

Viktor Györffy, lic iur., Rechtsanwalt, Peyrot Schlegel Györffy Rechtsanwälte, Zürich
gyoerffy@psg-law.ch¹

Quellenschutz im Strafprozess

Mangelhafte Reichweite des gesetzgeberischen Konzepts

Résumé L'importance de la protection des sources, en tant que condition essentielle et pierre angulaire de la liberté de la presse, est unanimement reconnue. La protection des sources est un principe ancré de manière constante dans les jurisprudences du Tribunal fédéral et des organes de la CEDH. Toutefois, en ce qui concerne la mise en œuvre concrète de la protection des sources dans le procès pénal, des disparités et des lacunes subsistent, notamment concernant les saisies et les mesures de surveillance secrètes. Dans la pratique, la protection des sources ne sera prise en considération que dans les cas pour lesquels elle est justifiée. Le processus législatif ne peut empêcher, dans certaines situations, la connaissance des dénonciations aux autorités de poursuite pénale, des cas qui relèvent de la protection des sources.

I. Grundrechtliches Fundament und Bedeutung des Quellenschutzes

1. Quellenschutz im digitalen Zeitalter

Quellenschutz ist essenziell für die journalistische Tätigkeit. Die Bedeutung der journalistischen Tätigkeit¹ und der Stellenwert des Quellenschutzes werden von Lehre und Rechtsprechung im Prinzip anerkannt. Eine andere Frage ist aber, in wie weit der Quellenschutz in der Praxis effektiv gewährleistet werden kann. Mit der zunehmenden Digitalisierung fallen immer grössere Datenmengen an. Kommunikation und Informationsbearbeitung hinterlassen Datenspuren und können mit technischen Mitteln überwacht werden. Das gilt auch für die journalistische Arbeit. Diese steht jedoch unter besonderem Schutz. Damit steht der Staat vor der Herausforderung, die Überwachungskompetenzen gesetzlich so zu regeln und in der Praxis so umzusetzen, dass der Quellenschutz nicht untergraben wird. Die bestehenden gesetzlichen Konzepte werden dem nicht durchwegs gerecht, und auch in der Praxis treten Lücken auf.

2. Praxis des EGMR und des Bundesgerichts

Der Schutz journalistischer Quellen wird vom EGMR und vom Bundesgericht als Grundbedingung und Eckpfeiler der Medienfreiheit anerkannt.² Die Praxis des EGMR stützt sich dabei auf die Freiheit der Meinungsäusserung,³ die Praxis des Bundesgerichts überdies auf das Redaktionsgeheimnis.⁴ Geschützt ist namentlich die Identität des Autors sowie Inhalt und Quelle der Information.⁵ Medienschaffende können ihre Aufgabe als Informationsvermittler und Wächter nur erfüllen, wenn sie die erforderliche Information von Dritten erhalten, insbesondere Hinweise auf Vorkommnisse von gesellschaftlichem Interesse, die sonst verborgen bleiben würden. Dies wiederum setzt voraus, dass die Informationsgeber darauf vertrauen können, dass ihr Name nicht preisgegeben wird. Eine Pflicht zur Preisgabe der anvertrauten Informationen könnte Informanten abschrecken (chilling effect).⁶ Unter Schutz steht damit insbesondere die Identität der Quelle.

1 Interessenbindung des Autors: Der Autor vertritt mehrere Personen, darunter Journalisten, die in einem beim Bundesverwaltungsgericht hängigen Verfahren die Löschung ihrer Vorratsdatenspeicherung gemäss Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) verlangen, sowie den in BGE 140 IV 108 erwähnten Bankangestellten.

2 EGMR, 27.3.1996, Goodwin v. The United Kingdom (GC), 17488/90; EGMR, 22.11.2007, Voskuil v. The Netherlands, 64752/01; BGE 132 I 184; BGE 140 IV 108; Müller/Schefer, Grundrechte in der Schweiz, 4. Aufl., Bern 2008, 472 f.; BaslerKomm/Zeller, Art. 172 StPO, N 2, N 7 f.; Donatsch, in: Kommentar zur Schweizerischen Strafprozessordnung, Donatsch/Hansjakob/Lieber (Hrsg.), 2. Aufl., Zürich/Basel/Genf 2014, Art. 172 N 4.

3 Art. 10 EMRK; Art. 19 des internationalen Pakts über bürgerliche und politische Rechte (IPBPR).

4 Art. 17 Abs. 3 BV.

5 Donatsch (Fn. 2), Art. 172 N 2 f.

6 BaslerKomm/Bommer/Goldschmid, Art. 264 StPO, N 15; Müller/Schefer (Fn. 2), 472 f.; EGMR Goodwin v. The United King-

- 3 Gemäss Strassburger Praxis vermögen nur zwingende Gründe des öffentlichen Interesses die Aufhebung des Redaktionsgeheimnisses zu rechtfertigen. Es ist jedenfalls ein überwiegendes öffentliches Interesse erforderlich. Nach der Praxis des Bundesgerichts bedarf die Offenbarungspflicht ausserordentlicher Umstände.⁷

II. Strafprozessuale Umsetzung

1. Gesetzgeberisches Konzept

A) Zeugnisverweigerungsrecht als Grundlage

- 4 Der Gesetzgeber hat im StGB und in der StPO eine Reihe von Vorschriften verankert, damit Journalisten oder ihre Quellen den ihnen zustehenden Schutz vor strafprozessualen Massnahmen erhalten. Diese bauen auf dem Zeugnisverweigerungsrecht auf, welches mit Art. 28a StGB und Art. 172 StPO gewährleistet wird. Demnach können Personen, die sich beruflich mit der Veröffentlichung von Informationen im redaktionellen Teil eines periodisch erscheinenden Mediums befassen, sowie ihre Hilfspersonen das Zeugnis über die Identität der Autorin oder des Autors oder über Inhalt und Quellen ihrer Informationen verweigern. Nachdem der Quellenschutz auch durch Zwangsmassnahmen im Strafverfahren tangiert sein kann, braucht es weitere Vorschriften in Bezug auf die jeweiligen Zwangsmassnahmen.

B) Übertragung auf Beschlagnahme und Überwachungsmassnahmen

a) Beschlagnahme

- 5 Eine Zwangsmassnahme, die für einen Journalisten mindestens ebenso gravierend sein kann wie eine Zeugnispflicht, ist die Beschlagnahme. Art. 264 Abs. 1 StPO lit. c postuliert ein Beschlagnahmeverbot für Gegenstände und Unterlagen aus dem Verkehr der beschuldigten Person mit Personen, die nach den Artikeln 170-173 StPO das Zeugnis verweigern können und im gleichen Sachzusammenhang nicht selber beschuldigt sind.

b) Geheime Überwachungsmassnahmen

- 6 Im Weiteren können Journalisten von geheimen Überwachungsmassnahmen betroffen sein. Bei der Überwachung einer Person, die einer in den Artikeln 170-173 StPO genannten Berufsgruppe angehört, sind gemäss Art. 271 StPO Informationen, die mit dem Gegenstand der Ermittlungen und dem Grund, aus dem diese Person überwacht wird, nicht in Zusammenhang stehen, unter der Leitung eines Gerichtes auszusondern. Dabei dürfen der Strafverfolgungsbehörde keine Berufsgeheimnisse zur Kenntnis gelangen.

