungsdaten* grundsätzlich eine *Bestandesdatenabfrage* (im Sinne von Art. 14 Abs. 4 BÜPF) dar.[35]

Um eine Abfrage von blossen Registrierungsdaten kann es sich insbesondere handeln, falls sie eine bereits *bekannte* «statische» IP-Adresse betrifft.[36] Wenn den Strafverfolgungsbehörden hingegen lediglich strafbare Internet-*Kommunikationsaktivitäten* bekannt geworden sind, zum Beispiel Postings auf (passwortgeschützten bzw. beschränkt zugänglichen) *sozialen Netzwerken,* und über die *Verbindungs-Randdaten* der betreffenden Internet-Kommunikation die zugewiesenen IP-Adressen («IP-History») und registrierten Kunden *erst eruiert* werden sollen, sind bei Überwachungen in der Schweiz grundsätzlich die Vorschriften von Art. 273 StPO anwendbar.[37] Nach dem Gesagten kann von einer klaren gesetzlichen Abgrenzung der Datenerhebungen zur Identitätsfeststellung im Internetverkehr keine Rede sein.[38]

II. Überwachung des digitalen Nachrichtenverkehrs

1. Edition von gespeicherten Nachrichten

Weitere juristische Abgrenzungsfragen stellen sich beim *mobilen Nachrichtenverkehr.* Wenn Handys und Smartphones *physisch sichergestellt* werden und die Staatsanwaltschaft die *gespeicherten Daten auswerten* will (also Kontaktnummern, Verbindungs-

[35] Vgl. Hansjakob (Fn. 23), S. 177; Hansjakob (Fn. 19), Art. 273 Rz. 8; zur amtl. Publ. bestimmtes Urteil BGer 1B_344/2014 vom 14. Januar 2015, E. 5.1; BGE 139 IV 98.

[36] Vgl. Hansjakob (Fn. 23), S. 177; BGE 139 IV 98. Allerdings sind *statische* IP-Adressen gerade *untypisch* (bzw. technisch ungebräuchlich) bei *mobilem verschlüsseltem Internetverkehr* und insbesondere Kommunikationen über *Social Media.*

[37] Zur amtl. Publ. bestimmtes Urteil BGer 1B_344/2014 vom 14. Januar 2015, E. 5.1 (vgl. oben, Ziff. 2); Schweingruber (Fn. 3), Rz. 29; s.a. BGE 126 I 50 E. 5–6 S. 60 ff.; Botschaft BÜPF (Fn. 3), 2743. In solchen Fällen wird eruiert «wer wann mit wem» über das Internet «kommuniziert» hat. Dies entspricht auch den Definitionen der *Verkehrsdaten*erhebung gemäss Art. 1 Bst. d CCC (s. oben, Bst. a) bzw. der *Randdaten*erhebung (nach Art. 273 StPO) bei Hansjakob (Fn. 19), Art. 273 Rz. 8; teilweise *a.M.* offenbar Hansjakob (Fn. 23), S. 177, der die «Frage, wer in einem Social Media eine bestimmte Mitteilung verfasst hat», sogar zu den «praktisch häufigsten» Anwendungsfällen von «Abklärungen nach Art. 14 Abs. 4 BÜPF» zählt.

[38] Soweit in der Literatur kritisiert wird, das Bundesgericht habe bei der heiklen Abgrenzung zwischen Randdaten- und Bestandesdatenerhebung im Internetverkehr *Unklarheiten* offen gelassen, fällt dieser Vorwurf letztlich auf die Lehre zurück: Es dürfte kaum die Aufgabe des Bundesgerichtes sein, in diesem juristisch neuen sowie technisch hoch komplexen und dynamischen Bereich die systematisierende dogmatische Grundlagenarbeit zu leisten.

daten, inhaltliche SMS- und E-Mail-Korrespondenz[39] usw.), liegt nach der Praxis des Bundesgerichtes grundsätzlich *keine Überwachung* (Art. 269 StPO) vor und auch *keine* rückwirkende *Randdatenerhebung* (Art. 273 StPO). Der Rechtsschutz läuft hier in der Weise, dass die betroffene Person die *Siegelung* (Art. 248 StPO) des edierten oder sichergestellten Gerätes verlangen kann (wie bei PCs, Notebooks, Servern usw). Die Staatsanwaltschaft, welche die elektronischen Aufzeichnungen durchsuchen will, muss dann beim Zwangsmassnahmengericht ein *Entsiegelungsgesuch* stellen.[40]

2. Aktives «Abfangen» von E-Mails und SMS

Anders ist die Rechtslage, wenn *keine* Geräte *physisch* sichergestellt und ausgewertet (und keine gespeicherten Nachrichten nachträglich ediert) werden, sondern wenn die Staatsanwaltschaft E-Mails und SMS geheim «*abfangen*» (bzw. aktiv, noch während des Kommunikationsvorgangs, beim Provider edieren) lässt. Die Abgrenzung zwischen *Überwachung*[41] und *Edition* (bzw. Beschlagnahme) von aufgezeichneten digitalen Nachrichten[42] ist in mehrfacher Hinsicht von grosser Bedeutung: Praktisch wird die Internet-Kommunikation über digitale Nachrichtendienste und Social Networks immer wichtiger (s. oben, Ziff. I/1). Und juristisch werden bei der Abgrenzung zwischen Überwachung und Edition/Beschlagnahmung *prozessentscheidende Weichen* gestellt: Die gesetzlichen Voraussetzungen und Verfahrenswege dieser Zwangsmassnahmen unterscheiden sich stark.[43] Falls die Staatsanwaltschaft die Massnahme juristisch falsch einstuft bzw. glaubt, sie könne in jedem Fall (ohne vorgängige richterliche

[39] Und zwar *Nachrichteninhalte*, die vom Empfänger schon «*abgerufen*» worden sind. Bei *noch nicht abgerufenen* SMS und E-Mails liegt eine *aktive geheime Überwachung* vor (dazu unten, Ziff. 2).

