Universität St.Gallen

Working Paper VÜPF-Revision

Eine Analyse der Rechtmässigkeit der vorgeschlagenen Änderungen der Ausführungserlasse zum Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs

Prof. Dr. Monika Simmler
St. Gallen, 18. November 2025

Executive Summary

Im Vollzug des per 2018 totalrevidierten Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) erwies sich die Auslegung der Kategorien an mitwirkungspflichtigen Diensteanbieterinnen als strittig. Das betraf insbesondere den Umgang mit Over-the-Top-Diensten wie Threema und ProtonMail, welche die Gerichte nicht als Fernmeldedienstanbieterinnen (FDA), sondern als Anbieterinnen abgeleiteter Kommunikationsdienste (AAKD) qualifizierten. Aufgrund dieser Schwierigkeiten wurde der Bundesrat im Zuge der Revision des Fernmeldegesetzes (FMG) mit dem Erlass einer neuen Delegationsnorm (Art. 2 Abs. 2 nBÜPF) ermächtigt, die Kategorien von Mitwirkungspflichten «näher zu umschreiben». In Anbetracht dieser Änderung und des Bedürfnisses, in den Ausführungsbestimmungen zum BÜPF die technologischen Entwicklungen zu berücksichtigen, widmete sich der Bundesrat in zwei Schritten der Teilrevision der vier Verordnungen zum BÜPF (VÜPF, EFPD, VD-ÜPF und VVS-ÜPF).

Das erste Revisionspaket war weitgehend unstrittig und trat per 1. Januar 2024 in Kraft. Das nun vorgelegte zweite Revisionspaket soll weitergehende Änderungen umfassen. Im Zentrum steht die Neukategorisierung der Anbieterinnen. FDA können weiterhin «voll verpflichtet» oder «reduziert verpflichtet» sein. AAKD sollen neu in solche mit «vollen», «reduzierten» und «minimalen Pflichten» unterteilt werden. Weiter würden die Kriterien angepasst, die darüber entscheiden, welcher Kategorie eine Anbieterin zugeordnet wird, gewisse Pflichten sowie Auskunfts- und Überwachungstypen sollen zudem präzisiert oder neu eingeführt werden.

Die Anfang 2025 vorgelegten Vorschläge des Bundesrats stiessen auf grosse Kritik in den Medien, der Vernehmlassung und der Wissenschaft. Von Seiten der Behörden wird entgegnet, es ändere sich durch die Revision im Grundsatz nichts. Aufgrund dieser doch grossen Diskrepanz möchte das vorliegende Arbeitspapier mit einer Analyse zu einem differenzierten Diskurs abseits der Schlagzeilen beitragen. Das Zusammenspiel von BÜPF und VÜPF ist sowohl technisch als auch juristisch hoch komplex, weshalb eine detaillierte Betrachtung notwendig ist.

Die Analyse legt offen, dass die Revision einer Ausweitung des Kreises der Verpflichteten und der Verpflichtungen gleichkäme. Selbstredend versprechen die strafprozessrechtlichen Regeln einen den rechtstaatlichen Ansprüchen im Grundsatz genügenden Rechtsschutz, weshalb gewisse in den Medien geäusserte Befürchtungen als zu pauschal zurückzuweisen sind. Die Betrachtung zeigt aber, dass die Rechtmässigkeit verschiedener vorgeschlagener Änderungen zu verneinen ist.

Die Ergebnisse der Analyse lassen sich im Wesentlichen wie folgt zusammenfassen:

- Die Umsetzung der Gesetzesdelegation in Art. 2 Abs. 2 nBÜPF ist zulässig, sofern die Verordnungsbestimmungen lediglich Präzisierungen darstellen, sich im Rahmen des BÜPF bewegen und dessen Ratio entsprechen.
- Die Neuerung, dass bei den Voraussetzungen einer Herunterstufung von FDA zur solchen mit «reduzierten Pflichten» der Jahresgesamtumsatz des Unternehmens massgeblich sein soll, ist unrechtmässig, da sie nicht im Einklang mit Art. 26 Abs. 6 BÜPF steht.

- Dass AAKD mit über 5000 Teilnehmenden als «AAKD mit reduzierten Pflichten» einem erweiterten Pflichtenkatalog unterstehen sollen, ist weder verhältnismässig noch von Art. 22 Abs. 4 und Art. 27 Abs. 3 BÜPF umfasst. Das Gesetz sieht die Beschränkung vor, dass nur «Dienstleistungen von grosser wirtschaftlicher Bedeutung oder für eine grosse Benutzerschaft» eine Hochstufung rechtfertigen können, was beim Kriterium von 5000 Teilnehmenden nicht der Fall ist. Zusätzliche Pflichten sind unzulässig, sofern sie nicht ebenso für AAKD ohne erweiterte Pflichten vorgesehen werden könnten.
- Bei den Voraussetzungen einer Hochstufung zu einer AAKD mit vollen Pflichten ist es unzulässig, auf den Umsatz des Gesamtunternehmens abzustellen, da diese Voraussetzung vom Gesetzestext nicht gedeckt ist. Auch die heutige Regelung, das Abstellen auf die «Auskunfts- oder Überwachungsrelevanz» ist indes als unzulässig zu erachten und hätte einer gerichtlichen Überprüfung kaum standgehalten.
- AAKD mit vollen Pflichten können verpflichtet werden, Teilnehmende mit geeigneten Mitteln zu identifizieren. Eine entsprechende Pflicht für AAKD mit reduzierten Pflichten, d.h. solche mit über 5000 Teilnehmenden, ist nicht zulässig.
- Die genauen Pflichten betreffend die Aufbewahrung und Herausgabe von Bestandes- und Randdaten lassen sich für die Mitwirkungspflichtigen im Geflecht von BÜPF und VÜPF nur unzureichend erkennen. Unklare Vorgaben wie diese zu Daten betreffend die «benachbarten Netze», aber ebenso die fehlende Auflistung der zu speichernden Randdaten zum Zwecke der Überwachungen sind der Rechtssicherheit nicht zuträglich. Die hohe Invasivität der Vorratsdatenspeicherung, aber auch der Inhalts- und Randdatenerhebung im Allgemeinen verlangt nach einer klaren Regelung. Da die Pflichten nicht nur schwer erkennbar, sondern darüber hinaus wenig differenziert ausfallen, ist folglich generell zweifelhaft, ob sie einer Verhältnismässigkeitsprüfung standhalten würden und Anbieterinnen – auch die voll Verpflichteten – gestützt darauf rechtmässig zur entsprechenden Mitwirkung angehalten werden könnten.
- FDA mit vollen Pflichten können weiterhin und AAKD mit vollen Pflichten können neu dazu angehalten werden, serverseitige Verschlüsselungen und Transportverschlüsselungen aufzuheben, wenn sie über den Schlüssel verfügen und ihn nutzen können. Dies ist rechtmässig. Von der (unbestimmten) Regelung lässt sich hingegen keine Pflicht ableiten, Verschlüsselungen zu unterlassen oder Schlüssel per se zur Verfügung zu halten.
- Die vorgeschlagene Pflicht, bei Auskünften zu statischen IP-Adressen bei Mehrfachergebnissen die Anzahl der Ergebnisse bekanntzugeben, ist nicht zu beanstanden. Dass bei dynamischen IP-Adressen im Falle von Mehrfachergebnissen nicht nur die Anzahl, sondern auch die Ergebnisse selbst geliefert werden müssen, ist weitreichender, da unbeteiligte Dritte von dieser Massnahme berührt sind. Die Rechtmässigkeit dieser Massnahme hängt entscheidend von der Anzahl gelieferter Datensätze sowie dem Ermittlungszweck ab.
- Ein neuer Auskunftstyp soll zur Schnittmengenbildung bei IP-Adressen verpflichten. Die Massnahme verlangt den Anbieterinnen die Teilnehmeridentifikationen zu vorhandenen Randdaten im grösseren Stil (Massenabfragen) ab. Den Behörden wird zwar nur die Schnittmenge geliefert, als Zwischenschritt ist jedoch eine Bearbeitung von Daten zahlreicher Nutzer:innen nötig, womit die Massnahme eine grosse Streubreite erhält. Es ist

mindestens als fraglich zu werten, ob dieser neue Auskunftstyp bei allen Delikten und ohne staatsanwaltliche oder richterliche Überprüfung als verhältnismässig gelten kann.

- Eine ähnliche, wenn auch weitergehende Problematik zeigt sich bei den Auskunftstypen, die eine Auskunftserteilung betreffend die IP-Adresse des letzten Zugriffs vorsehen sollen. Der Zugriff muss nicht zwingend, wird aber sehr oft einen Bezug zu einer Kommunikation aufweisen. Die Abfrage hat das Potenzial, das Fernmeldegeheimnis zu berühren. Darüber hinaus verlangt sie, dass Anbieterinnen Randdaten fortlaufend erheben, auf Vorrat (mindestens 6 Monate) speichern und im Falle eines Auskunftsbegehrens bearbeiten. Es ist zu bestreiten, dass die Einordnung dieser Massnahme als nach dem vereinfachten Verfahren durchzuführende Bestandesdatenabfrage zulässig ist.
- Auch die neue Pflicht von Kommunikationsdiensten, Angaben zu getätigten Zahlungen und Transaktionen, Zahlungsmitteln usw. zu machen, betrifft das Verhalten von Online-Nutzer:innen und nicht bloss «beständig» bei den Anbieterinnen vorliegende Daten. Die Qualifikation als Bestandesdatenabfrage überzeugt nicht.

Dem Bundesrat ist gestützt auf diese Ergebnisse zu empfehlen, die Vorlage zu überarbeiten. Die Gesetzesdelegation in Art. 2 Abs. 2 nBÜPF ermächtigt zu Ausführungsbestimmungen, weshalb sich der Bundesrat – auch aus demokratiepolitischen Überlegungen – auf Präzisierungen beschränken sollte. Es ist in diesem Sinne zu empfehlen, (1.) AAKD mit über 5000 Teilnehmenden nicht einem erweiterten Pflichtenkatalog zu unterstellen. Die Hochstufung muss in Einklang mit dem BÜPF stehen und verhältnismässig sein, was bei grossen wirtschaftlichen Akteuren anders zu beurteilen ist als bei kleinen und mittelgrossen. Da mit der vollen Verpflichtung von AAKD sehr weitgehende Pflichten einhergehen, ist dem Bundesrat (2.) zu empfehlen, dass er die Kriterien zur Hochstufung erneut überprüft. Das Abstellen auf den Gesamtumsatz wird mutmasslich zu Beschwerdeverfahren führen, die in der Nichtanwendung von Normen resultieren könnten.

Aufgrund der Invasivität der Vorratsdatenspeicherung ist (3.) das komplexe Zusammenspiel der VÜPF- und BÜPF-Normen diesbezüglich erneut zu überprüfen. Das gilt umso mehr, als der Bundesrat einen Anschluss an das neue E-Evidence-System der EU zum vereinfachten grenzüberschreitenden Zugriff auf elektronische Beweismittel prüft und auf Vorrat gespeicherte Daten folglich auch international vereinfacht erhältlich gemacht werden könnten. Unabhängig davon lassen die neuen Auskunftstypen die Frage aufkommen, inwiefern es rechtmässig ist, gestützt auf vereinfachte Bestandesdatenabfragen, d.h. ohne gerichtliche Überprüfung, die Bearbeitung von Randdaten zu verlangen. Das ist besonders heikel, da die entsprechenden Randdaten von den voll verpflichteten Anbieterinnen auf Vorrat gespeichert und in der Folge faktisch ohne Einschränkung genutzt werden können, was in vielen Fällen zu einem Missverhältnis zwischen Eingriffsintensität und Rechtsschutz führen wird. Auskünfte und Überwachungen sind deshalb klarer zu trennen und Auskünfte, die implizit eine Bearbeitung vorrätig gespeicherter Randdaten (insbesondere Logfiles) involvieren, dem Rechtsschutz der Randdatenerhebung zu unterstellen.

In der Summe zeigt die Analyse, dass das Schweizer Überwachungsrecht aufgrund seiner historisch bedingten Ausrichtung auf Post- und Fernmeldedienste Schwächen aufweist. Überwachungen und die Ermittlungsarbeit im Allgemeinen betreffen heute zu einem sehr wesentlichen Teil Internetdienste. Sie weisen oft, aber nicht immer einen Bezug zu einer konkreten Kommunikation auf. Der Fokus des BÜPF auf Eingriffe in das Fernmeldegeheimnis schmälert den Anwendungsbereich von vornherein. Durch die rechtlichen Neuerungen werden zudem zunehmend Online-

Dienste gestützt auf Normen verpflichtet, die ursprünglich auf Fernmeldedienste zugeschnitten waren. Die Balance zwischen Sicherheits- und Strafverfolgungsinteressen sowie Grundrechtsschutz könnte gestützt auf ein weniger komplexes Normengeflecht transparenter ausgehandelt werden, Befürchtungen aber auch entgegengewirkt werden. Es handelt sich bei den bestehenden und angedachten Regelungen nicht um solche, wie sie autoritären Überwachungsstaaten entsprechen. Dennoch hat die Vorlage rechtliche Schwächen und wäre in der vorliegenden Form in mehreren Belangen unrechtmässig.

Inhaltsverzeichnis

1. Einleitung

1.1. Historie und Rechtsetzungsprozess

Das totalrevidierte Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF; SR 780.1) trat zusammen mit der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF; SR 780.11), der Verordnung des eidgenössischen Justiz- und Polizeidepartements (EJPD) über die Durchführung der Überwachung des Post- und Fernmeldeverkehrs (VD-ÜPF; SR 780.117) und der Verordnung über das Verarbeitungssystem für die Überwachung des Post- und Fernmeldeverkehrs (VVS-ÜPF; SR 780.12) am 1. März 2018 in Kraft. Mit den totalrevidierten Erlassen sollte den Strafverfolgungsbehörden das nötige Instrumentarium für eine ***effektive Aufklärung von Straftaten*** zur Verfügung gestellt werden, die mittels moderner Technologien begangen werden.[1]

Im Vollzug des neuen BÜPF erwies sich die Auslegung des ***Begriffs der Fernmeldedienstanbieterin*** (FDA) als strittig. Der Dienst ÜPF wollte grosse Over-the-Top-Dienste (OTT-Dienste) wie die Messaging-Dienstanbieterin Threema und den E-Mail-Provider ProtonMail als FDA klassifizieren und den entsprechenden (erweiterten) Mitwirkungspflichten unterstellen. Das Bundesgericht (im Falle von Threema)[2] und das Bundesverwaltungsgericht (im Falle von ProtonMail)[3] schoben diesem weiten Begriffsverständnis indes im Jahr 2021 einen Riegel vor. Gemäss Bundesgericht handelt es sich unter Anwendung aller anerkannten Auslegungsmethoden bei diesen Unternehmen um Anbieterinnen abgeleiteter Kommunikationsdienste (AAKD). Ein anderes Verständnis der Mitwirkungspflichtigen oder -pflichten zu etablieren, bedürfe einer Gesetzesrevision. Die beiden Kategorien von Mitwirkungspflichtigen können aneinander, so das Bundesgericht, zudem durch Herauf- und Herabstufung angeglichen werden. Dadurch könne sichergestellt werden, dass der Fernmeldeverkehr ausreichend überwacht sei, zugleich aber verhältnismässige Mitwirkungspflichten auferlegt werden.

Befeuert durch diese Rechtsstreitigkeit wurde die am 1. Januar 2021 in Kraft getretene Revision des Fernmeldegesetzes (FMG; SR 784.10) genutzt, um den Bundesrat dazu zu ermächtigen, ***weitergehende Ausführungsbestimmungen*** bezüglich der durch das BÜPF verpflichteten Anbieterinnen zu erlassen.[4] Der im Zuge der FMG-Revision verabschiedete Art. 2 nBÜPF soll zeitgleich mit einer entsprechenden Revision der VÜPF in Kraft treten.[5] Der revidierte Art. 2 nBÜPF knüpft einerseits den Begriff des Fernmeldedienstes nicht mehr an denjenigen des FMG (Abs. 1). Andererseits hält er fest, dass der Bundesrat die Kategorien von Mitwirkungspflichtigen näher umschreibt (Abs. 2). Insbesondere ist der Bundesrat dazu aufgefordert, die Kategorien der FDA, der AAKD und der Personen, die ihren Zugang zu einem öffentlichen Fernmeldenetz Dritten zur Verfügung

[1] Medienmitteilung des Bundesrats v. 15.11.2017, <https://www.news.admin.ch/de/nsb?id=68799> (Abruf: 1.11.2025).

[2] BGer 2C_544/2020 v. 29.4.2021; vgl. auch BVGer A-550/2019 v. 19.5.2020.

[3] BVGer A-5373/2020 v. 13.10.2021.

[4] EJPD, VÜPF/VD-ÜPF Erläuternder Bericht, 3.

[5] EJPD, VÜPF/VD-ÜPF Erläuternder Bericht, 3.

stellen, zu präzisieren. Des Weiteren erachtete der Bundesrat technologische Entwicklungen, namentlich im Bereich der 5G-Technologie, als Anlass, die Ausführungsbestimmungen zum BÜPF einer Überprüfung zu unterziehen.

Resultat dieser Überprüfung waren zunächst gewisse eher technische und wenig umstrittene Neuerungen im Rahmen einer Teilrevision der VÜPF, der VS-ÜPF und der VVS-ÜPF vom 15. November 2023 (***erstes Revisionspaket***, Inkrafttreten 1. Januar 2024).[6] Primär ging es um Anpassungen betreffend die 5G-Technologie und die IP Multimedia Subsysteme (IMS)[7]. In ein zweites Revisionspaket vertagte der Bundesrat die Wahrnehmung seiner Kompetenz zur präziseren Definition der Kategorien von Mitwirkungspflichtigen. Zu diesem ***zweiten Revisionspaket*** legte der Bundesrat mittlerweile Entwürfe vor und eröffnete am 29. Januar 2025 die Vernehmlassung.[8] Nach eigenen Angaben beabsichtigt er, die kategorische Zuordnung von Anbieterinnen von Post- und Fernmeldedienstleistungen transparenter und eindeutiger zu gestalten.[9] Auferlegte Pflichten für die Mitwirkungspflichtigen sollen klarer ersichtlich werden.[10] Die Vorschläge dieses zweiten Revisionspakets der Ausführungsbestimmungen zum BÜPF sind Gegenstand der nachfolgenden Analyse. Da es sich bei den Änderungen in den VVS-ÜPF und der VD-ÜPF lediglich um redaktionelle Änderungen sowie um analoge Anpassungen der Bearbeitungsfristen handelt, welche unumstritten sind, konzentriert sich die vorliegende Analyse auf die VÜPF.

1.2. Kritik in Öffentlichkeit und Lehre

Die ***Vernehmlassung*** endete am 6. Mai 2025.[11] Die Beteiligung einer Vielzahl von Kantonen, politischen Parteien, Dachverbänden, der Bundesanwaltschaft, weiterer Organisationen aus Wirtschaft und Zivilgesellschaft, sowie Privatpersonen war rege und ergab Rückmeldungen von gesamthaft 830 Seiten.[12] In den Stellungnahmen wurde mehrheitlich Kritik an der Vorlage geäussert. Einzig die Kantone zeigten sich mit der Vorlage weitgehend einverstanden. Dagegen waren die Parteien des gesamten politischen Spektrums, namhafte Wirtschaftsverbände, betroffene Unternehmen und dem Ziel des Schutzes der Privatsphäre verpflichtete Nichtregierungsorganisationen in überraschend deutlicher Einigkeit unzufrieden mit dem vorgelegten Revisionspaket.

Auch die ***mediale Aufarbeitung*** der Vorlage fiel kritisch aus: So häuften sich Schlagzeilen wie «Der Überwachungs-Staat Schweiz droht aus dem Ruder zu laufen – doch es gibt Gegenwehr» (Watson)[13], «Beat Jans will den Überwachungsstaat» (WOZ)[14], «Reformpläne zur Überwachung

[6] EJPD, BÜPF Erläuterungen, 3.

[7] EJPD, BÜPF Erläuterungen, 4.

[8] Medienmitteilung des Bundesrats v. 29.1.2025, <https://www.news.admin.ch/de/nsb?id=103968> (Abruf: 1.11.2025).

[9] EJPD, VÜPF/VD-ÜPF Erläuternder Bericht, 3.

[10] EJPD, VÜPF/VD-ÜPF Erläuternder Bericht, 3.

[11] Medienmitteilung des Bundesrats v. 29.1.2025, <https://www.news.admin.ch/de/nsb?id=103968> (Abruf: 1.11.2025).

[12] EJPD, VÜPF/VD-ÜPF Stellungnahmen, passim.

[13] Watson v. 10.5.2025, <https://www.watson.ch/digital/wirtschaft/916205370-vuepf-revision-kritik-an-ausweitung-der-staatlichen-ueberwachung> (Abruf: 1.11.2025).

[14] WOZ v. 15.5.2025, <https://www.woz.ch/2520/vuepf/beat-jans-will-den-ueberwachungsstaat/!5PVH5GHWYXNR> (Abruf: 1.11.2025).

der Telekommunikation fallen durch» (Blick)[15] oder «Die Schweiz ist drauf und dran, autoritäre Überwachungsstaaten zu kopieren» (Republik)[16]. 15'000 Personen unterzeichneten zudem eine im August 2025 von der Digitalen Gesellschaft und Campax eingereichte Petition unter dem Titel «Demokratie statt Überwachungsstaat».[17]

Vertreter der ***Behörden***[18] dementierten in der Folge öffentlich, dass neue Pflichten für die Anbieterinnen entstehen, welche Unternehmen in der Schweiz zum Wegzug zwingen würden. Der Bundesrat wies die Kritik entsprechend zurück, wonach Unternehmen durch die Änderungen zur Abwanderung gedrängt werden: Es würden keine neuen Pflichten eingeführt, sondern vielmehr bereits bestehende Pflichten umgesetzt, an deren Umsetzung es bislang mangelte.[19] Vertreter von Proton und Threema widersprachen dieser Einschätzung. So müsste Threema nach eigenen Aussagen ihren Grundsatz aufgeben, nur so viele Daten wie technisch notwendig zu erheben.[20] Investitionen würden zudem künftig ins Ausland verschoben.[21] Proton wiederum spricht von einer «kompletten» Aufweichung des Schutzes der Privatsphäre und drohte bereits mit einem Wegzug aus der Schweiz.[22]

Schliesslich wurde von Seiten der ***Lehre*** Kritik laut, so in einem Gutachten von ROLF WEBER[23]. Im Wesentlichen kritisiert er die vage Formulierung der Pflichten und bestreitet die Verhältnismässigkeit derselben.[24] Die Herabsenkung der Aufgreifkriterien der jeweiligen Kategorien der Mitwirkungspflichtigen führe zu einer weitgehenden Ausdehnung der Überwachung, weshalb fraglich sei, ob eine solch grundlegende und teils dem BÜPF widersprechende Diskussion im Rahmen einer Verordnungs-Vernehmlassung oder nicht vielmehr auf Stufe der Legislative zu führen sei. Er erblickt ein erhebliches Risiko darin, dass das Bundesgericht in einem Individualverfahren und unter Anwendung einer akzessorischen Prüfung Bestimmungen der nVÜPF aufheben könnte.[25]

---

[15] Blick v. 7.5.2025, <https://www.blick.ch/politik/kritik-an-bundesrat-reformplaene-zur-ueberwachung-der-telekommunikation-fallen-durch-id20846813.html> (Abruf: 1.11.2025).

