www.jusletter-it.eu

Samuel Klaus / Roland Mathys

«The Best of BÜPF» – Was ändert sich mit der Revision?

The referendum against the revised BÜPF has not been achieved. The version of the BÜPF that has been adopted by the councils will thus come into force, presumably in 2018. The article provides an overview of the changes the revision brings about – and what these changes entail practically.

Category: Articles
Region: Switzerland
Field of law: Telecommunications law

Citation: Samuel Klaus / Roland Mathys, «The Best of BÜPF» – Was ändert sich mit der Revision?, in: Jusletter IT 22 September 2016

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

Inhaltsübersicht

I. Einleitung

[Rz 1] Am 18. März 2016 wurde das revidierte BÜPF[1] von den Räten verabschiedet. Am 7. Juli 2016 lief die Frist zur Einreichung des Referendums ab,[2] ohne dass die notwendige Anzahl beglaubigter Unterschriften eingereicht wurde.[3] Das revidierte BÜPF (nachfolgend «**nBÜPF**») wird somit in absehbarer Zeit in Kraft treten: Sofern die für Frühjahr 2017 vorgesehene Vernehmlassung zu den Ausführungsbestimmungen nicht noch zu Überraschungen führt, dürfte das Gesamtpaket gemäss Behördenauskunft **per 2018** in Kraft treten.

[Rz 2] Aufgrund der kontrovers geführten Diskussion lohnt sich jedoch bereits jetzt ein kurzer Blick auf einige relevante Bestimmungen. Wir rekapitulieren dazu kurz die Entstehungsgeschichte des nBÜPF und greifen dann die am stärksten diskutierten Punkte auf – ohne Anspruch auf Vollständigkeit. Eine umfassendere Beurteilung wird erst mit Vorliegen der Ausführungsbestimmungen möglich sein.[4]

[Rz 3] Auf die aktuelle Revision des Nachrichtendienstgesetzes (NDG) gehen wir in diesem Beitrag nicht ein. Zur Abgrenzung der beiden Gesetze nur soviel: Beim NDG steht die präventive Überwachung durch den Nachrichtendienst des Bundes in verschiedensten Formen und ohne konkreten Verdacht auf eine Straftat im Zentrum. Das BÜPF hingegen dient dazu, den Strafverfolgungsbehörden im Rahmen konkreter Strafverfahren den Zugriff auf bestimmte Kommunikations- und Randdaten des Post- und Fernmeldeverkehrs zu ermöglichen.

---

1 Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs vom 6. Oktober 2000, SR 780.1.

2 BBl 2016 1991.

3 BBl 2016 6791.

4 Vgl. die generelle Verordnungskompetenz des Bundesrates gem. Art. 43 nBÜPF sowie die in einzelnen Artikeln (insb. Art. 21–23 und Art. 26–27 nBÜPF) vorgesehenen spezifischen Regelungsbereiche.

II. Entstehungsgeschichte

1. Hintergrund der Revision

[Rz 4] Das zurzeit (noch) gültige BÜPF (nachfolgend «**aBÜPF**») trat am 1. Januar 2002 in Kraft,[5] basierend auf der Botschaft vom **1. Juli 1998**.[6] Die technologische Entwicklung, insbesondere im Bereich der Mobilkommunikation, der IP-basierten Kommunikation (VoIP, Messenger, Whatsapp, etc.) sowie der Verschlüsselungstechnik führten zu einer immer grösseren Diskrepanz zwischen dem technisch Möglichen (sowohl auf Seiten der Überwachten wie der Überwacher) und dem rechtlich Geregelten. Um dem Abhilfe zu schaffen, wurde wenige Jahre nach dem Inkrafttreten des aBÜPF bereits dessen Revision ins Auge gefasst.

2. Vorgeschichte und Beratung in den Räten

[Rz 5] Im **März 2006** beauftragte der Bundesrat das UVEK und das EJPD mit der Klärung der offenen Fragen. Das EJPD erstellte dazu einen Bericht und beauftragte im **Mai 2007** das BJ mit der Ausarbeitung eines Vorentwurfs («**VE-BÜPF**») inklusive erläuterndem Bericht. Das BJ setzte im September 2008 eine breitgefächerte Expertengruppe ein. Im Mai 2010 gab der Bundesrat den VE-BÜPF und den erläuternden Bericht in die Vernehmlassung (bis August 2010). Die Stellungnahmen wurden in einem Bericht vom Mai 2011 zusammengefasst und flossen in den Entwurf («**E-BÜPF**») und die **Botschaft** vom **27. Februar 2013** ein.[7]

[Rz 6] In den Räten wurde die Vorlage im **März 2014** (**Ständerat**) und **Juni 2015** (**Nationalrat**) behandelt und bildete von Dezember 2015 bis März 2016 Gegenstand des Differenzbereinigungsverfahrens. Im **März 2016** wurde das BÜPF dann in der vorliegenden Form verabschiedet. Beide Räte änderten relevante Punkte des Entwurfs und führten zum Teil neue Bestimmungen ein. Dabei standen sie unter starker Beobachtung der Presse und Bevölkerung, sensibilisiert durch diverse aktuelle Enthüllungen und Entwicklungen in diesem heiklen Bereich (vgl. unten Ziff. II.4).

3. Vorgezogene VÜPF-Revision

[Rz 7] Mit der fortschreitenden Entwicklung der Telekommunikation, der Mobilkommunikation und des mobilen Internetzugangs entstand Klärungsbedarf, ob und in welchem Ausmass solche **neuen Kommunikationsformen** überwacht werden konnten. Fraglich war insbesondere, bezüglich welcher Kommunikationsformen eine Vorleistungspflicht der Anbieter zur Erstellung der Überwachungsbereitschaft bestand.[8]

[Rz 8] Aufgrund der Vernehmlassung zum VE-BÜPF zeichnete sich ab, dass nicht mit einer schnellen Umsetzung der Gesetzesrevision zu rechnen war. Der Bundesrat zog deshalb die **Revi-**

5 Vgl. zur Entstehungsgeschichte Thomas Hansjakob, Kommentar zum Bundesgesetz und zur Verordnung über die Überwachung des Post- und Fernmeldeverkehrs, St. Gallen 2006, S. 25 ff.

6 BBl 1998 IV 4241.

7 Vgl. zum Ganzen die Zusammenstellung in der Botschaft, BBl 2013 2683, 2690–2694.

8 Vgl. dazu Simon Schlauri, Fernmeldeüberwachung à discrétion?, in: sic! 4/2012, S. 238 ff.

sion der VÜPF[9] (und der GebV-ÜPF[10]) zeitlich vor und sah darin – in rechtsstaatlich nicht unbedenklicher Weise – erweiterte Regelungen zur Überwachung im Internet-Bereich vor.[11] Immerhin wurde die bereits im Entwurf zur revidierten VÜPF vorgesehene Ausweitung des persönlichen Geltungsbereichs von Zugangs- auch auf reine Dienste-Anbieter im Internet wieder fallengelassen – zumindest im Rahmen der zeitlich vorgezogenen VÜPF-Revision.[12] Ein zweiter Versuch, den Geltungsbereich auszuweiten, erfolgte dann – erfolgreicher – im Rahmen der BÜPF-Revision (vgl. unten Ziff. III.1).

[Rz 9] Die von der Schweiz bereits 2001 unterzeichnete **CyberCrimeConvention** (CCC)[13] trat für die Schweiz per 1. Januar 2012 in Kraft. Um den darin vorgeschriebenen **Verpflichtungen zur Echtzeitüberwachung** (Art. 20–21 CCC) gerecht zu werden, wurden in Art. 16 VÜPF (Telefon) und Art. 24a VÜPF (Internet) neue Bestimmungen zur Echtzeit-Überwachung eingeführt. Damit einher gingen neue Pflichten zur Bereitstellung entsprechender Schnittstellen gemäss Spezifikation durch den Dienst ÜPF[14] (Art. 17 Abs. 4–5 und Art. 25 Abs. 4–5 VÜPF) sowie zur Sicherstellung einer 24/7-Bereitschaft (Art. 18 Abs. 3 und Art. 26 Abs. 3 VÜPF).