C.) Problematik des gesetzgeberischen Konzepts

- 7 Auf diese Weise soll nach dem Konzept des Gesetzgebers der Quellenschutz bei der Durchführung von Strafverfahren gewährleistet sein. Gesetzgebungstechnisch wird dem Medienschaffenden zur Wahrung des Quellenschutzes ein Zeugnisverweigerungsrecht eingeräumt. Der Schutz des Quellenschutzes vor Beschlagnahme und Überwachung knüpft sodann an das Zeugnisverweigerungsrecht an. Damit ist jedoch das Problem, dass der Quellenschutz durch Beschlagnahme und Überwachungsmassnahmen vereitelt werden kann, nicht zureichend gelöst. Der gesetzgeberische Ansatz greift zu kurz. Er trägt dem Umstand nicht genügend Rechnung, dass bei Beschlagnahme und Überwachung Informationen alleine durch das Vorgehen der Strafverfolgungsbehörde in ihre Sphäre gelangen können. Beim Zeugnisverweigerungsrecht ist dies nicht so. Hier kann der angerufene Zeuge einfach durch Schweigen verhindern, dass Informationen offen gelegt werden. Mit der Beschlagnahme verschafft sich die Strafverfolgungsbehörde das zu beschlagnahmende Gut. Die Überwachung erfolgt heimlich. Hierbei den Quellenschutz zu gewährleisten erscheint um einiges anforderungsreicher.
- 8 Wird der Journalist als Zeuge vorgeladen, so steht er als Person im Fokus der Strafverfolgungsbehörden, und die gewünschten Informationen sind bei ihm. Er hat es in der Hand, den Strafverfolgungsbehörden Informationen nicht zu offenbaren, soweit er sich auf den Quellenschutz stützen kann. Tut er dies, so gelangt sein Wissen, soweit es sich auf den Inhalt der von der Quelle stammenden Informationen und auf die Person der Quelle bezieht, nicht ins Strafverfahren. Soweit Zwangsmassnahmen den Quellenschutz tangieren, ist die Problematik komplexer.

dom (Fn. 2); EGMR Voskuil v. The Netherlands (Fn. 2).

7 BaslerKomm/Bommer/Donatsch, Art. 172 StPO, N 4; EGMR Goodwin v. The United Kingdom (Fn. 2); EGMR, 15.12.2009, Financial Times LTD u.a. v. The United Kingdom, 821/03; BGE 132 I 185.

2. Gewährleistung des Quellenschutzes bei Beschlagnahmen

A) Beschlagnahmeverbot

Gemäss Art. 264 StPO dürfen Gegenstände und Unterlagen aus dem Verkehr der beschuldigten Person mit Personen, die nach den Artikeln 170–173 StPO das Zeugnis verweigern können, nicht beschlagnahmt werden. Dieses Beschlagnahmeverbot ist somit u.a. als Schutzmechanismus für den Quellenschutz gedacht und soll der Gewährleistung des Redaktionsgeheimnisses dienen. Es erstreckt sich insoweit auf Unterlagen, die auf den Autor, den Inhalt oder die Quelle einer Information hinweisen.⁸ Die Strassburger Praxis hebt hervor, dass Hausdurchsuchungen und Beschlagnahmen bei Medienschaffenden aus Sicht der Medienfreiheit noch problematischer sind als die Pflicht zur Zeugenaussage, da sie den Behörden den Zugriff auf sämtliche Arbeitsunterlagen der betroffenen Medienschaffenden ermöglichen.⁹

B) Gewährleistung durch Siegelung nach Beschlagnahme

Auch wenn die zu beschlagnahmenden Unterlagen unter ein Berufsgeheimnis fallen, haben Beschuldigte, zeugnisverweigernde Geheimnisträger und Dritte eine Pflicht, Durchsuchungen und Beschlagnahmen zu dulden. Dem Schutz des Berufsgeheimnisses dient das Institut der Siegelung gemäss Art. 248 StPO:¹⁰ Macht eine berechtigte Person geltend, eine Beschlagnahme von Gegenständen und Vermögenswerten sei wegen eines Aussage- oder Zeugnisverweigerungsrechts oder aus anderen Gründen nicht zulässig, so gehen die Strafbehörden nach den Vorschriften über die Siegelung vor (Art. 264 Abs. 3 StPO).

C) Beschlagnahmeverbot im Fall der Beschlagnahme bei der beschuldigten Person

Das Beschlagnahmeverbot gilt gemäss Wortlaut von Art. 264 Abs. 1 StPO ungeachtet des Ortes, wo sich die zu beschlagnahmenden Unterlagen befinden, und des Zeitpunktes, in welchem sie geschaffen worden sind. Das Bundesgericht hat in einem Entscheid die Tragweite dieser Bestimmung in Bezug auf den Quellenschutz klargestellt. Zu entscheiden war, ob das Beschlagnahmeverbot auch Geltung beansprucht, wenn die Gegenstände und Unterlagen, welche aus dem Verkehr zwischen der beschuldigten Person und Journalisten stammen, bei der beschuldigten Person beschlagnahmt werden. Das Bundesgericht hält dafür, unter das Beschlagnahmeverbot würden nicht nur Gegenstände und Unterlagen aus dem Verkehr des Beschuldigten mit Journalisten fallen, die sich in deren Gewahrsam befinden, sondern auch solche, die sich im Gewahrsam des Beschuldigten und Dritter befinden. Dass es für das Beschlagnahmeverbot nicht darauf ankommt, wo sich die Gegenstände und Unterlagen befinden, entspreche dem klaren Willen des Gesetzgebers. Der Zweck von Art. 264 Abs. 1 lit. c i.V.m. Art. 172 StPO spreche ebenfalls gegen ein Abweichen vom Wortlaut. Erfolge die Kommunikation zwischen dem Informanten und dem Journalisten schriftlich, hinterlasse das Spuren. Dabei werde namentlich beim heute stark zunehmenden E-Mail-Verkehr oft hin- und hergeschrieben. Insoweit sei in der Regel jeweils der gesamte Schriftverkehr zwischen den Beteiligten ersichtlich. Müsste der Informant damit rechnen, dass Inhalte der Kommunikation mit Journalisten bei ihm beschlagnahmt werden, müsste er die E-Mails jeweils sofort löschen. Selbst dann müsste er gewärtigen, dass die Strafverfolgungsbehörden diese gegebenenfalls wiederherstellen könnten. Die Aussicht darauf, dass Inhalte der Kommunikation mit dem Journalisten beim Informanten beschlagnahmt werden könnten, könnte diesen somit davon abhalten, dem Journalisten die Information zukommen zu lassen. Der Informant könne zudem kaum je völlig sicher sein, dass der Journalist Unterlagen, aus denen sich die Quelle der Information ergibt, nicht einem Dritten übergibt. Müsste der Informant damit rechnen, dass die Unterlagen beim Dritten beschlagnahmt werden, könnte ihn das ebenso davon abhalten, die Information dem Journalisten zukommen zu lassen. Dies alles wäre dem Wächteramt der Medien abträglich. Sowohl das Bundesgericht als auch der Europäische Gerichtshof für Menschenrechte würden dem Quellenschutz als Eckpfeiler der Pressefreiheit erhebliches Gewicht zumessen. Dies spreche für einen tendenziell weiten Quellenschutz und damit gegen eine einengende Auslegung entgegen dem Wortlaut. Insgesamt bestünden keine triftigen Gründe dafür, ausnahmsweise vom klaren Wortlaut von Art. 264 Abs. 1 StPO abzuweichen.¹¹

D) Wirksamer Quellenschutz durch Beschlagnahmeverbot?