[16] Republik v. 7.5.2025, <https://www.republik.ch/2025/05/07/die-schweiz-ist-drauf-und-dran-autoritaere-ueberwachungsstaaten-zu-kopieren> (Abruf: 1.11.2025).

[17] Campax Petition, <https://act.campax.org/petitions/demokratie-statt-uberwachungsstaat?utm.com> (Abruf: 1.11.2025).

[18] Der stellvertretende Leiter des Dienstes ÜPF sagte in der Tagesschau v. 29.4.2025: «Es wird nicht verschärft, es wird präzisiert», <https://www.srf.ch/news/schweiz/strafverfolgung-in-der-schweiz-mehr-ueberwachungen-im-schweizerischen-fernmeldenetz> (Abruf: 1.11.2025).

[19] AB NR 2025 7311.

[20] Inside IT v. 14.8.2025, <https://www.inside-it.ch/15000-unterschriften-gegen-vupf-revision-eingereicht-20250814> (Abruf: 1.11.2025).

[21] Tagesanzeiger v. 23.7.2025, <https://www.tagesanzeiger.ch/techfirma-proton-kehrt-der-schweiz-den-ruecken-126325644688> (Abruf: 1.11.2025).

[22] Zum Ganzen siehe Inside IT v. 14.8.2025, <https://www.inside-it.ch/15000-unterschriften-gegen-vupf-revision-eingereicht-20250814> (Abruf: 1.11.2025).

[23] WEBER, passim.

[24] WEBER, 12.

[25] WEBER, 11.

1.3. Gegenstand und Ziel der nachfolgenden Analyse

Nach Abschluss der Vernehmlassung liegt der Ball erneut beim Bundesrat. Aufgrund der breiten Resonanz des Geschäfts stellen sich betreffend die Überarbeitung verschiedene rechtspolitische Fragen. Darüber hinaus scheinen die Meinungen über den juristischen Gehalt der Vorlage sowie deren Rechtmässigkeit auseinanderzugehen. Zwischen der Kritik am Überwachungsstaat und dem durch die Behörden vertretenen Standpunkt, es ändere sich kaum etwas, besteht doch eine grosse Diskrepanz. Das vorliegende Arbeitspapier möchte mit einer genaueren Analyse zum weiteren Vorgehen sowie zu einem differenzierten Diskurs abseits der Schlagzeilen beitragen.

Das Zusammenspiel von BÜPF und VÜPF ist sowohl technisch als auch juristisch von hoher Komplexität. Entsprechend kann sich die nachfolgende Analyse nicht den Details verwehren. Die Materie ist nicht einfach und soll folglich auch nicht verkürzt oder vereinfacht dargestellt werden. Ansonsten könnte sie dem soeben beschriebenen Zweck nicht gerecht werden. Dennoch ist eine gewisse Fokussierung auf die strittigen Punkte vonnöten, bei gänzlich unstrittigen Aspekten[26] wird dagegen auf weitergehende Ausführungen verzichtet. Nach einer kurzen, dem Verständnis dienenden Einbettung in das Geflecht des Überwachungsrechts (Kap. 2) wird auf die wichtigsten Aspekte der Revisionsvorlage eingegangen und die Rechtmässigkeit der Neukategorisierung der Mitwirkungspflichtigen (Kap. 3) und der Änderung der Mitwirkungspflichten sowie der neuen Auskunfts- und Überwachungstypen (Kap. 4) werden beurteilt. Zum Schluss sollen diese zur Synthese gebracht und gewürdigt werden (Kap. 5).

Es sei an dieser Stelle angemerkt, dass die Analyse durch die Autorin unabhängig, d.h. ohne Auftraggeber, durchgeführt wurde.[27] Sie beschränkt sich zudem auf eine juristische Würdigung, die politische lässt sie aussen vor. Als ***Working Paper*** ist die Analyse zudem in der Annahme ausgestaltet, dass die Diskussion in den kommenden Monaten noch weitergeführt werden wird und allenfalls eine Weiterentwicklung denkbar wäre. Rückmeldungen und Inputs sind explizit willkommen.

2. Überblick: Datenkategorien und Zwangsmassnahmen

Grundlage für die Überwachung des Post- und Fernmeldeverkehrs im praxisrelevantesten Feld, der Strafverfolgung, bilden die in der Strafprozessordnung (StPO; SR 312.0) normierten ***geheimen Überwachungsmassnahmen*** (Art. 269 ff.) sowie das ***BÜPF***. Die zu Beginn des letzten Jahrzehnts initiierten Revisionen dieser Rechtsgrundlagen hatten zum Ziel, die Überwachung an die technologischen Entwicklungen anzupassen.[28] Während die StPO die Eingriffe in das Fernmeldegeheimnis durch Strafverfolgungsbehörden (Zwangsmassnahmen) regelt, regeln das BÜPF und die zugehörigen Ausführungserlasse das konkrete behördliche Vorgehen beim Erhältlichmachen der Daten im Besitz privater Anbieterinnen (Mitwirkungspflichtige) sowie deren Auskunfts- und Überwachungspflichten (Mitwirkungspflichten). Der sachliche Anwendungsbereich beschränkt

[26] So z.B. bei einigen Präzisierungen wie den im Auskunftsgesuch enthaltenen Informationen bei juristischen Personen (Art. 27 Abs. 2 nVÜPF) oder den Grössen, ab wann ein WLAN-Zugang «professionell betrieben» ist (Art. 16h nVÜPF).

[27] Besten Dank an dieser Stelle an Silvan Peter, wissenschaftlicher Mitarbeiter an der Universität St. Gallen, für das engagierte Mitdenken in diesem Projekt.

[28] Botschaft BÜPF, 2685.

sich auf die Zwecke der Strafverfolgung (lit. a), den Vollzug von Rechtshilfeersuchen (lit. b), der Suche nach vermissten Personen (lit. c), der Fahndung nach straffälligen Personen (lit. d), den Vollzug des Nachrichtendienstgesetzes (NDG; SR 121) (lit. e) sowie Mobilfunklokalisierungen zur Wahrung der inneren Sicherheit (lit. f). Damit widmet sich das BÜPF der Frage, wann und in welcher Form private Diensteanbieterinnen bei der staatlichen Überwachung mitwirken müssen.

Die materiellen Voraussetzungen der Überwachung von ***Inhaltsdaten*** sind in Art. 269 StPO geregelt. Vorausgesetzt wird mit Blick auf die Begehung einer in Abs. 2 aufgeführten Katalogstraftat ein dringender Verdacht, eine gewisse Schwere der Tat sowie die Erfolglosigkeit, Aussichtslosigkeit oder Unverhältnismässigkeit bisheriger Untersuchungshandlungen. Beim Einsatz besonderer technischer Geräte (Art. 269bis StPO) oder Informatikprogrammen (Art. 269ter StPO) treten weitere Voraussetzungen hinzu. Überwacht werden können beschuldigte Personen und Drittpersonen, welche für die beschuldigte Person bestimmte Mitteilungen entgegennehmen oder weiterleiten (Art. 270 StPO). Jedenfalls bedarf es für geheime Überwachungsmassnahmen betreffend die Echtzeitüberwachung von Inhaltsdaten der Genehmigung durch das Zwangsmassnahmengericht (Art. 282 StPO). Nicht der geheimen Überwachung, sondern der Beschlagnahme nach Art. 263 ff. StPO unterliegt die rückwirkende Erhebung von Inhaltsdaten.

Sogenannte ***Randdaten*** im Sinne von Art. 8 lit. b BÜPF, d.h. «Daten, aus denen hervorgeht, mit wem, wann, wie lange und von wo aus die überwachte Person Verbindung hat oder gehabt hat, sowie die technischen Merkmale der entsprechenden Verbindung», können gemäss Art. 273 StPO bei allen Verbrechen und Vergehen überwacht werden, sofern es sich dabei um eine verhältnismässige und subsidiäre Massnahme handelt (Abs. 1). Randdaten können zudem in Echtzeit sowie für 6 Monate rückwirkend herausverlangt werden (Abs. 2). Auch bei ihrer Erhebung bedarf es indes einer vorgängigen gerichtlichen Genehmigung (Abs. 3). Mit Randdaten werden Informationen rund um den Kommunikationsverkehr zwischen zwei oder mehreren Fernmeldeteilnehmenden erhoben.[29] Zu den Randdaten gehören bspw. der Ursprung sowie das Ziel einer Nachricht, der Standort des Geräts, das Datum, die Uhrzeit, die Dauer, die Grösse, die Route, das Format und das verwendete Protokoll.[30]

Als dritte Datenkategorie sind die ***Bestandesdaten*** zu nennen. Mit ihnen wird festgestellt, welcher Person die mittels Randdaten festgestellte Kommunikation zugeordnet werden kann.[31] Die Bestandesdatenabfrage zielt somit auf die Identifizierung der Fernmeldeteilnehmenden ab.[32] Sie gibt Auskunft über «feststehende Abonnementsverhältnisse, die sich nicht auf einzelne Gespräche oder Sendungen beziehen»[33]. Bestandesdaten sind insofern «beständig», als sie bei den Dienstanbieterinnen unverändert und unabhängig von einem bestimmten Fernmeldeverkehr vorliegen.[34] Zu den Bestandesdaten gehören z.B. der Name des Inhabers eines Anschlusses, Verträge sowie der Personal Unblocking Key.[35] Diese Informationen über die Teilnehmenden des Post- und

[29] HANSJAKOB, 104.

[30] Art. 3 Ziff. 11 E-Evidence-Verordnung, diskutiert in SIMMLER, 135.

[31] BGE 141 IV 108, E. 3.5.3.

[32] OGer ZG S 2023 28 v. 27.10.2023, E. 3.5.3.

[33] BSK StPO-JEAN-RICHARD-DIT-BRESSEL 2023, Art. 273 N 7; SIMMLER, 136.

[34] HANSJAKOB, 236; SIMMLER, 136.

[35] BGE 141 IV 423; BSK StPO-JEAN-RICHARD-DIT-BRESSEL, Art. 273 N 7; HANSJAKOB, 89 und 441; SIMMLER, 136.

Fernmeldeverkehrs sind genereller Natur und geben keinen Aufschluss über einzelne Fernmeldeverbindungen. Deshalb unterliegen sie auch nicht dem Fernmeldegeheimnis.

Die nicht immer unstrittige (vgl. → Kap. 4.6.4) ***Unterscheidung von Rand- und Bestandesdaten*** ist von besonderer Relevanz, da für Bestandesdaten keine richterliche Genehmigung vonnöten ist, ihre Erhebung sich allein auf das BÜPF abstützen lässt (Art. 21 f.) und folglich die Polizei eigenständig entsprechende Auskünfte in einem vereinfachten Verfahren bei Diensteanbieterinnen einholen kann.[36] Die Unterscheidung spiegelt sich auch in den Begrifflichkeiten des BÜPF und der VÜPF wieder: Sind Inhalts- oder Randdatenerhebungen gestützt auf die StPO betroffen, ist die Rede von *Überwachungen*. Geht es um Bestandesdaten, spricht man hingegen von *Auskünften*.

Abbildung 1: Datenkategorien sowie Grundlagen und Voraussetzungen ihrer Erhebung

Bestandesdaten	Art. 21 f. BÜPF	Polizeiliche Erhebung via ÜPF
Randdaten	Art. 273 StPO	Genehmigung durch das Zwangsmassnahmengericht + nur bei Vergehen und Verbrechen
Inhaltsdaten	Art. 263 ff. StPO (rückwirkend) Art. 269 ff. StPO (Echtzeit)	Siegelung Genehmigung durch das Zwangsmassnahmengericht + nur bei Katalogtaten

3. Neukategorisierung der Mitwirkungspflichtigen

3.1. Gesetzesdelegation des neuen Art. 2 Abs. 2 BÜPF

Art. 2 Abs. 2 nBÜPF bestimmt, dass der Bundesrat die Kategorien von Mitwirkungspflichtigen «näher umschreibt», insbesondere diejenigen der FDA, der AAKD sowie derjenigen Personen, die ihren Zugang zu einem öffentlichen Fernmeldenetz Dritten zur Verfügung stellen. Während Art. 31 BÜPF den Bundesrat bereits ermächtigte, die Auskunfts- und Überwachungstypen in Ausführungsbestimmungen näher zu umschreiben, sollte mit der Einfügung des Art. 2 Abs. 2 nun derselbe Auftrag für die Kategorien der Mitwirkungspflichtigen erteilt werden.

Wie WEBER in seinem Gutachten zutreffend festhält, erlaubt die neue ***Delegationsnorm*** dem Bundesrat den Erlass von Ausführungsbestimmungen, um die Kategorien präziser zu umschreiben. Nicht aber könnten ganz neue Pflichten eingeführt werden. Bei der Konkretisierung sei zudem

[36] Botschaft BÜPF, 2733.

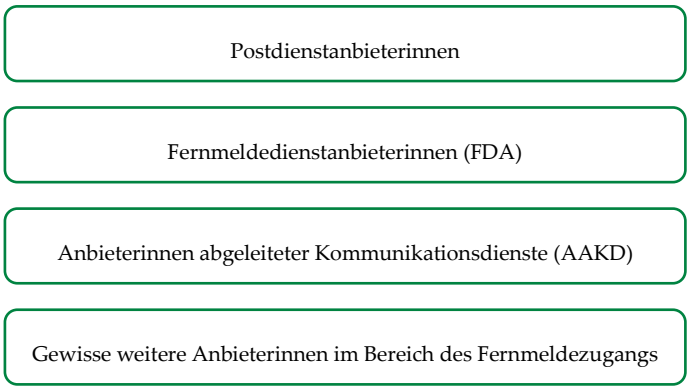
dem «Grundgedanken des BÜPF» Rechnung zu tragen.[37] Betreffend die anerkannten Voraussetzungen der Gesetzesdelegation erachtet es WEBER als fraglich, ob sich die Delegation auf genau umschriebene Aspekte beschränkt und ob die wichtigsten Regelungen im Gesetz enthalten sind.[38] Der Bundesrat hingegen sah es als sein Ziel an, mit der näheren Umschreibung der Kategorien von Anbieterinnen zu einer «ausgewogeneren und dem verfassungsrechtlichen Grundsatz der Verhältnismässigkeit (Art. 5 Abs. 2 BV) besser entsprechenden Abstufung der Pflichten» beizutragen.[39]

Unstrittig ist zunächst, dass Gesetzesdelegationen zur weiteren Konkretisierung von Begrifflichkeiten grundsätzlich zulässig sind. Der Bundesrat wird ermächtigt, die in Art. 2 Abs. 1 nBÜPF vorgesehenen Kategorien weiter zu umschreiben. Weder wird er jedoch dazu ermächtigt, für diese Kategorien andere als die im Gesetz vorgesehenen Pflichten einzuführen, noch kann er den Kerngehalt, d.h. die *ratio legis* der Unterscheidung zwischen den verschiedenen Kategorien und den zugehörigen Pflichten, missachten oder sich von den gesetzlichen Unterscheidungen loslösen. Mit WEBER ist somit einig zu gehen, dass es sich bei den entsprechenden Verordnungsbestimmungen um reine ***Konkretisierungen*** handeln muss. Ob die Revisionsvorlage diesem Anspruch gerecht wird, ist nachfolgend zu zeigen. *Die Gesetzesdelegation in Art. 2 Abs. 2 BÜPF an sich ist aber jedenfalls (verfassungsrechtlich) zulässig.*

3.2. Kategorien von Diensteanbieterinnen im Überblick

Das BÜPF definiert den ***persönlichen Anwendungsbereich*** in Art. 2. Dabei unterscheidet es zwischen verschiedenen Kategorien von Diensteanbieterinnen (Abbildung 2). Die Pflichten der Anbieterinnen von Postdiensten sind in Art. 19 f. BÜPF geregelt und bleiben von der aktuellen Revision unberührt. Die weiteren Anbieterinnen wie die Betreiberinnen von internen Fernmeldenetzen, von öffentlichen Fernmeldenetzen sowie die professionellen Wiederverkäuferinnen von Mitteln, die den Zugang zu öffentlichen Fernmeldenetzen erlauben (Art. 2 Abs. 1 lit. d, e und f nBÜPF), stehen ebenfalls nicht im Vordergrund der aktuellen Auseinandersetzung. Entsprechend konzentrieren sich nachfolgende Ausführungen auf die Kategorien der FDA und AAKD.

Abbildung 2: Mitwirkungspflichtige nach Art. 2 BÜPF



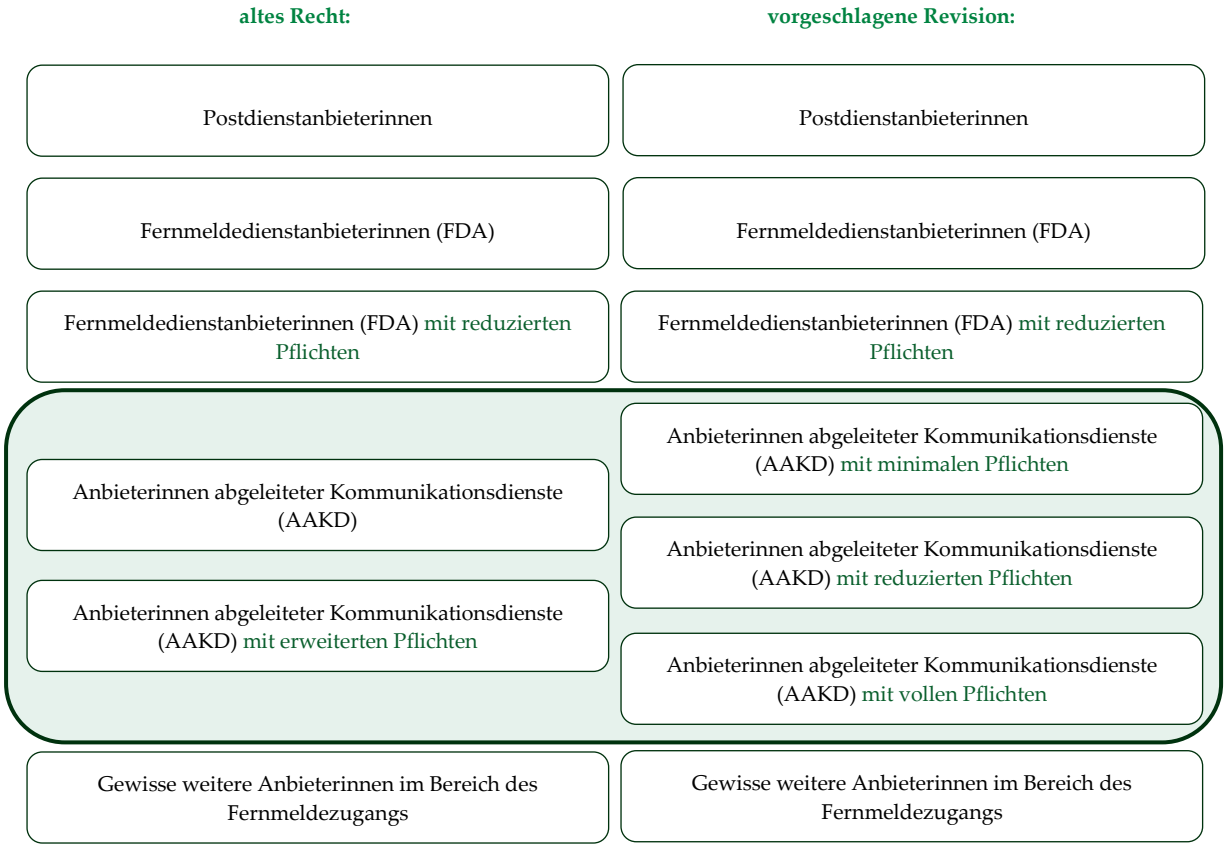
[37] WEBER, 2.

[38] WEBER, 2 f.

[39] EJPD, VÜPF/VD-ÜPF Erläuternder Bericht, 52.

De lege ferenda schlägt der Bundesrat bei den AAKD eine ***Neukategorisierung*** vor. Neu sollen drei Kategorien unterschieden werden, genauer AAKD mit minimalen, solche mit reduzierten und solche mit vollen Pflichten (Abbildung 3). Diese Neukategorisierung würde verschiedene Änderungen mit sich bringen. Es änderten sich sowohl bei den FDA als auch den AAKD aber auch die Voraussetzungen von Hoch- bzw. Herunterstufungen, d.h. der Zugehörigkeit zu den Kategorien (dazu für die FDA → Kap. 3.3.2, für die AAKD → Kap. 3.4.2).