[Rz 10] Es waren dann insbesondere diese **Bereitstellungspflichten**, die bei der (nunmehr im Rahmen der BÜPF-Revision beabsichtigten) Ausweitung des persönlichen Geltungsbereichs auf grossen Widerstand der Dienste-Anbieter stiessen (vgl. dazu unten Ziff. III.1). Durch die Ausweitung des persönlichen Geltungsbereichs wären nämlich auch solche reinen Dienste-Anbieter neu der kostenintensiven Bereitstellungs- und Bereitschaftspflicht unterworfen worden.

4. Externe Einflüsse und Referendum

[Rz 11] Zwischen der Botschaft (Februar 2013) und der Behandlung in den Räten (ab März 2014) sorgten ab **Juni 2013** die **Snowden-Enthüllungen** zum Überwachungseifer der amerikanischen (NSA) und britischen Abhörbehörden (GCHQ) für weltweite Schlagzeilen. Zudem erging, kurz nachdem der Ständerat als Erstrat die Vorlage im März 2014 beraten hatte, ein **Urteil des Europäischen Gerichtshofs (EuGH) zur Vorratsdatenspeicherung**. Darin erklärte der EuGH die «Vorratsdatenspeicherungs-Richtlinie»[15] als mit der Europäischen Grundrechtecharta[16] nicht vereinbar.[17] Das EuGH-Urteil erklärte zwar nicht die Vorratsdatenspeicherung per se für unzulässig, sondern stellte nur fest, dass die Richtlinie den Kriterien der Verhältnismässigkeit nicht zu genügen vermöge.[18] In der für Datenschutzaspekte mittlerweile (über)sensibilisierten

9 Verordnung über die Überwachung des Post- und Fernmeldeverkehrs vom 31. Oktober 2001, SR 780.11.

10 Verordnung über die Gebühren und Entschädigungen für die Überwachung des Post- und Fernmeldeverkehrs vom 7. April 2004, SR 780.115.1.

11 Zur Beurteilung dieser Vorgehensweise des Bundesrates aus rechtsstaatlicher Sicht vgl. Schlauri (Fn. 8).

12 Vgl. dazu Schlauri (Fn. 8), S. 241.

13 Übereinkommen über die Cyberkriminalität vom 23. November 2001, SR 0.311.43.

14 Dienst Überwachung Post- und Fernmeldeverkehr (Art. 3 nBÜPF), im Folgenden «Dienst ÜPF» oder einfach «Dienst».

15 Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG (ABl. L 105, S. 54).

16 Charta der Grundrechte der Europäischen Union (GRC), vom 18. Dezember 2000 (ABl. C 364, S. 1).

17 Verbundene Rechtssachen des EuGH C-293/12 und C-594/12 vom 8. April 2014.

18 Vgl. Rn. 45 ff. des EuGH-Urteils, insb. Rn. 65 und 69.

Öffentlichkeit wurde das EuGH-Urteil jedoch schnell mit einem generellen Verbot der Vorratsdatenspeicherung gleichgesetzt.

[Rz 12] Dies führte nicht nur zu einer starken öffentlichen Beachtung der parlamentarischen Beratungen, sondern auch zu spezifischen Vorstössen wie dem Vorschlag einer Vorschrift, dass die Speicherungspflichtigen die erfassten Daten innerhalb der Schweiz zu speichern haben (vgl. dazu unten III.4).[19]

[Rz 13] Vor diesem Hintergrund vermag es nicht zu erstaunen, dass gegen das nBÜPF das **Referendum** ergriffen wurde. Damit wäre zumindest eine «Gnadenfrist» bis zum Inkrafttreten verbunden gewesen, wenn nicht gar eine gänzliche Aufhebung. Dem vor allem von der IT-Branche und technologienahen Gruppierungen getragenen Referendumskomitee gelang es aber schlussendlich nicht, bis zum Ablauf der Referendumsfrist am **7. Juli 2016** die nötigen Unterschriften beizubringen.[20] Das nBÜPF wird somit in der von den Räten verabschiedeten Form (nach Erlass der Ausführungsbestimmungen) in absehbarer Zeit in Kraft treten.

III. Die kritischen Punkte

[Rz 14] Höchste Zeit also, sich die kritischen Punkte nochmals vor Augen zu führen und zu rekapitulieren, was in den Räten dazu diskutiert wurde – und vor allem, was letztlich jeweils entschieden wurde. Im Vordergrund sollen dabei die praktischen Aspekte der neuen gesetzlichen Regelung stehen, nicht die zugrundeliegenden Grundrechtsfragen.

1. Ausweitung des persönlichen Geltungsbereichs

[Rz 15] Im **aBÜPF** finden die Überwachungspflichten nur Anwendung auf die meldepflichtigen Post- und Fernmeldedienste-Anbieter sowie «Internet-Anbieterinnen» (Art. 1 Abs. 2 aBÜPF). Unter diesen Begriff fallen **nur Zugangs-Anbieter** («Access Provider»), nicht aber reine Dienste-Anbieter («Service Provider»).[21] Dies war zuerst umstritten,[22] wurde dann aber mit der VÜPF-Revision 2012 geklärt.[23]

[Rz 16] Um auch die Überwachung solcher Kommunikation zu ermöglichen, die über Dienste geführt wird, die von reinen Dienste-Anbietern zur Verfügung gestellt werden (d.h. solchen, die nicht zugleich auch als Zugangs-Anbieter tätig sind), sollte gemäss VE-BÜPF der Geltungsbereich auch auf Dienste-Anbieter (und weitere an der Bereitstellung der Kommunikations-Infrastruktur Beteiligte) ausgeweitet werden (Art. 2 Abs. 1 lit. b VE-BÜPF).[24] Diese Bestimmung war nicht

19 Das EuGH-Urteil beanstandete in Rn. 68 ausdrücklich, dass die Richtlinie die Anbieter und Netzbetreiber nicht verpflichte, die fraglichen Daten im Gebiet der EU zu speichern. Dadurch könne die Einhaltung der Erfordernisse des Datenschutzes nicht in dem Umfange garantiert werden, wie dies die EU-Grundrechtecharta ausdrücklich fordere.

20 Vgl. die Verfügung der Bundeskanzlei über das Nichtzustandekommen des Referendums, BBl 2016 6791.

21 Hansjakob (Fn. 5), S. 122 N 24 und S. 124 N 28.

22 Vgl. dazu Marc Wullschleger, Die Durchsetzung des Urheberrechts im Internet, in: SMI – Schriften zum Medien- und Immaterialgüterrecht Nr. 101, Bern 2015, S. 24–26 N 38–41.

23 Vgl. Art. 1 Abs. 2 lit. e VÜPF und Ziff. 1 im Anhang zum VÜPF (Begriffe und Abkürzungen).

24 Vgl. den Erläuternden Bericht zum VE-BÜPF, S. 16 f.

nur extrem weit, sondern auch äusserst unscharf formuliert.[25] Nach massiver Kritik in der Vernehmlassung[26] wurde darauf eine **weniger weitgehende und präziser differenzierte Regelung** vorgeschlagen.