Diese prinzipielle Klärung der Tragweite des Quellenschutzes garantiert für sich alleine noch nicht die praktische Durchsetzung des Quellenschutzes. Werden Gegenstände und Dokumente beim Journalisten beschlagnahmt, so kann er die Siegelung verlangen und ist im daran anschliessenden Entsiegelungsverfahren involviert.

8 Heimgartner, in: Kommentar zur Schweizerischen Strafprozessordnung (Fn. 2), Art. 264 N 14.

9 Müller/Schefer (Fn. 2), S. 473; EGMR, 23.2.2003, Roemen & Schmit v. Luxembourg, 51772/99

10 Heimgartner, in: Kommentar zur Schweizerischen Strafprozessordnung (Fn. 2), Art. 264 N 19

11 BGE 140 IV 108

Damit erscheint der Quellenschutz als gewährleistet. Es kann sichergestellt werden, dass Polizei und Staatsanwaltschaft keine Kenntnis von Tatsachen erhalten, die den Quellenschutz beschlagen, einschliesslich der Identität der Quelle.

- 13 Werden Gegenstände beschlagnahmt, welche sich nicht beim Journalisten befinden, so kann nicht einfach dieser die schützende Hand über die entsprechenden Informationen halten. Es liegt dann an der von der Beschlagnahme betroffenen Person, den Strafverfolgungsbehörden und allenfalls am Gericht, für den Quellenschutz besorgt zu sein. Der Journalist bzw. seine Quelle sind darauf angewiesen, dass die von der Beschlagnahme betroffene Person Quellenschutz geltend macht und Siegelung verlangt, oder dass die Strafverfolgungsbehörden von sich aus entscheiden, dem Quellenschutz unterstehendes Material nicht zu verwenden. Es stellen sich hier vergleichbare Probleme wie bei der Verwertung von Daten aus geheimen Überwachungsmaßnahmen (dazu nachstehend Ziff. 3). Insbesondere fehlt ein wirksames Verfahren, in dem sich der Journalist als Drittperson wehren könnte. Zudem wird eine Beschlagnahme nicht notwendigerweise gerichtlich überprüft (anders als bei geheimen Überwachungsmaßnahmen, welche vom Zwangsmassnahmengericht genehmigt werden müssen).
- 14 Die von der Beschlagnahme betroffene Person kann geltend machen, dass der Quellenschutz der Beschlagnahme entgegensteht, und kann die Siegelung verlangen. Tut sie dies, impliziert dies allerdings, dass sich im beschlagnahmten Material Hinweise auf journalistische Quellen und die von diesen gelieferten Informationen befinden. Allein dies kann den Quellenschutz bereits gefährden oder zunichte machen. Ist die von der Beschlagnahme betroffene Person selbst Quelle, so kann eben dieser Umstand nicht verborgen bleiben, wenn der Quellenschutz angerufen werden soll.
- 15 Soweit die Strafverfolgungsbehörden von sich aus entscheiden, Material, das dem Quellenschutz unterliegt, nicht zu verwenden, besteht dieselbe paradoxe Situation: Die Strafverfolgungsbehörde kann dies nicht tun, ohne zumindest gewisse Hinweise auf quellenschutzrelevante Informationen zu haben. Die Situation ist hier noch delikater als etwa beim Schutz des Anwaltsgeheimnisses. Wenn es um den Schutz der Verteidigerkorrespondenz geht, ist allen Beteiligten klar, dass und warum ein Beschlagnahmeverbot besteht.

3. Gewährleistung des Quellenschutzes bei geheimen Überwachungsmaßnahmen

A) Gewährleistung durch Aussonderung unter der Leitung eines Gerichts

- 16 Der Schutz von Berufsgeheimnissen ist sodann bei geheimen Überwachungsmaßnahmen (Art. 269 ff. StPO) zu beachten. Dies soll durch das in Art. 271 StPO vorgesehene Prozedere gewährleistet werden. Bei der Überwachung einer Person, die einer in den Artikeln 170-173 genannten Berufsgruppe angehört, sind Informationen, die mit dem Gegenstand der Ermittlungen und dem Grund, aus dem diese Person überwacht wird, nicht in Zusammenhang stehen, unter der Leitung eines Gerichtes auszusondern. Dabei dürfen der Strafverfolgungsbehörde keine Berufsgeheimnisse zur Kenntnis gelangen. Bei der Überwachung anderer Personen sind Informationen, über welche eine in den Artikeln 170-173 genannte Person das Zeugnis verweigern könnte, aus den Verfahrensakten auszusondern und sofort zu vernichten; sie dürfen nicht verwendet werden. Das Ziel der Bestimmung ist klar: Fallen bei einer geheimem Überwachung Informationen an, die dem Schutz des Berufsgeheimnisses bzw. dem Quellenschutz unterstehen, so sollen diese aus den Strafakten ausgesondert werden. Näher zu untersuchen bleibt, was die vorgesehene Triage unter Leitung des Gerichts als Schutzmechanismus zu leisten vermag.

B) Wirksamer Quellenschutz durch Aussonderung?

- 17 Die Auswertung soll so vorgenommen werden, dass der Strafverfolgungsbehörde keine Berufsgeheimnisse zur Kenntnis gelangen (Art. 271 Abs. 1 StPO). Dies würde voraussetzen, dass die Auswertung der Daten von einer Behörde ausserhalb der Strafverfolgungsbehörden (zu denen nach Art. 12 StPO auch die Polizei gehört) durchgeführt wird. Effektiv haben aber nur die Polizeibehörden Zugriff auf das zentrale System, auf dem die Überwachungsdaten des Dienstes¹² gespeichert sind.¹³ Das im Gesetz formulierte Ziel ist in der Realität insoweit nicht umsetzbar.
- 18 Zu beachten ist auch, dass die Staatsanwaltschaft die geheime Überwachung anordnet und das Zwangsmassnahmengericht erst nachträglich innert 5 Tagen über dessen Zulässigkeit entscheidet (Art. 274 StPO). Daten, die unmittelbar nach der Anordnung anfallen, sind für die Staatsanwaltschaft einsehbar und können von dieser ausgewertet werden. Tangieren die anfallenden Daten den Quellenschutz, ist dieser damit bereits durchbrochen.