[40] Vgl. BGer 1B_432/2013 vom 17. Februar 2013.

[41] Sogenanntes «Abfangen» von digitalen Nachrichten in Unkenntnis des Empfängers *während* des *Kommunikationsvorgangs,* d.h. bevor sie vom Empfänger auf dessen Nachrichtenkonto «abgerufen» wurden.

[42] Nach *Abschluss* des *Kommunikationsvorgangs,* also wenn der Empfänger *gesehen* hat (bzw. sehen konnte), dass die Nachricht bei ihm eingegangen ist.

[43] Wenn eine Massnahme als geheime *Überwachung* (Ue) einzustufen ist, bildet die vorgängige *richterliche Bewilligung* ein *Verwertbarkeitserfordernis*. Das heisst, wenn der Sachrichter später im Hauptverfahren feststellt, dass im Ue-Verfahren die Bewilligung durch den Zwangsmassnahmenrichter versäumt wurde, können die Ue-Ergebnisse nicht verwertet werden. Der Sachrichter prüft zwar die Rechtmässigkeit von rechtskräftig bewilligten Überwachungen nicht mehr: Die Rechtmässigkeit der Ue ist im Bewilligungs- und Beschwerdeverfahren rechtskräftig zu prüfen. Der Sachrichter prüft aber die Verwertbarkeit der ihm vorgelegten Beweismittel. Bei geheimen Überwachungen, die nicht vorgängig richterlich bewilligt wurden, sieht das Gesetz die *absolute Unverwertbarkeit* vor (Art. 277 Abs. 2 i.V.m. Art. 141 Abs. 1 Satz 2 StPO).

Bewilligung) die Edition von digitalen Nachrichten beim Provider anordnen, droht ihr ein *Beweisverlust*.[44]

3. Abgrenzung durch das Bundesgericht

Am 28. Mai 2014 hat das Bundesgericht dazu ein weiteres *Grundsatzurteil*[45] gefällt: Das Zwangsmassnahmengericht des Kantons Aargau hatte den Standpunkt vertreten, dass jegliche Herausgabe von *E-Mail-Verkehr* durch Internet-Provider eine *Edition* darstelle und keine geheime Überwachung. Das Bundesgericht hat eine *Analogie* getroffen zwischen dem *Briefverkehr* (mit Postfach) und dem E-Mail-Verkehr (über Mailkonten): Entscheidend ist der *Zeitpunkt,* in dem der Internet-User sein *Mailkonto öffnet* und *sieht* (bzw. sehen *kann*), dass die (neue) E-Mail *eingegangen* ist.[46] *Vor* diesem Zeitpunkt liegt eine geheime aktive *Überwachung* (Art. 269 StPO) vor, wenn der Provider versendete E-Mails der Staatsanwaltschaft zugänglich macht.[47] Hier braucht es also eine *vorgängige* richterliche Bewilligung.[48] *Ab* diesem Zeitpunkt *weiss* der Empfänger (bzw. er *kann* es zurechenbar wissen), dass ihm die Nachricht zugestellt wurde. Jede Herausgabe von Nachrichten seit *Kenntnis* des Mail-*Einganges* stellt keine geheime Überwachung mehr dar, sondern eine Edition (Art. 265 StPO) bzw. Sicherstellung/Beschlagnahmung (Art. 263 StPO) von aufgezeichneter Korrespondenz.[49]

---

[44] Eine «nachträgliche» Bewilligung durch den Sachrichter (oder das ZMG) ist nicht mehr möglich, wenn es sich um eine geheime aktive Überwachung gehandelt hat, d.h., wenn die E-Mails vor Abschluss des Kommunikationsvorganges «abgefangen» wurden (bevor der Empfänger Kenntnis vom Eingang der E-Mail erhielt). Zur «Fernwirkung» von Beweisverwertungsverboten s.a. unten, Ziff. III/1.

[45] BGE 140 IV 181.

[46] Sogenanntes «*Abrufen*» der E-Mail, nicht zu verwechseln mit dem *Anklicken* und *Lesen* der Mailnachricht.

[47] «Abfangen» von Nachrichten.

[48] Diese Überwachung ist eine geheime (aktive) *Echtzeit*-Überwachung von Kommunikation, da diese *noch nicht abgeschlossen* ist: Der Empfänger weiss noch nicht, dass die Nachricht zu ihm unterwegs ist bzw. war. Sie wird vorher «abgefangen». Da Echtzeit-Überwachungen zeitlich beschränkt sind (auf zunächst höchstens drei Monate Dauer, richterlich verlängerbar), können E-Mails «abgefangen» werden, die zwischen dem Überwachungs-Gesuch und dem Ablauf der richterlich bewilligten Ue-Frist versendet wurden. Ohne vorgängige richterliche Bewilligung dürfen «abgefangene» E-Mails später nicht als Beweismittel verwertet werden.

[49] Der Rechtsschutz erfolgt hier über ein *Siegelungsgesuch* und das Entsiegelungsverfahren. Entscheidend ist somit das sogenannte *Abrufen* der E-Mail, d.h. das *Öffnen* des Mail-*Kontos,* auf dem neue Mails (in der Regel fett hervorgehoben) *angezeigt* werden. Ob die angezeigte neue E-Mail «angeklickt» und *gelesen* wurde oder nicht, ist *nicht entscheidend,* analog zu einem *Postfachinhaber*, der zwar sein Postfach öffnet, den dort liegen-

III. Weitere markante Urteile zur Überwachung des digitalen Fernmeldeverkehrs

1. «Fernwirkung» von Beweisverwertungsverboten

Fall 1

Die Staatsanwaltschaft hat eine *aktive Telefonüberwachung* eines wegen *telefonischer Erpressung* Tatverdächtigen durchgeführt. Da die Überwachung richterlich nicht genehmigt wurde, verwendet die Staatsanwaltschaft die Tonbänder bloss als Sekundärbeweismittel (Folgebeweis) für ein *Gutachten.* Sie legt die Tonbänder einem forensischen Experten vor, der wissenschaftliche *Sprachanalysen* macht. Dieser kommt in seinem Gutachten zum Schluss, dass der Beschuldigte *auffällige Sprachmuster* verwendet, die auch der gesuchte Erpresser nachweislich verwendet hat.