[Rz 17] In Art. 2 nBÜPF wird neu unterschieden zwischen **6 Kategorien von Mitwirkungspflichtigen**, denen je unterschiedliche Pflichten auferlegt werden (Art. 19–34 nBÜPF). Die genaue Ausgestaltung der Mitwirkungspflichten wird dabei in den heiklen Bereichen mehrheitlich an den Bundesrat delegiert (Art. 22 Abs. 4, Art. 27 Abs. 3 nBÜPF). Als Mitwirkungspflichtige werden definiert:[27]

1. Anbieter von Postdiensten (**PDA**)
2. Anbieter von Fernmeldediensten (**FDA**)
3. Anbieter abgeleiteter Kommunikationsdienste (**AAK**)
4. Betreiber interner Fernmeldenetze (**BIF**)
5. Personen, die ihren Zugang Dritten zur Verfügung stellen (**PZD**)
6. Professionelle Wiederverkäufer von Zugangsmitteln (**PWV**)

[Rz 18] Bei den **PDA** und **FDA** (zu denen auch die Internet-Zugangs-Anbieter zählen) wird auf die Definitionen im PG[28] und FMG[29] abgestellt, womit diese weitgehend den bisherigen Betroffenen entsprechen.[30] Auch die **BIF** kamen in dieser Form bereits im aBÜPF vor (Art. 1 Abs. 4 aBÜPF).[31] Die **PWV** wurden neu ins Gesetz aufgenommen, um eine Lücke bei der Erfassung von Identifikationsdaten zu schliessen.[32] Diese Kategorien dürften wenig Anlass zur Diskussion geben.

[Rz 19] Die neuen Kategorien der **AAK** und **PZD** stellen dagegen echte Erweiterungen des Geltungsbereichs dar. Sie waren mit der Anlass für die hitzigen Debatten in den Räten – und die bisweilen reisserischen Schlagzeilen in der Presse. Im Folgenden sollen sie kurz definiert und die relevanten Rats-Voten dazu dargestellt werden.

1.1. Anbieter abgeleiteter Kommunikationsdienste (AAK)

[Rz 20] Unter dem Begriff der **Anbieter abgeleiteter Kommunikationsdienste** (**AAK**) werden Dienste-Anbieter verstanden, die weder FDA noch Internet-Zugangs-Anbieter sind, jedoch im Bereich des Internetverkehrs Dienste bereitstellen, die nur in Verbindung mit der Tätigkeit eines FDA (insbesondere eines Internet-Zugangs-Anbieters) angeboten werden können.[33] Als Abgrenzungskriterium dient die fernmeldetechnische Übertragung von Informationen gemäss Definition im FMG: Die von den AAK angebotenen Dienste setzen eine solche Übertragung zwar (als Basis der von den AAK angebotenen Dienste) voraus, ohne dass die AAK diese fernmeldetechnische

25 Vgl. Botschaft, BBl 2013 2683, 2705–2706.

26 Vgl. die Zusammenfassung der Ergebnisse des Vernehmlassungsentwurfs, Mai 2011, S. 14–18.

27 Hinweis: Um schwerfällige Wiederholungen zu vermeiden, haben wir jede Kategorie mit einer eingängigen Abkürzung versehen. Diese bildet sich aus den Anfangsbuchstaben der relevanten Begriffe der jeweiligen Kategorie.

28 Postgesetz vom 17. Dezember 2010, SR 783.0.

29 Fernmeldegesetz vom 30. April 1997, SR 784.10.

30 Vgl. dazu Botschaft, BBl 2013 2683, 2706–2707.

31 Vgl. dazu Botschaft, BBl 2013 2683, 2708–2709.

32 Botschaft, BBl 2013 2683, 2709.

33 Botschaft, BBl 2013 2683, 2707.

Übertragung von Informationen aber selbst vornehmen (würden sie dies, wären sie wiederum als FDA zu qualifizieren).[34]

[Rz 21] Mit dieser extrem breiten Definition werden **sämtliche Anbieter jedwelcher internetbasierten Dienste** erfasst. Als Beispiele werden in der Botschaft Dienste zur Einwegkommunikation, z.B. zum Hochladen von Dokumenten (wie GoogleDocs oder Microsoft Office Live), sowie zur Mehrwegkommunikation (wie Facebook) genannt. Ob die Kommunikation synchron oder asynchron erfolgt, ist dabei irrelevant.[35] Somit fallen auch jegliche Arten von Hosting-Providern darunter,[36] Anbieter von E-Mail-Diensten, Chat-Plattformen, Online-Koordinations-Diensten (wie z.B. Doodle) sowie Blog-Anbieter generell. Jeder Website-Betreiber, der auf seiner Website eine Gästebuch-, Kommentar- oder sonstige Kommunikations-Funktion implementiert hat, ist demnach als AAK zu qualifizieren. Denn er ermöglicht durch den Betrieb seiner Website zumindest eine asynchrone Kommunikation (z.B. vom Kommentar-Poster zum Kommentar-Leser) auf Basis fernmeldetechnisch übertragener Information.

[Rz 22] Umso wichtiger ist angesichts dieser breiten Definition die **Einschränkung der Mitwirkungspflichten der AAK**: Sie sind nur zur **Duldung** der Überwachung der Kommunikation verpflichtet, die über die von ihr angebotenen Dienste erfolgt (Art. 27 Abs. 1 nBÜPF), sowie zur Lieferung der **Randdaten**, sofern und soweit ihnen diese zur Verfügung stehen (Art. 27 Abs. 2 nBÜPF). Auch hinsichtlich der **Identifikationsdaten** müssen sie nur die ihnen vorliegenden Angaben liefern (Art. 22 Abs. 3 nBÜPF). Eine aktive Überwachungspflicht oder eine Pflicht zur Erhebung und Speicherung der Randdaten oder Identifikationsdaten trifft sie grundsätzlich nicht. Der Bundesrat kann aber, «soweit für die Überwachung des Fernmeldeverkehrs notwendig», solche AAK denselben Pflichten wie die FDA unterstellen, die «**Dienstleistungen von grosser wirtschaftlicher Bedeutung oder für eine grosse Benutzerschaft anbieten**» (Art. 27 Abs. 3 nBÜPF). AAK, die diese Voraussetzungen erfüllen, können ebenfalls zur Erhebung der Identifikationsdaten nach Art. 22 Abs. 2 nBÜPF verpflichtet werden (Art. 22 Abs. 4 nBÜPF). Ob bzw. für welche Dienste-Anbieter sich nun die im Vorfeld der Revision geäusserten Befürchtungen allenfalls doch bewahrheiten, wird sich somit erst anhand der aktuell noch nicht öffentlich einsehbaren Ausführungsbestimmungen zeigen.

1.2. Personen, die ihren Zugang Dritten zur Verfügung stellen (PZD)

[Rz 23] Unter den Begriff der **Personen, die ihren Zugang Dritten zur Verfügung stellen** (**PZD**) fallen sämtliche (natürlichen wie juristischen) Personen, die ihren Internetzugang (egal über welche Technologie oder welches Medium) Dritten zugänglich machen.[37] Darunter fallen z.B. Geschäfte, die ihrer Kundschaft instore WLAN zugänglich machen, Spitäler und Schulen, die ihren Patienten bzw. Schülern/Studenten den Internetzugriff ermöglichen, jedoch auch Privatpersonen, die ihren privaten WLAN-Zugang ihren Gästen (oder dem Nachbarn) zur Verfügung stellen, oder diesen – allenfalls auch unbeabsichtigt – nicht vor fremdem Zugriff schützen und so dessen (Mit-

34 Botschaft, BBl 2013 2683, 2707–2708.

35 Botschaft, BBl 2013 2683, 2708.

36 Worunter sowohl die Botschaft (BBl 2013 2683, 2708) wie auch der Ständerat (Votum Graber, AB 2014 S 115) auch Datacenterbetreiber und Housing-Anbieter («server colocation», «server housing») zu verstehen scheinen, zumindest sofern auf die entsprechenden Server von extern zugegriffen werden kann (vgl. die Formulierung in der Botschaft «mit Zugriff», BBl 2013 2683, 2708).