12 Lawful Interception System (LIS) des Dienstes Überwachung Post- und Fernmeldeverkehr (Dienst ÜPF).

13 Hansjakob, in: Kommentar zur Schweizerischen Strafprozessordnung (Fn. 2), Art. 271 N 9.

Es besteht insoweit keine wirksame Garantie gegen die Verwendung von Daten, die dem Quellenschutz unterliegen. Es ist zudem unerfindlich, wie die Strafverfolgungsbehörden die in Echtzeit hereinkommenden Daten für das laufende Strafverfahren nutzen können und dabei gleichzeitig Daten, die dem Quellenschutz unterliegen, nicht zur Kenntnis nehmen sollen. Diese Praxis ist somit mit den vom Bundesgericht und vom EGMR angerufenen Grundrechten nicht vereinbar, sie verletzt die BV und die EMRK.

Die Überwachung laufender Kommunikation läuft immer über sogenannte Direktschaltungen, bei denen das Ergebnis der Überwachung unmittelbar an die Strafverfolgungsbehörden übermittelt wird. Die in Art. 271 Abs. 2 StPO vorgesehene Einschränkung von Direktschaltungen zum Schutz von Berufsgeheimnissen ist nicht umsetzbar, da es technisch nur noch Direktschaltungen gibt. Die Bestimmung von Art. 274 Abs. 4 lit. b StPO, wonach sich das Zwangsmassnahmengericht zur Zulässigkeit von Direktschaltungen äussern muss, ist damit obsolet.¹⁴

Übrig bleibt im Wesentlichen nur noch das Postulat, die Triage so zu organisieren, dass die Strafverfolgungsbehörden nicht während laufendem Triageprozess von Geheimnissen Kenntnis erhalten.¹⁵

Geheimnisgeschützte Informationen, die aus Überwachungen Dritter resultieren, sind ebenfalls auszusondern. Dies betrifft Fälle, in denen Geheimnisträger als Kommunikationspartner der überwachten Person in Erscheinung treten. Die Weiterleitung von Geheimnissen, die durch Art. 170 - 173 geschützt sind, an Dritte ist gleich zu behandeln.¹⁶ Das Gesetz verlangt, dass Informationen, welche geschützte Geheimnisse betreffen, aus den Verfahrensakten ausgesondert und sofort vernichtet werden. Sie dürfen nicht verwendet werden. In Bezug auf die Protokolle des Kommunikationsvorgangs lässt sich dies zweifelsohne umsetzen. Soweit es um die Datenträger geht, ergeben sich Probleme: Das verwendete System lässt die Löschung von einzelnen Kommunikationen nicht ohne Weiteres zu. Grundsätzlich ist die Datenintegrität zu wahren. Der auswertenden Behörde soll es nicht möglich sein, einzelne Gespräche (die auch entlastend sein können) zu löschen. Vielmehr muss nachvollziehbar sein, dass die Überwachungsdaten vollständig sind. Auf Antrag der anordnenden Staatsanwaltschaft ist die Löschung einzelner Kommunikationen möglich. Ein weiteres Problem besteht insoweit, als die überwachte Person ein Interesse haben kann, dass auch Kommunikationsdaten mit Geheimnisträgern Eingang in die Untersuchung finden. Werden solche Daten sofort ausgesondert und vernichtet, dann können sie nicht mehr ins Verfahren eingeführt werden, auch wenn dies die betreffende Person später beantragt. Schliesslich kommt es immer wieder vor, dass Kommunikation teilweise geschützte Geheimnisse betrifft, aber auch Passagen beinhaltet, die verwertbar sind. Die teilweise Löschung einzelner Kommunikationsvorgänge ist allerdings vom System her nicht möglich und wäre auch bedenklich aufgrund der damit verbundenen Missbrauchsgefahr. Etwas entschärft werden könnte die Problematik, wenn die Informationen über Geheimnisse aus den Verfahrensakten ausgesondert, aber bis zur Gewährung der Akteneinsicht noch nicht vernichtet werden.¹⁷

Weil Überwachungsmassnahmen geheim sind, weiss der betroffene Journalist zunächst nichts von diesen. Er wird allenfalls im Nachhinein darüber orientiert, was allerdings auch nicht in jeder Konstellation garantiert ist. Gemäss Art. 279 StPO muss die überwachte Person, sei diese selbst beschuldigt oder sei sie als Drittperson überwacht worden, früher oder später über die Überwachung orientieren. Verbindungspartner der überwachten Person werden praxisgemäss nicht orientiert. Wenn also der Journalist selbst nicht Subjekt der Überwachungsmassnahme ist, in der Überwachung aber Kommunikationsdaten hängen bleiben, die ihn betreffen, etwa als Kommunikationspartner, wird er nicht orientiert. Er hat nach h. L. nicht einmal ein Beschwerderecht, was der Praxis des EGMR widerspricht, gemäss der Gesprächspartner von überwachten Personen Anspruch auf eine wirksame Beschwerde nach Art. 13 EMRK haben.¹⁸

Wird die Aussonderung durch das Gericht vorgenommen, bevor die Betroffenen über die Überwachung orientiert sind, so ist der Journalist bei der Aussonderung nicht involviert, dies unabhängig davon, ob ihn diese als überwachte Person oder sonstwie betrifft.

In dieser Situation obliegt die Gewährleistung des Quellenschutzes den übrigen Beteiligten, also der mit der Auswertung betrauten Behörde und dem mit der Leitung betrauten Gericht. Es ist keine klare Praxis greifbar, wie das umzusetzen ist. Jedenfalls kann es sich wegen der Relativität von gewissen Zeugnisverweigerungsrechten ergeben, dass die Beschlagnahme anordnende Behörde von Tatsachen Kenntnis erhält, deren Schutz nach Art. 264 Abs. 1 StPO gerade bezweckt ist.¹⁹ Der Wortlaut des Gesetzes (... sind Informationen ... auszusondern) und der Zweck der Bestimmung legt eine Aussonderung von Amtes wegen nahe. Ziel der Triage ist, dass diejenigen Informationen ausgesondert werden, welche schützenswerte Geheimnisse betreffen; der Strafverfolgungsbehörde dür-

14 BaslerKomm/Jean-Richard-Dit-Bressel, Art. 269 StPO N 12, Art. 271 StPO N 10, Art. 274 StPO N 8.

15 BaslerKomm/Jean-Richard-Dit-Bressel, Art. 271 StPO N 10.

16 Hansjakob (Fn. 13), Art. 271 N 14; Schmid, StPO Praxiskommentar, Art. 271 N 9.

17 Hansjakob (Fn. 13), Art. 271 N 15.

18 BaslerKomm/Jean-Richard-Dit-Bressel, Art. 279 StPO N 11; EGMR, 16.2.2000, Amman v. Schweiz, 27798/95.

19 BaslerKomm/Bommer/Goldschmid, Art. 264 StPO, N 59.

fen gemäss Gesetzestext keine Berufsgeheimnisse zur Kenntnis gelangen.²⁰ Es ist für diese aber nicht unbedingt ersichtlich, dass der Quellenschutz tangiert ist. Im Prinzip würde sich auch die Frage stellen, ob und in wie weit sich der Journalist überhaupt auf den Quellenschutz berufen und eine Aussonderung will. In der Literatur wird die Auffassung vertreten, dass die Strafverfolgungsbehörde auch ohne entsprechendes Ersuchen die Siegelung in jenen Fällen vorzunehmen hat, in denen die berechtigte Person weder ausdrücklich noch konkludent auf die Siegelung verzichtet hat. Daraufhin kann die Behörde ein Entsiegelungsgesuch stellen mit dem Ziel, die Zulässigkeit der Beschlagnahme überprüfen zu lassen, ohne dass die anordnende Behörde selbst vom Inhalt der beschlagnahmten Objekte Kenntnis nehmen muss.²¹