Art. 141 StPO unterscheidet zwischen *absolut unverwertbaren* (Abs. 1), *ungültigen* (oder strafbar erlangten) nur *bedingt* verwertbaren (Abs. 2) und *ordnungswidrig* erlangten (aber verwertbaren) Beweisen (Abs. 3). Für diverse Beweiserhebungen, etwa die Fernmeldeüberwachung, gelten *Spezialregeln,* insbesondere zur Frage der Verwertbarkeit von indirekten *Folgebeweisen* und von *Zufallsfunden*. Nach dem Wortlaut von Art. 141 Abs. 4 StPO gilt bei *ungültigen* Beweisen *keine* absolute «Fernwirkung»: Darauf gestützte *Folgebeweise* können *verwertet* werden, wenn sie auch *ohne* den ungültigen Primärbeweis «möglich» gewesen wären. In BGE 138 IV 169 bemühte sich das Bundesgericht um eine gewisse Kohärenz zwischen der *bisherigen* (altrechtlichen) Praxis und der neuen StPO. Es ging dort um einen *Folgebeweis* nach einer *nicht* richterlich genehmigten *Telefonüberwachung* in *Slowenien,* die zu einem «Tipp» an die Schweizer Grenzwache betreffend eine bevorstehende Drogenlieferung führte. Bei der Grenzkontrolle wurden (als Folgebeweis) *6 kg Heroin sichergestellt.* Das Bundesgericht wies darauf hin, dass die nicht genehmigte Telefonüberwachung zwar *absolut unverwertbar* sei. Trotzdem bezeichnete es den *Folgebeweis,* die Kontrolle und Sicherstellung an der Grenze, als zulässig, da die Telefonüberwachung

den neuen Brief aber ungeöffnet liegen lässt. Analoges dürfte auch für *andere* Formen der Internet-Kommunikation und für *SMS* gelten. Geheime *inhaltliche* Kommunikations-Überwachungen erfolgen immer in *Echtzeit,* d.h. während des aktiven Kommunikationsvorgangs. *Rückwirkende* «Überwachungen» sind bloss im Rahmen der nachträglichen *Teilnehmeridentifikation* und von *Randdaten*erhebungen (Art. 273 StPO) möglich (rückwirkend beschränkt auf sechs Monate). Diese *rückwirkenden* Überwachungs-Massnahmen (Art. 273 StPO), welche sich *nicht* auf Kommunikations*inhalte* erstrecken, sind auch in *Echtzeit* (während des Kommunikationsvorgangs) zulässig.

keine «conditio sine qua non» (notwendige Bedingung) für die Sicherstellung der Drogen gewesen sei. Aufgrund des Verhaltens des Beschuldigten am Zollübergang und der Aufgaben der Grenzwacht sei die «Wahrscheinlichkeit» einer spontanen Kontrolle gross gewesen. Dieser BGE erging noch gestützt auf *altes* (kantonales) Strafprozessrecht. Das Bundesgericht liess dabei ausdrücklich *offen,* ob Art. 141 Abs. 4 StPO – entgegen seinem Wortlaut – nicht nur auf ungültige, sondern auch auf absolut unverwertbare Primärbeweise anwendbar sein könnte. Nachfolgend soll analysiert werden, wie der *Beispiel-Fall 1* («Sprachgutachten») und der in BGE 138 IV 169 beurteilte Fall nach geltender *StPO* zu beurteilen sind:

Die Bestimmungen von Art. 141 StPO über die Fernwirkung von Beweisverwertungsverboten sind auf die Fernmeldeüberwachung nur *ergänzend* anwendbar,[50] da hier *Spezialvorschriften* gelten. So regelt Art. 277 Abs. 2 StPO die Nichtverwertbarkeit von Ergebnissen aus *nicht genehmigten* Überwachungen; und für den Spezialfall der Verwendung von *Zufallsfunden* (aus genehmigten Überwachungen) gelten die Bestimmungen von Art. 278 StPO (dazu nachfolgend, Ziff. 2). Aus Art. 141 Abs. 2 StPO ergibt sich z.B., dass nach der Unterlassung einer *Zeugenbelehrung* (bei der es sich gemäss Art. 177 Abs. 1 StPO um eine *Gültigkeitsvorschrift* handelt) die ungültige Zeugenaussage nur verwertet werden darf, wenn dies zur *Aufklärung* einer *schweren Straftat* (Verbrechen und schwere Vergehen) *unerlässlich* erscheint. Nach den allgemeinen Regeln der Fernwirkung von Beweisverboten (Art. 141 Abs. 4 StPO) dürfen auch *Folgebeweise* oder indirekte Sekundärbeweise, die auf einem Primärbeweis *wesentlich aufbauen,*[51] *nicht verwertet* werden, wenn der *Primär*beweis eine *Gültigkeits*vorschrift verletzte *und nicht unerlässlich* schien zur Aufklärung einer schweren Straftat.[52]

Liesse sich im *Fall 1* («Sprachgutachten») argumentieren, eine Verwertung als Folgebeweis sei möglich, da die Überwachung bzw. das darauf gestützte Sprachgutachten «*unerlässlich*» seien für die Aufklärung eines Verbrechens? Art. 141 Abs. 4 (i.V.m. Abs. 2) StPO sehe hier eine *Ausnahme* von der Unverwertbarkeit vor? Die Frage ist zu *verneinen:* Art. 141 Abs. 4 (i.V.m. Abs. 2) StPO beschränkt sich ausdrücklich auf Folgebeweise nach Verletzung von *Gültigkeitsvorschriften* (bzw. gestützt auf strafbare Handlungen). Im *Fall 1* geht es jedoch um einen Sekundärbeweis gestützt auf gesetz-

[50] Vgl. Schmid Niklaus, Schweizerische Strafprozessordnung (StPO) – Praxiskommentar, 2. Aufl. Zürich 2013, Art. 141 Rz. 9.