Abbildung 3: Gegenüberstellung Diensteanbieterinnen nach geltendem und vorgeschlagenem Recht



3.3. Kategorien der FDA

3.3.1. Begriff des Fernmeldedienstes

Mit der Revision des FMG wurde, wie bereits erwähnt, Art. 2 des BÜPF angepasst. Neben der neuen Delegationsnorm in Abs. 2, wurde auch Abs. 1 lit. b nBÜPF angepasst. Bei den FDA soll zukünftig nicht mehr auf die entsprechende ***Definition des FMG*** verwiesen werden. Die Kategorie lautet zwar nach wie vor «Anbieterinnen von Fernmeldediensten», der Gesetzesverweis wird jedoch fallen gelassen. Dies ist eine Reaktion auf Unklarheiten hinsichtlich der Auslegung des Begriffes des «Fernmeldedienstes» im Überwachungsrecht, wie sie sich insbesondere im Bundesgerichtsurteil betreffend die Qualifikation der Diensteanbieterin Threema niedergeschlagen haben.[40] In der Botschaft zum FMG wird darauf hingewiesen, dass der Begriff der FDA im FMG weiter

[40] So explizit EJPD, VÜPF/VD-ÜPF Erläuternder Bericht, 4, mit Verweis auf BGer 2C_544/2020 v. 29.4.2021.

gefasst wird als im BÜPF.[41] Im FMG werden OTT-Dienste explizit als Anwendungsfall der FDA erwähnt, während dieselben in der Botschaft zum BÜPF den AAKD zugewiesen werden.[42] Entsprechend ist der Begriff des Fernmeldedienstes vom Verständnis im Fernmelderecht zu lösen.[43]

Ein Fernmeldedienst widmet sich gemäss Art. 3 lit. b FMG der «fernmeldetechnischen Übertragung von Informationen für Dritte», wobei gemäss lit. c derselben Bestimmung eine fernmeldetechnische Übertragung ein «elektrisches, magnetisches, optisches oder anderes elektromagnetisches Senden oder Empfangen von Informationen über Leitungen oder Funk» ist. Da der Verweis auf das FMG nunmehr wegfällt, kann sich die überwachungsrechtliche Definition des Fernmeldedienstes aber nicht mehr auf diese Gesetzesumschreibungen stützen. Dem delegierten Auftrag zur genaueren Umschreibung möchte der Bundesrat deshalb mit dem neuen Art. 16a nVÜPF begegnen. Es soll – im Einklang mit der ergangenen bundesgerichtlichen Rechtsprechung – normiert werden, dass nur als FDA gilt, wer einen ***Zugangsdienst*** betreibt, nicht jedoch wer bloss Informationen übermittelt.[44] Art. 16 Abs. 1 nVÜPF hält in diesem Sinne fest, dass ein Fernmeldedienst ist, wer ein öffentliches Fernmeldenetz betreibt (lit. a) oder wer einen direkten Zugangsdienst zu einem öffentlichen Fernmeldenetz (wie das Internet) (lit. b), öffentlichen Mobilfunkdienst (lit. c) oder öffentlichen Telefondienst (zusammen mit dem Netzzugang) (lit. d) für Dritte anbietet. Das Bundesgericht hatte im Rahmen der grammatikalischen Auslegung festgehalten, dass sich OTT-Dienste gerade dadurch kennzeichnen, dass die Kundschaft den Internetzugang separat dazukaufen muss.[45] Das Urteil hielt fest, dass das blosse Einspeisen von Signalen für ihre Nutzer:innen zum Zwecke der Informationsübertragung wie bei Messaging-Diensten nicht ausreiche, um von einer Informationsübermittlung für Dritte i.S.v. Art. 3 lit. b FMG sprechen zu können.[46] Kernelement der FDA-Definition ist folglich, dass es sich um Dienste handelt, die den *Zugang* gewähren.

In Art. 16a Abs. 2 lit. a nVÜPF wird weiter klargestellt, dass nicht als FDA gilt, wer nur Informationen überträgt, «die für die Allgemeinheit bestimmt sind». Diese ***Ausnahme*** betrifft namentlich «Massenmedien». Gemäss Bundesrat sind sie für die Fernmeldeüberwachung nicht von Belang, da hier kein Fernmeldegeheimnis besteht.[47] Die Reichweite des Fernmeldegeheimnisses ist insbesondere hinsichtlich des praxisrelevanten Anwendungsfalls der Internetüberwachung nicht restlos geklärt (→ dazu ausführlicher Kap. 3.4.1). Wird das Fernmeldegeheimnis indes weiterhin (überzeugend) als Kommunikationsgeheimnis im engeren Sinne verstanden und erstreckt sich der Anwendungsbereich der Art. 269 ff. StPO und des BÜPF folglich nicht auf «allgemeine Internetüberwachungen», ist diese Einschränkung in der revidierten VÜPF auf *nicht allgemein einsehbare Kommunikation zwischen Menschen* sinnvoll.

[41] Botschaft FMG, 6660.

[42] Botschaft FMG, 6660.

[43] EJPD, VÜPF/VD-ÜPF Erläuternder Bericht, 4.

[44] EJPD, VÜPF/VD-ÜPF Erläuternder Bericht, 4.

[45] BGer 2C_544/2020 v. 29.4.2021, E. 4.2.

[46] BGer 2C_544/2020 v. 29.4.2021, E. 4.2.

[47] EJPD, VÜPF/VD-ÜPF Erläuternder Bericht, 14.

3.3.2. FDA mit vollen und reduzierten Pflichten

Die FDA sollen weiterhin in die Kategorie der «FDA mit reduzierten Pflichten» und die «FDA mit vollen Pflichten» unterteilt werden.[48] Die Unterteilung entspricht im Grundsatz dem bisherigen Recht, d.h. es gibt weiterhin die «regulären FDA» und solche, die aufgrund gewisser Kriterien von gewissen Pflichten befreit werden können. Allerdings sollen die Kriterien für die Klassifikation angepasst werden. Standardmässig haben FDA die vollen Pflichten. Hier stellt sich also – anders als bei den AAKD (sogleich → Kap. 3.4.2) – nicht die Frage des «Upgrades», sondern der Herunterstufung.

Gemäss Art. 16b nVÜPF haben FDA ein Gesuch an den Dienst ÜPF zu stellen, um als ***FDA mit reduzierten Pflichten*** eingestuft zu werden. Voraussetzung für eine solche Herunterstufung ist, dass die FDA entweder ihre Dienste nur im Bereich Bildung und Forschung anbietet (Abs. 1 lit. a) oder gewisse Schwellenwerte nicht erreicht werden (Abs. 1 lit. b). Als Schwellenwerte definiert die nVÜPF, dass die FDA entweder (1.) unter Berücksichtigung aller angebotenen Fernmelde- und abgeleiteten Kommunikationsdienste weniger als 10 Überwachungsaufträge in den letzten 12 Monaten empfing oder die FDA (2.) über einen schweizweiten Jahresumsatz des gesamten Unternehmens von weniger als 100 Mio. Franken in den beiden vorhergehenden Geschäftsjahren verfügte. Im geltenden Recht (Art. 51 VÜPF) war betreffend die erste Variante nicht weiter präzisiert, ob Überwachungsaufträge pro Dienst oder für alle angebotenen Dienste zusammen massgeblich sind. Betreffend die zweite Variante war bis anhin ausschliesslich der Umsatz entscheidend, der mit Fernmelde- und abgeleiteten Kommunikationsdiensten erzielt wird, nicht jedoch der Gesamtumsatz des Unternehmens. Die Schwelle, um eine Herunterstufung zu erwirken, wird also höher angesetzt, können doch fortan Unternehmen, die z.B. 50 Mio. Umsatz mit Fernmelde- und Kommunikationsdiensten und 100 Mio. Gesamtumsatz erwirtschaften, nicht mehr von einer Herunterstufung profitieren. Dies dürfte jedoch von bescheidener Praxisrelevanz sein, da Dienste mit einem derartigen Umsatz i.d.R. die Schwelle von 10 Überwachungsaufträgen überschreiten dürften.

Die ***Delegationsnorm in Art. 26 Abs. 6 BÜPF*** ermächtigt den Bundesrat zu Herunterstufungen von FDA in Bezug auf die Überwachungspflichten «insbesondere wenn sie Dienstleistungen von geringer wirtschaftlicher Bedeutung oder im Bildungsbereich anbieten». Das «insbesondere» verdeutlicht dabei, dass es sich nicht um eine abschliessende Aufzählung handelt. Das BÜPF lässt also grundsätzlich Raum für andere Kriterien, wobei der Bundesrat sich am Telos der Bestimmung zu orientieren hat, kleinere Anbieterinnen zu entlasten. Die Verweigerung der Herunterstufung auf Grundlage einer hohen «Überwachungsrelevanz» scheint demnach gestützt auf diese nicht abschliessende gesetzliche Aufzählung naheliegend und zulässig (anderes gilt bei der Hochstufung der AAKD im heutigen Recht, siehe → Kap. 3.4.2).

Die gesetzliche Formulierung der «***Dienstleistungen von geringer wirtschaftlicher Bedeutung***» in Art. 26 Abs. 6 BÜPF wirft dagegen die Frage auf, ob das Abstellen auf den unternehmerischen Gesamtumsatz noch im Einklang mit der Gesetzesbestimmung steht. Der Gesetzestext ist so zu verstehen, dass es um «Anbieterinnen von Fernmeldediensten» geht, die «Dienstleistungen von geringer wirtschaftlicher Bedeutung» anbieten. Daraus erschliesst sich, dass die Relevanz der

[48] EJPD, VÜPF/VD-ÜPF Erläuternder Bericht, 11.

entsprechenden Dienstleitungen, also die für das BÜPF relevanten Diensteangebote, massgeblich sein muss. Eine anderweitige Auslegung, der Einbezug also von anderen Dienstleistungen, umgeht diese Einschränkung. Beispielsweise könnte ein grosses Unternehmen mit einem angebotenen Fernmeldedienst von völlig marginaler Relevanz von vornherein keine Herunterstufung beantragen, auch wenn die für die Überwachung massgebliche Dienstleistungen wirtschaftlich unbedeutend sind. Die Anbieterin würde über die vollen Pflichten verfügen, samt etwa der automatisierten Auskunftserteilung, und dem damit entsprechend verbundenen grossen Aufwand. Das widerspricht dem erwähnten Telos des Vorbehalts. Ebenso widerspricht es der historischen Auslegung, hat der Bundesrat diese Privilegierung doch für Dienste vorgesehen, bei denen von vornherein anzunehmen ist, dass sie nicht im Besitz von Daten sind, die für eine Überwachung des Fernmeldeverkehrs von Interesse sind – insbesondere aufgrund der beschränkten Zahl von Kund:innen, welche den Dienst nutzen.[49] Es ging also um das «Überwachungsinteresse» am spezifischen Dienst, nicht am Gesamtunternehmen. Bei diesem Aspekt handelt es sich folglich nicht mehr um eine reine Konkretisierung des Gesetzestextes. Er steht in einem Widerspruch zum Gesetz. *Dass der gesamte Jahresumsatz des Unternehmens massgeblich sein soll, ist konsequenterweise als unrechtmässig zu beurteilen.*

3.4. Kategorien der AAKD

3.4.1. Begriff des abgeleiteten Kommunikationsdienstes

Art. 2 lit. c BÜPF bzw. Art. 2 Abs. 1 lit. c nBÜPF erklärt das Gesetz anwendbar für «Anbieterinnen von Diensten, die sich auf Fernmeldedienste stützen und eine Einweg- oder Mehrwegkommunikation ermöglichen (Anbieterinnen abgeleiteter Kommunikationsdienste)». Anders als bei den FDA werden bei AAKD Kommunikationsdienste ***unabhängig vom eigentlichen Netzzugang*** erbracht.[50] AAKD übernehmen keine Verantwortung für die fernmeldetechnische Übertragung,[51] hingegen für das Ermöglichen der Kommunikation zwischen Nutzer:innen.[52] Anbieterinnen von OTT-Diensten fallen deshalb mehrheitlich, nicht jedoch vollständig in den Geltungsbereich des BÜPF – womit dieser weniger weitgehend ist, als Gesetze, welche die Internetüberwachung im Allgemeinen adressieren (wie z.B. die E-Evidence-Verordnung der EU[53], vgl. → Kap. 4.6.4). Entscheidendes Abgrenzungskriterium, damit eine Anbieterin als AAKD qualifiziert, ist erstens, ob sie ***Kommunikation (initial) «ermöglicht»*** oder lediglich «erleichtert».[54] Bietet eine Anbieterin ausschliesslich ein Verschlüsselungsprodukt für einen Messenger-Dienst an, so fällt diese im Gegensatz zum Messenger-Dienst, der die Ermöglichung der Kommunikation verantwortet, nicht in diese Kategorie.[55] Zweitens ist relevant, ob die ermöglichte Kommunikation überhaupt unter das ***Fernmeldegeheimnis*** und damit in den Anwendungsbereich des BÜPF fällt. Was nicht Gegenstand

[49] Botschaft BÜPF, 2742.

[50] EJPD, VÜPF/VD-ÜPF Erläuternder Bericht, 9.

[51] EJPD, VÜPF/VD-ÜPF Erläuternder Bericht, 9.

[52] Botschaft BÜPF, 2708.

[53] Verordnung (EU) 2023/1543 des europäischen Parlaments und des Rates vom 12. Juli 2023 über europäische Herausgabeanordnungen und europäische Sicherungsanordnungen für elektronische Beweismittel in Strafverfahren und für die Vollstreckung von Freiheitsstrafen nach Strafverfahren.

[54] Botschaft BÜPF, 2708.

[55] Botschaft BÜPF, 2708.

einer Überwachung des Post- und Fernmeldeverkehrs sein kann (vgl. Art. 1 Abs. 1 BÜPF) ist von BÜPF und VÜPF auch nicht adressiert. Zu verneinen ist das gemäss Bundesrat etwa für Streaming Plattformen wie Youtube, Spotify oder Kommentarspalten in öffentlichen Medien.[56]

Bei ***sozialen Medien*** ist zu differenzieren: Stellt eine Anbieterin wie etwa Instagram einem/einer Nutzerin:in einen Kommunikationskanal für direkte private Nachrichten zur Verfügung, so gilt sie in Bezug auf diese von ihr erbrachte Leistung als AAKD. Anders sieht es mit Blick auf öffentliche Beiträge («Posts») und Kommentare aus, welche nicht dem Fernmeldegeheimnis unterliegen, da diese Informationen für die Allgemeinheit bestimmt sind (dazu schon → Kap. 3.3.1). Bei Posts von privaten Konten aus, d.h. mit einem vom/von der Absender:in abschliessend definierten Kreis an «Followern» oder «Freunden», ist dagegen auf Anhieb fraglich, ob diese Kommunikation als öffentlich oder als dem Fernmeldegeheimnis unterstehend zu qualifizieren ist. Allgemein wird davon ausgegangen, dass das «Kommunikationsgeheimnis» nur die «Kommunikation zwischen individualisierten Einzelpersonen, nicht aber jene mit einer nicht näher spezifizierten Allgemeinheit» schützt.[57] Bei gänzlich privaten Accounts (wie z.B. bekannt von bei TikTok) mit einer überschaubaren Anzahl vernetzter Personen dürfte von entsprechend individualisierter Kommunikation ausgegangen werden, nicht dagegen bei sehr grossen, nicht durch persönliche Beziehungen gekennzeichneten «Gefolgschaften» oder bei Netzwerken, die von vornherein keine eigentlich privaten Accounts vorsehen (wie z.B. bekannt von LinkedIn).

Um als AAKD zu qualifizieren, muss der angebotene Dienst (die entsprechend vertrauliche) «***Einweg- oder Mehrwegkommunikation*** ermöglichen» (Art. 2 lit. c BÜPF). Mit der Revision der VÜPF sollen neu Definitionen der Einweg- und Mehrwegkommunikation verankert werden. Gemäss Ziff. 1bis Anhang nVÜPF ist eine Einwegkommunikation eine «Kommunikation ohne Rückkanal (Antwortmöglichkeit), z.B. das Hochladen eines Dokumentes». Gemäss Ziff. 1ter Anhang nVÜPF ist Mehrwegkommunikation dagegen «Kommunikation mit Rückkanal (Antwortmöglichkeit) zwischen zwei oder mehreren Benutzerinnen oder Benutzern, z. B. Mitteilungsdienste (Instant Messaging)». Als Beispiele von Angeboten der Mehrwegkommunikation erwähnt der Bundesrat Messenger-Dienste, E-Mail-Dienste, Plattformen für den Dokumentenaustausch zwischen Personen, Internettelefondienste oder VPN- und Proxy-Dienste.[58] Als Einwegkommunikation sollen insbesondere Cloud- oder Hosting-Angebote ohne zugehörige Kommunikationsdienste verstanden werden.[59]

Betreffend diese im Anhang zur nVÜPF vorgesehenen Definitionen scheint vor allem fraglich, inwiefern so verstandene Einwegkommunikation überhaupt Kommunikation erfasst, welche dem Fernmeldegeheimnis und folglich dem BÜPF untersteht. Das Begriffsverständnis der «Einwegkommunikation» hat demnach direkte Konsequenzen für die Abgrenzung des Begriffs der abgeleiteten Kommunikationsdienste. Das lässt sich besonders deutlich an der Qualifikation von ***Cloud-Speicherdiensten*** aufzeigen: Der Bundesrat ging bereits in der Botschaft zum neuen BÜPF davon aus, dass Cloud-Dienste erfasst sein können.[60] Im erläuternden Bericht zur aktuellen

[56] EJPD, VÜPF/VD-ÜPF Erläuternder Bericht, 10.

[57] BSK BV-DIGGELMANN/ELMER Art. 13 N 29 mit Verweis auf PETERS/ALTWICKER, § 30 Ziff 1.

[58] EJPD, VÜPF/VD-ÜPF Erläuternder Bericht, 19.

[59] Vgl. EJPD, VÜPF/VD-ÜPF Erläuternder Bericht, 21.

[60] Botschaft BÜPF, 2708; so in der Folge auch HANSJAKOB, 381.

Revision der VÜPF führt er aus, es handle sich bei derartigen Diensten um solche, deren Hauptfunktion im Speichern von Dateien besteht. Die «Kommunikationsmöglichkeit» bestehe über das Teilen der abgelegten Dateien oder die verteilte Bearbeitung von Inhalten.[61] Ausschlaggebend für die Qualifikation wäre konsequenterweise auch hier das Ermöglichen von Kommunikation, wofür gemäss Bundesrat bei Cloud-Speichern also bereits das Teilen von Dateien oder das gemeinsame Bearbeiten genügt.[62] HANSJAKOB versteht den Begriff weiter und spricht allgemein von «Anbieterinnen von Speicherplatz» oder «Hosting ohne Kommunikationsdienste».[63] In diesem weiten Sinne könnte auch die Definition im Anhang zur nVÜPF verstanden werden, wenn «Kommunikation ohne Rückkanal» meint, dass alle fernmeldetechnischen Übertragungen (auch einseitige Kommunikation zwischen einem Menschen und einer Applikation via Internet) erfasst sein sollen. Im Widerspruch dazu stehen die Ausführungen des erläuternden Berichts wie auch das herkömmliche Verständnis des Fernmeldegeheimnisses. Auf Letzteres ist abzustellen: Es kann richtigerweise nur in den Anwendungsbereich des BÜPF fallen, was eine Kommunikation betrifft, die dem Fernmeldegeheimnis unterliegt. Das Fernmeldegeheimnis nach Art. 13 Abs. 1 BV schützt den Kommunikationsvorgang *zwischen Menschen*.[64] Auch die geheimen Überwachungsmassnahmen der Art. 269 ff. StPO sind auf Zwangsmassnahmen ausgerichtet, die ins Fernmeldegeheimnis eingreifen. Ursprünglich fielen soziale Netzwerke wie Facebook als AAKD gemäss Bundesgericht gerade deshalb nicht unter die Vorschriften über die Fernmeldeüberwachung.[65] In der Tat sind auch unter dem neuem Recht AAKD nur von den Art. 269 ff. StPO i.V.m. dem BÜPF adressiert, sofern sie die Übermittlung von dem Fernmeldegeheimnis unterliegenden Informationen verantworten und sofern die Zwangsmassnahme im konkreten Fall die Erhebung solcher Kommunikationsinhalte betrifft.[66] Generelle Erhebungen von Inhalten, die zwar die Privatsphäre, nicht aber das Fernmeldegeheimnis berühren (also Art. 13 Abs. 2 und nicht Abs. 1 BV), sind weiterhin regulär über die Beschlagnahme bzw. Edition herauszuverlangen.

Entsprechend ist es konsequent, Cloud-Speicher und vergleichbare Angebote nur unter den Begriff des AAKD zu subsumieren, wenn sie eine ***Kommunikation zwischen Personen*** ermöglichen. Wählt sich jemand zwar durch die Nutzung eines Cloud-Speichers ins Internet ein, kann er dabei aber keinerlei Kommunikation mit anderen Nutzer:innen aufnehmen – weder synchron noch asynchron –[67], handelt es sich zwar um eine fernmeldetechnische Übertragung, nicht jedoch um einen Kommunikationsvorgang im Sinne des Fernmeldegeheimnisses. Ansonsten wäre jede Internetnutzung (auch ein Streaming oder der blosse Besuch einer öffentlichen Webseite) bereits ein Anwendungsfall des BÜPF. Das BÜPF sowie Art. 269 ff. StPO erfassen heute und primär historisch bedingt jedoch nicht die allgemeine Internetüberwachung im Sinne von Verhaltensüberwachung, sondern explizit die Überwachung von Kommunikation. Eigentliche Einwegkommunikation im engeren Sinne wäre diesfalls aber auch nicht ausreichend für die Qualifikation als AAKD. Zur Einwegkommunikation muss – wie der Bundesrat mit dem Erfordernis der

[61] EJPD, VÜPF/VD-ÜPF Erläuternder Bericht, 20.

[62] EJPD, VÜPF/VD-ÜPF Erläuternder Bericht, 20.

[63] HANSJAKOB, 316.

[64] Siehe z.B. BGer 1B_251/2017 v. 21.2.2018, E. 6.6., das festhält, dass bei IMSI-Catchern nur technische Geräte miteinander «kommunizierten», weshalb zwar die Privatsphäre, nicht jedoch das Fernmeldegeheimnis betroffen ist.

[65] BGE 143 IV 270, E. 7.1.; BGE 143 IV 21, E. 3.1.

[66] Siehe dazu schon SIMMLER, 135.

[67] Vgl. Botschaft BÜPF, 2708.

«Kommunikationsmöglichkeit»[68] einräumt – hinzutreten, dass im Rahmen des entsprechenden Dienstes auch Mehrwegkommunikation zumindest theoretisch ermöglicht würde (wie z.B. bei Google Docs oder Onedrive). Die Definition in der nVÜPF könnte hier irreführend sein und den Begriff des AAKD in der Konsequenz verwässern. Folglich sind aber auch die vom Bundesrat in der Botschaft explizit genannten Beispiele von Streaming-Angeboten[69] nur bedingt geeignet. Da sie zumeist auch über Kommunikationsfunktionen verfügen, die private Kommunikation (wenn ggf. auch nur am Rande) ermöglichen, wären sie zumindest für diesen Bereich der privaten Kommunikation als AAKD zu klassifizieren.