25 Formell stellt sich die Frage, wer berechtigte Person i.S.v. Art. 264 Abs. 3 StPO ist. Gemäss Literatur ist dies die beschuldigte Person. Diese kann eine Siegelung verlangen, und zwar auch dann, wenn die Beschlagnahme von Gegenständen nicht in ihrer Herrschaftssphäre erfolgt ist.²² Diese Auffassung führt folgerichtig dazu, dass bei einer Siegelung von Amtes wegen beachtet wird, was die beschuldigte Person effektiv oder mutmasslich will mit der Folge, dass Beweise nicht zu siegeln sind, soweit die beschuldigte Person auf eine Siegelung verzichtet. Damit kann der Quellenschutz auf der Strecke bleiben, wenn der Journalist nicht selbst beschuldigte Person ist, es sei denn, man misst dem Quellenschutz ein öffentliches Interesse zu, dem auch von Amtes wegen zum Durchbruch verholfen werden muss. Materiell liesse sich aufgrund der Bedeutung des Quellenschutzes und aufgrund des in Art. 264 Abs. 1 StPO verankerten Beschlagnahmeverbotes durchaus so argumentieren. Formell liegt es aber primär in der Hand der beschuldigten Person, ob sie eine Siegelung verlangt oder nicht. Zudem sind auch die Verteidigungsrechte der angeschuldigten Person zu beachten. Diese kann als primäres Verfahrenssubjekt nicht einfach übergangen werden, wenn sie keine Siegelung wünscht.

26 Davon abgesehen lässt sich die Problematik nur schon deshalb nicht vollständig lösen, als die Behörde überhaupt einmal realisieren muss, dass ein Zeugnisverweigerungsrecht tangiert sein könnte. Hierfür muss sie gewisse Kenntnis über den Inhalt der beschlagnahmten Objekte haben, was gerade beim Quellenschutz sehr heikel ist.

27 Zureichend wäre das Prozedere zur Garantie des Quellenschutzes nur, wenn der Journalist bei der Entscheidung darüber, ob ein Beweisverwertungsverbot vorliegt, involviert wäre. Die materiellen Grundsätze allein bieten keine durchgehende Garantie, zumal keine Gewähr dafür besteht, dass die Strafverfolgungsbehörden das Beweisverwertungsverbot erkennen und ihm zur Durchsetzung verhelfen.

III. Schutz vor Verwertung unzulässig beschaffter Daten: Der Fall Ritzmann als Beispiel

1. Datenerhebung ohne konkreten Tatverdacht

28 Die praktische Relevanz der Problematik lässt sich an Hand des Strafverfahrens gegen Iris Ritzmann verdeutlichen: Im Zuge der Mörgeli-Affäre erstattete die Universität Zürich Anzeige gegen Unbekannt, nachdem kritische Medienartikel über die Tätigkeit von Christoph Mörgeli erschienen waren. Darin wurden u.a. zwei Berichte erwähnt. Die Staatsanwaltschaft war der Auffassung, es handle sich um universitätsinterne und geheime Berichte, die Übergabe dieser Berichte an Journalisten stelle eine Amtsgeheimnisverletzung dar, und eröffnete ein Strafverfahren. In diesem Strafverfahren liess die Staatsanwaltschaft u.a. von der Universität Beweismittel zusammentragen. Auf entsprechende Ersuchen der Staatsanwaltschaft prüfte die Universität Zürich sämtliche universitären festen und mobilen Telefonanschlüsse im vorgegebenen Zeitraum sowie die E-Mail-Adressen aller Angehörigen (einschliesslich der Studenten) für denselben Zeitraum bezüglich Kontakten mit Telefonnummern und E-Mail-Adressen von mehreren Journalisten und Zeitungen und übermittelte die dabei aufgefundenen Randdaten elektronisch der Staatsanwaltschaft. Analoge Datenerhebungen wurden vom Hochschulamt durchgeführt. Die Datenerhebungen wurden durchgeführt, ohne dass ein konkreter Tatverdacht gegen eine bestimmte Person vorgelegen hätte. Die Auswertung der gewonnenen Daten führte dazu, dass die Staatsanwaltschaft ein polizeiliches Ermittlungsverfahren gegen Iris Ritzmann und ihren Ehemann einleitete, Hausdurchsuchungen durchführte und schliesslich Anklage gegen Iris Ritzmann erhob wegen mehrfacher Verletzung des Amtsgeheimnisses.

20 Hansjakob (Fn. 13), Art. 271 N 8.

21 BaslerKomm/Bommer/Goldschmid, Art. 264 StPO, N 59 f.

22 BaslerKomm/Bommer/Goldschmid, Art. 264 StPO, N 58.

2. Folge: Beweisverwertungsverbot

Sowohl das Bezirksgericht Zürich als auch das Obergericht des Kantons Zürich haben entschieden, dass die erhobenen Daten einem Beweisverwertungsgebot unterliegen.²³ Beide Instanzen kamen zu denselben Schlüssen: Auch wenn die Universität Zürich die Informationen zusammengetragen und den Strafverfolgungsbehörden eingereicht habe, handle es sich um von einer Strafbehörde erhobene Beweise. Die massgeblichen Beweise seien von der Universität Zürich nach den Vorgaben der Staatsanwaltschaft zusammengetragen worden. Sie habe keinen eigenen Entscheidungsspielraum gehabt, sondern letztlich lediglich die Anweisungen der Staatsanwaltschaft umgesetzt.²⁴ Die Staatsanwaltschaft hätte nach den Bestimmungen über geheime Überwachungsmaßnahmen (Art. 273 StPO) vorgehen müssen. Daran ändere nichts, dass die Kommunikation über die Infrastruktur der Universität Zürich abgewickelt wurde und die Kommunikationsdaten deshalb nicht bei einer Fernmeldediensteanbieterin herausverlangt werden mussten, sondern direkt bei der Universität erhoben werden konnten. An eine Fernmeldeüberwachung würden insbesondere aufgrund der Heimlichkeit des staatlichen Handelns erhöhte Anforderungen gestellt. Insbesondere hätte eine richterliche Genehmigung eingeholt werden müssen. Nachdem sich die betroffenen Personen nicht wie bei anderen Zwangsmassnahmen direkt nach dem Eingriff hätten zur Wehr setzen können, hätte das Zwangsmassnahmengericht die Rechtmässigkeit des Eingriffs und insbesondere auch dessen Verhältnismässigkeit überprüfen müssen.²⁵ Zwangsmassnahmen setzen generell voraus, dass ein hinreichender Tatverdacht vorliegt und die Untersuchungshandlung verhältnismässig erscheint (Art. 197 Abs. 1 lit. b-d StPO). Der Verdachtsgrad, so das Obergericht, müsse umso höher sein, je schwerer der Eingriff in die Grundrechte der Betroffenen wiegt. Bei den besonders schwer wiegenden Massnahmen der Überwachung des Post- und Fernmeldeverkehrs sei stets ein dringender Tatverdacht verlangt (Art. 269 Abs. 1 lit. a StPO; Art. 273 Abs. 1 StPO). In diesem Zusammenhang monierte das Obergericht, dass die Staatsanwaltschaft heimliche Überwachungsmaßnahmen veranlasst hatte, ohne dass ein Tatverdacht gegen eine bestimmte Person bestanden hatte, dass diese Überwachungsmaßnahmen zahlreiche Personen und betrafen und einen Zeitraum von fast einem Jahr umfassten, wodurch eine enorme Datenmenge zusammenkam. Der Einsatz von Zwangsmassnahmen gegen Personen, die nicht unter Tatverdacht stehen, müsse besonders zurückhaltend erfolgen (Art. 197 Abs. 2 StPO). Zwangsmassnahmen hätten sich primär gegen die tatverdächtige Person zu richten, weil gerade sie durch den Tatverdacht die Rechtsordnung störe. Soweit sich Zwangsmassnahmen gegen nichtbeschuldigte Personen richten, fehle diesen gegenüber der Tatverdacht als die Zwangsmassnahme legitimierendes und begrenzendes Kriterium. Deshalb sei hier besondere Zurückhaltung erforderlich. Alle geheimen Überwachungsmaßnahmen würden in schwerwiegender Weise in die Grundrechte eingreifen, weshalb sie auch einen dringenden Tatverdacht erfordern. Das Vorgehen der Staatsanwaltschaft weise zumindest eine gewisse Ähnlichkeit mit einer unzulässigen, weil verdachtsunabhängigen Beweisausforschung auf. Die von der Staatsanwaltschaft angeordnete Randdatenerhebung erscheine unverhältnismässig.²⁶

