www.jusletter-it.eu

Damian K. Graf

Strafverfolgung 2.0: Direkter Zugriff der Strafbehörden auf im Ausland gespeicherte Daten?

Besprechung des «Facebook»-Urteils des Bundesgerichts 1B_29/2017 vom 24. Mai 2017 (zur Publikation vorgesehen)

Are Swiss criminal law enforcement authorities legally authorized to use Facebook credentials collected in the context of a criminal investigation in order to sign in to the account and search chat messages, and is the resulting evidence admissible in criminal proceedings – even though the accessed data is stored on a server abroad? The Swiss Federal Court answered yes when it recently affirmed the decision of a lower court which had lifted the sealing of such evidence. In doing so, it misjudged the boundaries set forth by both the principle of territoriality and the Cybercrime Convention (CCC).

Category: Articles
Region: Switzerland
Field of law: Data Protection; Criminal Law

Citation: Damian K. Graf, Strafverfolgung 2.0: Direkter Zugriff der Strafbehörden auf im Ausland gespeicherte Daten?, in: Jusletter IT 21 September 2017

ISSN 1664-848X, https://jusletter-it.weblaw.ch, Weblaw AG, info@weblaw.ch, T +41 31 380 57 77 EDITIONS WEBLAW

Inhaltsübersicht

I. Einleitung

[Rz 1] Mit der zunehmenden Verschiebung der Kommunikation auf Internetdienste (E-Mails, soziale Medien, Internettelefonie) und der technischen Entwicklung hin zu «Cloud Computing» hat sich auch der Ermittlungsfokus der Strafverfolgungsbehörden verschoben. Deren Arbeit wird durch diese *Beweisverlagerung* in die digitale Welt zunehmend komplexer, was besonders darin gründet, dass die gängigen Internetdienste vom Ausland aus (üblicherweise den USA) operieren – man denke an Google, Facebook, WhatsApp oder Microsoft. Der Blick der Strafverfolger schweift damit regelmässig über die Landesgrenzen hinaus. In diesem grenzüberschreitenden Kontext müssen den Behörden *effektive Eingriffsbefugnisse* zur Verfügung gestellt werden, die es ihnen ermöglichen, die für inländische Strafverfahren erforderlichen Beweismittel weiterhin sicherzustellen.[1]

[Rz 2] Einer konkreten Fragestellung in diesem digitalen Dunstkreis hat sich das Bundesgericht in einem jüngeren Entscheid angenommen: *Dürfen schweizerische Strafverfolgungsbehörden im Rahmen eines inländischen Strafverfahrens*, als Ausfluss ihrer strafprozessualen Befugnisse, *direkt auf Benutzerkonten bei ausländischen abgeleiteten Internetdiensten* (im konkreten Fall Facebook) *zugreifen, beweisrelevante Daten sicherstellen und diese sodann im inländischen Strafverfahren verwerten?*[2] Mit dem *direkten Zugriff* ist hier nicht die Aufforderung an ausländische Provider zur Herausgabe von Daten gemeint, die ebenfalls Problemfelder aufwirft, sondern vielmehr das *eigenhändige*

[1] Wolfgang Bär, in: Heinz-Bernd Wabnitz/Thomas Janovsky (Hrsg.), Handbuch des Wirtschafts- und Steuerstrafrechts, 4. Aufl., München 2014, Kap. 12 N 2.

[2] Die Frage wurde bereits früh von Niklaus Schmid, Strafprozessuale Fragen im Zusammenhang mit Computerdelikten und neuen Informationstechnologien im allgemeinen, in ZStrR 111 (1993), S. 81 ff., S. 109, aufgeworfen.

Einloggen auf Benutzerkonten durch eine Strafbehörde unter Verwendung ihr bekannter Zugangsdaten.

[Rz 3] Der direkte Zugriff auf elektronische Informationen im Ausland würde die Strafverfolgung schlagkräftiger und effizienter machen: Zufolge der Trägheit der internationalen Rechtshilfe würde das Risiko minimiert, dass beweisrelevante Informationen nicht mehr erhältlich, weil gelöscht, sind.[3] Allein, mit der Billigung des unmittelbaren Online-Datenzugriffs könnten die offiziellen Rechtshilfewege und das völkerrechtliche Territorialitätsprinzip untergraben werden.[4] Dies besonders vor dem Hintergrund, dass das durch die Schweiz ratifizierte Übereinkommen über Cyberkriminalität vom 23. November 2001 (*Cybercrime-Konvention*, CCC)[5] bereits gewisse Erleichterungen für die grenzüberschreitende Beweisbeschaffung vorsieht (vgl. nachstehend, Rz. 33 ff.).

II. Urteil des Bundesgerichts 1B_29/2017 vom 24. Mai 2017

1. Vorbemerkungen

[Rz 4] Das Urteil des Bundesgerichts 1B_29/2017 vom 24. Mai 2017 wird vorliegend nur unter dem Aspekt der geschilderten Fragestellung des direkten Online-Zugriffs auf Daten im Ausland untersucht. Entsprechend wird auf eine Erläuterung sämtlicher Erwägungen – es handelt sich um einen speziellen Sachverhalt versuchter Kollusionshandlungen durch einen Untersuchungshäftling bzw. dessen Lehrerin – verzichtet. Insbesondere werden die Ausführungen des Bundesgerichts, wonach die Kommunikation über abgeleitete Internetdienste wie Facebook nicht den Art. 269 ff. der Strafprozessordnung (StPO) unterliege, womit es seine in BGE 143 IV 21 ff. begründete Rechtsprechung bestätigte,[6] nicht näher untersucht.

2. Sachverhalt und Verfahrensgeschichte

[Rz 5] Gegen den sich in Untersuchungshaft befindenden Beschwerdeführer führte die Staatsanwaltschaft eine Strafuntersuchung wegen qualifizierten Betäubungsmittelhandels. Anfangs Juni 2016 stellte das Personal des Untersuchungsgefängnisses einen Zettel sicher, den der Beschwerdeführer aus dem Gefängnis schmuggeln wollte. Auf diesem Papier hatte er die Zugangsdaten (Benutzername und Passwort) zu seinem Facebook-Account notiert. Mit Verfügung vom 9. Juni 2016 liess die Staatsanwaltschaft das Facebook-Konto des Beschwerdeführers unter Verwendung der ermittelten Login-Daten sichten und beweisrelevante Chat-Nachrichten sicherstellen.[7] Nach-

3 Siehe Marc Forster, Marksteine der Bundesgerichtspraxis zur strafprozessualen Überwachung des digitalen Fernmeldeverkehrs, Probleme der grenzüberschreitenden Strafverfolgung bei Delikten über soziale Netzwerke und den mobilen Internetverkehr, in: Lukas Gschwend et al. (Hrsg.), Recht im digitalen Zeitalter, Festgabe Schweizerischer Juristentag 2015 in St. Gallen, Zürich 2015, S. 615 ff., S. 617 f.

4 Bär (Fn. 1), Kap. 12 N 26.

5 SR 0.311.43, in Kraft seit 1. Januar 2012.

6 Vgl. Urteil des Bundesgerichts 1B_29/2017 vom 24. Mai 2017 E. 4.7 f., 7.1 und 7.7.

7 Urteil des Bundesgerichts 1B_29/2017 vom 24. Mai 2017, Sachverhalt A.

dem der Beschwerdeführer anlässlich einer Einvernahme mit so erlangten Nachrichten konfrontiert worden war, beantragte er deren Siegelung.[8]

[Rz 6] Die Vorinstanz – das Regionale Zwangsmassnahmengericht Berner Jura-Seeland – prüfte in ihrem Entscheid vom 14. Dezember 2016 die Zulässigkeit der der Erhebung der versiegelten Aufzeichnungen zugrunde liegenden Untersuchungsmassnahmen. Das Gericht erwog, die Chat-Nachrichten seien zwar als grundsätzlich durchsuchbare Aufzeichnungen i.S.v. Art. 246 StPO einzustufen. Jedoch hätten sich die Server, auf die zugegriffen worden sei, im Ausland befunden, weshalb die Staatsanwaltschaft ein Gesuch um internationale Strafrechtshilfe hätte stellen müssen. In Anwendung von Art. 141 Abs. 2 StPO erkannte die Vorinstanz jedoch nicht auf Unverwertbarkeit der rechtswidrig erlangten Nachrichten, da die Beweiserhebung hier der Aufklärung einer schweren Straftat diene.[9] Zumal der Sichtung der Nachrichten auch keine überwiegenden Geheimnisinteressen der beschuldigten Person entgegenstünden, könnten die Aufzeichnungen entsiegelt werden.