3.4.2. AAKD mit vollen, reduzierten und minimalen Pflichten

Als nicht ursprüngliche Hauptadressatinnen der Post- und Fernmeldeüberwachung werden den AAKD im Vergleich zu den FDA durch das BÜPF grundsätzlich weniger weitgehende Mitwirkungspflichten auferlegt (im Detail → Kap. 4.2.1). Allerdings räumen dem Bundesrat Art. 22 Abs. 4 BÜPF für die Auskunftspflichten bei Cyberdelinquenz und Bedrohungen der inneren Sicherheit und Art. 27 Abs. 3 BÜPF für die Überwachungspflichten die Möglichkeit ein, AAKD, «die Dienstleistungen von grosser wirtschaftlicher Bedeutung oder für eine grosse Benutzerschaft anbieten» betreffend Pflichtenkatalog den FDA ganz oder teilweise gleichzustellen. Es gibt also die ***Möglichkeit einer Hochstufung*** bzw. eines «Upgrades». Im Gegensatz zur Formulierung bei den FDA mit reduzierten Pflichten (soeben → Kap. 3.3.2) enthält der Wortlaut der Delegationsnorm bei den AAKD kein «insbesondere». Es handelt sich bei den Kriterien der «grossen wirtschaftlichen Bedeutung» oder «grossen Benutzerschaft» um einen abschliessenden Kriterienkatalog, was überzeugt, da eine weitergehende Verpflichtung gestützt auf eine unbestimmte Gesetzesdelegation ungleich heikler wäre als eine Pflichtenbefreiung.

Gemäss Art. 22 der geltenden VÜPF erklärt der Dienst ÜPF eine AAKD als den ***weitergehenden Auskunftspflichten*** nach Art. 22 Abs. 4 BÜPF unterstellt, wenn sie entweder 100 Auskunftsgesuche in den letzten 12 Monaten zu bearbeiten hatte (lit. b) oder *alternativ*, wenn sie einen Jahresumsatz von 100 Mio. Franken in zwei aufeinander folgenden Geschäftsjahren erzielte, wobei ein grosser Teil ihrer Geschäftstätigkeit im Anbieten abgeleiteter Kommunikationsdienste besteht, *und* ihre Dienste von mindestens 5000 Teilnehmenden in Anspruch genommen werden (lit. b). ***Weitergehende Überwachungspflichten*** können AAKD gemäss Art. 52 VÜPF ebenfalls aufgrund der Anzahl an Überwachungsaufträgen (mindestens 10 in den letzten 12 Monaten) (lit. a) *oder* aufgrund des Umsatzes (100 Mio. Franken in zwei aufeinander folgenden Geschäftsjahren bei primärer Geschäftstätigkeit im entsprechenden Feld) *und* der Teilnehmerzahl von mindestens 5000 (lit. b) auferlegt werden. De lege lata gibt es also «reguläre» AAKD sowie AAKD mit weitergehenden Auskunfts- und/oder Überwachungspflichten.

Bereits betreffend die geltende Rechtslage ist die Frage aufzuwerfen, inwiefern das Abstellen auf die «***Auskunfts- bzw. Überwachungsrelevanz***», d.h. auf die Anzahl Auskunfts- oder Überwachungsaufträge, im Einklang mit dem Wortlaut des Gesetzes («grosse wirtschaftliche Bedeutung» oder «grosse Benutzerschaft») steht. Das BÜPF ermächtigt den Bundesrat zu Upgrades von AAKD, die von wirtschaftlich hoher Relevanz sind oder deren Nutzung besonders verbreitet ist.

---

[68] Botschaft BÜPF, 2708.

[69] Vgl. EJPD, VÜPF/VD-ÜPF Erläuternder Bericht, 10.

Der Katalog ist, wie erwähnt, abschliessend. Ein Abstellen auf die Bedeutung der AAKD aus Sicht der Behörden mag aus Praktikabilitätsgründen legitim erscheinen, können diese AAKD doch bei den Aufträgen vereinfachten Verfahren unterstellt werden. Es steht aber nicht im Einklang mit dem Gesetzestext und ist deshalb nicht rechtmässig. Gemäss Aussagen eines Vertreters des Dienstes ÜPF hat die Schweiz heute allerdings keine Unternehmen, die gestützt auf die VÜPF zu AAKD mit erweiterten Pflichten hochgestuft wurden.[70] Das Kriterium war deshalb nie von praktischer Bedeutung und wurde folglich keiner gerichtlichen Überprüfung unterzogen. Da das Kriterium der Anzahl von Aufträgen de lege ferenda aufgegeben werden soll, erübrigt sich die Frage zudem. Sie mag für die politische Diskussion von Belang sein, da Anbieterinnen wie Threema und ProtonMail zwar allenfalls gestützt auf den Gesetzestext des BÜPF, nicht jedoch gestützt auf die heute geltende VÜPF rechtmässig hätten hochgestuft werden können. ProtonMail hat zwar über 100 Mio. Teilnehmende weltweit,[71] es mangelt dem AAKD allerdings am verlangten Umsatzerfordernis[72]. Gleiches gilt für die Anbieterin Threema, die zwar über etwa 11 Mio. Teilnehmende verfügt,[73] jedoch bei Weitem keinen Jahresumsatz von 100 Mio. aufweist[74].

Der Bundesrat beabsichtigt nun, mit der Revision eine ***weitere Präzisierung der Kategorien der AAKD*** vorzunehmen.[75] Art. 16d Abs. 1 nVÜPF soll dabei zunächst im Einklang mit dem BÜPF und den ergangenen Urteilen festhalten, dass als AAKD gilt, «wer für Dritte einen Einweg- oder Mehrwegkommunikationsdienst oder einen indirekten Zugangsdienst zu einem öffentlichen Fernmeldenetz erbringt, der unabhängig vom Netzzugangsdienst funktioniert». Gemäss Abs. 2 derselben Bestimmung gilt nicht als AAKD, wer Dienste anbietet, die aufgrund ihrer Öffentlichkeit gemäss dem bisherigen Verständnis gar nicht dem Fernmeldegeheimnis unterstehen, da sie an die Allgemeinheit gerichtet sind (i.S.v. Art. 16a Abs. 2 lit. a nVÜPF).

Der Bundesrat möchte mit der Revision des VÜPF nun aber eine Neukategorisierung der AAKD vornehmen. Die bisherige Zweiteilung wird aufgegeben und durch eine ***Dreiteilung*** ersetzt. Unterschieden werden sollen AAKD mit vollen Pflichten, solche mit reduzierten Pflichten und solche mit minimalen Pflichten. Er verspricht sich dadurch «eine ausgewogene und dem Grundsatz der Verhältnismässigkeit besser entsprechende Abstufung der Verpflichtungen».[76] Standardmässig hätte eine AAKD «minimale Pflichten». Den Kriterien der Hochstufung auf die «reduzierten Pflichten» nimmt sich Art. 16f nVÜPF an – wobei die Terminologie etwas irreführend ist, da diese reduzierten Pflichten für AAKD eigentlich erweiterte Pflichten i.S.v. Art. 22 und 27 BÜPF darstellen. Art. 16g nVÜPF nimmt sich den Voraussetzungen an, damit AAKD zu solchen «mit vollen

---

[70] dnip v. 13.3.2024, <https://dnip.ch/2024/03/13/800-schweizer-unternehmen-haetten-weniger-ueberwachungspflichten-wenn-sie-davon-wuessten/#Es-gibt-keine-hochgestuften-AAKDs-in-der-Schweiz> (Abruf: 1.11.2025).

[71] ProtonMail, <https://proton.me/de/mail> (Abruf: 1.11.2025).

[72] Der Umsatz wurde im Jahr 2020 auf ca. 30 Mio. geschätzt, siehe NZZ v. 18.4.2020, <https://www.nzz.ch/wirtschaft/protonmail-aus-genf-erfolg-mit-verschluesselter-kommunikation-ld.1792350> (Abruf: 1.11.2025).

[73] Threema, <https://threema.com/de/why-threema> (Abruf: 1.11.2025).

[74] Der Umsatz wird unterschiedlich geschätzt, teilweise ist die Rede von ca. 11 Mio. (im Jahr 2022), siehe SRF v. 14.12.2022, <https://www.srf.ch/news/wirtschaft/10-jahre-threema-threema-gruender-unsere-daten-gehen-niemanden-etwas-an> (Abruf: 1.11.2025); teilweise von ca. 60 Mio. (im Jahr 2021), siehe Bilanz v. 5.4.2021, <https://www.bilanz.ch/bilanz/warum-threema-anders-ist-als-die-andern-336336> (Abruf: 1.11.2025).

[75] EJPD, VÜPF/VD-ÜPF Erläuternder Bericht, 19.

[76] EJPD, VÜPF/VD-ÜPF Erläuternder Bericht, 3.

Pflichten» heraufgestuft werden können – wobei diese Terminologie ebenso verwirrlich sein könnte, da doch noch Differenzen zu den FDA mit vollen Pflichten bestehen (dazu unten → Kap. 4.1. und → Kap. 4.2).

Gemäss der vorgeschlagenen Revision gelten als ***AAKD mit reduzierten Pflichten*** Anbieterinnen, wenn sie im Durchschnitt der letzten 12 Monate für alle ihre angebotenen Kommunikationsdienste mehr als 5000 Teilnehmende haben (nicht aber zugleich als AAKD mit vollen Pflichten qualifizieren). Gemäss Bundesrat ist diese Kategorie – mit gewissen Abweichungen, die sich aus der Natur der angebotenen Dienste ergeben – mit derjenigen der FDA mit reduzierten Pflichten vergleichbar.[77] Als Teilnehmende gelten im Falle von Diensten, die keinen Vertrag oder Zugangsmittel erfordern, die aktiven Nutzer:innen («Unique User») pro Monat.[78]

Wie bereits betont, erhält der Bundesrat im BÜPF die Kompetenz, eine Hochstufung von AAKD zu veranlassen, wenn sie von ***grosser wirtschaftlicher Bedeutung*** sind oder über eine ***grosse Nutzerschaft*** verfügen. Gestützt auf Art. 16f nVÜPF soll die Schwelle für eine teilweise Hochstufung nicht zum vollen, aber doch einem erweiterten Pflichtenkatalog (zu den Pflichten → Kap. 3.4.2) bei 5000 Teilnehmenden angesetzt werden. Es scheint offenkundig, dass 5000 Teilnehmende einen OTT-Dienst noch nicht als dermassen praxisrelevant erscheinen lassen, dass von einer grossen Benutzerschaft im Sinne der *ratio legis* der BÜPF-Delegation gesprochen werden kann. Eine Hochstufung bewegt sich in den Schranken der Gesetzesdelegation und ist zudem mit Blick auf die Pflichten verhältnismässig, wenn die Anbieterin von einer gewissen erhöhten Verbreitung und folglich von Relevanz für die Fernmeldeüberwachung ist. Das ist bei 5000 Teilnehmenden nicht zu bejahen. Allfällige Kundenplattformen bzw. -applikationen kleinerer und mittlerer Unternehmen würden diese Schwelle wahrscheinlich rasch überschreiten, ebenso kleinere Hosting-Provider (z.B. beim Filesharing) mit Kommunikationsfunktion sowie auch Intranets oder Foren von Vereinen. Setzt man die Zahl ins Verhältnis zu tatsächlich weit bekannten Anbieterinnen wie die genannten Threema oder ProtonMail, deren Nutzerzahlen mehrere Millionen betragen, unterstützt dass die Annahme, dass bei 5000 nicht von einer «grossen Benutzerschaft» gesprochen werden kann. Zudem müssen diese 5000 gemäss vorgeschlagenen Verordnungswortlaut nicht auf die Schweiz beschränkt sein. Eine Anbieterin mit einem Schweizer Nutzer und 4999 Teilnehmenden aus Deutschland wäre bereits von dieser Hochstufung betroffen. *Dies ist nicht nur als nicht verhältnismässig zu qualifizieren, sondern darüber hinaus nicht mehr vom Gesetzeswortlaut und folglich der delegierten Kompetenz umfasst. Die vorgeschlagene Definition dieser Schwelle ist folglich nicht rechtmässig.*

Des Weiteren sei darauf hingewiesen, dass die AAKD mit erweiterten, d.h. (in neuer Terminologie) reduzierten oder vollen Pflichten gemäss Art. 16e Abs. 2 nVÜPF dem Dienst ÜPF innerhalb von drei Monaten nach Erreichen des entsprechenden Schwellenwerts ***proaktiv melden müssen***, wenn sie die Voraussetzungen für eine Hochstufung erfüllen. In Anbetracht der hohen Komplexität der Materie ist es mindestens als fragwürdig zu bewerten, wenn nicht gar als unverhältnismässig, dass AAKD mit nur 5000 Teilnehmenden gänzlich eigenständig merken müssen, dass sie die Voraussetzungen der entsprechenden Verordnungsbestimmungen erfüllen und ansonsten Konsequenzen drohen, die von aufsichtsrechtlichen Massnahmen, über die Kostenbeteiligung bis

[77] EJPD, VÜPF/VD-ÜPF Erläuternder Bericht, 21.

[78] EJPD, VÜPF/VD-ÜPF Erläuternder Bericht, 24.

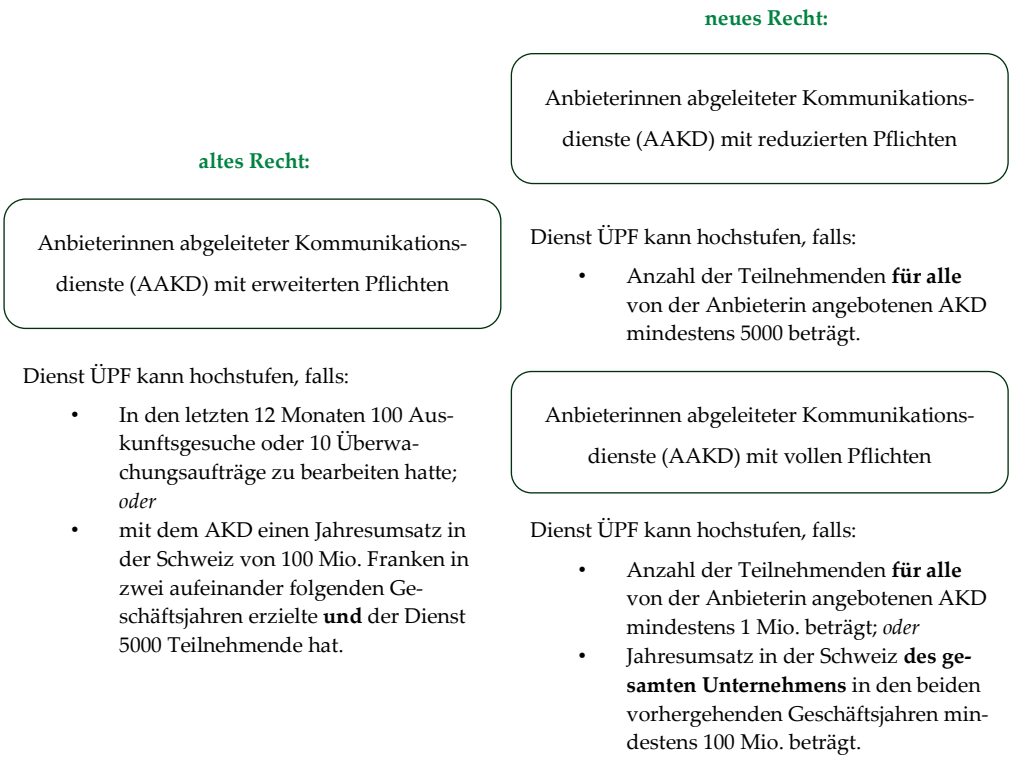
hin zu Bussen reichen.[79] Da eine Vielzahl nicht professioneller Anbieterinnen die Kriterien erfüllen dürften, erscheint das als heikel.

AAKD mit vollen Pflichten wären gemäss Art. 16g Abs. 1 nVÜPF diejenigen, welche entweder im Durchschnitt der letzten 12 Monate über 1 Million Teilnehmende hatten (lit. a) *oder* solche, bei denen der schweizweite Jahresumsatz des gesamten Unternehmens in den beiden vorhergehenden Geschäftsjahren mindestens 100 Mio. Franken betrug (lit. b). Diese Definition soll folglich zwei Änderungen erfahren: Einerseits soll auch hier der Umsatz des gesamten Unternehmens als massgeblich für den Schwellenwert sein. Die Präzisierung im alten Recht, dass ein grosser Teil der Geschäftstätigkeit im Anbieten abgeleiteter Kommunikationsdienste besteht (Art. 22 Abs. 1 lit. b VÜPF) würde weggelassen. Nunmehr ist die Rede vom Jahresumsatz in der Schweiz «des gesamten Unternehmens» (Art. 16g Abs. 1 lit. b nVÜPF). Andererseits sind (als alternativer Hochstufungsgrund) nicht mehr die Anzahl Auskunftsgesuche oder Überwachungsaufträge relevant, sondern die Anzahl Teilnehmende. Bei Umsatz und Teilnehmerzahl würde es sich zudem neu um alternative Voraussetzungen handeln. Um beispielhaft die bereits erwähnten Anbieterinnen Threema und ProtonMail anzuführen, wären diese also neu aufgrund der Anzahl Teilnehmende nach Art. 16g Abs. 1 lit. a nVÜPF als AAKD mit vollen Pflichten einzustufen.

Die Massgeblicherklärung der Anzahl von Teilnehmenden sowie des grossen Umsatzes steht grundsätzlich im Einklang mit der Gesetzesformulierung, dass Dienstleistungen «von grosser wirtschaftlicher Relevanz oder für eine grosse Benutzerschaft» (Art. 22 Abs. 4 und Art. 27 Abs. 3 BÜPF) erweiterten Pflichten unterstellt werden können. Anders als bei den soeben diskutierten AAKD mit reduzierten Pflichten sind die Schwellen von 1 Mio. Teilnehmenden oder 100 Mio. Umsatz im Allgemeinen geeignet, Akteure von einer gewissen Relevanz zu erfassen. Strittig sind dagegen das Abstellen auf die Anzahl Teilnehmenden für «***alle von der Anbieterin angebotenen abgeleiteten Kommunikationsdienste***» und den «***Jahresumsatz in der Schweiz des gesamten Unternehmens***» in Art. 16 g Abs. 1 nVÜPF. Art. 22 Abs. 4 und Art. 27 Abs. 3 BÜPF wählen die Formulierungen, dass es um AAKD geht, «die Dienstleistungen von grosser wirtschaftlicher Bedeutung oder für eine grosse Benutzerschaft anbieten». Wie bereits für die FDA festgehalten (→ Kap. 3.3.2), ergibt sich zwar nicht aus einer engen grammatikalischen, doch aber klar aus einer teleologischen Auslegung, dass das BÜPF Anbieterinnen anvisieren will, die betreffend den vom Gesetz anvisierten Gegenstand, d.h. der Überwachung des Post- und Fernmeldeverkehrs von einer hohen Relevanz sind, nicht jedoch solche, die einfach ganz generell relevant sind. Ein grosser Detailhändler, der einen sehr kleinen Kommunikationsdienst betreibt, würde nach der vorgeschlagenen Definition unter die vollen Pflichten fallen. Das wäre – mit Blick auf die massgebliche Dienstleistung – nicht verhältnismässig. Entsprechend haben die Kommunikationsdienste massgeblich zu sein. Die Formulierung von Art. 16g Abs. 1 lit. a nVÜPF, dass die Teilnehmendenzahl alle von der Anbieterin angebotenen Kommunikationsdienste betrifft, ist folglich vom Wortlaut gedeckt, nicht jedoch das Abstellen auf den Umsatz des Gesamtunternehmens. *Der vorgeschlagene Art. 16g Abs. 1 lit. b nVÜPF steht also nicht im Einklang mit dem Gesetz.*

[79] Vgl. EJPD, VÜPF/VD-ÜPF Erläuternder Bericht, 23 f.

Abbildung 4: Gegenüberstellung der Hochstufung nach geltendem und vorgeschlagenem Recht



4. Änderung der Mitwirkungspflichten

4.1. Pflichten der FDA

4.1.1. Heutige Regelung

FDA haben gestützt auf das BÜPF verschiedene Auskünfte zu erbringen und Überwachungen zu ermöglichen. Sie sind gemäss Art. 21 BÜPF zunächst (1.) insofern mitwirkungspflichtig, als dass sie Auskünfte über die Teilnehmenden (mindestens Name, Geburtsdatum und Adresse) (lit. a), Adressierungselemente gemäss Art. 3 lit. f FMG (d.h. die «Informationen zur Identifikation von Personen, Computerprozessen, Maschinen, Geräten oder Fernmeldeanlagen, die an einem fernmeldetechnischen Kommunikationsvorgang beteiligt sind») (lit. b), die Arten der Dienste (lit. c), weitere vom Bundesrat bezeichnete Daten administrativer oder technischer Natur sowie zur Identifikation von Personen (lit. d) erteilen müssen. Liegt kein Abonnementsverhältnis vor, müssen FDA zusätzlich die Person identifizieren, welche das für den Zugang zum Dienst erforderliche Mittel abgegeben hat (lit. e). Im Wesentlichen sind FDA demzufolge verpflichtet, stets die Teilnehmeridentifikation, d.h. ***Auskünfte betreffend Bestandesdaten*** (vgl. → Kap. 2) gestützt auf den Katalog an Informationen zu ermöglichen**.** Gemäss Art. 21 Abs. 2 BÜPF müssen FDA mit vollen Pflichten, d.h. ohne Herunterstufung (→ Kap. 3.3.2), diese spezifischen Informationen während der Dauer der Kundenbeziehung sowie 6 Monate nach deren Beendigung liefern können.