29

3. Erhebung der Daten ist geheime Überwachungsmaßnahme

Die von der Staatsanwaltschaft verlangte Auswertung betraf Randdaten, keine Daten über den Inhalt der Kommunikation. Die Daten enthielten unter anderem Informationen über den Absender und Empfänger der Emailnachricht sowie den Zeitpunkt des Versands der Nachricht. Ob der Zugriff auf diese Daten als geheime Überwachungsmaßnahme zu qualifizieren ist, hängt auch davon ab, bei wem und in welchem Zeitpunkt die Daten erhoben werden. Werden die Daten während des Kommunikationsvorgangs erhoben, so liegt eine geheime Überwachungsmaßnahme vor. Nach der Übermittlungsphase können die Randdaten grundsätzlich bei den Kommunikationsteilnehmern erhoben werden. Im konkreten Fall wurden die Daten jedoch nicht von den Kommunikationsteilnehmern selbst, sondern von der Universität Zürich bezogen. Werden die Verbindungsdaten ohne Kenntnis des Betroffenen bei der Fernmeldediensteanbieterin erhoben, so besteht ein besonderes Schutzbedürfnis, denn der Kommunikationsteilnehmer kann Entstehung und Speicherung solcher Daten bei der Anbieterin nicht verhindern. Informationen, die nach dem Transport auf dem Transportweg zurückbleiben und sich dort erheben lassen, sind deshalb durch das Fernmeldegeheimnis geschützt. Die Erhebung von Randdaten bei der Fernmeldediensteanbieterin ist deshalb nur nach den Vorschriften über die geheimen Überwachungsmaßnahmen möglich. Aus diesen Gründen stellt die Erhebung der Randdaten des Emailverkehrs durch die Staatsanwaltschaft nach der

30

23 BeZGer ZH, 5.12.2014, GG140151; OGer ZH, 1.12.2015, SB150090.

24 OGer ZH, 1.12.2015, SB150090, E. II.2.1.

25 OGer ZH, 1.12.2015, SB150090, E. II.4.4.

26 OGer ZH, 1.12.2015, SB150090, E. 4.6., mit Hinweis auf die Botschaft zur Vereinheitlichung des Strafprozessrechts vom 21. Dezember 2005, BBl 2006 1085, 1216.

Beurteilung des Obergerichts eine Form der geheimen Kommunikationsüberwachung dar. Die Staatsanwaltschaft hätte diese Informationen nur unter Einhaltung der Voraussetzungen von Art. 273 StPO erheben dürfen. Insbesondere wäre eine richterliche Genehmigung erforderlich gewesen.²⁷

31 Gestützt auf die Auswertung der Randdaten beauftragte die Staatsanwaltschaft die Universität Zürich später damit, die persönlichen Emailboxen von dreizehn namentlich genannten Angehörigen der Universität Zürich sowie drei nicht persönlich zuordenbare Emailboxen der Universität Zürich mit fünf Emailadressen von Journalisten abzugleichen und ihr die Inhalte der fraglichen Emails zukommen zu lassen. Die Universität Zürich liess der Staatsanwaltschaft die gewünschten Daten zukommen. Diese Anordnung der Staatsanwaltschaft bezog sich nicht mehr nur auf die Verbindungsdaten, sondern umfasste neu auch die Inhalte der E-mailkommunikation. Das Obergericht erwog, dass diese Beweiserhebung ebenfalls nicht unter Einhaltung der dafür geltenden Vorschriften erfolgt war.²⁸ Nach bundesgerichtlicher Rechtsprechung liegt keine Fernmeldeüberwachung vor, wenn elektronische Kommunikationsinhalte, welche vom Empfänger bereits abgerufen wurden, bei einer Fernmeldediensteanbieterin sichergestellt werden. Das Fernmeldegeheimnis entfaltet seine Wirkung im Zeitpunkt der Informationsübertragung. Eine Fernmeldeüberwachung liegt deshalb nur solange vor, als die betreffenden Nachrichten vom Empfänger noch nicht auf dem Gerät abgerufen worden sind. Das Obergericht argumentiert demgegenüber, wenn bereits für die Erhebung der Randdaten, die lediglich den Nachweis von Kontakten ermöglichen, die Voraussetzungen für eine Überwachungs-massnahme Geltung beanspruchen, gelte dies umso mehr, wenn Kommunikationsinhalte erhoben werden, aus denen in aller Regel auch Randdaten ersichtlich seien. Vorliegend sei der Kommunikationsvorgang im Zeitpunkt der staatsanwaltschaftlichen Beweiserhebung bereits abgeschlossen gewesen. Die Erhebung der Kommunikationsinhalte habe jedoch wiederum heimlich, d.h. ohne Information der davon betroffenen Personen, stattgefunden. Diese hätten sich dagegen nicht unmittelbar zur Wehr setzen können, womit der Rechtsschutz nicht gewährleistet gewesen sei. Inhaltlich stelle das Vorgehen der Staatsanwaltschaft deshalb nichts anderes als eine heimlichen Überwachungs-massnahme dar. Damit hätte die Staatsanwaltschaft die für eine Fernmeldeüberwachung geltenden Voraussetzungen einhalten müssen.²⁹