[51] Sonst «nicht möglich» bzw. «conditio sine que non» (vgl. Botschaft zur Vereinheitlichung des Strafprozessrechts vom 21. Dezember 2005 [nachfolgend Botschaft StPO], BBl 2006 1085 ff., 1184; Schmid [Fn. 50], Art. 141 Rz. 14).

[52] Der *Primär*beweis darf *dann* «nach Abs. 2 *nicht verwertet* werden» (Abs. 4). Bei *Unerlässlichkeit* besteht trotz ungültigem Primärbeweis *kein* Verwertungsverbot (Abs. 2).

lich *unverwertbare* Beweiserhebungen.[53] Art. 141 Abs. 4 i.V.m. Abs. 2 StPO (fehlende «Fernwirkung») wäre demgegenüber anwendbar, wenn z.B. ein *Zeuge ungenügend belehrt* wurde[54] und dieser einen *Tatbeteiligten* nennt. Der zweite Tatbeteiligte darf trotzdem *verfolgt* oder seinerseits als Zeuge oder Auskunftsperson *einvernommen* werden, sofern nicht ausgeschlossen erscheint, dass er *ohnehin* hätte eruiert werden können.[55] Analoges gilt, wenn der ungültig einvernommene Zeuge den *Ort* nennt, wo sich die *Tatwaffe* befindet. Diese darf *beschlagnahmt* werden, wenn aufgrund der übrigen (oder konkret in Aussicht stehender) Beweisergebnisse ohnehin eine Durchsuchung am Fundort durchzuführen gewesen wäre.[56] Absolut *unverwertbar* sind hingegen *alle* Primär- und Sekundärbeweise, bei denen das Gesetz ausdrücklich die Unverwertbarkeit (des Primärbeweises) statuiert.[57] Absolute Unverwertbarkeit gilt insbesondere bei nicht richterlich genehmigten Überwachungen (Art. 277 Abs. 2 StPO). Eine solche kann also weder für das Erstellen einer (verwertbaren) Sprachanalyse *(Fall 1)* verwendet werden, noch für andere Sekundärerhebungen. Meines Erachtens müsste auch der Fall mit dem «Drogentipp» aus Slowenien (BGE 138 IV 169) nach heutigem Recht mit einem entsprechenden *Verwertungsverbot* enden.[58] Am klaren Wortlaut des Gesetzes (und an den Materialien) wird die Bundesgerichtspraxis kaum herumkommen.[59]

Zwar gibt es in BGE 138 IV 169 (E. 3.3.2) auch gewisse *obiter dicta* zur neuen StPO, die Zweifel an einem absoluten Verwertungsverbot erkennen lassen könnten, wenn der Folgebeweis auch «unabhängig» hätte erhoben werden können. In Lehre und Praxis wird hier aber oft nicht ausreichend zwischen *Primärbeweis* und (echtem) *Fol-*

[53] Art. 141 Abs. 1 Satz 2 bzw. Art. 277 Abs. 2 StPO; die Überwachung wurde nicht richterlich genehmigt.

[54] *Gültigkeits*vorschrift, Art. 177 Abs. 1 StPO.

[55] Wenn der Tatbeteiligte auch *ohne* die ungültige erste Zeugenussage eruiert worden wäre, liegt *kein* Fall vor, wo der Folgebeweis ohne den Primärbeweis «nicht möglich» gewesen wäre (Art. 141 Abs. 4 StPO). Falls die ungültige erste Zeugeneinvernahme zur Aufklärung einer schweren Straftat sogar *unerlässlich* erschiene (Abs. 2), läge gar kein «nicht verwertbarer» Primärbeweis (i.S.v. Abs. 2 und Abs. 4) vor. Für den Folgebeweis bestünden daher *keine* Verwertungsbeschränkungen i.S.v. Abs. 2 und Abs. 4.

[56] Bei *Unerlässlichkeit* zur Aufklärung eines Verbrechens oder *schweren* Vergehens (Art. 141 Abs. 2 StPO) bestünde hier zum Vornherein *kein Verwertungshindernis* bezüglich des ungültigen Primärbeweises und damit auch *kein unverwertbarer Folgebeweis* (i.S.v. Abs. 2 i.V. Abs. 4), und zwar *unabhängig* von der Frage der Bedeutung des ungültigen Primärbeweises. Allerdings wird an die «Unerlässlichkeit zur Aufklärung schwerer Straftaten» (Abs. 2) ein *strenger Massstab* angelegt.

[57] Art. 141 Abs. 1 Satz 2 StPO: «in keinem Fall».

[58] Sofern die Kontrolle und Beschlagnahme als *echte* (kausale) *Folgebeweise* eingestuft werden können, s. dazu den nächsten Abschnitt.