37 Botschaft, BBl 2013 2683, 2709.

)Nutzung durch irgendwelche Dritte ermöglichen. Nicht angenommen wurde der im Ständerat vorgebrachte Vorschlag, den Begriff der PZD zu beschränken auf die Zurverfügungstellung des Zugangs «im Rahmen einer wirtschaftlichen Tätigkeit».[38]

[Rz 24] Auch hier gilt, wie bei den AAK, dass die **PZD** nur zur **Duldung** der Überwachung verpflichtet sind (Art. 29 Abs. 1 nBÜPF), sowie zur Lieferung der **Randdaten**, sofern und soweit ihnen diese zur Verfügung stehen (Art. 29 Abs. 2 nBÜPF), z.B. in Form der Log-Dateien ihres WLAN-Access-Points. Die Lieferung allfälliger zusätzlicher Identifikationsdaten i.S.v. Art. 22 nBÜPF hingegen ist nicht vorgesehen (soweit solche Daten nicht bereits als Randdaten i.S.v Art. 29 Abs. 2 nBÜPF qualifizieren), da solche (zusätzlichen) Identifikationsdaten den PZD regelmässig nicht vorliegen. Festzuhalten ist, dass die PZD **keine aktive** Überwachungspflicht oder Pflicht zur Erhebung und Speicherung von Randdaten (oder Identifikationsdaten) trifft. Im Gegensatz zu den AAK ist bei den PZD auch nicht vorgesehen, dass sie der Bundesrat allenfalls doch noch solchen Pflichten unterstellen könnte. Zumindest die Hotels, Restaurant, Cafés und Privaten, die ihren Netzzugang Dritten zur Verfügung stellen, können in dieser Hinsicht aufatmen. Ihre allfällige Mitwirkungspflicht erschöpft sich in der Duldung und der Lieferung der vorhandenen Randdaten – und geht somit nicht weiter als die allgemeine Mitwirkungspflicht gemäss StPO.[39]

2. Vorab-Information über neue Dienstleistungen

[Rz 25] Eine Neuerung stellt die in Art. 25 nBÜPF vorgesehene **Pflicht zur Vorab-Information** dar. Dort ist vorgesehen, dass FDA den Dienst ÜPF auf dessen Verlangen jederzeit ausführlich über Art und Merkmale nicht nur derjenigen Dienstleistungen informieren, die sie bereits auf den Markt gebracht haben, sondern auch über solche, die sie innerhalb von 6 Monaten auf den Markt bringen wollen. Damit soll dem Dienst ÜPF ermöglicht werden, Schwierigkeiten vorauszusehen, die sich bei künftigen Überwachungen der neuen Dienste ergeben könnten, und proaktiv – statt rein reaktiv – darauf zu reagieren.[40] Vereinzelt wurde die Befürchtung geäussert, dass diese Bestimmung es insbesondere Tech-Startups erschweren könnte, neue Produkte mit Kommunikationsfähigkeit auf den Markt zu bringen.[41] Bei genauerer Betrachtung erhellt, dass diese Befürchtung wohl noch auf dem viel zu weitgehend formulierten Art. 25 VE-BÜPF basierte, der sämtliche «Überwachungspflichtigen» erfasste, deren Kreis im VE-BÜPF viel weiter gefasst war als im jetzigen nBÜPF.[42]

[Rz 26] In Art. 25 nBÜPF wurde die Informationspflicht auf die **FDA** beschränkt und auf die bereits im Markt eingeführten sowie in den nächsten 6 Monaten einzuführenden Dienstleistungen limitiert. Gemäss der Botschaft müssen die FDA dem Dienst ÜPF auf Verlangen genau darlegen, um welche Dienstleistungen es sich handelt und worin diese bestehen, d.h. wozu sie die-

38 AB 2013 S 109–110.

39 Votum Sommaruga, AB 2013 S 110.

40 Botschaft, BBl 2013 2683, 2737.

41 Vgl. z.B. Stellungnahme der SWICO zum BÜPF-Referendum (18. März 2016), S. 1; http://www.swico.ch/downloads/dokumente/stellungnahme-von-swico-zum-buepf-referendumpdf/3329 (alle Websites zuletzt besucht am 21. August 2016).

42 Vgl. VE-BÜPF 2, insb. 2.1.b.

nen – nicht aber welche Merkmale der Technologie der neuen Dienstleistung zugrundeliegen.[43] Festzuhalten ist zudem, dass **keine aktive Informationspflicht** besteht, sondern der Dienst ÜPF **nur auf dessen Verlangen zu informieren ist**, und dass allfällige Geschäftsgeheimnisse, die dem Dienst ÜPF im Rahmen der Vorab-Information mitgeteilt werden, dem **Amtsgeheimnis** unterstehen (Art. 320 StGB).[44]

[Rz 27] Auch bleiben die FDA frei, die neuen Dienstleistungen gemäss ihren Plänen im Markt einzuführen bzw. die **Pläne zur Markteinführung allenfalls zu ändern** (d.h. gegebenenfalls auch vorzuziehen).[45] Es wird also nicht etwa eine «Zwangspause» für die Einführung neuer Dienstleistungen verordnet oder die Einführung von einer Freigabe durch den Dienst ÜPF abhängig gemacht. Vor diesem Hintergrund ist nicht nachzuvollziehen, wie Art. 25 nBÜPF zum «Innovationskiller» oder zur «Startup-Bremse» werden soll, wie dies bisweilen in der Branche und der Presse kolportiert wurde.[46] Relevant werden könnte in diesem Zusammenhang hingegen die Abgrenzung zwischen FDA (die Art. 25 nBÜPF unterstehen) und AAK, welche Art. 25 nBÜPF nicht unterstehen (vgl. dazu oben Ziff. III.1.1).

3. Schnittstelle für Echtzeit-Zugriff

[Rz 28] Bereits per Januar 2012 wurde – in Umsetzung der Verpflichtungen aus der CCC – die VÜPF revidiert, um breitere Überwachungsmassnahmen im Internet-Bereich zu ermöglichen (vgl. dazu oben Ziff. II.3).[47] Dies brachte für die FDA die **Pflicht zur Bereitstellung einer Schnittstelle zur Echtzeit-Überwachung** mit sich. An dieser Pflicht ändert sich mit dem nBÜPF nichts.

[Rz 29] Hingegen war im VE-BÜPF vorgesehen, die Überwachungspflichten undifferenziert auch auf reine Dienste-Anbieter auszuweiten, die damit ebenfalls zur Sicherstellung des Echtzeit-Zugriffs verpflichtet gewesen wären (Art. 2 Abs. 1 lit. b i.V.m. Art. 21 Abs. 2–3 VE-BÜPF).[48] Dadurch hätten diese die notwendige Infrastruktur bereitstellen und ihre Dienste mit einer Schnittstelle für den Echtzeit-Zugriff nachrüsten müssen. Insbesondere kleinere und mittlere Dienstanbieter hätten dadurch sozusagen «auf Vorrat» massgebliche Investitionen tätigen müssen zur Ermöglichung einer Überwachung, von welcher sie aufgrund ihres kleinen Kundenkreises wohl nur in Ausnahmefällen je betroffen gewesen wären.

[Rz 30] Aufgrund der heftigen Reaktionen in der Vernehmlassung[49] wurde bereits im E-BÜPF einerseits der persönliche Geltungsbereich präziser definiert und nach verschiedenen Arten von Anbietern differenziert (vgl. oben Ziff. III.1). Andererseits wurden die Überwachungspflichten ebenfalls nach Art der Anbieter differenziert und dabei zwischen FDA und AAK unterschieden.