3. Urteilserwägungen

[Rz 7] Das Bundesgericht wies die von der beschuldigten Person dagegen erhobene Beschwerde ab. Die Durchsuchung des Zettels als solchen, auf dem der Beschwerdeführer seine Login-Daten notiert hatte, stufte das Bundesgericht zunächst als ebenso zulässig ein wie die anschliessende Onlinerecherche, hinsichtlich welcher auf Art. 246 i.V.m. Art. 241 Abs. 3, Art. 263 Abs. 3 und Art. 265 Abs. 4 StPO habe abgestützt werden können.[10] Berechtigte Geheimnisinteressen seitens der beschuldigten Person, die gegen eine Entsiegelung sprächen, sah das Bundesgericht sodann keine.[11]

[Rz 8] Der Einwand der beschuldigten Person, die Chat-Nachrichten dürften nicht verwertet werden, da die online erhobenen Nachrichten auf Servern im Ausland (vermutungsgemäss in den USA) gespeichert gewesen seien, weshalb der direkte Zugriff auf die Chat-Nachrichten gegen das Territorialitätsprinzip verstossen habe und die Rechtshilfe umgangen worden sei,[12] wurde vom Bundesgericht ebenso wenig gehört. Es hielt in Erwägung 7.10 fest:

> «Im vorliegenden Fall erfolgte kein Datenerhebungs- oder Editionsbefehl der Untersuchungsbehörde gegenüber FB USA, FB Irland oder FB Schweiz. Ebenso wenig nahm die Staatsanwaltschaft (gestützt auf die Cybercrime-Convention oder auf dem Rechtshilfeweg) hoheitliche Handlungen im Ausland vor. *Vielmehr hat die Untersuchungsbehörde – von in der Schweiz befindlichen Computern, Servern und IT-Infrastrukturen aus – eigene Ermittlungen im Internet aufgenommen.* Diese Online-Recherche war möglich geworden, weil die Staatsanwaltschaft über einen abgefangenen Kassiber (den der Beschuldigte aus dem Untersuchungsgefängnis zu schmuggeln versucht hatte) in den Besitz der Zugangsdaten des FB-Accounts des Beschuldigten gelangt war.

8 Urteil des Bundesgerichts 1B_29/2017 vom 24. Mai 2017, Sachverhalt B.

9 Urteil des Bundesgerichts 1B_29/2017 vom 24. Mai 2017 E. 2.

10 Urteil des Bundesgerichts 1B_29/2017 vom 24. Mai 2017 E. 7.5.

11 Urteil des Bundesgerichts 1B_29/2017 vom 24. Mai 2017 E. 8 ff.

12 Urteil des Bundesgerichts 1B_29/2017 vom 24. Mai 2017 E. 7.10.

> *Wer über einen Internetzugang im Inland einen abgeleiteten Internetdienst benutzt, der von einer ausländischen Firma angeboten wird, handelt nicht im Ausland.* Auch der blosse Umstand, dass die elektronischen Daten des betreffenden abgeleiteten Internetdienstes auf Servern (bzw. Cloud-Speichermedien) im Ausland verwaltet werden, lässt eine von der Schweiz aus erfolgte gesetzeskonforme Online-Recherche nicht als unzulässige Untersuchungshandlung auf ausländischem Territorium (im Sinne der dargelegten Praxis) erscheinen [...].»[13]

III. Anmerkungen

1. Auswirkungen des Urteils – aus Sicht eines Strafverfolgers

a. Direkter Zugriff auf bei ausländischen abgeleiteten Internetdiensten gespeicherte Daten

[Rz 9] Das bundesgerichtliche Verdikt, das sich nicht auf Facebook beschränkt, sondern sich ausdrücklich auf sämtliche *abgeleiteten Internetdienste* – darunter ausländische Host-Provider, Anbieter von Cloud-Services, Chat-Foren, Austauschplattformen von Dokumenten, Shopping-Portale, Google hinsichtlich von Suchabfragen[14] wie auch (jedoch nur in Schranken)[15] E-Mail-Dienst-Anbieter – bezieht, zeitigt für die Praxis massive Auswirkungen: *Soweit die allgemeinen Durchsuchungsvoraussetzungen erfüllt sind,*[16] *kann direkt auf Konten der beschuldigten Person oder Dritter bei derartigen ausländischen Diensten zugegriffen werden*. Verwertbarkeitsprobleme stellen sich, jedenfalls aus dogmatischen Überlegungen (Stichwort: Territorialitätsprinzip), anscheinend keine.

b. Gezieltes Suchen nach Zugangsdaten

[Rz 10] Unerheblich wird dabei sein, ob die betroffene Person in die Durchsuchung der Online-Konten einwilligt und ihre Login-Daten freiwillig preisgibt oder die Strafverfolgungsbehörden diese auf anderem Wege erhältlich machen, etwa durch Sichtung beschlagnahmter Unterlagen. Ebenfalls nicht ausgeschlossen ist, dass auf den sichergestellten elektronischen Geräten spezifisch nach den Login-Daten zu derartigen Internetdiensten geforscht wird. Solch *gezielte Nachforschungen* dürften im Nachgang zum gegenständlichen Urteil vielmehr zunehmen.

[Rz 11] Einfach gemacht wird dieses Vorgehen durch die Benutzer selber, nämlich dadurch, dass man gemeinhin aus Bequemlichkeit seine wichtigsten – oder, wie der Verfasser, aus Vergesslich-

---

13 Urteil des Bundesgerichts 1B_29/2017 vom 24. Mai 2017 E. 7.10.

14 Google speichert auch Suchverläufe und kann diese seinen Nutzern zumindest teilweise zuordnen.

15 Vgl. zu den Schranken der Edition von E-Mails BGE 140 IV 181 ff. E. 2.6 f., insb. E. 2.7 S. 186 ff.: «Die abgerufenen E-Mails auf dem Server der Y. AG können – soweit sie dort noch vorhanden sind – beschlagnahmt werden. Die nicht abgerufenen E-Mails können unter den Voraussetzungen der Echtzeit-Überwachung erhoben werden». Für letztere sind folglich die Art. 269 ff. StPO anwendbar. Für den Zugriff auf *noch nicht abgerufene E-Mails* ist daher eine Genehmigung des Zwangsmassnahmengerichts nötig. Das dürfte auch für noch nicht abgerufene E-Mails bei *ausländischen* Dienstanbietern gelten. Nota: Mit «noch nicht abgerufenen» Nachrichten sind nicht sämtliche ungelesenen Nachrichten gemeint, sondern allein diejenigen, die nach dem letzten Login seitens der berechtigten Person eingegangen sind, d.h. die (fingierte) Kenntnis des *Eingangs* einer E-Mail reicht aus, damit diese ediert werden kann.

16 I.e. ein Durchsuchungsbefehl oder Gefahr in Verzug (Art. 241 StPO), ein hinreichender Tatverdacht (Art. 197 Abs. 1 lit. b StPO), die Verhältnismässigkeit (Art. 197 Abs. 1 lit. c und d StPO) sowie die Vermutung, dass sich in den Aufzeichnungen Informationen befinden, die der Beschlagnahme unterliegen (Art. 246 StPO).

keit der jeweils gewählten Benutzernamen und Passwörter *sämtliche* – Zugangsdaten für solche Dienste in seinem Internet-Browser abspeichert. Diese Aufzeichnungen sind je nach Browser entweder als ungeschützte Listen frei zugänglich oder – so im Falle des weit verbreiteten Internet-Explorers – zwar in einem speziellen Format abgespeichert, jedoch mit entsprechenden, auch online verfügbaren Tools lesbar. Noch einfacher gestaltet sich der Zugriff über ein sichergestelltes Mobiltelefon, das sich bei erstmaliger PIN-Eingabe oder bei Aufstarten entsprechender Apps direkt mit den verschiedensten Diensten verbindet, ohne dass eine Eingabe der Zugangsdaten erforderlich wäre. Es existieren spezielle Programme, mit denen nicht nur die lokalen Daten eines Mobiltelefon oder Tablets gespiegelt, sondern auch Daten eines Facebook-Accounts über das Gerät direkt «abgesaugt» werden können, sofern dieses mit Facebook verbunden ist. Diese Programme werden von den Strafverfolgungsbehörden bereits eingesetzt.

c. Anforderungen an die Durchsuchung in formeller Hinsicht

[Rz 12] Der vom Bundesgericht als rechtmässig erachtete Online-Zugriff setzt zum einen voraus, dass die *Zugangsdaten* in strafprozessual zulässiger Weise erhoben worden sind. Zum anderen muss – nebst Vorliegen der üblichen Voraussetzungen einer Zwangsmassnahme gemäss Art. 197 StPO – *vermutet* werden, dass sich in den online bzw. im Ausland gespeicherten Aufzeichnungen zu beschlagnahmende Informationen befinden, insbesondere Beweismittel (Art. 246 StPO).[17] An diese Vermutung werden in der Rechtsprechung keine hohen Anforderungen gestellt: Es genügt bereits die *potenzielle Erheblichkeit*,[18] denn «[d]ie Durchsuchung erst soll gerade Aufschluss über den konkreten Zusammenhang mit den untersuchten Straftaten ergeben»[19]. Einzige Schranke dürfte hier das Verbot von «fishing expeditions» darstellen, also das gezielte Durchsuchen von Aufzeichnungen nach Beweisen ohne ausreichenden Anfangsverdacht bzw. um einen solchen erst zu begründen.[20]

[Rz 13] Wie und von wo aus der Online-Zugriff erfolgt, also bspw. noch anlässlich einer Hausdurchsuchung nach freiwilliger Bekanntgabe der Login-Daten durch die betroffene Person an dessen Computer, durch die Strafverfolgungsbehörden im Nachgang zur Hausdurchsuchung auf dem sichergestellten Gerät oder von polizeieigenen EDV-Anlagen aus, ist dabei irrelevant. Die Einschränkung Simon Bangerters[21], ein Zugriff auf solche externen Daten, hinsichtlich derer die betroffene Person zugriffsberechtigt sei, dürfe nur innerhalb der Räumlichkeiten erfolgen, die vom Hausdurchsuchungsbefehl abgedeckt seien, findet in den Überlegungen des Bundesgerichts keine Stütze. Erforderlich ist nur, aber immerhin, dass die Zugriffe hinreichend dokumentiert werden, sodass den im Nachgang zuweilen erhobenen Manipulationsvorwürfen vorderhand der Boden entzogen wird.