[59] Ebenso Schmid (Fn. 50), Art. 141 Rz. 13: «Nach dem Willen des Parlaments sollen also allein ungültige Beweise zu verwertbaren Sekundärbeweisen führen».

gebeweis (mit Fernwirkungsproblematik) unterschieden: Wenn der slowenische «Tipp» (Drogenfall) *kausal* war für die erfolgte Kontrolle an der Grenze, dann ist sie ein *Folgebeweis* und nach neuem Recht nicht verwertbar.[60] Wenn jedoch der «Tipp» überhaupt *keine kausale* Rolle für die Anordnung der Kontrolle spielte, liegt gar kein Folgebeweis im Sinne des Gesetzes vor sondern ein (verwertbarer) *Primär*beweis.[61] Hier besteht auch ein wesentlicher *Unterschied* zum *Fall 1* («Sprachgutachten»): Das Gutachten beruht *zwangsläufig* und unmittelbar auf den Ergebnissen der Telefonüberwachung. Ohne die Tonbänder gibt es das Vergleichsgutachten nicht. Im *Drogenfall* hingegen hätte die Kontrolle und Sicherstellung an der Grenze auch *ohne* den «Tipp» gestützt auf die Telefonüberwachung erfolgen können. Im Drogenfall ist also (nach neuem Recht) zu untersuchen, ob überhaupt ein kausaler *Folgebeweis* vorliegt. Wenn ja, ist er nicht verwertbar.

2. Zufallsfunde und «Kaskadenüberwachung»

Nach der neuen StPO ist im richterlichen *Genehmigungsverfahren* (Art. 272 Abs. 1 und Art. 274 StPO) auch über die Verwendung von *Zufallsfunden* aus separaten Überwachungen zu entscheiden (Art. 278 Abs. 3 StPO).[62] *Zufallsfunde* stammen aus früheren Überwachungen, die wegen anderen *Delikten* gegen die *gleiche* Zielperson oder gegen andere *Ziel*personen durchgeführt wurden. Es stellt sich die Frage, ob sie als Beweismittel (gegen die beschuldigte Person) oder als Grundlage einer neuen Überwachung verwendet werden dürfen. Im Vordergrund stehen zwei *Hauptfälle,* nämlich *(a)* eine neue Überwachung (Ue) gegen die *bisherigen* betroffenen *Zielpersonen* wegen zufällig *neu* entdeckten *Straftaten* (Art. 278 Abs. 1 StPO), und *(b)* eine neue Überwachung wegen den *bisherigen* untersuchten (oder auch neu entdeckten) *Straftaten* gegen zufällig *neu* ermittelte *Beteiligte* (Art. 278 Abs. 2 StPO). Eine neue Ue gestützt auf Zufallsfunde setzt *erstens* voraus, dass eine *rechtskräftig genehmig-*

[60] Da der *Primärbeweis* (Telefonüberwachung) *absolut unverwertba*r ist (Art. 141 Abs. 1: «in keinem Falle» i.V.m. Art. 277 Abs. 2 StPO). Dies gilt unbeachtet, wie «wahrscheinlich» (so BGE 138 IV 169 nach altem Recht) eine Kontrolle *ohne* Tipp gewesen wäre, und auch unbeachtet, wie «unerlässlich» (Art. 141 Abs. 2 StPO) der Primärbeweis zur Verbrechensaufklärung erschien: Art. 141 Abs. 2 und Abs. 4 StPO sind auf *absolut* unverwertbare Primärbeweise gar nicht anwendbar.

[61] Art. 141 Abs. 4 StPO («*ermöglichte* ein Beweis ...») ist nur auf *Folge*beweise (bei ungültigen und nicht verwertbaren Primärbeweisen, Abs. 2) anwendbar. Als gültiger *Primär*beweis (hier wären Abs. 1–2 und Abs. 4 gar nicht anwendbar) wären Kontrolle und Sicherstellung ohne weiteres verwertbar.

[62] Falls die Staatsanwaltschaft nicht weiss, ob sie die Zufallsfunde verwenden darf, kann sie gestützt darauf keine neuen geheimen Überwachungen (oder andere Untersuchungsmassnahmen) anordnen.

te Erst-Ue bzw. Drittpersonen-Ue vorliegt, aus welcher der Zufallsfund entspringt.[63] *Zweitens* muss auch die Verwendung des Zufallsfundes noch *nachträglich* richterlich *genehmigt* werden (Art. 278 Abs. 3 StPO). Die Genehmigung des Zufallsfundes erfolgt im Fall *(a),* wenn auch wegen den *neu* gefundenen *Straftaten* (schon im Zeitpunkt des Zufallsfundes im Rahmen der Erst-Ue) eine Ue hätte verfügt werden dürfen,[64] *oder* im Fall *(b),* wenn auch gegen die *neu* ermittelte *Person* (wegen den ihr nun vorgeworfenen Delikten) eine Ue verfügt werden darf.[65] Falls der Zufallsfund auf einer nicht genehmigten Erst-Ue oder Drittpersonen-Ue beruht oder falls seine Verwendung nicht nachträglich genehmigt wird, ist er (gemäss Art. 277 Abs. 2 i.V.m. Art. 278 Abs. 3 StPO) *nicht verwertbar.*

Fall 2

In einem komplexen Drogenfall hat die Staatsanwaltschaft diverse Telefonüberwachungen durchgeführt. Die erste Ue (gegen A) hat bisher unbekannte *neue Beteiligte* (B und C) zutage gefördert, gegen die ihrerseits *neue Ue* angeordnet werden. Im Rahmen dieser Ue wird ein *weiterer Zufallsfund* ermittelt gegen einen neuen Verdächtigen, D. Auch gegen D wird (gestützt auf den Zufallsfund) eine Ue durchgeführt. D ficht die Ue und die Verwendung des Zufallsfundes nachträglich an. Er macht geltend, er müsse auch prüfen können, ob die Überwachungen gegen A, B und C rechtmässig waren. Zu diesem Zweck sei ihm Einsicht in alle Akten der früheren Ue zu geben. *Kann D sämtliche Überwachungen überprüfen lassen? Ist ihm volle Akteneinsicht zu gewähren?*