[Rz 31] Dadurch sind im nBÜPF nur noch die **FDA** (nicht aber die AAK) standardmässig zur Ermöglichung der Echtzeit-Überwachung über die definierten Schnittstellen verpflichtet (Art. 26 Abs. 1 lit. a i.V.m. Abs. 4 und Art. 31 Abs. 3 nBÜPF). Hingegen können **AAK** mittels Verordnung

43 Botschaft, BBl 2013 2683, 2737.

44 Botschaft, BBl 2013 2683, 2738.

45 Botschaft, BBl 2013 2683, 2738.

46 Vgl. z.B. NZZ am Sonntag vom 12. Juni 2016, S. 30.

47 Vgl. die Erläuterungen des ISC-EJP ÜPF zur Änderung der VÜPF vom 26. Oktober 2011, http://www.ejpd.admin.ch/dam/data/ejpd/aktuell/news/2011/2011-11-23/vn-ber-d.pdf.

48 Vgl. VE-BÜPF 2.1.b und den Erläuternden Bericht zum VE-BÜPF, S. 17.

49 Vgl. die Zusammenfassung der Ergebnisse des Vernehmlassungsentwurfs, Mai 2011, S. 14–18.

ebenfalls dieser Pflicht unterstellt werden (Art. 27 Abs. 3 nBÜPF), soweit dies der Bundesrat als «für die Überwachung des Fernmeldeverkehrs notwendig» erachtet. Ob und gegebenenfalls wie dies in den Ausführungsbestimmungen der Fall sein wird, lässt sich zurzeit noch nicht abschätzen. Umgekehrt können gewisse FDA von bestimmten Pflichten befreit werden, «wenn sie Dienstleistungen von geringer wirtschaftlicher Bedeutung oder im Bildungsbereich anbieten» (Art. 26 Abs. 6 nBÜPF). Auch hier wird abzuwarten sein, in welchem Umfang, aufgrund welcher Kriterien und hinsichtlich welcher FDA und Pflichten dies allenfalls der Fall sein wird.

4. Ort der Datenspeicherung

[Rz 32] Das aBÜPF äussert sich nicht zum **Ort der Datenspeicherung** – was auch im nBÜPF so bleiben wird. Die Frage, wo die von den FDA erhobenen Randdaten zu speichern sind, ist vor dem Hintergrund des **EuGH-Urteils zur Vorratsdatenspeicherung** zu sehen.[50] Dieses hielt im April 2014 fest, dass Art. 8 Abs. 3 GRC ausdrücklich fordert, dass die Einhaltung der Datenschutzvorgaben «durch eine unabhängige Stelle überwacht» werde, was nicht gewährleistet werden könne, wenn die fraglichen Daten nicht auf Unionsgebiet gespeichert würden.[51]

[Rz 33] Obwohl das EuGH-Urteil für die Schweiz keine direkte Wirkung hat, wurde dieser Gedanke auch in der Schweiz aufgenommen. So beantragte eine Minderheit im Nationalrat, dass die von den Anbietern erhobenen Randdaten nur in der Schweiz aufbewahrt werden dürfen.[52] Während die Bestimmung beim Postverkehr abgelehnt wurde,[53] fand sie bezüglich des Fernmeldeverkehrs im Nationalrat eine Mehrheit.[54] Im Ständerat wurde dies hingegen abgelehnt,[55] unter Hinweis darauf, dass zum einen die in der Schweiz aktiven Anbieter das DSG[56] in jedem Fall einzuhalten hätten und zum anderen, dass eine solche Norm im BÜPF verfehlt wäre.[57] Wenn schon wäre eine solche Pflicht zur Speicherung bestimmter Daten im DSG oder allenfalls im FMG zu regeln.[58] Zudem könnte sich eine derartige Pflicht negativ auf die FDA auswirken, denen es dann z.B. nicht mehr erlaubt wäre, die Aufbereitung der Daten für die Rechnungsstellung im Ausland vorzunehmen, da hierfür auch die Randdaten nötig sind.[59]

[Rz 34] Nach längerem Hin und Her zwischen den Räten[60] ging dieser Punkt in die Einigungskonferenz. Dort wurde schliesslich entschieden, den vorgeschlagenen Abs. 5^{bis} zu Art. 26 endgültig zu streichen.[61] Damit enthält das nBÜPF nunmehr **keine Vorschriften zum Ort der Datenspeicherung**, d.h. dazu, wo die von den FDA erhobenen Randdaten zu speichern sind. Dies bleibt

50 Urteil des EuGH (Fn. 17).

51 Rn. 68 des Urteils des EuGH (Fn. 17).

52 AB 2015 N 1163 (Postverkehr, Art. 19 Abs. 4^{bis} E-BÜPF), 1164 (Fernmeldeverkehr, Art. 26 Abs. 5^{bis} E-BÜPF).

53 AB 2015 N 1164.

54 AB 2015 N 1165.

55 AB 2015 S 1198.

56 Bundesgesetz über den Datenschutz vom 19. Juni 1992, SR 235.1.

57 Votum Engler, AB 2015 S 1197, vgl. dazu auch Votum Vogler, AB 2016 N 136 und Votum Sommaruga, AB 2016 N 138.

58 Votum Engler, AB 2015 S 1197.

59 Votum Sommaruga, AB 2015 S 1197.

60 AB 2016 N 139 (3. März 2016), AB 2016 S 120 (8. März 2016), AB 2016 S 356 (14. März 2016).

61 AB 2016 S 209 (16. März 2016) und AB 2016 N 452 (16. März 2016).

– wie bis anhin – der Entscheidung der FDA überlassen. Dabei müssen die Vorgaben des DSG beachtet werden. Es bleibt abzuwarten, ob der Vorschlag, für gewisse Daten den Speicherort vorzuschreiben, allenfalls im Rahmen der DSG-Revision aufgenommen wird.[62]

5. Dauer der Datenspeicherung

[Rz 35] Im aBÜPF ist eine Frist zur Speicherung der Randdaten von 6 Monaten vorgesehen, sowohl beim Post- wie Fernmeldeverkehr.[63] Der Bundesrat schlug im VE-BÜPF vor, die Frist auf 12 Monate auszudehnen.[64] Diese Frist von 12 Monaten fand auch in den E-BÜPF Eingang.[65]

[Rz 36] In der Beratung dazu wurden im Stände- und Nationalrat verschiedene Varianten diskutiert, z.T. auch mit unterschiedlichen Fristen für den Post-/Fernmeldeverkehr.[66] Der Ständerat glich die beiden Bestimmungen schliesslich bei 6 Monaten an.[67] Im Rahmen des Differenzbereinigungsverfahrens schwenkte der Nationalrat auf die für beide Bestimmungen vereinheitlichten 6 Monate des Ständerates ein,[68] wenn auch mehr aus praktischen Gründen denn aus innerer Überzeugung.[69]

[Rz 37] Bei der **Aufbewahrungsfrist für Randdaten** bleibt somit alles beim Alten – auch das nBÜPF sieht dafür eine Dauer von **6 Monaten** vor (Art. 19 Abs. 4 nBÜPF für Postverkehr und Art. 26 Abs. 5 nBÜPF für Fernmeldeverkehr).