Art. 22 BÜPF sieht darüber hinaus bei ***Cyberdelikten im weiteren Sinne***, d.h. Delikten, die «über das Internet» begangen wurden, oder bei der Identifikation von Personen, welche ***die innere oder äussere Sicherheit*** bedrohen, eine umfassende Pflicht zur Lieferung der Daten vor, welche die Teilnehmeridentifikation ermöglichen. FDA müssen diesfalls alle vorhandenen Bestandesdaten liefern, welche die Identifikation der Täterschaft ermöglichen könnten (Art. 22 Abs. 1 BÜPF). Das Gesetz delegiert dem Bundesrat, weiter festzumachen, welche Angaben davon FDA während der Dauer der Kundenbeziehung sowie 6 Monate darüber hinaus aufbewahren und liefern müssen (Art. 22 Abs. 2 BÜPF). Er kann also die Pflicht zur Vorratsdatenspeicherung um diese zusätzlichen Bestandesdaten erweitern. Als Beispiel nennt die Botschaft einzig die Herausgabe des Namens, der einer spezifischen (bereits bekannten) IP-Adresse zugewiesen wurde.[80] Welche Daten von Art. 22 BÜPF genau umfasst sind, d.h. die Auslegung der Kategorie der Bestandesdaten sowie die Natur dieser Bestimmung, ist teilweise strittig, was sich insbesondere an der Frage der Qualifikation von IP-Adressen niederschlägt (dazu → Kap. 4.6.4).

Gemäss Art. 22 BÜPF müssen FDA ferner «dem Dienst ***weitergehende Angaben liefern, über die sie verfügen***» (Art. 22 Abs. 2 BÜPF). In zeitlicher Hinsicht bedeutet dies, dass FDA auch diejenigen gespeicherten Daten liefern müssen, deren Erfassung länger als 6 Monate zurückliegt.[81] In sachlicher Hinsicht heisst es, dass die in der VÜPF vorgesehenen Auskunftstypen zwar abschliessend den Mindestkatalog an zu speichernden und zu liefernden Bestandesdaten definieren. Wenn Dienste darüber hinausgehend mehr speichern, sind sie aber auch bezüglich dieser die Teilnehmeridentifikation ermöglichender Zusatzinformationen herausgabepflichtig.

Betreffend die ***Modalitäten der Auskunftserteilung*** wird der Bundesrat weitgehend zum Erlass von Ausführungen ermächtigt (Art. 23 BÜPF). Insbesondere kann er FDA verpflichten, Bestandesdaten im Abrufverfahren zugänglich zu machen *(automatisierte Abfragen).* Des Weiteren müssen FDA dem Dienst ÜPF auf Verlangen *technische Informationen* liefern, die für eine Überwachungsanordnung notwendig sind (Art. 24 BÜPF) sowie über *Art und Merkmale der angebotenen Dienstleistungen* Auskunft erteilen (Art. 25 BÜPF).

Von diesen Bestandesdatenauskünften zu unterscheiden sind die Pflichten der Anbieterinnen betreffend die Überwachung und die ***Herausgabe von Rand- und Inhaltsdaten***. FDA sind verpflichtet, Inhalt und Randdaten des Fernmeldeverkehrs zu liefern (Art. 26 Abs. 1 BÜPF). In diesem Zusammenhang müssen sie zudem die Informationen liefern, die für die Durchführung der Überwachung notwendig sind, die Überwachung dulden, Zugang zu ihren Anlagen gewähren sowie von ihnen angebrachte Verschlüsselungen entfernen (Art. 26 Abs. 2 BÜPF). Es ist sowohl die Echtzeit- als auch die rückwirkende Überwachung möglich (Art. 26 Abs. 4 BÜPF). Randdaten müssen während 6 Monaten aufbewahrt werden *(Vorratsdatenspeicherung* → Kap. 4.4.1*)*. Auch bei den Inhalts- und Randdatenüberwachungen wird von den FDA eine permanente *«Überwachungsbereitschaft»* verlangt, d.h. sie müssen jederzeit in der Lage sein, die Massnahmen durchzuführen, wenn die Überwachungen standardisiert sind. Ob sie zu diesen standardisierten Auskünften und Überwachungen in der Lage sind, müssen sie zudem auf Verlangen des Dienstes ÜPF jederzeit auf eigene Kosten nachweisen können (Art. 31 Abs. 1 BÜPF).

---

[80] Botschaft BÜPF, 2736.

[81] HANSJAKOB, 449.

In Umsetzung dieser gesetzlichen Vorgaben regelt die heute geltende VÜPF u.a. die ***Umsetzung der Überwachungsmassnahmen*** (z.B. die Pikett-Regelung, Art. 10 f. VÜPF) und die Überprüfung der Auskunfts- und Überwachungsbereitschaft (Art. 31 ff. VÜPF). Ebenso hält sie fest, dass die Identifikation bei Mobilfunkdiensten mittels amtlicher Dokumente (Art. 20a VÜPF) und bei anderen FDA «mit geeigneten Mitteln» (Art. 19 VÜPF) erfolgen kann. Es ist ferner u.a. genauer präzisiert, welche Bestandesdaten auf Vorrat zu speichern sind (Art. 21 VÜPF). Art. 35 ff. VÜPF für die Auskünfte und Art. 54 ff. VÜPF für die Überwachungen sehen zudem die genauen standardisierten Typen vor, nach deren Muster die Auskünfte einzuholen und die Zwangsmassnahmen durchzuführen sind. FDA mit vollen Pflichten haben den Grossteil der Auskünfte automatisiert, d.h. über die Abfrageschnittstelle des Verarbeitungssystems des Dienstes ÜPF zu erbringen (Art. 18 VÜPF).

4.1.2. Vorgeschlagene Änderungen

Der ***Pflichtenkatalog der FDA*** bleibt von der vorgeschlagenen Revision im Grundsatz weitgehend unberührt (Abbildung 5). Voll verpflichtete FDA haben weiterhin umfassende Auskunfts- und Überwachungspflichten, betreffend Bestandes- und Randdaten zudem die Pflicht zur Vorratsdatenspeicherung. In Bezug auf die weiteren Modalitäten (automatisierte Erteilung der Auskünfte, Nachweise) bleiben sie voll verpflichtet. Art. 26 Abs. 2 lit. c BÜPF sah für FDA bereits vor, dass sie von ihnen angebrachte Verschlüsselungen entfernen müssen, weshalb sie de lege lata – anders als die AAKD (dazu → Kap. 4.2.1) – bereits eine entsprechende Mitwirkungspflicht haben. Betroffen sind sie aber durch die neuen Auskunfts- und Überwachungstypen (→ Kap. 4.6).

Für FDA mit reduzierten Pflichten ändert sich im Grundsatz ebenfalls nichts. Allerdings müssen sie aufgrund der vorgeschlagenen Präzisierung von Art. 31 Abs. 1 nVÜPF konsequenterweise nur den Nachweis der Auskunfts- nicht jedoch den der Überwachungsbereitschaft erbringen.

Abbildung 5: Gegenüberstellung Pflichten der FDA nach geltendem und vorgeschlagenem Recht

	FDA mit vollen Pflichten (VÜPF)	FDA mit reduzierten Pflichten (VÜPF)	FDA mit vollen Pflichten (nVÜPF)	FDA mit reduzierten Pflichten (nVÜPF)
Pikettpflicht	✓	×	✓	×
Automatisierte Erteilung bestimmter Auskünfte	✓	×	✓	×
Auskünfte über Abfrageschnittstelle	✓	×	✓	×
Vorratsdatenspeicherung Bestandesdaten	✓	✓	✓	✓
Vorratsdatenspeicherung Randdaten	✓	×	✓	×
Überwachungspflichten Inhalts- und Randdaten	✓	×	✓	×
Auskunftspflichten Bestandesdaten	✓	✓	✓	✓
Identifikationspflichten	✓	✓	✓	✓
Duldungspflichten Überwachung	✓	✓	✓	✓
Entfernung angebrachter Verschlüsselungen	✓	✓	✓	✓
Nachweis der Auskunfts- & Überwachungsbereitschaft	✓	✓	✓	(✓)

4.2. Pflichten der AAKD

4.2.1. Heutige Regelung

AAKD sind nach Art. 22 Abs. 3 BÜPF bei Cyberdelinquenzen sowie bei Bedrohungen der inneren und äusseren Sicherheit dazu verpflichtet, dem Dienst betreffend die Auskünfte zur Identifikation der Täterschaft «die ihnen vorliegenden Angaben, welche die Identifikation ermöglichen, zu liefern. Auch sie müssen also ***Bestandesdaten*** liefern, indes besteht kein Katalog, welche Bestandesdaten sie verpflichtend erfassen müssen. Zudem gilt grundsätzlich keine Pflicht zur Vorratsdatenspeicherung. Ausnahmen bestehen dort, wo AAKD gestützt auf Art. 22 Abs. 4 BÜPF erweiterten Pflichten unterstellt werden (zu den Voraussetzungen der Hochstufung bereits → Kap. 3.4.2).

Bei der Überwachung von ***Inhalts- und Randdaten*** müssen «reguläre» AAKD die Massnahmen, welche Informationen betreffen, die unter Verwendung ihres Dienstes übermittelt oder gespeichert werden, dulden und zu diesem Zweck Zugang zu den Anlagen gewähren sowie die notwendigen Auskünfte erteilen (Art. 27 Abs. 1 BÜPF). Auf Verlangen müssen sie zudem diejenigen Randdaten liefern, die ihnen zur Verfügung stehen (Art. 27 Abs. 2 BÜPF). Im Falle einer Hochstufung gelten für AAKD mit erweiterten Pflichten die Regeln von Art. 26 BÜPF sinngemäss.

Wie bereits erwähnt, wurden gestützt auf das heutige Recht keine AAKD hochgestuft (→ Kap. 3.4.2). Wäre von der Hochstufung Gebrauch gemacht worden, hätten AAKD mit erweiterten Pflichten allerdings der Pikettpflicht, der Pflicht zur automatisierten Erteilung bestimmter Auskünfte sowie der Nutzung der Abfrageschnittstelle, der Vorratsdatenspeicherung bei gewissen Bestandes- und Randdaten, den Überwachungspflichten und den Identifikationspflichten unterstellt werden können. Sie hätten damit zwar nicht über den identischen, doch aber über einen vergleichbaren Pflichtenkatalog wie FDA verfügt.

4.2.2. Vorgeschlagene Änderungen

Die vorgeschlagene Dreiteilung der AAKD in solche mit vollen, reduzierten und minimalen Pflichten (→ Kap. 3.4.2) führte auch zu einer ***Neuordnung der Pflichtenkataloge***, wobei eine Gegenüberstellung offenbart (Abbildung 6), dass sich insbesondere für AAKD, die neu als solche «mit reduzierten Pflichten» qualifizieren, ein erweiterter Pflichtenkatalog ergäbe.

AAKD mit minimalen Pflichten wären in Zukunft weiterhin nur von den «Duldungspflichten, aber weder Auskunfts- noch Überwachungspflichten» betroffen.[82] Gemäss Bundesrat entspricht die Kategorie derjenigen der AAKD ohne weitergehende Pflichten nach dem alten Recht.[83] Sie würden weder verpflichtet, ihre Teilnehmenden zu identifizieren, noch müssten sie automatisierte Auskünfte ermöglichen oder Auskunftstypen beachten. Allerdings müssten weiterhin auch die AAKD mit minimalen Pflichten «auf Verlangen die ihnen zur Verfügung stehenden Randdaten des Fernmeldeverkehrs der überwachten Person» im Sinne von Art. 27 Abs. 2 BÜPF liefern.

AAKD mit reduzierten Pflichten müssten gemäss neuem Recht innerhalb von 6 Monaten nach dem Erreichen der entsprechenden Schwelle (Art. 16f Abs. 4 nVÜPF) Personen mit geeigneten

[82] EJPD, VÜPF/VD-ÜPF Erläuternder Bericht, 12.

[83] EJPD, VÜPF/VD-ÜPF Erläuternder Bericht, 21.

Mitteln identifizieren (Art. 19 nVÜPF), Bestandesdaten zur Teilnehmeridentifikation für 6 Monate aufbewahren (Art. 21 nVÜPF), standardisierte und besondere Auskünfte erteilen (Art. 18 und 25 nVÜPF) und den Nachweis der Auskunftsbereitschaft erbringen können (Art. 31 nVÜPF). Gänzlich neu ist zudem die Regelung, dass AAKD mit reduzierten – und auch mit vollen – Pflichten angebrachte Verschlüsselungen entfernen müssen (Art. 50a nVÜPF) (Weiteres in → Kap. 4.5). Diese AAKD mit reduzierten Pflichten würden im heutigen Recht zur Kategorie der regulären AAKD gehören. Verneint man nicht bereits die Rechtmässigkeit für diesen Kreis an AAKD überhaupt erweiterte Pflichten vorzusehen (wie in → Kap. 3.4.2), bedeutete dies für diese Dienste insbesondere weitergehende Pflichten betreffend die Teilnehmeridentifikation, d.h. die Erhebung und Speicherung von Bestandesdaten (dazu sogleich in → Kap. 4.3).

AAKD mit vollen Pflichten sollen de lege ferenda «alle Auskunfts- und Identifikationspflichten, die Pflicht zur automatisierten Erteilung bestimmter Auskünfte, die Überwachungspflichten, die Pflicht zur Aufbewahrung der Randdaten während 6 Monaten und die Pikettpflicht» haben.[84] Gemäss Art. 16g Abs. 3 nVÜPF muss diese Kategorie von AAKD einen Pikettdienst bereitstellen, Randdaten aufbewahren und zunächst innerhalb von 6 Monaten Auskünfte über die Abfrageschnittstelle bereitstellen. Nach 12 Monaten ist sie ferner verpflichtet, Auskünfte automatisiert zu erteilen, Inhalts- und Randdaten zu überwachen und den Nachweis ihrer Auskunfts- und Überwachungsbereitschaft zu erbringen. Der Katalog entspricht im Grundsatz dem altrechtlichen der AAKD mit erweiterten Pflichten, wobei auch hier die neuen Auskunfts- und Überwachungstypen Änderungen bedeuten (→ Kap. 4.6). Zudem wäre diese Kategorie ebenfalls von der Neuerung in Art. 50a nVÜPF betroffen, angebrachte Verschlüsselungen zu entfernen (→ Kap. 4.5).

Abbildung 6: Gegenüberstellung Pflichten der AAKD nach geltendem und vorgeschlagenem Recht

	AAKD mit erweiterten Pflichten (VÜPF)	AAKD (VÜPF)	AAKD mit vollen Pflichten (nVÜPF)	AAKD mit reduzierten Pflichten (nVÜPF)	AAKD mit minimalen Pflichten (nVÜPF)
Pikettpflicht	✓	×	✓	×	×
Automatisierte Erteilung bestimmter Auskünfte	✓	×	✓	×	×
Auskünfte über Abfrageschnittstelle	✓	×	✓	×	×
Vorratsdatenspeicherung Bestandesdaten	✓	×	✓	✓	×
Vorratsdatenspeicherung Randdaten	✓	×	✓	×	×
Überwachungspflichten	✓	×	✓	×	×
Auskunftspflichten Bestandesdaten	✓	✓	✓	✓	✓
Identifikationspflichten	✓	×	✓	✓	×
Duldungspflichten Überwachung	✓	✓	✓	✓	✓
Lieferung vorhandener Randdaten	✓	✓	✓	✓	✓
Entfernung von angebrachten Verschlüsselungen	×	×	✓	✓	×

[84] EJPD, VÜPF/VD-ÜPF Erläuternder Bericht, 12.

4.3. Ausweitung der Identifikationspflichten im Besonderen

Gemäss dem heutigen Art. 19 Abs. 1 VÜPF haben FDA sowie AAKD mit erweiterten Pflichten (und die Wiederverkäuferinnen) «sicherzustellen, dass die Teilnehmenden mit geeigneten Mitteln ***identifiziert*** werden». Im revidierten Art. 19 Abs. 1 nVÜPF soll diese Pflicht den FDA, den AAKD mit vollen sowie auch den AAKD mit reduzierten Pflichten zukommen. Diese Neuerung gab Anlass zu Diskussionen, wird sie doch teilweise so gelesen, dass «Schweizer Internetnutzer künftig mit Ausweis oder Telefonnummer» zu identifizieren sein werden.[85] Es stellt sich deshalb die Frage, welche Pflichten sich de lege ferenda für AAKD tatsächlich ergeben würden und wie die vorgeschlagene Änderung rechtlich zu beurteilen ist.

Der Bundesrat hält in den Erläuterungen fest, dass unter «***geeigneten Mitteln***» «implizite oder vereinfachte Registrierungen mittels vertrauenswürdiger (trusted) Angaben zu verstehen» seien. Es soll lediglich die Pflicht bestehen, Teilnehmende zu identifizieren, nicht jedoch Endnutzer:innen, welche in einer grösseren Zahl bei bspw. Familien vorliegen können.[86] Als Beispiele für eine Identifikation mit geeigneten Mitteln führt er Zugangscodes per SMS an Mobiltelefone, Identifikationen mittels Kreditkarte und Speicherung der Autorisierungsdaten, Identifikationen mittels gültiger Bordkarten auf Flughäfen oder mittels Karten eines Vielfliegerprogramms, individuelle Zugangscodes im Hotel, die an eine Gästeregistrierung gekoppelt sind oder die Identifikation über die SIM-Karte an.[87] *E contrario* lässt sich daraus ableiten, dass der Bundesrat nicht davon ausgeht, dass eine Identifikation mit amtlichen Dokumenten notwendig ist. Bei Mobilfunkdiensten ist explizit vorgesehen, dass eine Identifikation von natürlichen Personen mit einem Reisepass, Identitätskarte, Ausländerausweis oder Führerausweis zu erfolgen hat (Art. 20a nVÜPF). Eine entsprechende Bestimmung findet sich für andere Dienste nicht. Faktisch legen die vom Bundesrat angeführten Beispiele allerdings offen, dass eine Identifikationsart vonnöten ist, die *indirekt*, d.h. mittels einer weiteren Zwangsmassnahme, eine Identifikation gestützt auf amtliche Dokumente zulassen würde. Die Beispiele der SIM-Karte oder der Zugangscodes in Hotels können das gut illustrieren: Gibt die AAKD eine überprüfte Telefonnummer heraus, können die Behörde damit beim FDA in einem zweiten Schritt die Person identifizieren (mittels Bestandesdatenabfrage nach Art. 21 BÜPF). Gibt die AAKD einen Hotelcode bekannt, können die Behörden beim Hotel die zugehörigen überprüften Gästeinformationen herausverlangen (mittels Beschlagnahme nach Art. 263 ff. StPO). Die AAKD sind folglich nicht verpflichtet, selbst amtliche Dokumente zu überprüfen oder gar zu speichern, sie müssen aber eine Identifikationsart vorsehen, welche dies indirekt (d.h. via weiterer Auskunftsersuchen) ermöglicht. Eine eigentlich anonyme Nutzung von Kommunikationsdiensten wäre damit verunmöglicht.

In Bezug auf die ***Rechtmässigkeit*** dieser Pflichten stellen sich verschiedene Fragen. Bereits festgehalten wurde, dass Dienste mit über 5000 Teilnehmenden nicht per se von grosser wirtschaftlicher Bedeutung sind oder für eine grosse Nutzerschaft angeboten werden, weshalb Art. 22 Abs. 4 BÜPF auf sie nicht anwendbar sein dürfte (→ Kap. 3.4.2). Ein erweiterter Pflichtenkatalog für diese Kategorie ist folglich ohne Gesetzesänderung allgemein nicht opportun. Umgekehrt

---

[85] So etwa die Republik v. 7.5.2025, <https://www.republik.ch/2025/05/07/die-schweiz-ist-drauf-und-dran-autoritaere-ueberwachungsstaaten-zu-kopieren> (Abruf: 1.11.2025).

[86] EJPD, VÜPF/VD-ÜPF Erläuternder Bericht, 30.

[87] EJPD, VÜPF/VD-ÜPF Erläuternder Bericht, 30 f.

kann für AAKD, die tatsächlich von einer gewissen Grösse oder Relevanz sind, eine weitergehende Pflicht zur Identifikation grundsätzlich vorgesehen werden. Der dazu ermächtigende Art. 22 Abs. 4 BÜPF verweist allerdings allein auf die Auskünfte nach Art. 22 BÜPF, d.h. solchen «zur Identifikation der Täterschaft bei Straftaten über das Internet und zur Identifikation von Personen bei Bedrohungen der inneren oder äusseren Sicherheit». Der allgemeine Katalog an Angaben gestützt auf Art. 21 BÜPF ist davon nicht betroffen. Richtigerweise sind AAKD also nicht etwa verpflichtet, Namen und Geburtsdaten der Teilnehmenden (Art. 21 Abs. 1 lit. a BÜPF) zu erfassen. Zudem sind entsprechende Bestandesdatenabfragen nur bei Cyberdelinquenz und Bedrohungen gestützt auf das BÜPF möglich. Da bei allen Arten von Daten gemäss Art. 263 ff. StPO die Beschlagnahme vorgesehen bleibt, ist allerdings klar, dass einmal zu diesem Zwecke gespeicherte Daten ggf. für Behörden zugänglich gemacht werden müssen. Diesfalls, d.h. bei anderen Delikten ist aber der Rechtsschutz (Anordnung durch die Staatsanwaltschaft und Siegelung) erweitert und die Sonderregelung von Art. 22 BÜPF zum vereinfachten Verfahren nicht einschlägig.

Welche ***Teilnehmerdaten*** genau erfasst werden müssen, ist vom Wortlaut des Art. 22 BÜPF offengelassen. Es sind dies schlicht Angaben, «welche die Identifikation der Täterschaft» ermöglichen. Die Regelung der VÜPF, dass dafür «geeignete Mittel» gewählt werden müssen, ist folglich rechtlich nicht zu beanstanden und auch der Umstand, dass diese Mittel wie soeben ausgeführt, indirekt eine Identifikation auch tatsächlich ermöglichen, entspricht dem Grundgedanken des Art. 22 BÜPF. *AAKD von grosser wirtschaftlicher Bedeutung oder mit einer grossen Nutzerschaft voll zu verpflichten und ihnen abzuverlangen, dass sie entsprechende Identifikatoren erheben, ist dementsprechend im Allgemeinen rechtmässig.*

Aufschlussreich in Bezug auf die genaue Ausgestaltung der Identifikationspflichten bei den von diesen Pflichten betroffenen Anbieterinnen sind auch die weiteren Erläuterungen des Bunderats betreffend E-Mail-Dienste. Sie könnten die Identifikation u.a. «mittels Speicherung und Lieferung der Angaben über den Ursprung der Verbindung beim letzten Zugriff (Art. 42a)» vornehmen.[88] Nicht hingegen genüge «die Speicherung der Angaben über den Ursprung der Verbindung lediglich bei der Eröffnung des E-Mail-Kontos (Mailbox) oder bei der erstmaligen Aktivierung des Dienstes», da diese Angaben nur während 6 Monaten (Aufbewahrungszeit der Zuteilungsdaten dynamischer IP-Adressen und NAT[89]-Daten) für die Identifikation der Teilnehmenden verwendet werden könnten.[90] Damit würde also faktisch nicht nur für AAKD mit vollen, sondern auch solchen mit reduzierten Pflichten eine spezifische fortlaufende Vorratsdatenspeicherung für Randdaten (Logfiles) etabliert. Da nach Art. 27 Abs. 2 BÜPF alle AAKD diejenigen Randdaten liefern müssen, die ihnen zur Verfügung stehen, müssten sie diese ***Logfiles***, d.h. die gesamte ihnen vorliegende IP-History, bei einer entsprechenden Überwachungsanordnung auch herausgeben. Diesbezüglich ist festzuhalten, dass zwar IP-Adressen zum Zeitpunkt der Registrierung eines Online-Kontos i.d.R. zu den normalen «Subscriber information», d.h. zu den Bestandesdaten gehören, dass aber die Möglichkeit, stets Auskunft über den «letzten Zugriff» zu geben, es erfordert, Logfiles fortlaufend zu erheben (zu diesem Auskunftstyp erneut in → Kap. 4.6.4). Müssen E-Mail-Provider jedoch alle Zugriffe auf E-Mail-Konten dynamisch und fortwährend erfassen, um

[88] EJPD, VÜPF/VD-ÜPF Erläuternder Bericht, 31.