---

17 Vgl. Olivier Thormann/Beat Brechbühl, in: Marcel Alexander Niggli/Marianne Heer/Hans Wiprächtiger (Hrsg.), Schweizerische Strafprozessordnung/Jugendstrafprozessordnung, Basler Kommentar, 2. Aufl., Basel 2014, Art. 246 N 7.

18 Vgl. Urteil des Bundesgerichts 1B_314/2013 vom 9. Januar 2014 E. 2.2; BGE 122 II 367 ff. E. 2c S. 371.

19 Andreas Keller, in: Andreas Donatsch/Thomas Hansjakob/Viktor Lieber (Hrsg.), Kommentar zur Schweizerischen Strafprozessordnung (StPO), 2. Aufl., Zürich/Basel/Genf 2014, Art. 246 N 7; vgl. Urteil des Bundesstrafgerichts TPF 2004 12 vom 26. Mai 2004 E. 2.1.

20 Vgl. zu «fishing expeditions» etwa BGE 137 I 218 ff. E. 2.3.2 S. 222; BGE 128 II 407 ff. E. 5.2.1 S. 417.

21 Simon Bangerter, Hausdurchsuchungen und Beschlagnahmen im Wettbewerbsrecht unter vergleichender Berücksichtigung der StPO, Diss. ZH 2014, S. 280 ff.

[Rz 14] Zutreffen dürfte der Einwand Bangerters aber insoweit, als der *Durchsuchungsbefehl* hinreichend bestimmt zu sein hat, damit der Eingriff für die von der Massnahme betroffene Person rechtsgenüglich ersichtlich ist und im Nachgang auf seine Rechtmässigkeit überprüft werden kann. Freilich müssen der Online-Zugriff wie auch die vorgängige Suche nach entsprechenden Zugangsdaten gesetzeskonform angeordnet werden (vgl. Art. 241 StPO). Sofern etwa im Rahmen einer Durchsuchung explizit nach Zugangsdaten zu für die Untersuchung potenziell relevanten Internetdiensten geforscht werden soll, sollte dies im Befehl explizit aufgeführt werden, möglichst bereits mit namentlicher Nennung der Online-Plattformen, auf denen beweisrelevante Informationen vermutet werden (vgl. jedoch die Einschränkung in Rz. 18). Falls sodann bspw. ein sichergestelltes EDV-Gerät direkt dazu verwendet werden soll, um auf Daten bei ausländischen abgeleiteten Internetdiensten zuzugreifen, so ist dies in der Anordnung ebenfalls entsprechend zu verzeichnen.

[Rz 15] Es gilt dabei darauf zu achten, dass nicht anwaltlich vertretene Durchsuchungsbetroffene über die weiten Möglichkeiten des Zugriffs auf Online-Datenbanken orientiert werden, gerade wenn sie um Einwilligung in die Entsperrung ihrer Datenträger ersucht werden.[22] Bei anwaltlich vertretenen Personen ist dagegen davon auszugehen, dass der Rechtsanwalt mit den rechtlich und technisch möglichen Instrumenten der Strafverfolgungsbehörden vertraut ist. In jedem Fall sind die betroffenen Personen über die erfolgte Sicherstellung der Daten zu informieren und ihnen ist Gelegenheit zu geben, die Siegelung zu verlangen.[23]

[Rz 16] Im Kontext der *Siegelung* ist gemäss Bundesgericht zu unterscheiden zwischen der Siegelung der *Zugangsdaten* als solchen – die in Papierform oder auf einem elektronischen Gerät sichergestellt worden sind –, die ihrerseits unter das Privatgeheimnis fallen können (Art. 13 BV und Art. 264 Abs. 1 lit. b StPO),[24] und der Siegelung der *im Internet sichergestellten Informationen*. Soweit sich der Betroffene ganz grundsätzlich gegen den Gebrauch der Zugangsdaten und die Durchsuchung seiner Konten bei abgeleiteten Internetdiensten zur Wehr setzen will, hat er bereits gegen die Verwendung der Login-Daten Einsprache zu erheben bzw. deren Siegelung zu verlangen. Will er dagegen bloss einwenden, die konkreten beschlagnahmten Nachrichten dürften nicht verwertet werden, so kann er dies auch noch tun, wenn er die Zugangsdaten als solche nicht versiegeln lassen hat (vgl. Art. 264 Abs. 3 StPO). Die zwei Einwände fallen insoweit zeitlich wie sachlich auseinander. Anzumerken bleibt, dass, auch wenn die Siegelung hinsichtlich der Zugangsdaten beantragt wird, dies die Ermittler nicht daran hindert, eine *Grobsichtung* der Online-Aufzeichnungen vorzunehmen und diese insbesondere zur *Beweissicherung* vorsorglich sicherzustellen.[25]

[Rz 17] Problematisch ist im Zusammenhang mit der Ausgestaltung des Durchsuchungsbefehls wie auch der Information über die Durchsuchung und das Siegelungsrecht das zeitliche Moment: Wird der beschuldigten Person bereits im Vorfeld angezeigt, dass bspw. ihr Facebook-Account durchsucht werden soll, so wird ihr u.U. ermöglicht, vor der Datensicherung ihr Passwort zu ändern oder ihre Daten zu löschen. Dadurch würde die Ermittlungsmassnahme vereitelt. Es

22 Zur laiengerechten Information (im Kontext der Siegelung) vgl. Urteil des Bundesgerichts 1B_309/2012 vom 6. November 2012 E. 5.3 f.

23 Eingehend zur Siegelung unlängst der Autor: Damian K. Graf, Aspekte der strafprozessualen Siegelung, in: AJP 2017, S. 553 ff.

24 Urteil des Bundesgerichts 1B_29/2017 vom 24. Mai 2017 E. 7.2.

25 Urteil des Bundesgerichts 1B_29/2017 vom 24. Mai 2017 E. 7.5 f.; vgl. Urteil des Bundesgerichts 1B_636/2011 vom 9. Januar 2012 E. 2.4.2.

wird daher sachgerecht sein, der beschuldigten Person den Durchsuchungsbefehl betreffend die Online-Konten erst nach Sicherung der Daten zu eröffnen. Ebenfalls sollte entsprechend, aus Praktikabilitätsüberlegungen, im Regelfall vom vorstehend genannten Erfordernis der namentlichen Nennung der Online-Plattformen im vorgelagerten Durchsuchungsbefehl (i.e. Suche nach den Zugangsdaten; vgl. vorstehend, Rz. 14) verzichtet werden; ein allgemeiner Hinweis darauf, dass sich die Suche mitunter auch auf Login-Daten zu allfälligen für die Strafuntersuchung relevanten Plattformen erstreckt, dürfte in diesem Stadium genügen.

[Rz 18] Diese Spezifizierungen hinsichtlich des Inhalts der Durchsuchungsbefehle sowie der Siegelung gelten übrigens auch dann, wenn Daten *inländischer* abgeleiteter Internetdienste Gegenstand der Ermittlungen sind.

d. Konsequenzen

[Rz 19] Sofern die Strafverfolgungsbehörden folglich vermuten, dass sich auf Konten ausländischer abgeleiteter Internetdienste – etwa bei Gmail, auf Facebook, Dropbox oder in einer Cloud – zu beschlagnahmende Informationen befinden, wird es inskünftig zum Standard gehören, anlässlich von Hausdurchsuchungen oder im Rahmen der forensischen Auswertung elektronischer Geräte nach entsprechenden Zugangsdaten zu forschen, soweit diese durch die berechtigten Personen nicht freiwillig ausgehändigt werden, und sich unter Verwendung der ermittelten Login-Daten Zugang zu den Benutzerkonten zu verschaffen.[26] Die in der Folge sichergestellten elektronischen Beweise können dann im inländischen Strafverfahren verwertet werden. So kann der prima vista beschwerliche Gang über die Rechtshilfe bzw. direkte Anfragen bei den ausländischen Providern (vgl. dazu nachstehend, Rz. 35 und 36) vermieden werden; an die Datenherausgabe stellen die verschiedenen ausländischen Dienste denn auch zuweilen hohe, teilweise voneinander abweichende Anforderungen.[27]

[Rz 20] Mit der Möglichkeit des direkten Zugriffs auf im Ausland gespeicherte Daten qua inländischen Strafprozessrechts stellt das Bundesgericht den Strafverfolgungsbehörden ein griffiges Instrument zur Verfügung, um der zunehmenden Verschiebung von Beweismitteln in die digitalen Weiten des Internets Herr zu werden. So sachgerecht dies rechtspolitisch auch sein mag: Es ist vor dem Hintergrund des völkerrechtlichen Territorialitätsprinzips (vgl. nachstehend, Rz. 21 ff.) und der engen Leitlinien der Cybercrime-Konvention (vgl. nachstehend, Rz. 33 ff.) *de lege lata nicht umsetzbar*.

---

26 Dasselbe gilt übrigens auch für von einem Privatkläger bekanntgegebene Login-Daten einer beschuldigten Person, soweit sie vom Privatkläger nicht widerrechtlich erlangt worden sind. Ein solches Ersuchen eines Privatklägers – explizit gestützt auf das hier besprochene Urteil – um Zugriff auf Online-Daten der beschuldigten Person zzgl. beigelegter Login-Informationen ist bei der Staatsanwaltschaft Nidwalden zwischenzeitlich bereits eingegangen.