Nach der bundesgerichtlichen Praxis kann die Rechtmässigkeit einer bereits rechtskräftig genehmigten Erst-Ue oder Drittpersonen-Ue mit der Anfechtung der Verwendung des Zufallsfundes *nicht nochmals* geprüft werden. Nur die Rechtmässigkeit der Verwendung des *Zufallsfundes* (Art. 278 i.V.m. 269 StPO) und das Vorliegen einer rechtskräftig *genehmigten* Erst-Ue bzw. Drittpersonen-Ue[66] werden geprüft. Daher hat die überwachte Person D im obigen *Fall 2* grundsätzlich *keinen* Zugang zu den Akten der bereits rechtskräftig genehmigten Erst-Ue bzw. Drittpersonen-Ue, soweit die Rechtmässigkeit der Verwendung des Zufallsfundes[67] aufgrund der Akten des *aktuellen* Verfahrens *geprüft* werden kann. In BGE 140 IV 40 (E. 4.2–4.3 S. 43 f.) ging es um einen Zufallsfund, der *neue Verdachtsgründe* gegen eine *andere Person* zutage förderte, die an den ersten (rechtskräftig bewilligten) Ue-Verfahren noch nicht

63 Art. 277 StPO *e contrario*.
64 Fall von Art. 278 Abs. 1 i.V.m. Art. 269 StPO, Katalogtat usw.
65 Fall von 278 Abs. 2 i.V.m. Art. 269 StPO.
66 Art. 277 StPO *e contrario*.
67 Art. 278 i.V.m. 269 StPO.

beteiligt gewesen war. Gestützt auf den Zufallsfund wurde auch gegen den neu Beschuldigten eine Ue angeordnet, die dieser nachträglich anfocht. Der Anwalt des Beschuldigten stellte sich auf den Standpunkt, er müsse die Rechtmässigkeit *aller früheren* Überwachungen überprüfen können, die «kaskadenweise» zum Zufallsfund gegen seinen Mandanten führten. Das Bundesgericht entschied, dass jene Beweisergebnisse der früheren Überwachungen, welche *unmittelbar* den Zufallsfund *begründen,* in die Akten des neuen Verfahrens *übernommen* werden müssen. Eine rechtmässige Verwendung des Zufallsfundes und eine rechtmässige neue Ue setzen insbesondere den dringenden *Tatverdacht* eines *Katalogdeliktes* voraus (Art. 269 Abs. 1 Bst. a i.V.m. Abs. 2 StPO). Soweit der dringende Tatverdacht auf den *Zufallsfund* gestützt wird, müssen die betreffenden Ue-Ergebnisse dem Zufallsfund-Betroffenen offengelegt werden. Auch muss überprüfbar sein, dass die *früheren* Überwachungen *rechtskräftig* bewilligt und durchgeführt wurden. Kein Anspruch besteht hingegen auf volle Einsicht in die *übrigen* Akten und Ergebnisse früherer Überwachungen gegen Drittpersonen.[68]

3. Dauer der Überwachung (Dauerdelikte)

Bei *Dauerdelikten,* insbesondere Drogenhandel, ergibt sich die Problematik, dass die deliktische Tätigkeit während der geheimen aktiven Fernmeldüberwachung und bis zu deren Auswertung bzw. bis zur *Mitteilung* (Art. 279 StPO) an den Betroffenen (oder anderen ihn warnenden Untersuchungsmassnahmen) *weiter* läuft. Die Staatsanwaltschaft kann bestrebt sein, weitere *Beteiligte* (insbesondere über «Kaskadenüberwachungen», dazu oben, Ziff. 2) zu eruieren und die konnexen Überwachungen (Ue) unterdessen *geheim* zu halten. In diesem Zusammenhang ist dem Einwand Rechnung zu tragen, die Staatsanwaltschaft könnte unzulässigen *Einfluss* auf das *Strafmass* nehmen bzw. die Schwere des Drogendelikts «künstlich aufblähen», indem unnötig zugewartet worden sei, anstatt den Beschuldigten nach ein paar Wochen zu verhaften oder ihm die Ue möglichst rasch nach deren Beendigung mitzuteilen.

Zunächst fällt auf, dass das Gesetz *keine* klaren zeitlichen *Limiten* setzt für die Ue, deren Auswertung und die Mitteilung. Art. 275 Abs. 1 StPO verweist auf die *allgemeinen Voraussetzungen* der Ue (Bst. a), wozu insbesondere die zeitliche *Verhältnismässigkeit* gehört,[69] sowie auf die richterliche Genehmigungs- bzw. Verlängerungspflicht (Bst. b): Das Zwangsmassnahmengericht hat die Ue (nach Art. 274 Abs. 5 StPO)

[68] Mit anderen Worten kann der Zufallsfund-Betroffene die bereits rechtskräftig genehmigten Erst-Ue bzw. Drittpersonen-Ue (gegen andere Beschuldigte und Betroffene) nicht nochmals vollständig aufrollen und anfechten. Geprüft wird nur, ob die gesetzlichen Voraussetzungen der Verwendung des *Zufallsfundes* und der *neuen* Ue erfüllt sind.

[69] Art. 269 Abs. 1 Bst. b–c StPO.

zeitlich zu *beschränken;* eine Verlängerung muss zusätzlich bewilligt und *befristet* werden. Dabei kann das Zwangsmassnahmengericht der Staatsanwaltschaft *Auflagen* für die Untersuchungsführung erteilen (Art. 274 Abs. 2 StPO). Im Grundsatz darf die Ue damit so lange dauern und richterlich verlängert werden, wie es für eine sorgfältige Sachverhaltsermittlung *notwendig* ist. Je länger die Ue dauert bzw. verlängert wird, desto schwieriger dürfte allerdings die Begründung der Verhältnismässigkeit werden: Art. 269 Abs. 1 Bst. c StPO (auf den Art. 275 Abs. 1 Bst. a verweist) setzt ja voraus, dass andere Ermittlungsperspektiven erfolglos *ausgeschöpft* wurden bzw. aussichtslos erscheinen. Nach einer längeren Ue dürften aber regelmässig neue Ermittlungsergebnisse auftauchen, die *alternative Untersuchungsmassnahmen* zulassen (z.B. Hausdurchsuchungen, Beschlagnahmungen, Verhaftungen oder Einvernahmen). Dies setzt der Ue bereits von Gesetzes wegen gewisse zeitliche Schranken.