[89] «Verfahren zur Übersetzung von Netzwerkadressen. Dabei werden die Adressinformationen in IP-Paketen von einem Netzwerkelement (z. B. Router) automatisiert durch andere Adressinformationen ersetzt.», Anhang 1 Ziff. 7 VÜPF.

[90] EJPD, VÜPF/VD-ÜPF Erläuternder Bericht, 31.

gestützt darauf eine Identifikation zu ermöglichen, wäre eine umfassendere Verhaltensüberwachung im Kontext von Kommunikation (E-Mails) möglich. Insbesondere sind Anbieterinnen so befähigt, im Falle einer entsprechenden Überwachungsanordnung in Bezug auf einzelne E-Mail-Versände Auskunft zu geben, von welcher IP-Adresse zum entsprechenden Zeitpunkt eine Kommunikation erfolgte. Diese Information untersteht jedoch dem Fernmeldegeheimnis, es sind Randdaten der Kommunikation (→ Kap. 4.6.4). *Es ist folglich als unzulässig zu erachten, dass die Identifikationspflichten so ausgelegt werden, dass E-Mail-Anbieterinnen und andere AAKD, die nicht den vollen Pflichten unterstehen, zwingend fortlaufend Logfiles erheben und vorrätig speichern müssen.*

4.4. Ausweitung der Vorratsdatenspeicherung im Besonderen

4.4.1. Allgemeines

Das BÜPF sieht für Post- und Fernmeldedienstanbieterinnen eine Pflicht zur sog. Vorratsdatenspeicherung von Bestandes- und vor allem Randdaten für einen Zeitraum von 6 Monaten vor (Art. 19 Abs. 4, Art. 21 Abs. 2, Art. 22 Abs. 2 und Art. 26 Abs. 5 BÜPF). Randdatenerhebungen können gemäss Art. 273 Abs. 3 StPO «bis 6 Monate rückwirkend» verlangt werden, wobei teilweise strittig ist, was betreffend die freiwillig länger gespeicherten Daten gilt.[91] Die Vorratsdatenspeicherung war seit jeher Gegenstand politischer und rechtlicher Kontroversen. Sie gilt als besonders invasiv, da private Unternehmen nicht nur zur Herausgabe verfügbarer Informationen, sondern zu deren Erfassung verpflichtet werden. Gegen die Schweizer Regelung zur Vorratsdatenspeicherung ist seit 2018 eine ***Beschwerde der Digitalen Gesellschaft*** beim Europäischen Gerichtshof für Menschenrechte (EGMR) hängig.[92] Die Digitale Gesellschaft bringt vor, dass die Pflicht zur Aufbewahrung von Randdaten für 6 Monate gegen das Recht auf Privatleben (Art. 8 Europäische Menschenrechtskonvention (EMRK; SR 0.101), die Meinungsäusserungsfreiheit (Art. 10 EMRK), die Versammlungs- und Vereinigungsfreiheit (Art. 11 EMRK), das Recht auf wirksame Beschwerde (Art. 13 EMRK) sowie gegen die Unschuldsvermutung (Art. 6 EMRK) verstösst.[93] Die gesetzliche Grundlage im BÜPF sei mit Blick auf den schweren Eingriff in das Privatleben ungenügend, da sich die Details der Datenspeicherung und ihrer Verwendung nicht aus dem Gesetz selbst, sondern nur aus untergeordneten, technisch komplexen Verordnungen

[91] Art. 21 Abs. 7 VÜPF sieht grundsätzlich betreffend spezifischer von dieser Regelung betroffener Daten explizit die Löschung vor. Das Bundesgericht sah in Auslegung des Art. 273 StPO, wenn auch noch gestützt auf das alte BÜPF, die Grenze von 6 Monaten ebenfalls als absolut an (BGE 139 IV 195, E. 2.3). Stimmen in der Literatur gingen aber teilweise davon aus, dass freiwillig länger gespeicherte Daten auch nach Ablauf der Frist zu liefern seien (so für die Daten nach Art. 22 BÜPF: HANSJAKOB, 449).

[92] Digitale Gesellschaft v. 5.7.2023, <https://www.digitale-gesellschaft.ch/2023/07/05/vorratsdatenspeicherung-am-europaeischen-gerichtshof-fuer-menschenrechte-digitale-gesellschaft-vs-schweiz/> (Abruf: 1.11.2025); zur Beschwerde der Digitalen Gesellschaft: <https://www.digitale-gesellschaft.ch/uploads/pdfs/beschwerde_20180927.pdf> (Abruf: 1.11.2025).

[93] Digitale Gesellschaft v. 5.7.2023, <https://www.digitale-gesellschaft.ch/2023/07/05/vorratsdatenspeicherung-am-europaeischen-gerichtshof-fuer-menschenrechte-digitale-gesellschaft-vs-schweiz/> (Abruf: 1.11.2025).

und Richtlinien ergebe. Zudem sei die Vorratsdatenspeicherung in dieser Form unverhältnismässig.[94]

Zuvor hatte das ***Bundesgericht*** die Beschwerde gegen die Vorratsdatenspeicherung abgewiesen.[95] Das Gericht betonte zwar, dass mit der Vorratsdatenspeicherung von Randdaten grosse Mengen an Daten erfasst werden und die Massnahme alle Nutzer:innen von Fernmeldediensten gleichermassen trifft, ohne dass diese dazu Anlass geboten hätten. Die Eingriffsintensität sei jedoch zu relativieren, da es sich lediglich um Randdaten handelt. Zudem werden die Daten bei der Erhebung nicht gesichtet und die Behörden hätten keinen unmittelbaren Zugriff darauf. Schliesslich sähe das Datenschutzrecht wirksame und angemessene Garantien zum Schutz vor Missbrauch und Willkür vor. Unter Berücksichtigung, dass der EGMR den Konventionsstaaten betreffend Art. 8 EMRK einen Ermessensspielraum zugesteht, erscheinen die Einschränkungen der entsprechenden Grundrechte gemäss Bundesgericht nicht als unverhältnismässig.[96]

Auch in anderen europäischen Staaten führte die Frage der Vereinbarkeit der Vorratsdatenspeicherung mit übergeordnetem Recht zu rechtlichen Auseinandersetzungen. Der ***Europäische Gerichtshof (EuGH)*** hatte 2014 ein Leiturteil zur Richtlinie der EU über die Vorratsdatenspeicherung (Richtlinie 2007/24/EG) gefällt.[97] Er erklärte hierbei die Speicherpflicht als mit Art. 7 (Achtung des Privat- und Familienlebens) und Art. 8 (Recht auf Schutz personenbezogener Daten) der EU-Grundrechtecharta allgemein für unvereinbar.[98] Die Richtlinie wurde daher aufgehoben.

In Deutschland hatte das ***Bundesverfassungsgericht (BVerfG)*** im Jahr 2010 bereits geurteilt, dass eine sechsmonatige, anlasslose Speicherung von Telekommunikationsverkehrsdaten durch Diensteanbieter verfassungswidrig sei.[99] 2022 urteilte der EuGH ferner in einem Vorabentscheidungsverfahren über die Vereinbarkeit einer neuen deutschen Regelung (§ 113a und § 113 b des Telekommunikationsgesetzes (aTKG)) mit dem Unionsrecht. § 113b aTKG sah eine Pflicht für Telekommunikationsdienste zur Speicherung von Verkehrsdaten für zehn Wochen und zur Speicherung von Standortdaten für vier Wochen vor. Der EuGH kam zum Schluss, dass die anlasslose und flächendeckende Speicherung dieser Daten nur zulässig ist, wenn sie zur Bekämpfung von schwerer Kriminalität oder im Bereich der nationalen Sicherheit für die Bekämpfung von realen und ernsten Bedrohungen erfolgt.[100] Auch die Speicherung von IP-Adressen sei nur zulässig zum Schutz der nationalen Sicherheit, zur Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit für einen auf das absolut Notwendige begrenzten Zeitraum.[101] In engen Grenzen erachtete er also die Vorratsdatenspeicherung für EU-konform.

---

[94] Beschwerde der Digitalen Gesellschaft: <https://www.digitale-gesellschaft.ch/uploads/pdfs/beschwerde_20180927.pdf> (Abruf: 1.11.2025), 8.

[95] BGer 1C_598/2016 v. 2.3.2018.

[96] BGer 1C_598/2016 v. 2.3.2018, E. 8.4.

[97] EuGH, Urteil v. 8.4.2014, Digital Rights Ireland und Seitlinger u.a., C-293/12 und C-594/1.

[98] EuGH, Urteil v. 8.4.2014, Digital Rights Ireland und Seitlinger u.a., C-293/12 und C-594/1, Rz. 65.

[99] BVerfG 1 BvR 256/08 v. 2.3.2010.

[100] EuGH, Urteil v. 20.9.2022, SpaceNet, C-793/19 und C-794/19, Rz. 72 ff. und 102.

[101] EuGH, Urteil v. 20.9.2022, SpaceNet, C-793/19 und C-794/19, Rz. 131.

Unvereinbar mit dem Unionsrecht wäre eine Regelung, die präventiv eine allgemeine und unterschiedslose Vorratsdatenspeicherung vorsieht.[102]

Nachdem der EuGH die Richtlinie für ungültig erklärt hatte,[103] folgte auch in Österreich eine Anfechtung der zugehörigen Umsetzungsakte.[104] Der ***Verfassungsgerichtshof (VfGH)*** hob daraufhin mit Urteil vom 27. Juni 2014 die entsprechenden Bestimmungen des Telekommunikationsgesetzes, der StPO und dem Sicherheitspolizeigesetz aufgrund ihrer Verfassungswidrigkeit auf.[105] Gemäss VfGH war die Verhältnismässigkeit schon deshalb nicht gewahrt, weil die Regelung nicht gewährleistete, dass über Vorratsdaten nur dann Auskunft erteilt wird, wenn sie zur strafprozessualen Verfolgung und Aufklärung von gravierenden Straftaten dienen.[106]

Einzelne Europäische Staaten sehen weiterhin Vorratsdatenspeicherungen vor und reizen die Ausnahmemöglichkeiten des EuGH kreativ aus.[107] In ***Frankreich*** hat der Verfassungsgerichtshof die im Land trotz der EuGH-Rechtsprechung praktizierte Vorratsdatenspeicherung weiterhin für zulässig erklärt.[108] Die Regelung verpflichtet Anbieter elektronischer Kommunikationsdienste zur Speicherung von Verkehrs- und Standortdaten für 12 Monate.[109] Bemerkenswert ist, dass es in den ***USA*** keine Pflicht zur Vorratsdatenspeicherung gibt.[110] Zu beachten ist in diesem Zusammenhang, dass es aufgrund des Territorialitätsprinzips nicht als möglich erachtet wird, dass Daten grosser US-Unternehmen von Schweizer Behörden gestützt auf das BÜPF herausverlangt werden können.[111]

Ob die ***Schweizer Regelung*** de lege lata mit dem übergeordneten Recht vereinbar ist, wird der EGMR beurteilen müssen. Die vorliegende Revision wird daran nichts ändern. Die Grundsatzdebatte und die bestehenden Urteile zur Vorratsdatenspeicherung sind für die rechtliche Beurteilung der Revisionsvorlage der VÜPF aber insoweit von Bedeutung, als dass sie aufzeigen, dass es sich bei der Vorratsdatenspeicherung von Bestandes- und noch mehr von Randdaten um schwere Grundrechtseingriffe mit einer grossen Streubreite handelt. Die Anforderungen an die gesetzlichen Grundlagen sind folglich hoch anzusetzen. Zu undifferenzierte Regelungen, aber auch unklare Regelungen sind zu vermeiden. Das gilt umso mehr, als dass – anders als die Urteile gestützt auf die EU-Regelung verlangten – die rückwirkende Erhebung nach Art. 273 StPO nicht auf einen Katalog von schweren Straftaten beschränkt ist, wenn auch die Schwere der Straftat die Überwachung rechtfertigen muss (Art. 269 Abs. 1 lit. b StPO). Bei der Herausgabe von vorrätig gespeicherten Bestandesdaten ist dagegen keinerlei Begrenzung vorgesehen.

---

[102] EuGH, Urteil v. 20.9.2022, SpaceNet, C-793/19 und C-794/19, Rz. 131.

[103] EuGH, Urteil v. 8.4.2014, Digital Rights Ireland und Seitlinger u.a., C-293/12 und C-594/1.

[104] REINDL-KRAUSKOPF/SALIMI/STRICKER, Rz. 5.140.

[105] VfGH G 47/2012-49 u.a. v. 27.6.2014.

[106] VfGH G 47/2012-49 u.a. v. 27.6.2014, Rz. 172.

[107] Verfassungsblog v. 27.11.2024, <https://verfassungsblog.de/die-vorratsdatenspeicherung/> (Abruf: 1.11.2025).

[108] Conseil d'Etat, Assemblée v. 21.4.2021, N° 393099.

[109] Article R10-13 du Code des postes et des communications électroniques.

[110] Siehe Internet Lawyer Blog v. 13.12.2021, <https://www.internetlawyer-blog.com/united-states-data-retention-laws/> (Abruf: 1.11.2025); RINGLAND, 13 ff.

[111] Botschaft BÜPF, 2708.

4.4.2. Reichweite der Vorratsdatenspeicherung de lege ferenda

Gemäss Art. 21 Abs. 1 VÜPF müssen FDA und AAKD mit weitergehenden Pflichten heute die ***Daten zur Identifikation (Bestandesdaten)*** während der Dauer und 6 Monate nach der Beendigung der Kundenbeziehung aufbewahren. Die FDA mit vollen Pflichten müssen zudem zum Zwecke der Identifikation, d.h. zur Erteilung von Auskünften, die Randdaten gemäss Art. 21 Abs. 5 VÜPF aufbewahren, d.h. die Randdaten über die tatsächlich benutzten Geräteidentifikatoren, die Randdaten über die Zuteilung und Übersetzung (NAT) von IP-Adressen und Portnummern für den Netzzugang und die Randdaten zur Bestimmung der unmittelbar benachbarten Netze einer Kommunikation oder eines Kommunikationsversuchs bei Telefonie- und Multimediadiensten. Unter die Randdaten über die benutzen Geräteidentifikatoren fallen z.B. die International Mobile Equipment Identity (IMEI), der Permanent Equipment Identifier (PEI) oder die Media Access Control (MAC-Adresse) sowie die Bezeichnung der Geräte (Art. 36 Abs. 1 lit. b Ziff. 4 und Art. 41 Abs. 1 lit. b Ziff. 2 VÜPF). Randdaten über NAT umfassen z.B. den Benutzernamen, die Quell-/Ziel-IP-Adresse, die Quell-/Ziel-IP-Portnummer, den Typ des Transportprotokolls oder den massgeblichen Zeitpunkt (Art. 38 f. VÜPF). Die dritte Kategorie, die Randdaten zur Bestimmung der unmittelbar benachbarten Netze einer Kommunikation oder eines Kommunikationsversuchs bei Telefonie- und Multimediadiensten, beinhaltet z.B. die IP-Adresse oder den Inter-Operator-Identifier, den Zeitpunkt der Kommunikation sowie die Adressierungselemente (Art. 48c VÜPF). AAKD mit weitergehenden Überwachungspflichten müssen nach der heutigen Regelung die ersten beiden dieser Randdatenkategorien auf Vorrat speichern.

Gemäss der Vorlage des Bundesrats müssten im neuen Recht die Bestandesdaten nicht nur von AAKD mit vollen, sondern auch von denjenigen mit reduzierten Pflichten gespeichert werden. Das bedeutet zunächst, dass der Kreis derjenigen, welche Bestandesdaten auf Vorrat speichern müssen, massgeblich erweitert würde. Betreffend Randdaten bliebe die Regelung bestehen, dass FDA mit vollen Pflichten grundsätzlich gesamthaft aufbewahrungspflichtig sind, d.h. betreffend die Daten, welche für die standardisierten Überwachungstypen vonnöten sind. Was das genau bedeutet und was in Bezug auf AAKD mit vollen Pflichten gelten soll, ist allerdings nicht auf Anhieb ersichtlich und deshalb nachfolgend noch weiter zu diskutieren.

AAKD mit vollen Pflichten müssten zunächst gemäss Art. 21 nVÜPF nicht mehr die Geräteidentifikatoren und Randdaten über die Zuteilung und Übersetzung (NAT) speichern, sondern nur diese zur Bestimmung der unmittelbar benachbarten Netze. Gemäss erläuterndem Bericht seien die AAKD von Abs. 5 lit. a und b gar nicht betroffen, da sie keine Mobilfunkdienste und Netzzugangsdienste anbieten[112], weshalb sich eine entsprechende Verpflichtung erübrige. Dass sie bis anhin vom Auskunftstyp gemäss Art. 48c VÜPF zu den benachbarten Netzen ausgenommen waren, war mutmasslich ungewollt bzw. ein Fehler. AAKD mit vollen Pflichten müssten gemäss Art. 21 Abs. 6 nVÜPF neu also – neben den zu speichernden Bestandesdaten – auch diese ***Randdaten zu «benachbarten Netzen bei Telefonie- und Multimediadiensten»*** im Sinne des unveränderten Art. 48c VÜPF vorrätig speichern. Sie müssten in Bezug auf «Kommunikation» oder «Kommunikationsversuche» demnach insbesondere IP-Adressen speichern und herausgeben können. Bei diesem Auskunftstyp soll es offenbar um die Identifikation bei anonymen oder «gespooften»

[112] EJPD, VÜPF/VD-ÜPF Erläuternder Bericht, 32.

Anrufen (z.B. Bombendrohungen) gehen.[113] Es ist fraglich, inwiefern AAKD überhaupt in der Lage sind, Angaben zu solchen Anrufen zu machen bzw. um was es bei den benachbarten Netzen genau geht. Sind sie ganz generell dazu verpflichtet, IP-Adressen zu speichern (z.B. bei der Nutzung von Web-Telefonie-Funktionen) käme diese Pflicht einer allgemeinen Aufbewahrungspflicht von Logfiles gleich. Das wäre – wie das oben diskutierte Urteil des deutschen BVerfG offenlegt (→ Kap. 4.4.1) – durchaus sehr invasiv. Gestützt auf die Materialien lässt sich jedoch nicht klären, ob dies tatsächlich so zu verstehen ist. Die Vorratsdatenspeicherung für AAKD mit vollen Pflichten bezieht sich jedenfalls grundsätzlich auf die Bestandesdaten betreffend Teilnehmeridentifikation nach Art. 19 nVÜPF, was in Ausführung von Art. 22 Abs. 4 BÜPF zulässig ist. Würde die Einführung der Kategorie der AAKD mit reduzierten Pflichten – entgegen der hier vertretenen Ansicht (→ Kap. 3.4.2) – als rechtmässig erachtet, würden zudem auch diese von der Pflicht betroffen. Welche Vorratsdatenspeicherung bei Randdaten gestützt auf Art. 21 Abs. 5 und 6 nVÜPF vorgesehen werden soll, bleibt schwer zu eruieren, was für sich bereits als problematisch zu bewerten ist.

Des Weiteren stellt sich betreffend die ***Vorratsdatenspeicherung von Randdaten*** allgemein die Frage, ob hier AAKD weitergehend verpflichtet werden sollen und werden dürfen. Der Bundesrat ist gemäss Art. 27 Abs. 3 BÜPF ermächtigt, AAKD von grosser Bedeutung «allen oder einem Teil der in Artikel 26 genannten Pflichten» zu unterstellen. Gemäss Art. 16f nVÜPF würden AAKD mit reduzierten Pflichten betreffend Randdaten grundsätzlich nicht weitergehend verpflichtet. Für AAKD mit vollen Pflichten würde gemäss Art. 16g Abs. 3 nVÜPF jedoch gelten, dass sie innerhalb von 6 Monaten nach der Hochstufung die Randdaten aufbewahren müssen, «die für Auskünfte (Art. 21 Abs. 6 und 7) und Überwachungen (Art. 27 Abs. 3 i.V.m. Art. 26 Abs. 5 BÜPF) erforderlich sind» und nach 12 Monaten zudem den Inhalt und die Randdaten «des Fernmeldeverkehrs der überwachten Person» (Art. 27 Abs. 3 i.V.m. Art. 26 Abs. 1 BÜPF)» liefern müssen. Wie die Terminologie offenbart, geht es nur bei der ersten Pflicht um eine «Aufbewahrung». Diese soll vorgesehen sein für die soeben diskutierten Auskünfte nach Art. 21 nVÜPF, d.h. diejenigen zu den «benachbarten Netzen». Bei den Daten, die auf Vorrat zum Zwecke von Überwachungen gespeichert werden müssen, wird generisch auf Art. 26 Abs. 5 BÜPF verwiesen, d.h. die allgemeine Pflicht, Randdaten des Fernmeldeverkehrs während 6 Monaten aufzubewahren.