27 Siehe dazu das Background Paper «Criminal justice access to data in the cloud: Cooperation with «foreign» service providers» der T-CY Cloud Evidence Group des Cybercrime Convention Committee (T-CY) vom 3. Mai 2016 (abrufbar unter https://rm.coe.int/168064b77d [alle Websites zuletzt besucht am 9. August 2017]).

2. Kritik

a. Beweiserhebungen mit Auslandsbezug und das völkerrechtliche Territorialitätsprinzip

[Rz 21] Das *Territorialitätsprinzip* stellt eine der völkerrechtlichen Souveränität entfliessende Schranke staatlichen Handelns dar. Es dient nicht nur der Begrenzung der Anwendbarkeit innerstaatlichen Strafrechts auf ausländische Sachverhalte – wovon freilich Ausnahmen existieren[28] –, sondern limitiert zugleich staatliches Handeln auf das eigene Hoheitsgebiet.[29] Gänzlich verboten ist die Vornahme amtlicher Handlungen auf fremdem Territorium zwar nicht.[30] Sofern derartiges Verhalten aber nicht ausdrücklich durch internationale (Rechtshilfe-)Abkommen, bilaterale Verträge oder zumindest ad hoc-Genehmigungen erlaubt ist, stellt es einen unzulässigen Eingriff in die staatliche Souveränität dar und kann nach ausländischem Recht gegebenenfalls entsprechend geahndet werden; unbewilligte amtliche Handlungen auf fremdem Territorium werden auch nach schweizerischem Recht sanktioniert (Art. 299 StGB; vgl. auch Art. 271 StGB). In Verletzung des Territorialitätsprinzips erhobene Beweise können zudem im innerstaatlichen Strafverfahren gegebenenfalls nicht verwertet werden (vgl. nachstehend, Rz. 42 f.).

[Rz 22] Insbesondere «eigenmächtige Handlungen mit *Zwangs- und Eingriffscharakter auf fremdem Hoheitsgebiet*»[31] verletzen die staatliche Souveränität und sind daher völkerrechtswidrig. Somit sind, sofern dafür nicht die Rechtshilfe des fremden Staats in Anspruch genommen wird, etwa Verhaftungen von Personen im Ausland durch schweizerische Beamte ebenso unzulässig wie die Durchführung von Einvernahmen, die Vornahme von Augenscheinen oder die direkte Vollstreckung von Urteilen.[32] Dasselbe gilt gemäss Bundesgericht für den Versand von Vorladungen an im Ausland domizilierte beschuldigte Personen, die nicht mit Zwangsandrohungen versehen sein dürfen, mithin als blosse Einladungen auszugestalten sind.[33]

[Rz 23] Klar erscheint damit, dass die Strafverfolgungsbehörden nicht *physisch* im Ausland Beweise erheben dürfen, ohne den Rechtshilfeweg zu beschreiten resp. ohne dass solche Handlungen in einem Abkommen explizit erlaubt wären. Eigenmächtige Hausdurchsuchungen oder die Sicherstellung und Durchsuchung von elektronischen Geräten oder Unterlagen auf fremdem Staatsgebiet sind damit untersagt.

[Rz 24] Nicht anders gelagert sind Beweisbeschaffungssituationen, in denen sich die Strafbehörden zwar nicht physisch auf ausländischem Staatsgebiet aufhalten, aber *in der Schweiz* Untersuchungshandlungen vornehmen, die sich *auf die fremde Gebietshoheit auswirken*. Der Zugriff auf

---

28 Vgl. bspw. Art. 4–7 StGB.

29 Nadja Capus, Strafrecht und Souveränität: Das Erfordernis der beidseitigen Strafbarkeit in der internationalen Rechtshilfe in Strafsachen, Habil. Basel 2010, S. 193; BGE 140 IV 86 ff. E. 2.4 S. 89 f.; vgl. Urteil des Bundesstrafgerichts BV.2006.37 vom 13. September 2006 E. 2.

30 Urteil des Bundesgerichts 1B_87/2007 vom 22. Juni 2007 E. 2.7: «Verfahrens- und Untersuchungshandlungen durch schweizerische Beamte im Ausland sind [nur, aber immerhin,] an die Voraussetzung gebunden, dass die zuständigen Stellen des Staates, auf dessen Hoheitsgebiet die Handlung vorgenommen werden soll, dem zustimmen».

31 Capus (Fn. 29), S. 193; Sabine Gless, Beweisverbote in Fällen mit Auslandsbezug, in: JR 2008, S. 317 ff., S. 322.

32 Vgl. Esther Omlin, in: Marcel Alexander Niggli/Hans Wiprächtiger (Hrsg.), Strafrecht II, Basler Kommentar, 3. Aufl., Basel 2013, Art. 299 N 14; Lea Unseld, Internationale Rechtshilfe im Steuerrecht, Akzessorische Rechtshilfe, Auslieferung und Vollstreckungshilfe bei Fiskaldelikten, Diss. Zürich 2011, S. 6; differenzierend Nicolas Bottinelli, L'obtention par l'autorité pénale des données informatiques situées à l'étranger, in: AJP 2016, S. 1327 ff., S. 1329 f.

33 BGE 140 IV 86 ff. E. 2.4 S. 89 ff.; vgl. die Kritik bei Albert Largiadèr, Vorladungen ins Ausland nur Einladungen?, in: forumpoenale 5/2014, S. 293 f.

Computersysteme im Ausland von einem Standort in der Schweiz aus stellt gerade einen solchen Anwendungsfall sog. *extraterritorialer Hoheitsakte* dar.[34] Auch die Observation von Personen auf der deutschen Uferseite des Rheins durch schweizerische Polizisten von einer Badi in Schaffhausen aus könnte man als solches Handeln einstufen, genauso wie die Video-Einvernahme eines im Ausland befindlichen Beschuldigten durch ein schweizerisches Gericht. Solches Verhalten verletzt das Völkerrecht ebenfalls, soweit es *in seinen Wirkungen einem Hoheitsakt direkt auf fremdem Staatsgebiet gleichkommt*.[35] Immerhin dort, wo kein eigentlicher sich auf ein fremdes Staatsgebiet auswirkender *Zwang* vorliegt, wird keine Souveränitätsverletzung zu erblicken sein.[36]

[Rz 25] Eine *Beschlagnahmeverfügung*, die sich auf Vermögenswerte «im Ausland» bzw. «weltweit» bezog, wurde entsprechend vom Bundesstrafgericht als Verletzung der Souveränität desjenigen Staates eingestuft, in dem sich das Vermögen befand.[37] *Editionsverfügungen* an eine im Inland ansässige Partei zur Beschaffung von im Ausland gelagerten Aufzeichnungen würden die Souveränität des ausländischen Staates ebenso verletzen und wären entsprechend völkerrechtswidrig, selbst wenn die Person Zugang zu derartigen Beweismitteln hätte.[38]

b. Das Territorialitätsprinzip und die Erhebung von Daten im Besonderen

[Rz 26] Dasselbe hat und muss prinzipiell für im Ausland gespeicherte *Daten* gelten, wie das Bundesgericht denn auch unlängst im Zusammenhang mit einer direkt von Facebook USA herausverlangten «IP-History» festgestellt hat: «Aufgrund des internationalstrafrechtlichen Grundsatzes der Territorialität ist ein direkter hoheitlicher Zugriff der schweizerischen Strafbehörden auf im Ausland domizilierte Anbieter von Internetdiensten nicht zulässig. Vielmehr war für die von der Staatsanwaltschaft gewünschte Datenerhebung der Weg der internationalen Rechtshilfe in Strafsachen zu beschreiten»[39].

[Rz 27] In BGE 143 IV 21 ff. sodann, in dem die schweizerische Facebook-Tochtergesellschaft zur Herausgabe von Informationen aufgefordert worden war, die effektiv von Facebook Irland gehalten wurden, verneinte das Bundesgericht, dass Facebook Schweiz «titulaire des informations» wäre, weshalb die Staatsanwaltschaft auf den Rechtshilfeweg verwiesen wurde.[40] Hingewiesen wurde darin zudem darauf, dass die schweizerische Gesellschaft weder einen direkten noch sonstigen tatsächlichen Zugriff auf die ausländischen Daten hätte.[41] Nicht ausdrücklich beurteilt wurde dabei, ob eine Edition an Facebook Schweiz möglich gewesen wäre, hätte die Gesellschaft über die angesprochene *Zugriffsmöglichkeit bzw. -berechtigung* auf die in Irland gespeicherten Da-

34 Nadine Dombrowski, Extraterritoriale Strafrechtsanwendung im Internet, Diss. Potsdam 2011/2012, S. 12.

35 Dombrowski (Fn. 34), S. 13 f.; vgl. Daniel Burgermeister, Beweiserhebung in der Cloud, Luzern 2015, S. 20 f.; Carsten Grave/Christoph Barth, Von «Dawn Raids» zu «eRaids», Zu den Befugnissen der Europäischen Kommission bei der Durchsuchung elektronischer Daten, in: EuZW 2013, S. 360 ff., S. 373.

36 Vgl. Stefan Heimgartner, Strafprozessuale Beschlagnahme, Wesen, Arten und Wirkungen, Habil. Zürich 2011, S. 267.

37 Urteil des Bundesstrafgerichts BV.2006.35 vom 13. September 2006 E. 2.1 f.: «Damit ist auch gesagt, dass sich die stattliche Souveränität nur bis zu den Staatsgrenzen erstreckt; die Wirksamkeit hoheitlicher Akte ist folglich auf das Staatsterritorium beschränkt: locus regit actum»; Capus (Fn. 29), S. 193.