[Rz 38] Eine Änderung ergibt sich hingegen bezüglich der **Identifikationsdaten**, die im aBÜPF zusammen mit den Randdaten in Art. 12 Abs. 2 aBÜPF (Postverkehr) und Art. 15 Abs. 3 aBÜPF (Fernmeldeverkehr) geregelt sind. Im nBÜPF sind sie für den Postverkehr nicht mehr speziell geregelt, für den Fernmeldeverkehr finden sich hingegen ausdrückliche Regelungen in Art. 21 nBÜPF (Auskünfte über Fernmeldedienste) und Art. 22 nBÜPF (Auskünfte zur Identifikation der Täterschaft bei Straftaten über das Internet). Unter beiden Artikeln bestimmt der Bundesrat, welche Daten hierunter fallen (Art. 21 Abs. 1 lit. d und Art. 22 Abs. 2 nBÜPF). Diese sind **sowohl während der Dauer der Kundenbeziehung** wie auch **während 6 Monaten nach deren Beendigung** aufzubewahren, wobei der Bundesrat für gewisse Daten vorsehen kann, dass diese nicht während der ganzen Dauer der Kundenbeziehung, sondern nur während 6 Monaten (ab Erfassung/Anfall der Daten z.B. im Rahmen der Zuteilung dynamischer IP-Adressen) aufzubewahren sind (Art. 21 Abs. 2 und Art. 22 Abs. 2 nBÜPF). Unter die Identifikationsdaten nach Art. 21 nBÜPF fallen insbesondere auch Angaben zu Prepaid-SIM-Karten (und neu auch zu Prepaid-Wireless-Karten), unter diejenigen nach Art. 22 nBÜPF insebesondere auch solche Daten, die eine Zuordnung der IP-Adressen zu einzelnen Kunden (bzw. deren Anschlüssen) erlauben.[70]

---

62 Vgl. dazu https://www.edoeb.admin.ch/datenschutz/00628/00784/index.html?lang=de. Der per Ende August 2016 erwartete Vorentwurf zum revidierten DSG war im Zeitpunkt der Verfassung dieses Artikels noch nicht verfügbar.

63 Art. 12 Abs. 2 aBÜPF für Postverkehr, Art. 15 Abs. 3 aBÜPF für Fernmeldeverkehr.

64 Art. 19 Abs. 2 VE-BÜPF für Postverkehr, Art. 23 VE-BÜPF für Fernmeldeverkehr.

65 Art. 19 Abs. 4 E-BÜPF für Postverkehr, Art. 26 Abs. 5 E-BÜPF für Fernmeldeverkehr.

66 AB 2014 S 115–116, AB 2014 S 111–113, AB 2015 N 1163–1164 (Postverkehr), AB 2015 N 1164–1165 (Fernmeldeverkehr).

67 AB 2015 S 1193–1195 (Postverkehr), AB 2015 S 1196–1198 (Fernmeldeverkehr).

68 AB 2016 N 131–136 (Post- und Fernmeldeverkehr).

69 Vgl. dazu das Votum Sommaruga, AB 2016 N 134–135.

70 Botschaft, BBl 2013 2683, 2732–2733, 2736.

[Rz 39] Im Zusammenhang mit der Dauer der Datenspeicherung im Bereich des Internets ist zudem Art. 22 Abs. 2 nBÜPF, letzter Satz bemerkenswert, gemäss dem die FDA dem Dienst ÜPF **weitergehende Angaben** liefern müssen, über die sie verfügen. Eine Löschungspflicht nach Ablauf der 6-monatigen Aufbewahrungspflicht ist nicht vorgesehen. Sofern also ein FDA gewisse Daten – allenfalls mit Zustimmung der betroffenen Kunden – länger als die vorgeschriebenen 6 Monate aufbewahrt, müssen diese ebenfalls geliefert werden. Aufgrund der gesetzlichen Aufbewahrungspflicht müssen die Anbieter die für die Rechnungslegung relevanten Buchungsbelege aufbewahren, womit zumindest gewisse Randdaten während rund 10 Jahren greifbar sind.[71] Und angesichts der Tatsache, dass sich die FDA aufgrund des zunehmenden wirtschaftlichen Wertes von nutzerbezogenen Daten von ihren Kunden immer weiter reichende Befugnisse zur Datenerhebung und -speicherung einräumen lassen, scheint die Diskussion, ob gewisse Daten nunmehr 6 oder 12 Monate lang gespeichert werden sollen, in diesem Bereich je länger je hinfälliger zu werden: Daten, die beim FDA vorhanden sind, und die unter Art. 22 nBÜPF die Identifikation der Täterschaft einer über das Internet begangenen Straftat ermöglichen können, sind nämlich dem Dienst ÜPF **unabhängig von der Aufbewahrungsfrist** nach nBÜPF zu liefern und zwar **soweit zurück, wie sie beim FDA vorliegen**.[72] Da es sich dabei nicht um eine «Überwachung» i.S. des BÜPF handelt, ist die Straftat, deren Aufklärung Anlass zur Auskunftsanfrage gibt, auch nicht an den Katalog von Art. 269 Abs. 2 StPO gebunden.[73]

6. Kostentragung und Entschädigung

[Rz 40] Das aBÜPF sieht vor, dass die **Kosten** für die notwendigen **Einrichtungen** zu Lasten der Anbieter gehen, diese jedoch für die Kosten der einzelnen **Überwachung** eine «angemessene Entschädigung» erhalten (Art. 16 Abs. 1 aBÜPF). Diese wird in der GebV-ÜPF geregelt.[74] Im Vorentwurf war vorgesehen, diese Entschädigung ersatzlos zu streichen (Art. 30 VE-BÜPF).[75] Aufgrund der negativen Reaktionen in der Vernehmlassung, die – wenig erstaunlich – insbesondere aus der Telekombranche verlautete, kam der Bundesrat darauf zurück und schlug im Entwurf vor, doch die bisherige Regelung beizubehalten (Art. 38 E-BÜPF).[76] Dabei stützte er sich auf eine Erhebung von Juni 2012.[77]

[Rz 41] Während schnell klar war, dass die **Investitionskosten** weiterhin von den Anbietern getragen werden müssen, bestand im Ständerat (als Erstrat) grosse Meinungsverschiedenheit zur Entschädigung für die einzelnen Überwachungen. Die Anträge reichten von einer *kostendecken-*

71 Art. 957a Abs. 3 i.V.m. Art. 958f OR.

72 Vgl. dazu BGE 139 IV 98, gemäss dem Art. 14 Abs. 4 aBÜPF (alle vorhandenen Angaben sind zu liefern) als lex specialis Art. 273 Abs. 3 StPO (nur bis 6 Monate rückwirkend) vorgeht. Dasselbe wird für Art. 22 nBÜPF gelten.

73 Botschaft, BBl 2013 2683, 2733; Hansjakob (Fn. 5), Art. 14 N 23.

74 Diese sieht z.B. für Identifikationsinformationen eine Entschädigung von CHF 4. – vor, für eine Randdaten-Auskunft CHF 540.– sowie für eine Echtzeit-Überwachung CHF 1'330. –.

75 Vgl. den Erläuternden Bericht zum VE-BÜPF, S. 37 f. sowie die Botschaft, BBl 2013 2683, 2758.

76 Botschaft, BBl 2013 2683, 2758.

77 Bericht «Erhebung und Analyse der Kosten der Post- und Fernmeldeüberwachung» der KPMG im Auftrag des Informatik Service Center ISC-EJPD, Leiter Dienst ÜPF, vom 12. Juni 2012: https://www.bj.admin.ch/dam/data/bj/sicherheit/gesetzgebung/fernmeldeueberwachung/ber-isc-ejpd-fda-pda-d.pdf.

den[78] über zumindest eine *angemessene* Entschädigung für die Überwachung[79] bis zu *gar keiner* Entschädigung irgendwelcher Art.[80] Zudem lässt sich den Protokollen eine gewisse Konsternation entnehmen, dass die Anbieter anscheinend nicht bereit waren, Auskunft über die tatsächlich anfallenden Kosten zu geben.[81] Schliesslich wurde der Status Quo beibehalten, nicht zuletzt aufgrund einer gewissen Angst vor der möglichen Verweigerungshaltung der FDA, welche die Umsetzung des BÜPF massgeblich erschweren würde.[82] Der Nationalrat folgte darin dem Ständerat.