In der VÜPF finden sich neben Art. 21 VÜPF zur Auskunftserteilung keine zusätzlichen Informationen zur Vorratsdatenspeicherung bei Randdaten. Bei welchen Randdaten sich ***weitere Aufbewahrungspflichten*** nach Art. 16g Abs. 3 lit. a Ziff. 2 nVÜPF ergeben sollen, ist folglich nicht ohne Weiteres zu erkennen. Die Norm kann sowohl so gelesen werden, als dass sie per se alle Randdaten zu speichern haben. Die sehr spezifische Regelung in Art. 21 VÜPF, dass die Randdaten zu den benachbarten Netzwerken zu speichern sind, spräche gegen diese Lesart. Wiederum für eine weite Vorratsdatenspeicherungspflicht spricht die Praxis, dass auch bei FDA in der VÜPF schlicht implizit eine umfassende Aufbewahrungspflicht betreffend Randdaten vorgesehen ist, deren Spezifikationen sich erst aus den Überwachungstypen ergeben. Art. 62 VÜPF etwa sieht die rückwirkende Überwachung von Randdaten bei E-Mail-Diensten vor. Es seien u.a. die IP-Adressen und Portnummern (Logfiles) zu übermitteln. Aus Art. 16g Abs. 3 lit. a Ziff. 2 nVÜPF ergibt sich nun, dass alle Randdaten, die für derartige Überwachungen erforderlich sind, aufbewahrt werden müssen, d.h. eine umfassende Vorratsdatenspeicherungspflicht eben insbesondere für Logfiles.

[113] EJPD, BÜPF Erläuterungen, 41.

Der bisherige Art. 50 VÜPF hatte AAKD mit weitergehenden Pflichten zwar ebenfalls verpflichtet, dazu in der Lage zu sein, die Überwachungen – auch die rückwirkenden wie eben etwa gestützt auf Art. 62 VÜPF – auszuführen, schwieg sich aber zu einer eigentlichen Aufbewahrungspflicht aus. Da keine AAKD eine Hochstufung erfuhren, stellte sich die konkrete Auslegungsfrage indes diesbezüglich in der Praxis bis anhin nicht. Die Pflichten betreffend Vorratsdatenspeicherung für voll verpflichtete Anbieterinnen ergeben sich also (wahrscheinlich) nur indirekt über die entsprechenden Überwachungstypen, was zu einer gewissen Unübersichtlichkeit führt. Diese Unübersichtlichkeit ist in Anbetracht der hohen Eingriffsintensität, die mit der Herausgabe von anlasslos auf Vorrat gespeicherten Randdaten wie IP-Histories einhergeht, zu kritisieren. Sie ist jedoch keine Problematik des neuen Rechts. Sowohl unter bisherigem als auch unter dem vorgeschlagenen Recht wäre bei den voll verpflichteten AAKD grundsätzlich davon auszugehen, dass sie Bestandes- und Randdaten 6 Monate zu speichern haben, damit alle Typen der rückwirkenden Überwachung, die sie betreffen, auch durchgeführt werden können.

Fraglich ist auf den ersten Blick, wie sich die Lage bei ***AAKD mit reduzierten Pflichten*** gestaltet. Hier besteht grundsätzlich keine allgemeine Pflicht, rückwirkende Überwachungen durchführen zu können und auch Art. 21 Abs. 5 und 6 VÜPF adressieren sie nicht. Folglich ist eine Vorratsdatenspeicherung bei Randdaten grundsätzlich ausgeschlossen. Das steht im Einklang mit dem Gesetzestext. Indirekt könnten sich mit dem neuen Recht aber möglicherweise Aufbewahrungspflichten bei IP-Adressen, d.h. Randdaten, ergeben, da gewisse Auskünfte faktisch die Speicherung von Randdaten erfordern (dazu erneut in → Kap. 4.6). Da für AAKD mit reduzierten Pflichten keine Regelung wie in Art. 16g Abs. 3 lit. a Ziff. 2 i.V.m. Art. 21 nVÜPF besteht, die eine Aufbewahrung von Randdaten für (gewisse) Auskünfte vorschreibt, ist gestützt auf den Verordnungstext allerdings anzunehmen, dass AAKD mit reduzierten Pflichten keinerlei Randdaten auf Vorrat speichern müssen, auch wenn dies bedeutet, dass sie nicht in der Lage sind, gewisse Auskünfte zu erbringen. Das ergibt sich auch aus dem erläuternden Bericht, der z.B. betreffend den neuen Auskunftstyp in Art. 42a nVÜPF (Auskünfte über den letzten Zugriff auf einen E-Mail-Dienst, dazu → Kap. 4.6.4) festhält, dass nicht voll verpflichtete FDA und AAKD auf Verlangen schlicht die ihnen zur Verfügung stehenden Randdaten herausgeben müssen.[114] Eine Vorratsdatenspeicherungspflicht besteht hier also auch in Zukunft nicht (Abbildung 7). *Die vorgeschlagene Regelung ist folglich als rechtmässig zu beurteilen. Das sehr komplexe Zusammenspiel der Bestimmungen in Bezug auf die Frage der Vorratsdatenspeicherung macht es für Normadressat:innen aber schwierig, die Rechtslage wirklich zu erkennen, was in Anbetracht der Schwere der mit ihr einhergehenden Grundrechtseingriffe zu kritisieren ist*.

[114] EJPD, VÜPF/VD-ÜPF Erläuternder Bericht, 38.

Abbildung 7: Vorratsdatenspeicherung bei AAKD nach altem und vorgeschlagenem Recht

	AAKD mit erweiterten Pflichten (VÜPF)	AAKD (VÜPF)	AAKD mit vollen Pflichten (nVÜPF)	AAKD mit reduzierten Pflichten (nVÜPF)	AAKD mit minimalen Pflichten (nVÜPF)
Daten zur Teilnehmeridentifikation (Bestandesdaten)	✔	✘	✔	✔	✘
Randdaten für Überwachungen im Allgemeinen (nach Art. 60 ff. VÜPF)	✔	✘	✔	✘	✘
Randdaten über tatsächlich genutzte Geräteidentifkatoren (für Auskünfte nach Art. 36 und 41 VÜPF)	✔	✘	✘	✘	✘
Randdaten über die NAT von IP-Adressen und Portnummern für den Netzzugang (für Auskünfte nach Art. 38 f. VÜPF)	✔	✘	✘	✘	✘
Randdaten betreffend benachbarte Netze einer Kommunikation (für Auskünfte nach Art. 48c VÜPF)	✘	✘	✔	✘	✘

4.5. Pflicht zur Entschlüsselung im Besonderen

Das BÜPF sieht in Art. 26 Abs. 2 lit. c vor, dass FDA «von ihnen angebrachte ***Verschlüsselungen entfernen***», wobei diese Pflicht i.V.m. Art. 27 Abs. 3 BÜPF auch hochgestuften AAKD auferlegt werden hätte können. Bis anhin kannte die VÜPF dazu allerdings keine Ausführungsbestimmung, weshalb für sie keine entsprechende Pflicht bestand. In der neuen Verordnung soll in Art. 50a nVÜPF nun aber festgehalten werden, dass die AAKD mit vollen und diejenigen mit reduzierten Pflichten «die von ihnen oder für sie angebrachten Verschlüsselungen» entfernen müssen. Sie müssten dabei «den Fernmeldeverkehr der überwachten Person an geeigneten Punkten erfassen und entschlüsseln, damit die Überwachungsdaten ohne die vorgenannten Verschlüsselungen geliefert werden». Die Ende-zu-Ende-Verschlüsselungen zwischen Endkund:innen seien davon nicht betroffen. Im Falle einer solchen Ende-zu-Ende-Verschlüsselung verfügt die Anbieterin über keinen Schlüssel. Die Verschlüsselung findet zwischen zwei Endgeräten oder zwei Applikationen statt. In einem solchen Fall könnte und müsste gemäss Bundesrat die Anbieterin keine Entschlüsselung vornehmen. Anders sei die Situation zu beurteilen, falls eine Verschlüsselung der Anbieterin verwendet wird und diese über einen Schlüssel verfügt.[115] Die Änderung war schon in der ersten «Revisionsetappe» 2023 vorgeschlagen und indes – mitunter aufgrund laut gewordener Kritik – in die vorliegende zweite Etappe verschoben worden, nun eben mit dem expliziten Hinweis, dass die Ende-zu-Ende-Verschlüsselung nicht tangiert sei. Auch die jetzt vorgeschlagene Regelung sorgte aber für Aufsehen. So wurde in der Öffentlichkeit gewarnt, in der Schweiz sei die sichere Verschlüsselung gefährdet[116] oder dass die Transportverschlüsselung «daran glauben muss»[117]. Es stellt sich deshalb die Frage, welche Wirkungen diese neue Regelung genau entfaltet.

Die Pflicht zur Entfernung der angebrachten Verschlüsselungen will der Bundesrat aus Art. 26 Abs. 2 lit. c BÜPF für die FDA und aus Art. 26 Abs. 2 lit. c i.V.m. Art. 27 Abs. 3 BÜPF für die

[115] EJPD, VÜPF/VD-ÜPF Erläuternder Bericht, 42 f.

[116] Techradar v. 26.3.2025, <https://www.techradar.com/vpn/vpn-privacy-security/secure-encryption-and-online-anonymity-are-now-at-risk-in-switzerland-heres-what-you-need-to-know> (Abruf: 1.11.2025).

[117] Digitec v. 7.5.2025, <https://www.digitec.ch/de/page/vuepf-revision-bundesrat-will-ueberwachung-per-verordnung-durchmogeln-37842> (Abruf: 1.11.2025).

AAKD, welche Dienstleistungen von grosser wirtschaftlicher Bedeutung oder für eine grosse Benutzerzahl anbieten, ableiten.[118] Es ist, wie bereits ausgeführt wurde (→ Kap. 3.4.2), zunächst zu bestreiten, dass AAKD mit reduzierten Pflichten, d.h. mit über 5000 Teilnehmenden, bereits von der verlangten wirtschaftlichen Relevanz oder Grösse sind, dass Art. 27 Abs. 3 BÜPF tatsächlich zur Anwendung gelangen kann. *Die Pflicht zur Entschlüsselung wäre insofern jedenfalls auf die Anbieterinnen mit vollen Pflichten zu beschränken.*

Ferner ist mit Blick auf die potenziell ***hohe Invasivität*** dieser Massnahme genauer zu klären, was mit der gesetzlich vorgesehenen Pflicht «angebrachte Verschlüsselungen zu entfernen» genau gemeint sein kann. Der erläuternde Bericht führt als Beispiel an, dass eine Anbieterin, die eine «abschnittsweise Verschlüsselung zwischen ihren Systemen und ihren Endkunden einsetzt», diesen Fernmeldeverkehr der überwachten Person an einem geeigneten Punkt unverschlüsselt erfassen und an den Dienst ÜPF ausleiten muss.[119] Bei der Ende-zu-Ende-Verschlüsselung dagegen verfüge die Anbieterin i.d.R. selbst nicht über den Schlüssel. Wenn jedoch ein Schlüssel der Anbieterin bei der Verschlüsselung verwendet werde, d.h. wenn die Anbieterin die Verschlüsselung selbst entfernen kann, dann müsse sie dies auch tun.[120]

Im Allgemeinen lassen sich die ***serverseitige Verschlüsselung***, die ***Transportverschlüsselung*** und die ***Ende-zu-Ende Verschlüsselung*** unterscheiden. Letztere ist, wie der Verordnungstext offenbart, ganz explizit nicht von der Regelung anvisiert. Bei serverseitigen Verschlüsselungen werden Verschlüsselungen angebracht, sobald sie auf dem Server eingetroffen sind. Daten werden so von einem ungeschützten Zugriff auf dem Server geschützt. Bei der serverseitigen Verschlüsselung besitzt die Anbieterin einen Decodierungsschlüssel und verwaltet diesen selbst. Die Schlüsselverwaltung ermöglicht ihr eine selbstständige Entschlüsselung der Daten.[121] Weit verbreitet ist sodann die Transportverschlüsselung. Transportverschlüsselung bedeutet, dass die Verbindung auf einem Transportabschnitt geschützt wird.[122] So kann die Verschlüsselung zwischen dem Sender und dem Server des Senders, zwischen dem Server des Senders und demjenigen des Empfängers sowie zwischen dem Server des Empfängers und dem Empfänger eingerichtet werden.[123] Entscheidend ist, dass die Transportverschlüsselung gerade nur die Verbindung und somit einen bestimmten Abschnitt des Datentransfers schützt. Der Server als Empfänger kann die Daten entschlüsseln und somit Einsicht in den Klartext nehmen, bevor er bspw. eine serverseitige Verschlüsselung vornimmt.

Mit der im Rahmen der VÜPF-Revision vorgeschlagenen Bestimmung zur Entfernung einer Verschlüsselung sowie mit Art. 26 Abs. 2 lit. c BÜPF müsste also gemeint sein, dass ***serverseitige Verschlüsselungen*** sowie ***Transportverschlüsselungen*** entfernt werden müssen. Eine angebrachte Ende-zu-Ende-Verschlüsselung kann von den Servern dagegen gerade nicht entfernt werden, weshalb eine Entfernungspflicht per se ins Leere laufen würde.

---

[118] EJPD, VÜPF/VD-ÜPF Erläuternder Bericht, 42.

[119] EJPD, VÜPF/VD-ÜPF Erläuternder Bericht, 42.

[120] EJPD, VÜPF/VD-ÜPF Erläuternder Bericht, 43.

[121] Siehe dazu z.B. HERFERT/LANGE/SPYCHALSKI, 128.

[122] Siehe z.B. DEUSCH/EGGENDORFER, 34.

[123] KNEUPER/MACKE, 77 f.

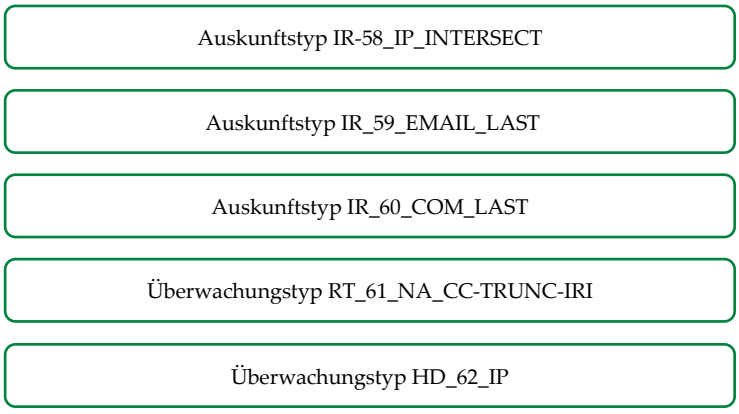
FDA mit vollen Pflichten und AAKD mit vollen Pflichten können gestützt auf das BÜPF rechtmässig dazu angehalten werden, serverseitige Verschlüsselungen sowie Transportverschlüsselungen aufzuheben, sofern sie selbst über den Schlüssel verfügen. Jedoch ist der Gesetzes- oder Verordnungswortlaut nicht dahingehend zu interpretieren, als dass es eine Pflicht gibt, irgendeine Form der Verschlüsselung vorzunehmen oder zu unterlassen. Alle ***Verschlüsselungstechniken*** bleiben erlaubt. Wer umgekehrt wie bei der End-zu-End-Verschlüsselung gar nicht über die Möglichkeit der Entschlüsselung verfügt, kann und muss diese auch nicht vornehmen. Um aus Art. 50a nVÜPF eine Pflicht abzuleiten, gewisse Schlüssel zwingend zu speichern oder zur Verfügung zu halten, ist die Bestimmung zu unbestimmt formuliert. Folglich beschränkt sich deren Gehalt darauf, dass die Anbieterinnen schlicht an «Entschlüsselung» bereitstellen müssen, was sie aufgrund der bei ihnen sowieso vorhandenen Daten entschlüsseln können.

4.6. Neue Auskunfts- und Überwachungstypen

4.6.1. Überblick

Der Bundesrat erhält mit Art. 31 BÜPF die Kompetenz, in Ausführungsbestimmungen die ***Auskunfts- und Überwachungstypen*** zu präzisieren und die zu liefernden Daten im Detail zu bezeichnen. Von dieser Kompetenz hat er schon bis anhin Gebrauch gemacht und verschiedenste Auskunfts- und Überwachungstypen normiert. Im Zuge der Revision möchte er nun «auf Wunsch der Strafverfolgungsbehörden» drei weitere Auskunfts- und zwei Überwachungstypen schaffen (Abbildung 8).[124] Zudem sind verschiedene Änderungen bei bestehenden Typen vorgesehen.

Abbildung 8: Überblick neue Auskunfts- und Überwachungstypen



Die neuen und veränderten ***Auskunftstypen*** betreffen insbesondere die Benutzeridentifikation durch Schnittmengenbildung sowie Auskünfte über letzte Zugriffe auf Dienste. Sie würden zu einer weitergehenden Verpflichtung der FDA und AAKD führen und werden in den nachfolgenden Kapiteln genauer diskutiert (→ Kap. 4.6.2 - 4.6.5). Bei gewissen Auskunftstypen werden ferner Präzisierungen vorgenommen, genauer eine Flexibilisierung der Lieferung der Multi-Device-Information via Auskunftstyp IR_4_NA oder IR_6_NA (Art. 35 und 36 VÜPF) sowie IR_10_TEL oder IR_12_TEL (Art. 40 und 41 VÜPF), gewisse redaktionelle Änderungen (z.B. Überschriften in

[124] EJPD, VÜPF/VD-ÜPF Erläuternder Bericht, 6.

Art. 37 f. VÜPF) und der stetigen Praxis angepasste Änderungen bei den Anforderungen an Auskunftsgesuche bei «kurzzeitig zugeordneten Identifikatoren» (Art. 48b VÜPF).

Bei den neuen ***Überwachungstypen*** (nachfolgend → Kap. 4.6.6) geht es um eine Änderung betreffend die Echtzeitüberwachung von Netzzugangsdiensten, mit der ein reduziertes Datenvolumen ermöglicht werden soll (Art. 55a nVÜPF), sowie um eine Änderung betreffend die rückwirkende Überwachung zum Zweck der Teilnehmeridentifikation (Art. 60 nVÜPF). Ferner sind weitere Detailanpassungen bei bestehenden Typen vorgesehen.

4.6.2. Umgang mit Mehrfachergebnissen bei Auskünften zu IP-Adressen

Eine erste Änderung betrifft den ***Auskunftstyp «IR_7__IP: Benutzeridentifikation bei eindeutig zugeteilten IP-Adressen»*** gemäss Art. 37 VÜPF. Es soll diesbezüglich neu in Abs. 3 festgehalten werden, dass, sofern kein oder mehr als ein Ergebnis gefunden wird, die Mitwirkungspflichtige das mitteilt, und, falls bekannt, die Anzahl der Ergebnisse ebenfalls mitliefert. Es geht hierbei um die Konstellation, dass es bei Auskünften zur Zuteilung von statischen (d.h. eindeutig zugeteilten) IP-Adressen zu Mehrfachergebnissen kommt. Während die Anbieterin bis anhin diesfalls nur festzuhalten brauchte, dass keine Benutzeridentifikation möglich war, müsste sie neu eine präzisere Rückmeldung liefern. Dies ermöglichte den Behörden, um Folgeauskünfte zu ersuchen. Insbesondere kann sie eine Randdatenüberwachung des neuen Typs «HD_62_IP: rückwirkende Überwachung zum Zweck der Teilnehmeridentifikation bei Internetverbindungen» anordnen (Art. 60a nVÜPF). Es kann also zu Identifikationszwecken eine Bearbeitung der Logfiles durch die Anbieterin und in der Folge die Bildung der Schnittmenge angeordnet werden. Es handelt sich dabei um eine Randdatenüberwachung, die grundsätzlich – bei Vorliegen der entsprechenden Voraussetzungen – von der StPO i.V.m. dem BÜPF vorgesehen ist. Dass zu diesem Zweck in einem ersten Schritt mitgeteilt werden muss, dass ein und welches Mehrfachergebnis vorliegt, kann als gerechtfertigt angesehen werden, da dieses Vorgehen den Behörden ermöglicht, abzuwägen, ob eine rückwirkende Randdatenerhebung in Anbetracht des Ermittlungszwecks verhältnismässig ist.

Beim ***Auskunftstyp «IR_8_IP_NAT: Benutzeridentifikation bei IP-Adressen mit NAT»*** geht es um die Identifikation von Nutzer:innen im Falle von dynamisch zugeteilten IP-Adressen. Bei diesen IP-Adressen sollen die Anbieterinnen bei diesem Auskunftstyp verpflichtet werden, mitzuwirken, um möglichst eindeutig festzustellen, welche Person oder welcher Netzzugang als Urheber:in der Internetverbindung infrage kommt.[125] Zu diesem Zweck müssen die Anbieterinnen grundsätzlich eruieren, welchem Anschluss die IP-Adresse zu einem bestimmten Zeitpunkt (dynamisch) zugeteilt war. Die Behörden liefern – vereinfacht erläutert – eine IP-Adresse X (von der aus z.B. auf eine Webseite zum Zeitpunkt Y zugegriffen wurde). Die FDA stellt fest, welchem Anschluss diese IP-Adresse X zum Zeitpunkt Y zugeteilt wurde, und liefert die zugehörigen Angaben zum Teilnehmenden, was im Idealfall die Identifikation der für den Zugriff verantwortlichen Person erlaubt. Es handelt sich hierbei um eine Auskunfts- und nicht um eine Überwachungspflicht, da die IP-Adresse bereits bekannt ist und entsprechend keine Überwachung des Internetverkehrs, sondern eine blosse Identifikation bzw. ein Identifikationsversuch erfolgt (zur Abgrenzung erneut → Kap. 4.6.4). Der Bundesrat beabsichtigt nun aber, dass bei den

[125] Vgl. auch EJPD, VÜPF/VD-ÜPF Erläuternder Bericht, 35.

dynamischen IP-Adressen Mehrfachergebnisse geliefert werden müssen. Anders als beim soeben diskutierten Auskunftstyp bezüglich der statischen IP-Adressen, wo nur die Anzahl der Ergebnisse geliefert werden muss, müssten hier aber die Mehrfachergebnisse selbst geliefert werden. Der Bundesrat will Art. 38 VÜPF entsprechend dahingehend revidieren, dass im eigentlichen «Misserfolgsfall», d.h. eben dann, wenn die dynamische IP-Adresse nicht eindeutig einem/einer Nutzer:in zugeteilt werden kann, den Behörden die Liste aller möglichen Kund:innen, die infrage kommen, bekannt gegeben wird. Die Anzahl an durch die Auskunft in ihren Grundrechten berührten Personen steigt damit unweigerlich an und kann ggf. sehr hoch sein. Allerdings ist anzumerken, dass die Anbieterinnen selbst mit technischen Vorkehrungen (insbesondere der vollständigen Einführung von IPv6) dazu beitragen können, diese Zahl tief zu halten.