4. Fernwirkung des Verwertungsverbot für Folgebeweise

32 Es lagen somit Ergebnisse aus nicht genehmigten Überwachungen vor, die gemäss Art. 277 Abs. 2 StPO i.V.m. Art. 141 Abs. 1 StPO nicht verwertet werden dürfen. Das Obergericht entschied, dass die Folgebeweise, die aufgrund der von der Universität erhaltenen Daten erhoben worden waren, ebenfalls nicht verwertet werden dürfen. Die Fernwirkung von unverwertbaren Beweisen sei für relative Beweisverwertungsverbote ausdrücklich in der Strafprozessordnung verankert. Für absolute Beweisverwertungsverbote gelte ebenfalls eine Fernwirkung. Dies ergebe sich aus der Gesetzessystematik sowie dem Sinn und Zweck von Beweisverboten. Die bundesgerichtliche Rechtsprechung zum alten Verfahrensrecht habe für die Frage der Verwertbarkeit von Folgebeweisen ebenfalls nicht danach unterschieden, ob der Grund für die Unverwertbarkeit des Primärbeweises ein absolutes oder ein relatives Beweisverwertungsverbot ist. Es müsse daher von einer Fernwirkung des Verwertungsverbots ausgegangen werden. Dabei obliege es den Strafbehörden darzulegen, dass sie den (Zweit-) Beweis im konkreten Fall auch ohne den illegalen (Erst-) Beweis hätten erheben können.³⁰ Die Erkenntnisse, die die Staatsanwaltschaft aus der Auswertung der universitären Kommunikation gewonnen hatte, führten zur Hausdurchsuchung bei Iris Ritzmann. Zum Zeitpunkt, in dem die Staatsanwaltschaft erstmals Fernmeldedaten erhob, bestand noch kein konkreter Tatverdacht gegen sie. Die Staatsanwaltschaft konnte nicht aufzeigen, dass sie die weiteren Beweise gegen Iris Ritzmann auch ohne die Erkenntnisse aus der unrechtmässigen Erhebung der Fernmeldedaten bei der Universität Zürich hätte erhältlich machen können. Das führte zu einem Beweisverwertungsverbot in Bezug auf diese Beweise, insbesondere für die Erkenntnisse aus der bei Iris Ritzmann durchgeführten Hausdurchsuchung.

27 OGer ZH, 1.12.2015, SB150090, E. 5.2.; Hansjakob, Kommentar BÜPF/VÜPF, 2. Aufl., Erscheinungsort 2006, 83 f.; BaslerKomm/Jean-Richard-dit-Bressel, Art. 269 StPO, N 22; Aepli, Die strafprozessuale Sicherstellung von elektronisch gespeicherten Daten, Diss. Zürich 2004, 23 f.

28 OGer ZH, 1.12.2015, SB150090, E. 6.1 f.

29 OGer ZH, 1.12.2015, SB150090, E. 6.2. unter Hinweis auf Heimgartner, Strafprozessuale Beschlagnahme, Zürich 2011, 179f., und Aepli (Fn. 27), 17 ff.; BGer, 24.08.2015, 1B_52 /2015, E. 1.1.; BaslerKomm/Jean-Richard-dit-Bressel, Art. 269 N 24; BGE 140 IV 181.

30 OGer ZH, 1.12.2015, SB150090, E. 7.1. unter Hinweis auf BaslerKomm/Gless, Art. 141 N 89 f., N 97; BaslerKomm/Jean-Richard-dit-Bressel, Art. 277 N 4 und BGE 138 IV 169.

5. Quellenschutz?

Iris Ritzmann hatte im Verfahren geltend gemacht, die Verwertung der Ergebnisse dieser Randdatenerhebungen sowie die darauf basierenden Akten würden gegen den Quellenschutz verstossen und seien deshalb aus dem Recht zu weisen. Im Ergebnis machte es keinen Unterschied, aufgrund welcher rechtlichen Grundlage die Beweise als unverwertbar erschienen. Die Gerichte mussten somit nicht darüber befinden, ob ein Verstoß gegen den Quellenschutz vorlag. Fest steht, dass die Staatsanwaltschaft sich die Daten beschaffen konnte. Das Zwangsmassnahmengericht war nicht involviert worden. Die angeschuldigte Person wehrte sich gegen die Verwertung dieser Daten und weiterer Beweise, und es bedurfte eines Entscheids des Sachgerichts, welches die Beweise als unverwertbar einstufte. Dieser Entscheid ist zwar im Ergebnis sehr klar ausgefallen, zeigt aber gleichzeitig, wie dornenvoll Quellenschutz sein kann, und unterstreicht die Schwierigkeiten bei der Gewährleistung fundamentaler Rechte. 33

IV. Vorratsdatenspeicherung und Quellenschutz

1. Speicherung von Metadaten auf Vorrat

Fernmeldeanbieterinnen sind verpflichtet, die für die Teilnehmeridentifikation notwendigen Daten sowie die Verkehrs- und Rechnungsdaten während sechs Monaten aufzubewahren (Art. 15 Abs. 3 BÜPF). Das Bundesgericht lässt eine Verwendung solcher Daten grundsätzlich auch zu, wenn die Daten länger als sechs Monate aufbewahrt worden sind.³¹ Seit Erlass des BÜPF³² hat die elektronische Kommunikation sehr stark an Bedeutung gewonnen. Die anfallenden Datenspuren nehmen immer mehr zu und erlauben immer weitgehendere Rückschlüsse. Im Fall Ritzmann sind zunächst nur Randdaten erhoben worden und keine Kommunikationsinhalte.³³ Der Fall illustriert, welche Aussagekraft solchen Metadaten zukommen kann. Sie können Verbindungen zwischen Journalisten und ihren Quellen aufzeigen, und genau deswegen hat sich die Staatsanwaltschaft auch für diese Daten interessiert. 34

2. Vorratsdatenspeicherung kollidiert mit Grundrechten

In jüngerer Zeit ist die Vorratsdatenspeicherung zum Schauplatz grundrechtlicher Auseinandersetzungen geworden. Der EuGH hat am 8. April 2014 die EU-Richtlinie 2006/24/EG über die Vorratsdatenspeicherung mit Urteil vom 8. April 2014 für ungültig erklärt.³⁴ Die Richtlinie verletze die Grundrechte der Achtung des Privat- und Familienlebens (Art. 7) und des Schutzes personenbezogener Daten (Art. 8) der Charta der Grundrechte der EU. Aus der Gesamtheit der gespeicherten Daten könnten sehr genaue Schlüsse auf das Privatleben der Personen, deren Daten auf Vorrat gespeichert werden, gezogen werden, etwa auf Gewohnheiten des täglichen Lebens, ständige oder vorübergehende Aufenthaltsorte, tägliche oder in anderem Rhythmus erfolgende Ortsveränderungen, ausgeübte Tätigkeiten, soziale Beziehungen und das soziale Umfeld. Bemängelt wurde u.a. auch der mangelhafte Schutz von Berufsgeheimnisträgern.³⁵ Auch die nationalen Verfassungsgerichte einer Reihe von EU-Staaten haben die entsprechenden Regelungen der Vorratsdatenspeicherung für grundrechtswidrig erachtet.³⁶ In Deutschland, wo das Bundesverfassungsgericht schon einmal eine gesetzliche Regelung der Vorratsdatenspeicherung kassiert hat, ist Ende 2015 ein neues Gesetz erlassen worden. Dieses enthält zwar Regelungen zur Gewährleistung des Berufsgeheimnisträgerschutzes. Die Erhebung von Verkehrsdaten, die sich gegen einen Berufsgeheimnisträger richten und die voraussichtlich Erkenntnisse erbringen würde, über die dieser das Zeugnis verweigern dürfte, wäre unzulässig. Dennoch erlangte Erkenntnisse dürften nicht verwendet werden. Dies wird jedoch von verschiedener Seite als unzureichend kritisiert.³⁷ Der Schutz des Berufsgeheimnisses dürfe nicht erst im Anschluss an die Speiche- 35