38 Heimgartner (Fn. 36), S. 267.

39 Zusammenfassung von BGE 141 IV 108 ff. E. 5.3 und 5.12 S. 121 f. und 127, in Urteil des Bundesgerichts 1B_29/2017 vom 24. Mai 2017 E. 4.7; so auch BGE 143 IV 21 ff. E. 3.2 S. 24; ferner Simon Roth, Die grenzüberschreitende Edition von IP-Adressen und Bestandesdaten im Strafprozess, in: Jusletter 17. August 2015, Rz. 30.

40 BGE 143 IV 21 ff. E. 3.4.2 S. 26.

41 BGE 143 IV 21 ff. E. 3.4.2 S. 26.

ten verfügt. Etwas weiter ging das Bundesgericht im gleichentags erschienenen, jedoch unpublizierten Urteil zu einer Edition bei Google Switzerland: Darin wies es die Sache an die Vorinstanz zurück, da nicht hinreichend eruiert worden sei, inwieweit die herausverlangten Daten zu einem Gmail-Account der schweizerischen Tochtergesellschaft zur Verfügung gestanden seien.[42] Es fügte dabei an: «[L]a personne visée par l'injonction de produire doit être le possesseur ou le détenteur des données visées, *ou tout au moins en avoir le contrôle, c'est-à-dire avoir un pouvoir de disposition, en fait et en droit, sur ces données* [...]. S'il devait apparaître que la société suisse ne peut effectivement pas, en fait ou en droit, disposer des données requises par le Ministère public, celui-ci n'aura d'autre choix que de s'adresser par voie d'entraide judiciaire aux autorités américaines pour obtenir les renseignements désirés»[43].

[Rz 28] Dem kann – jedenfalls soweit die Ausführungen auf die schweizerische StPO und nicht die Cybercrime-Konvention (CCC) abstützen[44] – indes nicht gefolgt werden. Eine inländische Person darf nicht gestützt auf inländisches Strafprozessrecht verfügungsweise aufgefordert werden, für die Strafverfolgungsbehörden im Ausland verfügbare Beweismittel zu beschaffen, auch wenn es sich dabei um Daten handelt, hinsichtlich derer sie zugriffsberechtigt ist.[45] Die rechtliche Situation ändert sich im Vergleich zu (bspw. in einem Archiv im Ausland gelagerten) Beweisen in Papierform nicht bloss deshalb, weil die Beweismittel hier in digitaler Form erhältlich sind. In beiden Fällen würde eine Privatperson für staatliche Zwecke instrumentalisiert, mithin die internationale Rechtshilfe unterlaufen. An aus- oder inländische Internetdienste gerichtete Zwangsmassnahmen – inklusive Editionsverfügungen – hinsichtlich im Ausland gespeicherter Daten sind damit nicht zulässig bzw. *nur, soweit das Rechtshilferecht (insbesondere die CCC) dies zulässt* (vgl. dazu nachstehend, Rz. 33 ff.).

[Rz 29] Das gilt im Grundsatz auch für den *direkten, eigenhändigen Zugriff* der Strafverfolgungsbehörden auf im Ausland gespeicherte Daten. Zulässig, zumal keine *Zwangs*massnahme, ist immerhin die Sicherstellung von Daten, die zwar im Ausland, jedoch *öffentlich zugänglich* sind («open source»), wie etwa ein öffentliches LinkedIn- oder Facebook-Profil, Informationen aus dem Web-Auftritt einer Firma oder einer Verwaltung, eine auf einer Sharing-Plattform frei verfügbare Datei oder die Ermittlung von Domaininformationen über «WhoIs»-Datenbanken. Auf solche Daten kann, mangels eigentlicher Zwangsausübung, von der Schweiz aus frei zugegriffen werden.[46] Insoweit ist Art. 32 lit. a CCC, der den direkten Zugriff auf derartige Informationen explizit erlaubt,

---

42 Urteil des Bundesgerichts 1B_142/2016 vom 16. November 2016.

43 Urteil des Bundesgerichts 1B_142/2016 vom 16. November 2016 E. 3.6.

44 Im genannten Google-Urteil stützte sich das Bundesgericht sinngemäss auf eine Bestimmung in der CCC (Art. 265 StPO i.V.m. Art. 18 CCC) ab, was in der Sache ebenfalls nicht überzeugt: Art. 18 Abs. 1 lit. b CCC statuiert für Bestandesdaten (vgl. zur Definition Art. 18 Abs. 3 CCC), dass «ein Diensteanbieter, der *seine Dienste im Hoheitsgebiet der Vertragspartei anbietet*, Bestandsdaten in Zusammenhang mit diesen Diensten, die sich in seinem Besitz *oder unter seiner Kontrolle* befinden, vorzulegen hat». Das Bundesgericht verkannte, dass Art. 18 CCC nicht self-executing ist (vgl. Roth [Fn. 39], Rz. 50 ff) und Art. 265 StPO nach Sinn und Wortlaut keine entsprechenden extraterritorialen Befugnisse bereithält. Falls Art. 18 CCC tatsächlich so interpretiert werden könnte, dass er derartige Editionsverfügungen erlauben würde, wäre daher hierfür eine Gesetzesanpassung notwendig.

45 Heimgartner (Fn. 36), S. 266; vgl. auch Botschaft des Bundesrates zu einem Bundesgesetz über internationale Rechtshilfe in Strafsachen und einem Bundesbeschluss über Vorbehalte zum Europäischen Auslieferungsübereinkommen vom 8. März 1976, in: BBl 1976 II 444 ff., S. 483, worin davon gesprochen wird, dass sich *sowohl* die betroffene Person *als auch* die Gegenstände in der Schweiz befinden müssten.

46 Vgl. Heimgartner (Fn. 36), S. 267; ferner Botschaft über die Genehmigung und die Umsetzung des Übereinkommens des Europarates über die Cyberkriminalität vom 18. Juni 2010, in: BBl 2010 4697 ff., S. 4737.

ohne dass ein Rechtshilfeersuchen gestellt werden müsste, bloss deklaratorischer Natur (zur CCC siehe nachstehend, Rz. 35).[47]

[Rz 30] Weitaus kniffliger wird es bei *nicht öffentlich zugänglichen*, insbesondere passwort- oder durch sonstige Barrieren geschützten ausländischen Quellen, da sich der Zugriff unter Überwindung der Zugangssicherung, die Durchsuchung sowie die anschliessende Sicherstellung und Beschlagnahme als Zwangsmassnahmen mit hoher Intensität auf das ausländische («digitale») Hoheitsgebiet auswirken. Verschiedentlich wird daher *der Zugriff durch Ermittlungsbehörden auf Daten im Ausland* als *Eingriff in die Gebietshoheit des betreffenden Staates* gewertet;[48] an derartige Beweismittel könne man nur über die internationale Rechtshilfe gelangen (bzw. bloss dann auf direktem Weg, falls dies in internationalen Übereinkommen explizit so vorgesehen ist).[49]

[Rz 31] Im diesem Zusammenhang fällt der Begriff des sog. *Zugriffsprinzips*.[50] Danach wird bei Computerdaten nicht auf den Standort des Datenträgers abgestützt, auf dem die Informationen gespeichert sind, sondern darauf, wer von wo aus Zugriff auf die verfahrensrelevanten Daten hat. Die Herrschaft über die Daten liege bei derjenigen Person, die über die Zugriffsberechtigung verfüge, und nicht bei derjenigen, die im physischen Besitze des Datenträgers sei.[51] Das führen einzelne Autoren – insbesondere der vom Bundesgericht im titelerwähnten Urteil angeführte Simon Bangerter – als Begründung an, weshalb in der Durchsuchung und Beschlagnahme von im Ausland gespeicherten Daten durch schweizerische Behörden in der Schweiz keine Souveränitätsverletzung zu sehen sei.[52] Die Zulässigkeit des Online-Zugriffs soll danach mit anderen Worten allein von der *Rechtmässigkeit der inländischen Ermittlungshandlung* abhängen.[53] Dem folgt implizit auch das Bundesgericht im gegenständlichen Urteil wie auch zuvor im angesprochenen Google-Entscheid.[54]

---

47 Vgl. Michael Bruns, in: Rolf Hannich et al. (Hrsg.), Karlsruher Kommentar zur Strafprozessordnung, 7. Aufl., Karlsruhe 2013, § 110 N 8a.

48 Dombrowski (Fn. 34), S. 159; Heimgartner (Fn. 36), S. 93; Dominic Ryser, «Computer Forensics», Eine neue Herausforderung für das Strafprozessrecht, in: Christian Schwarzenegger/Oliver Arter/Florian Jörg (Hrsg.), Internet-Recht und Strafrecht, Bern 2005, S. 553 ff., S. 575 ff.; ferner Michael Aepli, Die strafprozessuale Sicherstellung von elektronisch gespeicherten Daten, Unter besonderer Berücksichtigung der Beweismittelbeschlagnahme am Beispiel des Kantons Zürich, Diss. Zürich 2004, S. 130 f.; Stefan Heimgartner, Die internationale Dimension von Internetstraffällen, in: Christian Schwarzenegger/Oliver Arter/Florian Jörg (Hrsg.), Internet-Recht und Strafrecht, Bern 2005, S. 117 ff., S. 136.