In BGE 140 IV 40 (E. 4.4 S. 45 f.) wurde entschieden, dass der Beschuldigte grundsätzlich keinen Anspruch darauf hat, bei untersuchten Dauerdelikten quasi «vor sich selbst geschützt» zu werden. Das heisst, die Strafverfolgungsbehörde ist nicht verpflichtet, primär in dem Sinne aktiv zu werden, dass der Deliktsumfang möglichst gering ausfällt bzw. die Deliktsdauer möglichst kurz. Deshalb besteht kein Anspruch des Beschuldigten, so rasch wie möglich verhaftet oder anderweitig an der strafbaren Tätigkeit *gehindert* zu werden, etwa indem ihm die Ue möglichst früh mitgeteilt wird. Allerdings weist das Bundesgericht auf *Schranken* hin bzw. auf strafprozessuale Zielkonflikte: Zunächst dient das Strafrecht auch der Verbrechensprävention und dem *Rechtsgüterschutz*.[70] Ausserdem ist der *Grundsatz* der *gleichmässigen Durchsetzung* des *Strafrechts*[71] zu beachten. Der Gleichbehandlungsgrundsatz würde verletzt, wenn die Strafverfolgungsbehörde es in der Hand hätte, auf das *Strafmass* Einfluss zu nehmen, indem sie nach Belieben früher oder später einschreitet. Durch ein unbegründetes Hinauszögern von geheimen Ue-Massnahmen würden indirekt auch die *Verteidigungsrechte* tangiert.[72] Im genannten Leiturteil geht das Bundesgericht davon aus, dass bewilligte verhältnismässige Ue in diesem Rahmen so lange dauern dürfen, als ihre sachliche Notwendigkeit ausreichend dargelegt ist. Im konkreten Fall wurde unter anderem der *Komplexität* der Untersuchung und der *Schwere* der Delikte Rechnung getragen. Falls die Ue und deren Auswertung ungewöhnlich lange dauern,

[70] Bei der Drogenkriminalität (und anderen Delikten ohne *direkte* Opfer) wird dies vielleicht nicht sofort deutlich. Aber beim Beispiel des *sexuellen Kindesmissbrauchs* leuchtet ein, dass die Strafverfolgungsbehörden *nicht beliebig lange zuwarten* dürfen bis zum Zugriff. Der Rechtsgüterschutz darf dem Aufklärungsinteresse *nicht vollständig untergeordnet* werden.

[71] Art. 16 Abs. 1 i.V.m. Art. 3 Abs. 2 Bst. c StPO.

[72] Jedenfalls kann der Beschuldigte gegen geheime Massnahmen weder faktisch noch rechtlich Vorkehren treffen.

muss die Staatsanwaltschaft nachvollziehbar begründen, worauf der zusätzliche Zeitbedarf beruht, welche ergänzenden konnexen Ermittlungen[73] sich zum Beispiel aufdrängten, bevor die Ue mitgeteilt werden konnte.

4. Überwachung von Dritten

Zur Untersuchung von Delikten können auch gegen *nicht beschuldigte Drittpersonen*[74] strafprozessuale Zwangsmassnahmen verfügt werden. Gemäss den allgemeinen Vorschriften ist bei Grundrechtseingriffen gegen sie allerdings «besondere Zurückhaltung» geboten (Art. 197 Abs. 2 StPO). Für *Fernmeldeüberwachungen* (Ue) wird dies in Art. 270 Bst. b StPO näher konkretisiert. Von Zwangsmassnahmen *unmittelbar* betroffenen Dritten stehen die (zur Wahrung ihrer Interessen erforderlichen) *Verfahrensrechte* einer *Partei* zu.[75] Dazu gehört insbesondere der Anspruch auf nachträgliche *Mitteilung* und *Anfechtung* (Art. 279 StPO) der sie betreffenden Ue. Art. 270 Bst. b StPO regelt *zwei Grund-Konstellationen* von Dritt-Ue:[76] Art. 270 Bst. b *Ziff. 1* lässt die aktive Ue zu,[77] wenn konkrete Anhaltspunkte dafür bestehen, dass die *beschuldigte Person* den Drittanschluss *«benutzt».*[78] *Ziff. 2* regelt den Fall des Dritten als sogenannter *«Nachrichtenmittler».*[79]

Bei Art. 270 Bst. b *Ziff. 1* StPO hatte das Bundesgericht insbesondere zu klären, was «*Benutzen*» des Drittanschlusses bedeutet: Im Fall von *BGE 138 IV 232* war zu prüfen, ob auch die Ue eines Drittanschlusses zulässig ist, den der Beschuldigte *nicht selber* (wie einen eigenen) *benutzt,* sondern auf den er bloss (voraussichtlich) *anruft.* Das BGer hat die Frage grundsätzlich *bejaht.* Diese Praxis liegt allerdings (aufgrund des Gesetzeswortlautes) nicht ohne weiteres auf der Hand. In der *Botschaft* zur StPO[80] wurde sogar ausdrücklich die *gegenteilige* Meinung vertreten, und die Literatur hat

---

[73] In Drogenfällen z.B. Auswertungen und/oder zusätzliche (geheime) Abkärungen betreffend *Hauptbeteiligte,* wesentliches *Tatvorgehen* und wesentliche (im Durchschnitt) gehandelte *Drogenmenge*.

[74] «Durch Verfahrenshandlungen beschwerte Dritte» (Art. 105 Abs. 1 Bst. f StPO).