[Rz 42] Damit entspricht Art. 38 nBÜPF grundsätzlich der **bisherigen Regelung**, d.h. die Anbieter haben weiterhin vollumfänglich für die Kosten der notwendigen Einrichtungen (Fixkosten) aufzukommen, erhalten aber eine **angemessene Entschädigung für individuelle Überwachungen**. Ob die (erst per 2012 revidierte) GebV-ÜPF im Rahmen der Ausarbeitung der Ausführungsbestimmungen zum nBÜPF ebenfalls überarbeitet wird, bleibt abzuwarten.

[Rz 43] Im Vorfeld wurde insbesondere im Rahmen der Revision der VÜPF per 1. Januar 2012 seitens der Telekom-Verbände die Befürchtung geäussert, dass durch eine Ausweitung der zulässigen Überwachungsmöglichkeiten die Kosten gerade für **kleinere und mittlere Telekom-Anbieter** übermässig steigen. Sie müssten nämlich durch Bereitstellen der technischen Infrastruktur die kostenintensive Überwachungsbereitschaft für die standardisierten Überwachungen gewährleisten.[83] Diesen Bedenken versuchte der Bundesrat Rechnung zu tragen, indem in Art. 26 Abs. 6 nBÜPF nun vorgesehen wurde, dass der Bundesrat **kleinere FDA von bestimmten gesetzlichen Pflichten befreien kann**, insb. wenn sie Dienstleistungen «von geringer wirtschaftlicher Bedeutung oder im Bildungsbereich» anbieten. Die genaue Umsetzung dieser Ausnahmebestimmung wird sich erst den Ausführungsbestimmungen entnehmen lassen. In der Botschaft wurde dazu vermerkt, dass durch diese Befreiungsmöglichkeit eine Annäherung an die heutige Situation beabsichtigt sei.[84]

7. Staatstrojaner und IMSI-Catcher

[Rz 44] Unter dem aBÜPF war bereits während einiger Zeit die Zulässigkeit des Einsatzes neuer Überwachungstechnologien umstritten.[85] Um hier Klarheit zu schaffen, sollte im Rahmen der BÜPF-Revision mittels neuer Artikel in der StPO die **gesetzliche Grundlage** geschaffen werden für den Einsatz von **IMSI-Catchern** (Art. 269bis nStPO) und **Staatstrojanern** (Art. 269ternStPO), in der Botschaft euphemistisch als «GovWare» (für «Government Software») bezeichnet. Beides gab im Vorfeld sowie während der parlamentarischen Beratung stark zu reden. Besonderes Augenmerk lag dabei auf dem Staatstrojaner, aufgrund der Sensibilisierung der Öffentlichkeit durch diverse Enthüllungen der letzten Jahre:

---

78 Antrag Graber, AB 2014 S 118 (kostendeckende Entschädigung für die Überwachungen), vgl. Votum Graber, AB 2014 S 120.

79 Bundesrat in Art. 38 E-BÜPF und in der Botschaft, BBl 2013 2683, 2757–2760 (angemessene Entschädigung für Überwachungen).

80 Kommissionsantrag, AB 2014 S 118 (keine Entschädigung für die Überwachungen).

81 Votum Savary, AB 2014 S 104, 119.

82 Votum Schmid, AB 2014 S 119.

83 Vgl. dazu insb. Schlauri (Fn. 8), 238.

84 Botschaft, BBl 2013 2683, 2742.

85 Vgl. z.B. Ciril Riss/Nicole Beranek Zanon, Art. 280 StPO genügt nicht als gesetzliche Grundlage für den Einsatz von Staatstrojanern, in: Jusletter 9. Juli 2012.

- Bereits im **Januar 2009** wurde in Deutschland eine **Verfassungsbeschwerde** eingereicht gegen (unter anderem) die Bestimmungen des BKAG,[86] welche die Grundlage für den deutschen «Bundestrojaner» bilden.[87]
- Im **Oktober 2011** analysierte der deutsche Chaos Computer Club den vom BKA entwickelten deutschen «**Bundestrojaner**» eingehend und legte dessen Funktionsweise – und insbesondere sicherheitstechnischen Schwachstellen – offen.[88] Im **Dezember 2012** liess das BKA dann verlauten, dass eine verbesserte Version bis Ende 2014 vorliege.[89]
- Im **April 2016** – d.h. erst nach Abschluss der Beratungen zum BÜPF – erging dann das Urteil des deutschen Bundesverfassungsgerichts,[90] welches das BKAG zumindest teilweise für verfassungswidrig erklärte.[91] Darin wurden jedoch Staatstrojaner nicht etwa per se als unzulässig qualifiziert, sondern es wurden nur die bei deren Einsatz zu beachtenden rechtlichen Grundlagen und Voraussetzungen präzisiert.[92]
- Im **Juli 2015**, also kurz nach Abschluss der ersten Runde des E-BÜPF in den Räten, wurde ein italienischer Hersteller von Überwachungssoftware, namens «**Hacking Team**», selbst gehackt und es wurde u.a. dessen interne Kommunikation veröffentlicht.[93] Dadurch wurde bekannt, dass die **Kantonspolizei Zürich** bei diesem Anbieter bereits im **November 2014** entsprechende Überwachungssoftware bezogen hatte.[94] Dies hatte nicht nur politische Folgen,[95] sondern führte auch zu verstärkter Aufmerksamkeit für diesen speziellen Aspekt der BÜPF-Revision.

[Rz 45] Diese Entwicklungen führten in den Räten zu einigen Diskussionen, jedoch zu wenig konkreten Änderungen. Zumindest wurde bei beiden Artikeln in einem zusätzlichen Absatz ergänzt, dass die Staatsanwaltschaft eine Statistik über die Überwachungen zu führen hat (Art. 269bis Abs. 2 und Art. 269ter Abs. 4 nStPO). Damit soll die Kontrolle ermöglicht werden, ob sich der Einsatz solcher Überwachungstechnologie überhaupt lohnt und ob sich somit die damit verbundenen Grundrechtseingriffe rechtfertigen lassen.[96]

---

86 Deutsches Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (Bundeskriminalamtgesetz / BKAG).

87 http://www.heise.de/newsticker/meldung/Verfassungsbeschwerde-gegen-BKA-Gesetz-laeuft-202626.html und http://www.heise.de/newsticker/meldung/Bundesverfassungsgericht-entscheidet-ueber-die-Online-Durchsuchung-und-Bundestrojaner-2737283.html.

88 Vgl. http://www.heise.de/newsticker/meldung/CCC-knackt-Staatstrojaner-1357670.html sowie insb. http://www.ccc.de/de/updates/2011/staatstrojaner.

89 Vgl. http://www.heise.de/newsticker/meldung/Bundesregierung-Eigener-Trojaner-erst-Ende-2014-1765644.html.

90 Urteil des Deutschen Bundesverfassungsgerichts 1 BvR 966/09 und 1 BvR 1140/09 vom 20. April 2016.

91 Vgl. dazu http://www.heise.de/newsticker/meldung/Bundesverfassungsgericht-BKA-Gesetz-im-Grundsatz-rechtens-aber-teilweise-verfassungswidrig-3178248.html.

92 Vgl. http://www.heise.de/newsticker/meldung/Analyse-des-Urteils-zum-BKA-Gesetz-Karlsruhe-am-Limit-3192480.html.

93 Vgl. dazu z.B. den Halbjahresbericht der Melde- und Analysestelle Informationssicherung MELANI für 2015/II vom 28. April 2016, S. 29 f.

94 http://www.kapo.zh.ch/internet/sicherheitsdirektion/kapo/de/aktuell/medienmitteilungen/2015_07/1507071c.html.

95 Vgl. dazu die Chronologie in der NZZ online unter www.nzz.ch/zuerich/aktuell/ld.84486 bzw. http://ia.nzz.at/timeline/index.php/1wQLizMF8sSZbS0LehNlvFpCxudEJcTGUMFIutjy4sF4 sowie den Bericht der Geschäftsprüfungskommission über die Beschaffung und den Einsatz von Government Software im Kanton Zürich vom 19. Mai 2016, online unter http://www.kantonsrat.zh.ch/Dokumente/D62a80606-fa25-4563-9c11-66f248f43363/Bericht_166_2016.pdf.