49 Omar Abo Youssef, Smartphone-User zwischen unbegrenzten Möglichkeiten und Überwachung, in: ZStrR 130/2012, S. 92 ff., S. 105 f.; Wolfgang Bär, Transnationaler Zugriff auf Computerdaten, in: ZIS 2/2011, S. 53 ff., S. 54 f.; Jörn Hauschild, in: Christoph Knauer/Hans Kudlich/Hartmut Schneider (Hrsg.), Münchener Kommentar zur Strafprozessordnung, Band 1: §§ 1–150 StPO, München 2014-, § 110 N 18; Nils Obenhaus, Cloud Computing als neue Herausforderung für Strafverfolgungsbehörden und Rechtsanwaltschaft, in: NJW 2010, S. 651 ff., S. 654; Tobias Singelnstein, Möglichkeiten und Grenzen neuerer strafprozessualer Ermittlungsmassnahmen – Telekommunikation, Web 2.0, Datenbeschlagnahme, polizeiliche Datenverarbeitung & Co., in: NStZ 2012, S. 593 ff., S. 597; vgl. auch Sandra Schweingruber, Cybercrime-Strafverfolgung im Konflikt mit dem Territorialitätsprinzip, in: Jusletter 10. November 2014, Rz. 4.

50 Vgl. Bangerter (Fn. 21), S. 281 f.; Simon Bangerter, in: Marc Amstutz/Mani Reinert (Hrsg.), Kartellgesetz, Basler Kommentar, Basel 2010, Art. 42 N 131; Burgermeister (Fn. 35), S. 22.

51 So Burgermeister (Fn. 35), S. 22; de lege ferenda auch angetönt bei Bottinelli (Fn. 32), S. 1333.

52 Bangerter (Fn. 21), S. 281 f.; Burgermeister (Fn. 35), S. 22; im Ansatz Schmid (Fn. 2), S. 109; vgl. zu dieser Thematik (auf europäischer Stufe) sodann Grave/Barth (Fn. 35), S. 373.

53 So auch Magda Wicker, Durchsuchung in der Cloud, Nutzung von Cloud-Speichern und der strafprozessuale Zugriff deutscher Ermittlungsbehörden, in: MMR 2013, S. 765 ff., S. 768.

54 Urteil des Bundesgerichts 1B_29/2017 vom 24. Mai 2017 E. 7.10; Urteil des Bundesgerichts 1B_142/2016 vom 16. November 2016 E. 3.6; siehe auch BGE 143 IV 21 ff. E. 3.4.2 S. 26.

[Rz 32] Das Zugriffsprinzip ändert an den Auswirkungen staatlicher Online-Zugriffe auf das fremde Hoheitsgebiet, wo der eigentliche *Erfolg* der Massnahme eintritt, derweil nichts.[55] Zwar dürfte das fehlende physische Tätigwerden von Beamten auf fremdem Staatsgebiet die durch Art. 299 StGB gezogenen Grenzen noch nicht überschreiten. Sie treten jedoch, was ihre *Eingriffsintensität* betrifft, keineswegs hinter die äquivalenten physischen Ermittlungstätigkeiten (die Durchsuchung des Speicherträgers im Ausland durch schweizerische Beamten) zurück, die eindeutig unzulässig wären.[56] Dazu kommt, dass durch den Online-Abruf Datenverarbeitungsvorgänge im Ausland ausgelöst werden;[57] der Zugriff hinterlässt im Zielstaat folglich *nachvollziehbare Spuren*. Der ermittelnde Beamte kann sich dort schlimmstenfalls je nach nationaler Gesetzgebung wegen Hackings, der Verletzung von Geschäfts- und Fabrikationsgeheimnissen oder der Missachtung fremder Hoheitsrechte strafbar machen.[58] Digitale Beweisaufnahmen von der Schweiz aus erfolgen für den ausländischen Staat darüber hinaus heimlich, was sie – angesichts der Nachrichtendienst-Skandale der jüngeren Vergangenheit – aus dessen Sicht noch gefährlicher macht.[59] Es ist bereits aus diesen Gründen essenziell, dass derartige Ermittlungshandlungen durch das Rechtshilferecht abgesichert sind. Dazu kommt, dass die Cybercrime-Konvention den direkten Zugriff auf ausländische Daten bereits in beschränkter Weise erlaubt und damit, e contrario, jede darüber hinausgehende Beweisbeschaffung – zumindest im Verhältnis der Konventionsstaaten untereinander – als Eingriff in die staatliche Souveränität gewertet wird; auch der *direkte* grenzüberschreitende Zugriff auf Computerdaten, und nicht etwa allein Editions- bzw. Auskunftsaufforderungen an ausländische Internetdienste, untersteht nämlich der Cybercrime-Konvention.[60]

c. Durchbrechung des Territorialitätsprinzips auf Grundlage der Cybercrime-Konvention (CCC)

[Rz 33] Vom Bundesgericht im gegenständlichen Urteil unbeachtet blieb demnach, dass die Schweiz die internationale Zusammenarbeit hinsichtlich des Zugriffs auf in anderen Vertragsstaaten gespeicherte Computerdaten mit der Ratifizierung der Cybercrime-Konvention (CCC) explizit geregelt hat. Diese supranationale Lösung wurde gerade auch deshalb notwendig, weil die innerstaatlichen Ermittlungskompetenzen in diesem Bereich zufolge der staatlichen Souveränität limitiert sind. Die USA, in dem die in der Praxis wichtigsten abgeleiteten Internetdienste (darunter Facebook) domiziliert sind, haben die Konvention ebenfalls ratifiziert.

[Rz 34] Art. 31 Abs. 1 CCC – versehen mit der Marginalie «Rechtshilfe beim Zugriff auf gespeicherte Computerdaten» – sieht explizit den *Rechtshilfeweg für die Durchsuchung, Sicherstellung und Beschlagnahme sowie die Weitergabe von Daten* vor, *die auf Computersystemen gespeichert sind, welche sich im Hoheitsgebiet einer anderen Vertragspartei befinden*. Die Ratifizierungsstaaten haben damit gerade nicht das Territorialitätsprinzip zugunsten eines wie auch immer gearteten Zugriffsprin-

55 Annette Marberth-Kubicki, in: Astrid Auer-Reinsdorff/Isabell Conrad (Hrsg.), Handbuch IT- und Datenschutzrecht, 2. Aufl., München 2016, § 43 Fn 386.

56 Bär (Fn. 1), Kap. 12 N 27; ferner Grave/Barth (Fn. 35), S. 373.

57 Bär (Fn. 1), Kap. 12 N 27.

58 Bär (Fn. 1), Kap. 12 N 27; siehe auch Björn Gercke, Straftaten und Strafverfolgung im Internet, in: GA 2012, S. 474 ff., S. 489.

59 Marberth-Kubicki (Fn. 55), § 43 Fn 386.

60 So auch Bär (Fn. 1), S. 54 f.; Bruns (Fn. 47), § 110 N 8a; Hauschild (Fn. 49), § 110 N 18.

zips aufweichen wollen, sondern bestehen auch in diesem Bereich im Grundsatz weiterhin auf die förmliche Rechtshilfe in Strafsachen.

[Rz 35] Durch die Schaffung des (self-executing) Art. 32 CCC wurde immerhin *in zwei Konstellationen auf die Notwendigkeit eines Rechtshilfeersuchens verzichtet:* Einerseits ist der Zugriff auf *öffentlich zugängliche gespeicherte Computerdaten* zulässig, gleichwohl, wo sich die Daten geographisch befinden (lit. a). Andererseits – und im Vergleich zu anderen Rechtshilfeakkorden sehr weitgehend – darf eine Vertragspartei gemäss Art. 32 lit. b CCC «*auf gespeicherte Computerdaten, die sich im Hoheitsgebiet einer anderen Vertragspartei befinden, mittels eines Computersystems in ihrem Hoheitsgebiet zugreifen* oder diese Daten empfangen, wenn sie die *rechtmässige und freiwillige Zustimmung* der Person einholt, die *rechtmässig befugt* ist, die Daten mittels dieses Computersystems an sie weiterzugeben». Das legitimiert nicht nur eine direkte Anfrage bei ausländischen Providern zur Herausgabe von Informationen, sondern gerade auch den *eigenhändigen Zugriff der Behörden über bestehende Benutzerkonten*. Darüber hinaus sieht Art. 18 Abs. 1 lit. b CCC für sog. *Bestandesdaten*[61] vor, dass «ein Diensteanbieter, der seine Dienste im Hoheitsgebiet der Vertragspartei anbietet, Bestandsdaten in Zusammenhang mit diesen Diensten, die sich in seinem Besitz oder unter seiner Kontrolle befinden, vorzulegen hat». Die bundesgerichtliche Rechtsprechung zur (extraterritorialen) Auslegung dieser Bestimmung ist allerdings etwas ambivalent.[62]

[Rz 36] In der CCC wird folglich – jedenfalls für die Vertragsstaaten – verbindlich festgelegt, unter welchen Umständen die schweizerischen Behörden direkt auf im Ausland befindliche Daten zugreifen können und wann sie ein förmliches Rechtshilfebegehren zu stellen verpflichtet sind. Das erhellt, dass der Zugriff auf ausländische Daten unabhängig davon, dass sich die Strafverfolgungsbehörden bei derartigen Ermittlungen nicht physisch auf ausländischem Gebiet aufhalten, als prinzipieller Eingriff in die Territorialität gewertet wird. Im Rahmen der Ausarbeitung der CCC stellte sich denn auch gerade heraus, «dass kein Konsens erreicht werden konnte für weitergehende Regeln, unter welchen Voraussetzungen ein unilateraler Zugriff eines Staates auf Daten, die sich in einem anderen Vertragsstaat befinden, ohne Genehmigung desselben erfolgen kann»[63].