[75] Art. 105 Abs. 2 i.V.m. Abs. 1 Bst. f StPO.

[76] Art. 271 StPO enthält noch Spezialvorschriften für die Ue von *Berufsgeheimnisträgern.*

[77] Unter den Grundvoraussetzungen von Art. 269 StPO.

[78] In der Lehre wird diese Konstellation teilweise als «*Anschlussüberlassung*» bezeichnet, die Drittperson als «Anschlussüberlasser». Dieser Begriff erscheint mir unglücklich gewählt, da auch Fälle denkbar sind, bei denen der Beschuldigte den Drittanschluss *gegen den Willen* des Dritten benutzt oder sogar *ohne* dessen *Wissen.* Das Gesetz verlangt jedenfalls kein bewusstes oder sogar freiwilliges «Überlassen». (Andernfalls wären Opfer-Handys regelmässig nicht überwachbar.)

[79] Vgl. als Anwendungsfall Urteil 1B_441/2013 vom 6. Januar 2014.

[80] Botschaft StPO (Fn. 51), 1249.

vornehmlich (und ohne nähere Ausführungen) auf diese Äusserung des Bundesrates verwiesen. Es stellt sich die Frage, wieso das BGer davon abgewichen ist: Die in der Botschaft dargelegte Auffassung hätte zu einer *Praxisänderung* geführt gegenüber dem alten Recht[81] vor Inkrafttreten der StPO. Da darüber im Parlament nicht diskutiert worden war und der Gesetzeswortlaut weder die eine noch die andere Auslegung zwingend nahelegt, ist davon auszugehen, dass die Räte sich *nicht bewusst* waren, dass der *Bundesrat* hier faktisch eine *Änderung* der Bundesgerichtspraxis bzw. der bisherigen Rechtslage vorschlug, ohne sie in der Botschaft als solche zu deklarieren. Konkret hätte eine solche Praxisänderung bedeutet, dass Beschuldigte, die ihr *Mobiltelefon ständig wechseln, nicht überwacht* werden könnten, selbst wenn *bekannt* wäre, mit *welchen Personen* sie über die Delikte *reden* werden.[82] Auch der *Aufenthaltsort* von *flüchtigen* Beschuldigten könnte nicht mehr eruiert werden, obwohl absehbar wäre, bei wem sie sich voraussichtlich melden werden.

Gemäss BGE 138 IV 232 kann es für die Frage, welche *Kommunikation* zwischen der beschuldigten Person und Drittpersonen (unter den gesetzlichen Voraussetzungen) *überwacht* werden darf, nicht allein auf die ermittlungs- und fernmeldetechnische Zufälligkeit ankommen, welches Gerät oder welcher Anschluss (sogenannte «Targets») den Behörden *bereits bekannt* ist. *Entscheidend* muss primär sein, ob *(a)* beim *Beschuldigten* die gesetzlichen *Überwachungsvoraussetzungen* erfüllt sind, ob *(b)* die zu erwartenden *Gespräche* mit der Drittperson für die Aufklärung der Katalogtat (oder Fahndung nach dem Beschuldigten) *untersuchungsrelevant* sind, und *(c)* ob die Ue des Drittanschlusses in diesem Zusammenhang *sachlich notwendig* erscheint. Wenn diese Voraussetzungen erfüllt sind, kann der Umstand, dass erst der Anschluss der Drittperson bekannt ist, noch nicht aber derjenige des Beschuldigten, eine Ue nicht zum Vornherein ausschliessen. Aus dem *Verhältnismässigkeitsprinzip* ergeben sich nach dieser Praxis aber noch spezifische Einschränkungen: *(1)* Für eine Ue des *Dritten* müssen hinreichend konkrete *Anhaltspunkte* bestehen, dass der Beschuldigte *ihn anruft* und sich daraus *Hinweise* auf die untersuchte *Straftat* oder den *Aufenthaltsort* des Beschuldigten ergeben. *(2)* Die Abhörung des *Dritt*anschlusses ist *abzubrechen,* sobald der Anschluss, von dem aus der *Beschuldigte* Gespräche führt, *bekannt* wird und selber überwacht werden kann. Und schliesslich *(3)* hat die Behörde, welche die Ue anordnet, geeignete Vorkehren zu treffen, damit die mit der Ermittlung befassten Personen *keine Informationen* erhalten, die mit dem *Gegenstand* der *Un-*

[81] BÜPF bzw. kantonales Strafprozessrecht.

[82] Bei ständigem Wechsel zwischen diversen Anschlüssen könnte zwar eine *Rahmenbewilligung* (Ue sämtlicher «identifizierter» Anschlüsse der überwachten Person) erfolgen (Art. 272 Abs. 2 StPO). Dafür müssten aber die Anschlüsse *bekannt* sein.

tersuchung nicht in Zusammenhang stehen.[83] Insoweit hat das Bundesgericht die bisherige Rechtslage bestätigt und präzisiert.

5. Ausblick

Im Bereich der strafprozessualen Überwachung des digitalen Fernmeldeverkehrs (insbesondere mobiler verschlüsselter Nachrichtenverkehr und soziale Netzwerke) wird sich die Praxis zunehmend mit heiklen juristischen Fragen in einem neuen *dynamischen* und technisch sehr *komplexen* Rechtsbereich zu befassen haben. Während dieser Rechtsbereich für die Strafverfolgung an Bedeutung gewinnen wird, bleibt hier in Forschung und Rechtsprechung noch *erhebliche Grundlagenarbeit* zu leisten.

[83] Diese Pflicht besteht aufgrund des Verhältnismässigkeitsgrundsatzes (Art. 197 Abs. 1 Bst. c und Abs. 2 StPO) nach wie vor, auch wenn sie in der StPO nicht mehr – anders als früher noch in Art. 4 Abs. 5 BÜPF – ausdrücklich normiert ist.