31 BGE 139 IV 98.

32 Das BÜPF trat per 1. Januar 2002 in Kraft.

33 Konkret sind die Daten nicht bei einer Fernmeldeanbieterin erhoben worden, sondern bei der Universität Zürich, da diese direkten Zugriff auf die Verbindungsdaten hatte, was rechtlich besehen keinen Unterschied machte, vgl. OGer ZH, 1.12.2015, SB150090, E. 4.3.

34 vgl. Schlauri/Ronzani, EuGH: Vorratsdatenspeicherungsrichtlinie 2006/24/EG für ungültig erklärt, in: sic! 9/2014, 570 ff.

35 <http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054de.pdf> (22.06.2016).

36 <https://de.wikipedia.org/wiki/Vorratsdatenspeicherung> (22.06.2016).

37 <https://www.reporter-ohne-grenzen.de/pressemitteilungen/meldung/vorratsdatenspeicherung-gefaehrdet-quellenschutz/> (22.06.2016).

rung, sondern müsse bereits bei der Erhebung durch technische Maßnahmen stattfinden.³⁸ Gegen das Gesetz sind mehrere Beschwerden am Bundesverfassungsgericht erhoben worden.³⁹ Dabei ist u.a. moniert worden, mit der angefochtenen Regelung würden Berufsheimnisträger in ihren Grundrechten verletzt.⁴⁰

- 36 Vergleichbare Kritik ist auch in der Schweiz erhoben worden. Verschiedene Personen, darunter Journalisten, haben vom Dienst Überwachung Post- und Fernmeldeverkehr (Dienst ÜPF) verlangt, die Vorratsdatenspeicherung zu unterlassen. Der Dienst ÜPF hat die Begehren mit Verfügung vom 30. Juni 2014 abgelehnt. Die Beschwerden gegen diese Verfügungen sind am Bundesverwaltungsgericht hängig. Die Beschwerdeführer rügen u.a., die geltende Regelung biete Journalisten keinen wirksamem Schutz ihrer Grundrechte. Die Vorratsdatenspeicherung kompromittiere den Quellenschutz. Dagegen bestünden keine wirksamen Schutzmechanismen.⁴¹

V. Fazit: Mangelhafte Umsetzung des Quellenschutzes in Gesetz und Praxis

- 37 Für den Fall, dass das Interesse des Staates, Beweismittel im Strafverfahren zu gewinnen, und der Quellenschutz miteinander kollidieren, muss der Strafprozess Prozeduren bereitstellen, die den Quellenschutz in dem Umfang gewährleisten, wie es die grundrechtlichen Prinzipien erfordern. Abgesehen von der Zeugnispflicht, der sich der Journalist einfach dadurch entziehen kann, dass er sein Zeugnisverweigerungsrecht anruft, ist es in der Praxis nicht einfach, die Macht des Staates wirksam zu begrenzen und den Quellenschutz zu wahren. In gewissen Konstellationen erlangen die Strafverfolgungsbehörden faktisch Zugriff auf Beweismittel, die dem Quellenschutz unterliegen. Die für die Wahrung des Quellenschutzes vorgesehenen Verfahren schaffen nicht durchwegs Remedur. Der Quellenschutz kann schon durchlöchert sein, bevor diese Verfahren greifen. Besonders gross ist diese Gefahr bei heimlichen Zwangsmassnahmen. Die Durchsetzung des Quellenschutzes ist zudem dadurch erschwert, dass der betroffene Journalist unter Umständen gar nicht ins Verfahren involviert wird. Schliesslich hinkt die Durchsetzung des Quellenschutzes insoweit, als dessen Anrufung durch die angeschuldigte Person oder durch den Journalisten bereits dazu führen kann, dass Informationen durchscheinen, die mit dem Quellenschutz geheim gehalten werden sollen. Dies kann insbesondere die Tatsache betreffen, dass eine Person Quelle eines Journalisten ist.
- 38 Es gibt damit Konstellationen, in denen der Quellenschutz durchbrochen wird, ohne dass zwingende, überwiegende Gründe des öffentlichen Interesses bzw. ausserordentliche Umstände vorliegen, wie dies die Rechtsprechung des Bundesgerichts und des EGMR verlangt. Eine wirksame Umsetzung der höchstrichterlichen Grundsätze setzt voraus, dass die entsprechende Interessenabwägung vorgenommen wird, bevor der Eingriff in den Quellenschutz Tatsache ist. Gesetz und Praxis vermögen dies nicht durchwegs zu gewährleisten.
- 39 Für die journalistische Tätigkeit bedeutet dies, dass man nicht unbesehen auf die grundrechtlichen Garantien vertrauen kann, sondern die begrenzte Reichweite des Quellenschutzes im Strafprozess im Auge behalten muss.

Zusammenfassung Die Bedeutung des Quellenschutzes als Grundbedingung und Eckpfeiler der Medienfreiheit ist einhellig anerkannt. Der Quellenschutz ist als Grundsatz fest in der Rechtsprechung des Bundesgerichts und der Strassburger Organe verankert. Bei der konkreten Umsetzung des Quellenschutzes im Strafprozess offenbaren sich jedoch Ungereimtheiten und Lücken, namentlich bei Beschlagnahmen und bei geheimen Überwachungsmaßnahmen. In der Praxis wird der Quellenschutz in Fällen durchbrochen, in denen dies nicht zu rechtfertigen ist. Das gesetzgeberische Konzept vermag in gewissen Konstellationen nicht zu verhindern, dass die Strafverfolgungsbehörden Kenntnis von Tatsachen erhalten, die dem Quellenschutz unterliegen.

38 <https://netzpolitik.org/2015/vorratsdatenspeicherung-und-berufsheimnistragerschutz-voellig-miteinander-unvereinbar/> (22.06.2016).

39 <http://www.spiegel.de/netzwelt/netzpolitik/vorratsdatenspeicherung-wer-klagt-vor-dem-bundesverfassungsgericht-a-1074152.html> (22.06.2016).

40 <http://www.mueller-roessner.net/antrag-auf-erlass-einer-einstweiligen-anordnung-gegen-die-wiedereinfuehrung-der-vorratsdatenspeicherung-beim-bundesverfassungsgericht-eingereicht/> (22.06.2016).

41 <https://www.digitale-gesellschaft.ch/2014/09/02/vorratsdatenspeicherung-in-der-schweiz-digitale-gesellschaft-gelangt-mit-beschwerde-an-bundesverwaltungsgericht/> (22.06.2016).