[Rz 37] Im Jahr 2015 hat das Bundesgericht diese Grenzen – *in fast identischer Besetzung* wie im hier besprochenen Urteil – noch ausdrücklich anerkannt:

---

61 Bestandesdaten sind gemäss Art. 18 Abs. 3 CCC «alle in Form von Computerdaten oder in anderer Form enthaltenen Informationen, die bei einem Diensteanbieter über Teilnehmer seiner Dienste vorliegen, mit Ausnahme von Verkehrsdaten oder inhaltsbezogenen Daten, und durch die Folgendes festgestellt werden kann: a. die Art des genutzten Kommunikationsdienstes, die dafür getroffenen technischen Massnahmen und die Dauer des Dienstes; b. die Identität des Teilnehmers, seine Post- oder Hausanschrift, Telefon- und sonstige Zugangsnummer sowie Angaben über Rechnungsstellung und Zahlung, die auf der Grundlage des Vertrags oder der Vereinbarung in Bezug auf den Dienst zur Verfügung stehen; c. andere Informationen über den Ort, an dem sich die Kommunikationsanlage befindet, die auf der Grundlage des Vertrags oder der Vereinbarung in Bezug auf den Dienst vorliegen».

62 Im Urteil des Bundesgerichts 1B_344/2014 vom 14. Januar 2015 E. 6.4, wurde darauf hingewiesen, dass gestützt auf Art. 18 CCC nicht direkt mittels eines Herausgabebefehls an einen ausländischen Provider gelangt werden könne, selbst wenn dieser seine Dienste in der Schweiz anbiete, so auch Forster (Fn. 3), S. 619 f.; Roth (Fn. 39), Rz. 50 ff.; a.M. Schweingruber (Fn. 49), Rz. 21 ff.; vgl. Europarat, Explanatory Report to the Convention on Cybercrime vom 23. November 2001, N 173; «T-CY Guidance Note # 10 (DRAFT), Production orders for subscriber information (Article 18 Budapest Convention)» der T-CY Cloud Evidence Group des Cybercrime Convention Committee (T-CY) vom 14. September 2016 (abrufbar unter https://rm.coe.int/16806a495e). Derweil merkte das Bundesgericht im Google-Urteil 1B_142/2016 vom 16. November 2016 E. 3.6, an, Art. 18 Abs. 1 lit. b CCC (bzw. Art. 265 StPO) erlaube die Edition sämtlicher (auch ausländischer) Daten, auf welche der Verfügungsadressat zugreifen könne.

63 Botschaft CCC (Fn. 46), S. 4737.

> «Mit Art. 32 CCC haben sich die Vertragsstaaten auf einen *minimalen (restriktiven) gemeinsamen Konsens für einen grenzüberschreitenden («extraterritorialen») Zugriff* geeinigt [...].»[64]

[Rz 38] Weiter hielt es ausdrücklich fest:

> «Aus Art. 23, Art. 25 Abs. 4 und Art. 39 Abs. 3 CCC folgt, dass in allen Fällen, bei denen die (Ausnahme-)Voraussetzungen von Art. 32 CCC nicht gegeben sind, die fragliche Datenerhebung bzw. rückwirkende Überwachung im Ausland auf dem förmlichen Rechtshilfeweg (hier gestützt auf Art. 31 CCC bzw. das RVUS) zu beantragen ist. *Die Vertragsstaaten des Übereinkommens haben sich (über die Bestimmungen von Art. 32 CCC hinaus) nicht auf weitergehende «extraterritoriale» Zugriffe von Strafverfolgungsbehörden einigen können* [...].»[65]

[Rz 39] Weshalb diese Ausführungen keine Geltung mehr beanspruchen sollten, ist nicht ersichtlich. Soweit es sich beim neuen Urteil um eine implizite Praxisänderung handeln sollte, wäre eine solche jedenfalls nicht gerechtfertigt: Wird anerkannt, dass der Zugriff auf im Ausland gespeicherte Daten über den Rechtshilfeweg erfolgen muss, falls Art. 32 CCC nicht anwendbar ist, so bleibt für die bundesgerichtliche Erwägung, dass die Strafbehörde hier nicht «im Ausland» handle und der inländische Durchsuchungsbefehl ausreiche, kein Raum. Nationale Durchsuchungsbefugnisse können derartige Eingriffe in fremde Souveränitätsrechte nicht legitimieren.[66]

[Rz 40] In den Gremien des Europarates wird mittlerweile immerhin ein *Zusatzprotokoll zur CCC* erwogen, das einen weitergehenden direkten transnationalen Zugriff durch Ermittlungsbehörden erlauben soll.[67] Bis es jedoch soweit ist, entspricht es dem Willen der Ratifizierungsstaaten, direkte Ermittlungshandlungen nur in den geschilderten engen Grenzen zuzulassen.

[Rz 41] Hinsichtlich Ländern, die sich der Konvention nicht angeschlossen haben, muss schliesslich angesichts der vorstehenden Ausführungen davon ausgegangen werden, dass das Territorialitätsprinzip hier jedweden Online-Zugriff auf nichtöffentliche Daten verbietet und daher einzig die Beschreitung des Rechtshilfewegs in Frage kommt.[68]

d. Unverwertbarkeit als innerstaatliche Folge der Verletzung der völkerrechtlichen Souveränität

[Rz 42] Wird durch den direkten Zugriff auf ausländische Datenträger das Territorialitätsprinzip verletzt und damit die Rechtshilfe in Strafsachen umgangen bzw. die Befugnisse der CCC überschritten, so haben die Strafverfolgungsbehörden den *Beweisverlust zufolge Unverwertbarkeit* zu

64 Urteil des Bundesgerichts 1B_344/2014 vom 14. Januar 2015 E. 5.9.

65 Urteil des Bundesgerichts 1B_344/2014 vom 14. Januar 2015 E. 5.12.

66 So Dominik Brodowski/Florian Eisenmenger, Zugriff auf Cloud-Speicher und Internetdienste durch Ermittlungsbehörden, Sachliche und zeitliche Reichweite der «kleinen Online-Durchsuchung» nach § 110 Abs. 3 StPO, in: ZD 2014, S. 119 ff., S. 122; ebenso Bär (Fn. 1), S. 54.

67 Vgl. den Final Report «Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY» der T-CY Cloud Evidence Group des Cybercrime Convention Committee (T-CY) vom 16. September 2016, N 144 (abrufbar unter https://rm.coe.int/16806a495e).

68 Immerhin kann diskutiert werden, ob auch Art. 32 lit. b CCC nicht insoweit bloss *deklaratorischer* Natur ist, als hier die zugriffsberechtigte Person zustimmt und folglich nicht von einer eigentlichen Zwangsmassnahme gesprochen werden kann, vgl. dazu Brodowski/Eisenmenger (Fn. 66), S. 123, m.w.H.

gewärtigen. Die Verletzung des Territorialitätsprinzips bzw. die Umgehung des Rechtshilfewegs kann somit im inländischen Strafprozess gerügt werden.[69]

[Rz 43] Die Vorinstanz im gegenständlichen Fall ging dabei von einem *relativen Verwertungsverbot* i.S.v. Art. 141 Abs. 2 StPO aus, womit die Beweise verwertet werden dürfen, soweit sie zur Aufklärung einer schweren Straftat erforderlich sind.[70] Gleich entschieden die Zürcher Gerichte in ihren Urteilen zum «Kristallnacht-Tweet».[71] Fraglich ist derweil, ob das völkerrechtliche Territorialitätsprinzip und das Erfordernis des Beschreitens des Rechtshilfewegs tatsächlich bloss als Gültigkeitsvorschriften einzustufen sind[72] oder ob angesichts ihrer Wichtigkeit nicht vielmehr von einem *absoluten Verwertbarkeitsverbot* ausgegangen werden muss (bspw. in der Gestalt eines Verstosses gegen den ordre public).[73] Näher zu prüfen wäre immerhin, ob die Möglichkeit besteht, für in rechtswidriger Weise erlangte Beweismittel ein nachträgliches förmliches Rechtshilfeverfahren durchführen zu lassen, um die Unverwertbarkeit der Beweise abzuwenden.

3. Bedeutung des hier vertretenen Ansatzes für die Praxis

[Rz 44] Der eigenhändige Zugriff auf Benutzerkonten bei ausländischen abgeleiteten Internetdiensten im Rahmen eines inländischen Strafverfahrens ist nach vorliegender Auffassung nur in den engen Grenzen des Art. 32 CCC erlaubt, soweit die Konvention auf den Sachverhalt Anwendung findet; in allen anderen Fällen gilt es, ein förmliches Rechtshilfegesuch zu stellen. Das ist aus naheliegenden Gründen nicht sachgerecht, entspricht aber dem aktuellen internationalen Konsens. Bis dieser eine Anpassung widerfährt, gelten die folgenden Regeln:

[Rz 45] **Im Grundsatz:**

- Falls sich die Daten effektiv auf den sichergestellten EDV-Geräten befinden, etwa weil Gmail-E-Mails in Kopie im Microsoft Outlook abgespeichert oder Facebook-Informationen im Cache auffindbar sind, dann kommen die üblichen inländischen Regeln zur Beweisbeschaffung (Art. 246 StPO, bei E-Mails ggf. auch Art. 269 ff. StPO) zum Tragen.[74]

---

69 Siehe dazu Gless (Fn. 31), S. 322 f., m.w.H.; anders derweil BGHSt 37, 30 ff. (33): «Aus dem Völkerrecht ergibt sich für den Beschuldigten ein Beweisverwertungsverbot hier auch nicht als Reflexwirkung aus der Verletzung von Interessen eines anderen Staates. Vielmehr ist anerkannt, dass der einzelne, der von einer völkerrechtswidrigen Massnahme betroffen ist (insbesondere von der Verletzung eines völkerrechtlichen Vertrags, der ihm keine Rechte als Individuum gewährt), sich in einem anschliessenden gegen ihn gerichteten inländischen Strafverfahren wegen einer im Inland begangenen Straftat grundsätzlich nicht auf die vom Gewahrsamsstaat verübte Völkerrechtswidrigkeit berufen kann, um daraus strafprozessuale Vorteile für sich herzuleiten».