96 AB 2014 S 299–301; Votum Leutenegger Oberholzer, AB 2015 N 1168.

[Rz 46] Diesbezüglich wurde in den Räten auch mehrmals explizit festgehalten, dass mittels Einsatz von Staatstrojanern (bzw. «GovWare») **nur die Echtzeitüberwachung der Kommunikationsvorgänge** (akustisch wie optisch) über das Internet zulässig sein soll (wie z.B. VoIP-Telefonie oder Skype-VideoCalls), v.a. wenn diese in verschlüsselter Form erfolgt.[97] Insbesondere ausgeschlossen wurde die – technisch ohne weiteres mögliche – **Online-Durchsuchung** (durch Abgreifen anderer Daten als der reinen Inhalts- und Randdaten der vom infizierten Gerät aus geführten Kommunikation) sowie die **Fernüberwachung** (durch Remote-Aktivierung des Mikrofons oder der Kamera des infizierten Gerätes) oder die **Änderung von Daten**, die auf dem infizierten Gerät gespeichert sind.[98] Jegliche Daten, die über das in Art. 269ter nStPO explizit Erlaubte hinaus gesammelt würden, wären gemäss Art. 269ter Abs. 3 nStPO zu vernichten und Erkenntnisse aus diesen Daten wären nicht verwertbar.[99]

[Rz 47] Um die Verwertbarkeit der mittels einem Staatstrojaner abgegriffenen Kommunikationsdaten sicherzustellen, wurden vom Nationalrat in **Art. 269^{quater} nStPO** als **zusätzliche Anforderungen** an den Staatstrojaner definiert, dass die Überwachung lückenlos und unveränderbar zu **protokollieren** ist und dass dieses Protokoll in den Verfahrensakten aufzubewahren ist (Abs. 1), dass die Übermittlung der abgegriffenen Daten bis zur zuständigen Strafverfolgungsbehörde gesichert, also **verschlüsselt**, erfolgen muss (Abs. 2), und dass eine Möglichkeit zur Verifikation des **Quellcodes** sicherzustellen ist, damit geprüft werden kann, ob der Staatstrojaner nur über die gesetzlich zulässigen Funktionen verfügt (Abs. 3).[100]

[Rz 48] Im Nationalrat wurde weiter vorgeschlagen, dass die Entwicklung oder Beschaffung der einzusetzenden Staatstrojaner zentral über den Bund erfolgen solle und dass die Staatsanwaltschaft nur diese zentral entwickelten bzw. beschafften Staatstrojaner einsetzen dürfe.[101] Dies wurde vom Ständerat jedoch abgelehnt,[102] da eine solche Vorgabe als zu starker Eingriff in die Hoheit der Kantone empfunden wurde und für den Bund Haftungs- und Verantwortlichkeitsfragen aufgeworfen hätte.[103]

[Rz 49] Es wird abzuwarten sein, wie stark unter den nun in der StPO definierten Voraussetzungen das praktische Bedürfnis der Strafverfolgungsbehörden nach einem Einsatz von Staatstrojanern tatsächlich sein wird. Insbesondere die technischen und finanziellen Hürden, die durch den in der Beratung neu eingefügten Art. 269^{quater} nStPO noch erhöht wurden, dürften deren praktischen Einsatz beschränken. Immerhin wird sich der Nutzen dank der in der Beratung eingefügten Pflicht zur Führung einer Statistik (Art. 269bis Abs. 2 und Art. 269ter Abs. 4 nStPO) zumindest nach einer gewissen Zeit abschätzen lassen.

97 Vgl. dazu etwas ungenau die Botschaft, BBl 2013 2683, 2772.

98 Votum Engler, AB 2014 S 300; Votum Schwaab, AB 2015 N 1151.

99 Vgl. dazu auch Votum Engler, AB 2014 S 300; Votum Schneider Schüttel, AB 2015 N 1170; Votum Sommaruga, AB 2015 N 1174.

100 Votum Schwaab, AB 2015 N 1151–1152; Votum Schneider Schüttel, AB 2015 N 1170; Votum Huber, AB 2015 N 1171.

101 AB 2015 N 1178–1179.

102 AB 2015 S 1198.

103 Votum Engler, AB 2015 S 1198.

IV. Fazit und Ausblick

[Rz 50] Das nBÜPF bringt einige Neuerungen, ohne jedoch in den wirklich kritischen Punkten so weit zu gehen, wie ursprünglich vor allem aus Sicht der Telekom-Industrie und der Überwachungsgegner befürchtet wurde. Zusammenfassend lässt sich festhalten, dass das nBÜPF zwar zu einer Erweiterung des persönlichen Geltungsbereichs führt, deren Auswirkungen jedoch über die Definition unterschiedlicher Kategorien von Mitwirkungspflichtigen mit jeweils differenzierten Mitwirkungspflichten wieder eingeschränkt wird. Die Relevanz dieser Ausweitung und deren Umsetzung in der Praxis wird sich erst mit dem Vorliegen der Ausführungsbestimmungen abschätzen lassen. Weitere Neuerungen stellen die Vorab-Informationspflicht der FDA für neue Dienste und die explizite Regelung des Einsatzes von Staatstrojanern und IMSI-Catchern (in der StPO) dar.

[Rz 51] Dagegen ändert sich bei der Dauer der Datenspeicherung nichts, diese beträgt weiterhin 6 Monate. Auch die Pflicht zum Betrieb einer Schnittstelle für den Echtzeit-Zugriff bleibt auf FDA beschränkt und wird nicht auf Dienste-Anbieter (AAK) generell ausgeweitet (wobei aber gewisse AAK im Rahmen der Ausnahmeregelung ebenfalls den für die FDA geltenden Mitwirkungspflichten unterstellt werden können). Gleichermassen beibehalten wurde die geltende Regelung zur Kostentragung und Entschädigung. Bezüglich des Ortes der Datenspeicherung werden im nBÜPF – gleich wie bisher – keine Vorgaben gemacht.

[Rz 52] Die Neuerungen, die das nBÜPF mit sich bringt, können somit als zwar relevant, aber nicht übermässig bezeichnet werden. Betrachtet man das Schlussresultat der Gesetzesrevision vor dem Hintergrund des heftig umstrittenen Vorentwurfs und des ebenfalls kontroversen Entwurfs, so kann das heutige Resultat schon fast als «sanfte Aktualisierung» oder als «gutschweizerischer Kompromiss» bezeichnet werden. Ein abschliessendes Urteil darüber wird aber erst zu wagen sein, wenn auch die Ausführungsbestimmungen bekannt sind.

[Rz 53] Die Ausführungsbestimmungen werden voraussichtlich Anfang 2017 in die Vernehmlassung gegeben. Im Sommer/Herbst 2017 sollten dann die finalisierten Versionen vorliegen. Damit könnte das Gesamtpaket per Anfang 2018 in Kraft treten, wobei für die zusätzlichen Mitwirkungspflichten der FDA und AAK Übergangsfristen gelten sollen. Die epische Geschichte der BÜPF-Revision wird uns also noch etwas länger beschäftigen – auch im Jahre 2017 werden sich zu dieser Thematik weitere Fragen und Diskussionspunkte ergeben.

Samuel Klaus, Dr. iur., LL.M. (Berkeley), Rechtsanwalt / Associate, Schellenberg Wittmer AG, Zürich, samuel.klaus@swlegal.ch.
Roland Mathys, lic. iur. et lic. oec. publ., LL.M. (LSE), Rechtsanwalt / Partner, Schellenberg Wittmer AG, Zürich, roland.mathys@swlegal.ch.