70 Siehe Urteil des Bundesgerichts 1B_29/2017 vom 24. Mai 2017 E. 2.

71 BezGer Uster, Urteil vom 19. Mai 2014, wiedergegeben in: EKR 2014-005N, bestätigt durch OGer ZH, Urteil vom 27. April 2015, wiedergegeben in: EKR 2015-048N.

72 Im Kontext der Überschreitung kantonaler Hoheitsgebiete ging das Bundesgericht sodann gar von einer blossen Ordnungsvorschrift aus, siehe Urteil des Bundesgerichts 1P.599/2004 vom 11. Januar 2005 E. 1.2.

73 Von einem absoluten Verbot dürfte wohl, zu Recht, ausgehen: Sabine Gless, in: Marcel Alexander Niggli/Marianne Heer/Hans Wiprächtiger (Hrsg.), Schweizerische Strafprozessordnung/Jugendstrafprozessordnung, Basler Kommentar, 2. Aufl., Basel 2014, Art. 141 N 30: «Erkenntnisse, die ein Staat eigenmächtig im Ausland ohne Einwilligung des Territorialstaates gesammelt hat, [dürfen] im inländischen Verfahren nicht (ohne förmliche Zustimmung des fremden Staats) verwertet werden».

74 Zu E-Mails siehe BGE 140 IV 181 ff. E. 2.6 f. S. 186 f.; Andreas Donatsch/Albert Schmid, Der Zugriff auf E-Mails im Strafverfahren – Überwachung (BÜPF) oder Beschlagnahme?, in: Christian Schwarzenegger/Oliver Arter/Florian Jörg (Hrsg.), Internet-Recht und Strafrecht, Bern 2005, S. 151 ff., S. 161; Forster (Fn. 3), S. 623 f.

- Eine Aufforderung an einen inländischen oder ausländischen Provider zur Herausgabe von auf einem Datenträger im Ausland gespeicherten Informationen ist prinzipiell[75] unzulässig.
- Geht es um öffentlich zugängliche Daten im Ausland, so bedarf es keines Rechtshilfeersuchens, sondern es kann direkt darauf zugegriffen werden (für die Vertragsstaaten des CCC vgl. deren Art. 32 lit. a).

[Rz 46] **Im Geltungsbereich der CCC:**

- Gibt eine verfügungsberechtigte Person ihre Login-Daten zu ausländischen abgeleiteten Internetdiensten freiwillig preis und willigt in die Online-Durchsuchung ein, so steht es den Strafverfolgungsbehörden in Anwendung von Art. 32 lit. b CCC offen, an den ausländischen Serviceprovider zu gelangen und um Übermittlung der Daten zu ersuchen[76] *oder aber direkt durch Nutzung der Zugangsdaten auf die Informationen zuzugreifen und diese sicherzustellen*. Freilich steht es auch jeder Privatperson frei, die eigenen, bei einem ausländischen Provider gespeicherten Daten (etwa E-Mails oder Chat-Nachrichten) den Strafverfolgungsbehörden in Kopie zur Verfügung zu stellen.[77] Wer über die Daten i.S.v. Art. 32 lit. b CCC *rechtmässig* verfügen kann, beurteilt sich «primär nach dem nationalen Recht des Staates, in welchem die betreffende Person handelt»[78], i.e. nach schweizerischem Recht. Hinsichtlich der geschäftlichen E-Mail-Adresse kann folglich beispielsweise der Arbeitgeber in die Herausgabe einwilligen.
- Entgegen der Auffassung in der Botschaft[79] fällt unter die Ausnahme in Art. 32 lit. b CCC auch die Konstellation, in welcher der *ausländische Internetprovider bzw. -dienstanbieter* die Daten auf Aufforderung hin freiwillig herausgibt, soweit er dazu berechtigt ist.[80] Hierzu stellen die Strafverfolgungsbehörden bei den Diensten eine direkte Anfrage auf Herausgabe der gewünschten Daten. Diese sind zur Weiterleitung der Informationen berechtigt, wenn sie sich «in ihren Allgemeinen Nutzungsbedingungen bzw. Datenverwendungsrichtlinien ein solches Weiterleitungsrecht an in- und ausländische Strafverfolgungsbehörden gegenüber ihren Kunden ausbedungen haben'[81] – was bei den bekannten Internetdiensten in aller Regel der Fall ist.[82] Die konkludente Einwilligung in Gestalt einer formlosen Herausgabe der Daten reicht dabei aus, dass die Beweisbeschaffung als konventionskonform gilt.[83] Kooperieren die Dienstanbieter derweil aus welchen Gründen auch immer nicht – deren Verhalten ist denn auch zuweilen nicht nachvollziehbar –, so ist zur Erhebung der Daten auf den förmlichen Rechtshilfeweg auszuweichen.[84]

---

75 Immerhin näher zu prüfen wäre, inwieweit Art. 18 Abs. 1 lit. b CCC eine Rechtsgrundlage für die Edition von im Ausland befindlichen Bestandesdaten bereithält.

76 So auch Europarat, Explanatory Report (Fn. 62), N 294.

77 Botschaft CCC (Fn. 46), S. 4738.

78 Botschaft CCC (Fn. 46), S. 4738; Urteil des Bundesgerichts 1B_344/2014 vom 14. Januar 2015 E. 5.10.

79 Botschaft CCC (Fn. 46), S. 4738.

80 Urteil des Bundesgerichts 1B_344/2014 vom 14. Januar 2015 E. 5.9; Forster (Fn. 3), S. 619; Schweingruber (Fn. 49), Rz. 14 ff. Das entspricht dem Willen der Konventionsstaaten, siehe Europarat, Explanatory Report (Fn. 62), N 294.

81 Urteil des Bundesgerichts 1B_344/2014 vom 14. Januar 2015 E. 5.10; eingehend Roth (Fn. 39), Rz. 36 ff.

82 Zu Google bspw. Urteil des OGer ZH SB140420 vom 5. Mai 2015 E. 3.3.3 f.

83 Urteil des Bundesgerichts 1B_344/2014 vom 14. Januar 2015 E. 5.10; Urteil des OGer ZH SB140420 vom 5. Mai 2015 E. 3.3.4.

84 Urteil des Bundesgerichts 1B_344/2014 vom 14. Januar 2015 E. 5.11 f.; vgl. für einen neuen Ansatz Bottinelli (Fn. 32), S. 1331.

- Im Übrigen bleibt nur der Weg über die Rechtshilfe (Art. 31 CCC). Zur Beweissicherung sieht Art. 29 CCC immerhin ein spezielles vorläufiges Sicherungsverfahren vor.
- Namentlich ausgeschlossen ist damit der vom Bundesgericht erlaubte eigenhändige Zugriff der Strafverfolgungsbehörden auf ein Facebook-Benutzerkonto unter Verwendung rechtmässig sichergestellter Zugangsdaten, jedenfalls soweit die betroffene Person nicht in die Online-Durchsuchung einwilligt.

[Rz 47] **Hinsichtlich übriger Staaten:**

- Ausserhalb des Geltungsbereichs der CCC ist – vorbehältlich spezieller Regelungen in bilateralen Rechtshilfeverträgen (s.e.&o. bislang inexistent) – hinsichtlich nichtöffentlicher Daten stets der ordentliche Rechtshilfeweg zu beschreiten.

[Rz 48] **Folgen der Verletzung:**

- Werden diese Leitplanken nicht eingehalten, so gelten die im Ausland erhobenen Beweise als im innerstaatlichen Strafverfahren unverwertbar (mindestens relativ i.S.v. Art. 141 Abs. 2 StPO).

IV. Fazit

[Rz 49] Als Folge der voranschreitenden Digitalisierung und der damit einhergehenden Internationalisierung stossen die nationalen Rechtsordnungen im Bereich der strafprozessualen Beweisbeschaffung an ihre Grenzen. Für einmal besteht der legislatorische Handlungsbedarf nicht auf nationaler, sondern auf internationaler Ebene: Es gilt, zwischenstaatliche Lösungen zu suchen, mit denen dem dargelegten Problem der Beweisverschiebung ins Ausland effektiv begegnet werden kann. Das Territorialitätsprinzip darf und muss in diesem Bereich kritisch hinterfragt werden;[85] gegebenenfalls hat es hier zur Wahrung der Effektivität der Strafverfolgung gar gänzlich zurückzutreten. Durch bewusstes Überschreiten der in der Cybercrime-Konvention eingeräumten Befugnisse durch die Strafverfolgungsbehörden, was vom Bundesgericht im besprochenen Urteil grosszügig abgenickt wurde, ist dagegen nichts gewonnen.

PD Dr. Damian K. Graf, LL.M. (Cambridge), Rechtsanwalt und Solicitor of England and Wales (n.p.), Staatsanwalt für Wirtschaftsdelikte (NW).

85 Schweingruber (Fn. 49), Rz. 6.