Wird bei nicht eindeutiger Zuteilung von IP-Adressen gestützt auf diesen neuen Auskunftstyp eine ***Liste möglicher Personen*** bekanntgegeben, die allenfalls Urheber:in des Zugriffs sind, geraten diese – trotz uneindeutiger Zuteilung – allerdings ins Visier der Strafverfolgungsbehörden. Sie wären je nach Verständnis allenfalls prozedural sogar bereits als beschuldigte Personen zu qualifizieren (mit entsprechender Wirkung). Es stellt sich die Frage der Verhältnismässigkeit. Der strafprozessrechtliche Grundsatz, dass Zwangsmassnahmen, die in die Grundrechte nicht beschuldigter Personen eingreifen, besonders zurückhaltend einzusetzen sind (Art. 197 Abs. 2 StPO), ist dabei zu berücksichtigen. Einschränkend wirkt, dass der Bundesrat in Art. 38 Abs. 3 nVÜPF vorschlägt, dass nur Mehrfachergebnisse zu liefern sind, wenn diese geeignet sind, eine eindeutige Identifikation zu ermöglichen. Diese Einschränkung ist dahingehend auszulegen, dass die Herausgabe von Mehrfachergebnissen nur zulässig ist, wenn der Ermittlungserfolg entscheidend davon abhängt. Es stellt sich allerdings die Frage, wie die Anbieterinnen ohne Kenntnis der weiteren Ermittlungen feststellen können, ob ihre Informationen – in Kombination mit weiteren Ermittlungsergebnissen – eine Identifikation erlauben könnten. Es wird deshalb davon auszugehen sein, dass Mehrfachergebnisse nur im Falle einer sehr tiefen Anzahl von Möglichkeiten zulässig bzw. verhältnismässig sind. In diesem Sinne erläutert der Bundesrat auch, dass im Falle einer hohen Anzahl von Ergebnissen die Mitwirkungspflichtigen die Anfrage zurückweisen können, da es sich diesfalls um einen «Fehlerfall» handelt.[126] *Bei zurückhaltender Auslegung und Praxis wird die Rechtmässigkeit dieses neuen Auskunftstyps wohl zu bejahen sein.* Selbstredend handelt es sich bei der Pflicht zur Lieferung von Mehrfachergebnissen jedoch um eine Ausweitung des Pflichtenkatalogs der Anbieterinnen.

4.6.3. Identifikation durch Schnittmengenbildung bei IP-Adressen

Mit Art. 38a nVÜPF soll der Auskunftstyp ***«IR_58_IP_INTERSECT: Benutzeridentifikation durch Schnittmengenbildung»*** neu geschaffen werden. Es geht auch hier im Wesentlichen um die Pflicht der Anbieterinnen, die Identifikation gestützt auf IP-Adressen zu ermöglichen. Liegen bei den Behörden verschiedene IP-Adressen vor und wäre eine Identifikation des/der Urheber:in der Internetverbindung aufgrund der nicht eindeutigen Zuteilung der dynamischen IP-Adressen isoliert nicht möglich, können die Anbieterinnen verpflichtet werden, verschiedene Abfragen zu machen und die resultierenden Mehrfachergebnisse abzugleichen. Da die FDA die entsprechenden Informationen (Zuteilungen von dynamischen IP-Adressen) bereits heute für 6 Monate speichern müssen (→ Kap. 4.4.1), liegen ihnen diese Informationen grundsätzlich vor. So kann eine Behörde,

[126] EJPD, VÜPF/VD-ÜPF Erläuternder Bericht, 35.

die über eine gesamte IP-History verfügt, über diese «Mehrfachauskunft» bzw. Schnittmengenbildung die Identifikation des/der Nutzer:in vereinfacht erwirken.

Der neue Auskunftstyp ist zwar schwer verständlich, dürfte aber wie geschildert aufzufassen sein. Demnach führt die von der Behörde gestellte Abfrage zur Benutzeridentifikation also mittels statischer oder dynamischer IP-Adresse zunächst zu keinem eindeutigen Ergebnis. Stattdessen resultieren daraus Mehrfachergebnisse. Die Behörde übermittelt deshalb in der Folge sämtliche, jedoch mind. zwei IP-Adressen, welche sie mit dem Teilnehmenden in Verbindung bringt, an die Anbieterin. Die Anbieterin führt mit sämtlichen erhaltenen IP-Adresse eine Bestandesabfrage durch, bildet mit den Ergebnissen eine Schnittmenge, welche es erlaubt den mehrfach vorkommenden Teilnehmenden zu erkennen, und übermittelt den identifizierten Teilnehmenden (die «Schnittmenge») den Behörden.

Es handelt sich hierbei lediglich um eine Bestandesdatenabfrage, allerdings um eine eigentliche ***«Massenabfrage»***. Es stellt sich insofern die Frage der Verhältnismässigkeit. Sie ist im Einzelfall zu prüfen. Allerdings kommt erschwerend hinzu, dass bei Bestandesdatenabfragen nach Art. 22 BÜPF weder eine gerichtliche noch eine staatsanwaltliche Überprüfung vorgesehen ist. Die Polizei kann im Rahmen ihrer Ermittlungen eigenmächtig entsprechende «Massenauskünfte» einholen, bei den voll verpflichteten Anbieterinnen zudem im automatisierten Verfahren. Fraglich ist, ob Rechtsschutz und Invasivität hier noch in Einklang stehen, insbesondere da die Anbieterinnen keine expliziten «Abwehrmöglichkeiten» haben, sich gegen entsprechende Gesuche betreffend eigentliche «Mehrfachanalysen» zu wehren. Besonders heikel ist, dass die Anbieterinnen ohne jede staatsanwaltliche oder gerichtliche Überprüfung sowie für alle Delikte (auch Bagatellen) verpflichtet werden können, auf Vorrat gespeicherte Randdaten (IP-Adressen) zu bearbeiten und zu nutzen. Jedenfalls würde die Revision der VÜPF in dieser Form die Möglichkeiten der Strafverfolgungsbehörden ausweiten, IP-Adressen zuzuordnen. Das erhöht die Chancen auf Ermittlungserfolg, stellt aber auch einen grösseren Eingriff für die betroffenen Anbieterinnen und Teilnehmenden dar. Wie bereits geschildert (→ Kap. 4.4.1), wird die Vorratsdatenspeicherung nur in engen Grenzen und nur bei schweren Delikten als zulässig erachtet. Dass hier vorrätig gespeicherte Daten so generell zu Ermittlungszwecken genutzt werden, erscheint deshalb als heikel. *Es ist folglich mindestens als fraglich zu werten, ob dieser neue Auskunftstyp bei allen Delikten als verhältnismässig und deshalb rechtmässig gelten kann.* Das gilt vor allem bei denjenigen Anbieterinnen, die nicht sowieso eine umfassende Identifikationspflicht trifft, da diesfalls die Schnittmengenbildung nicht als Konsequenz dieser generellen Mitverantwortung zur Identifikation interpretiert werden kann.

4.6.4. Auskünfte über den letzten Zugriff auf Kommunikationsdienste

Ein weiterer neuer ***Auskunftstyp «IR_59_EMAIL_LAST: Auskunft über den letzten Zugriff auf einen E-Mail-Dienst»*** soll mit Art. 42a nVÜPF eingeführt werden. Mit ihm sollen E-Mail-Dienste zur Auskunft darüber, wer in den letzten 6 Monaten auf das entsprechende Konto zugegriffen hat, verpflichtet werden. Die Behörden liefern der Anbieterin z.B. eine E-Mail-Adresse. Sie muss daraufhin Auskunft geben, welche Nutzerangaben (z.B. Kundennummer oder weitere E-Mail-Adressen und Benutzernamen) ihr vorliegen. Darüber hinaus muss sie Datum und Uhrzeit des Zugriffs, das verwendete Protokoll sowie IP-Adresse und Portnummer des Clients bekanntgeben.

Es handelt sich dabei um eine Ausweitung der Pflicht, über den Zugriff auf explizit kommunikationsbezogene Dienste (E-Mail) Auskunft zu geben.

Vergleichbar soll mit dem ebenfalls neu eingeführten ***Auskunftstyp «IR_60_COM_LAST: Auskunft über den letzten Zugriff auf einen anderen Fernmelde- oder abgeleiteten Kommunikationsdienst»*** des Art. 43a nVÜPF eine Pflicht vorgeschlagen werden, über den letzten Zugriff auf den Dienst Auskunft zu geben und insbesondere IP-Adressen und Portnummern, aber etwa auch Nutzeradressen, Pseudonyme etc. mitzuteilen. Die Behörden erhalten somit die in der Praxis sicher vielfältig nutzbare Möglichkeit in einem ersten Schritt beim OTT-Dienst festzustellen, von welcher IP-Adresse aus eine Person auf einen Dienst zugegriffen hat, um dann in der Folge mit einem erneuten Begehren an die FDA die entsprechende IP-Adresse einem/einer Nutzer:in zuzuordnen. In der Anfrage müsse kein massgeblicher Zeitpunkt angegeben werden.[127] Zudem wird festgehalten, dass die Edition der IP-History nur über die rückwirkende Randdatenüberwachung möglich bleibe.[128] Es stellt sich jedoch trotzdem die Frage, inwieweit es sich bei einer solchen «LAST-Abfrage» noch um eine reine Bestandesdatenabfrage, d.h. eine Auskunft i.S.v. Art. 21 f. BÜPF handelt, oder ob die Herausgabe der Zugriffs-IP-Adressen nicht vielmehr bereits eine Randdatenabfrage, d.h. eine Überwachung darstellt.

In Bezug auf ***IP-Adressen*** müssen im Allgemeinen drei Konstellationen unterschieden werden: Sollen auf Grundlage einer bekannten IP-Adresse bei einer Anbieterin die dazugehörigen Registrierungsdaten abgefragt werden, dann handelt es sich um eine Bestandesdatenabfrage.[129] Davon zu unterscheiden ist die Variante, in welcher den Behörden lediglich eine Internet-Kommunikationsaktivität bekannt ist (z.B. eine E-Mail). Sollen die beteiligten Zugänge mittels IP-History eruiert werden und weist die IP-History einen solchen Kommunikationsbezug auf, so handelt es sich um eine Abfrage von Randdaten.[130] Weder eindeutig als Bestandesdaten- noch als Randdatenabfrage kann die Variante qualifiziert werden, bei der lediglich festgestellt wird, welche IP-Adressen mit einem Dienst in Verbindung gebracht werden können (z.B. Zugriffe auf einen E-Mail-Dienst allgemein, d.h. ohne direkten Bezug zu einer versendeten E-Mail). Sie sind keine eigentlichen Randdaten, da keine Modalitäten der Kommunikation auszumachen sind, aber auch keine blossen Bestandesdaten, da sie nicht nur «beständig» sind, sondern über das Dienste- und damit Internetnutzungsverhalten Aufschluss geben.[131] Diese Abgrenzung beschäftigte schon bis anhin und zeigt sehr deutlich auf, dass die Regelungen der Art. 269 ff. StPO und des BÜPF nicht auf eigentliche allgemeine Internetüberwachungen ausgerichtet sind. Die neue E-Evidence-Gesetzgebung der EU hat deshalb für IP-Adressen, die bearbeitet werden, um indirekt die Teilnehmeridentifikation zu ermöglichen, eine eigene Datenkategorie mit zugehörigen Regeln eingeführt. Sie unterscheidet Inhaltsdaten, Verkehrsdaten, *Zugangsdaten* und Bestandesdaten.[132] Im geltenden Schweizer Recht gibt es eine solche Sonderkategorie für IP-Adressen nicht. Ihre Erhebung ist deshalb entweder als Bestandes- oder als Randdatenerhebung zu klassifizieren – mit den entsprechenden Konsequenzen für den Rechtsschutz. Oder es wäre die äusserst kritische Haltung einzunehmen, dass die

[127] EJPD, VÜPF/VD-ÜPF Erläuternder Bericht, 38.

[128] EJPD, VÜPF/VD-ÜPF Erläuternder Bericht, 38.

[129] BGE 141 IV 108, E. 5.1; BGer 656_2015 v. 16.12.2016, E. 1.3.1; dazu auch BETSCHMANN, 360; SIMMLER, 136.

[130] BGer 6B_656/2015 v. 16.12.2016, E. 1.3.2.

[131] SIMMLER, 136.

[132] Dazu samt einer Gegenüberstellung mit dem Schweizer Recht: SIMMLER, 134.

Bearbeitung von IP-Adressen und Logfiles, die keinen direkten Bezug zu einer konkreten, dem Fernmeldegeheimnis unterstehenden Kommunikation aufweisen, gar keinen Anwendungsfall der Art. 269 ff. StPO und des BÜPF mehr darstellen und von vornherein nicht zulässig sind. Diesfalls müsste der Weg über Art. 263 ff. StPO gewählt werden, die VÜPF-Regelungen wären hinfällig. Sofern aber – und davon ist auszugehen – die Abfragen gestützt auf den neuen Auskunftstyp mindestens indirekt einen Kommunikationsbezug aufweisen, ist eine Anwendbarkeit des BÜPF-Regimes in dieser Konstellation zu bejahen.

Der erläuternde Bericht bestätigt diesen Bezug zur Kommunikationsüberwachung, indem er festhält, dass die gelieferten Angaben über die «***letzte zugriffsrelevante Aktivität***» zum einen der Identifikation dienen, zum anderen sei «der Zeitpunkt des letzten Zugriffs auf den E-Mail-Dienst massgeblich für den sogenannten Abschluss des Kommunikationsvorgangs». Die Staatsanwaltschaft könne nämlich alle E-Mails, die vor diesem letzten Zugriff eingetroffen sind – aufgrund des Umstands, dass diesfalls der Kommunikationsvorgang bereits als abgeschlossen gilt – nach Art. 263 ff. StPO edieren und ist nicht auf die vorgängige Genehmigung durch das Zwangsmassnahmengericht angewiesen. Inhalte, die nach dem letzten Zugriff eingehen, zu erlangen, stellte dagegen eine Echtzeitüberwachung dar. Für Randdaten sei diese Abgrenzung nicht erforderlich, da die Anbieterinnen mit vollen Pflichten Randdaten während 6 Monaten aufbewahren müssten.[133]

Der Bundesrat hält, wie schon erwähnt, weiter fest, dass die Speicherung der Angaben über den ***Ursprung der Verbindung*** (IP-Adresse bzw. Logfiles) lediglich bei Erstellung des Kontos nicht genüge, da diese Angaben im Allgemeinen nur für den Zeitraum der Vorratsdatenspeicherung eine Zuordnung zu einem Anschluss erlaubt.[134] Sind die Anbieterinnen fortan verpflichtet, stets Auskunft geben zu können, von welcher IP-Adresse und Portnummer der *letzte Zugriff* erfolgte, erfordert das allerdings eine fortlaufende Speicherung der Logfiles (Randdaten) für mindestens 6 Monate. Nur ein Dienst, der stets die Logfiles speichert, ist jederzeit in der Lage, Auskünfte über den letzten Zugriff zu gewähren. Das ist deutlich weitgehender als die Pflicht, bloss IP-Adressen zum Zeitpunkt der Kontoeröffnung zur Verfügung stellen zu müssen. Zur Vorratsdatenspeicherung dieser Randdaten verpflichtet sind nur FDA und AAKD mit vollen Pflichten, wie bereits eruiert wurde (→ Kap. 4.4). Andere AAKD müssten die Zugriffsinformationen nur liefern, sofern sie über diese verfügen.

Fraglich ist insofern nicht per se die Massnahme, sondern deren ***Einordnung als «Auskunft»*** und damit als Ausführungsbestimmung zu Art. 21 f. BÜPF. Zwar ist dem Bundesrat Recht zu geben, dass die letztlich gelieferte Auskunft selbst – je nach Verständnis – nicht zwingend direkt Randdaten einer Kommunikation betrifft, sondern eine einzelne IP-Adresse. Die Auskunft bedarf allerdings als Zwischenschritt einer Randdatenbearbeitung, also eben der Bearbeitung der IP-History. Hier wirkt erschwerend, dass ein letzter Zugriff auf einen Kommunikationsdienst i.d.R. direkten Kommunikationsbezug aufweist bzw. nicht nur die generelle Teilnehmeridentifikation ermöglicht, sondern unter Umständen auch Aufschluss darüber geben kann, wer der/die Absender:in einer konkreten Kommunikation war. Unglücklich ist in diesem Sinne besonders, dass die Normen zu den neuen Auskunftstypen – anders als andere – nicht explizit die Einschränkung

[133] EJPD, VÜPF/VD-ÜPF Erläuternder Bericht, 38.

[134] EJPD, VÜPF/VD-ÜPF Erläuternder Bericht, 38.

«zum Zweck der Benutzeridentifikation» enthalten. Der (mögliche) Kommunikationsbezug berührt das Fernmeldegeheimnis, weshalb das privilegierte Vorgehen nach Art. 21 f. BÜPF schwer zu rechtfertigen ist. *Die Rechtmässigkeit dieser neuen Auskunftstypen ist konsequenterweise infrage zu stellen. Eine Qualifikation als Überwachungstyp wäre aufgrund der indirekt zwingenden Randdatenbearbeitung und Auskunft über konkrete Zugriffe auf Kommunikationsdienste angemessen.*

4.6.5. Auskünfte über Zahlungen mittels Online-Transaktionen

Auch mit dem Art. 44 nVÜPF, d.h. beim ***Auskunftstyp «IR_17_PAY: Auskünfte über Zahlungen der Teilnehmenden von Fernmelde- und abgeleiteten Kommunikationsdiensten»*** würde der Pflichtenkatalog erweitert. Bis anhin fokussierten die Auskünfte auf herkömmliche bei der Anbieterin hinterlegte Banktransaktionen. Neu sollen «aufgrund der veränderten Zahlungsgewohnheiten» nicht mehr bloss Bankkontoinformationen, sondern auch Details über einzelne Kontozahlungen und elektronische Transaktionen abgefragt werden. Ermittlungsbehörden sollen damit Spuren einer Zahlungsquelle weiterverfolgen können.[135] Es sollen neu alle bekannten Angaben über getätigte Zahlungen, Transaktionen, Überweisungen, Zahlungsmittel und Zahlungskonten zur Bezahlung von Diensten, wie Datum, Betrag, Währung usf. abgefragt werden können.[136] Dieser Auskunftstyp wird damit massgeblich erweitert. Während es sich bei den bisher gestützt auf Art. 44 aVÜPF herausverlangten Kontoinformationen, d.h. Informationen zu Kontoinhaber:innen, um klassische Bestandesdaten (Teilnehmeridentifikation) handelt, sind die neuerlich erlangten Informationen von zweierlei Natur: Selbstredend werden die Daten zu Finanztransaktionen i.d.R. zum Zwecke der Identifikation einer unbekannten Person abgefragt. Allerdings ist die Auskunft über Transaktionen weitergehend auch eine Auskunft über das Zahlungsverhalten einer Person, d.h. eine eigentliche Überwachung eines Zahlungsverhaltens. Es stellt sich die Frage, ob sich das noch unter eine Bestandesdatenabfrage nach Art. 21 f. BÜPF subsumieren lässt und alleinig durch polizeiliche Abfragen erlangt werden darf. Vor allem die «Angaben zu getätigten Zahlungen» gemäss dem neuen Abs. 1 lit. f erscheinen diesbezüglich problematisch. Es geht aus der Norm auch nicht hervor, dass diese Zahlungsinformationen einzig zur Teilnehmeridentifikation genutzt werden können. Es könnten deshalb theoretisch auch Auskünfte nach IR_17_PAY getätigt werden, die über Bestandesdatenauskünfte hinausgehen. Dann wiederum bedürfte es aber einer gerichtlichen Genehmigung. *Je nach konkreter Ausgestaltung dieser Auskünfte in der Praxis ist die Qualifikation als Bestandesdatenabfrage nicht mehr zulässig. Stützen sich die Auskünfte zu solchen über reine Bestandesdaten hinausgehende Zahlungsinformationen nicht auf die StPO, samt entsprechenden Rechtsschutzvorkehrungen, wären sie folglich unrechtmässig.*

4.6.6. Änderungen bei den Überwachungstypen

Beim neu vorgeschlagenen ***Überwachungstyp «RT_61_NA_CC-TRUNC-IRI»*** geht es um die Echtzeitüberwachung von Netzzugangsdiensten mittels einer neuen standardisierten Variante der Überwachung (sog. Paketkürzung), die es erlaubt, das Datenvolumen zu reduzieren.[137] Im Vordergrund stehen Effizienzüberlegungen. Ein Ausbau der Überwachung ist damit nicht

[135] EJPD, VÜPF/VD-ÜPF Erläuternder Bericht, 40.

[136] EJPD, VÜPF/VD-ÜPF Erläuternder Bericht, 40.

[137] EJPD, VÜPF/VD-ÜPF Erläuternder Bericht, 43 f.

vorgesehen, da – gestützt auf die entsprechende Zwangsmassnahme – auch heute schon Rand- und Inhaltsdaten (auch ungekürzt) überwacht werden können.

Der neue ***Überwachungstyp «HD_62_IP: rückwirkende Überwachung zum Zweck der Teilnehmeridentifikation bei Internetverbindungen»*** betrifft die Pflicht der Anbieterinnen, bei Internetverbindungen alle Angaben über die Urheberschaft und Herkunft der Verbindung sowie im Falle von Mehrfachergebnissen ggf. die Schnittmenge zu liefern (Art. 60a nVÜPF). Der Typ werde eingeführt, um das Problem zu lösen, welches sich ergibt, wenn bei den Auskünften zu dynamischen IP-Adressen Mehrfachergebnisse geliefert werden, die keine eindeutige Identifikation zulassen und bei denen eine Lieferung der «Gesamtergebnisse» aufgrund der hohen Anzahl unbeteiligter Dritter unverhältnismässig wäre (dazu bereits → Kap. 4.6.2).[138] Bei diesem Überwachungstyp wird also bei einer hohen Anzahl von Anschlüssen eine Identifikation vorgenommen, weshalb der Bundesrat richtigerweise von einem Grundrechtseingriff ausgeht, der in der Schwere mit dem Antennensuchlauf vergleichbar ist.[139] Da dafür eine Bearbeitung von Randdaten und eine «Massenabfrage» von Bestandesdaten samt Schnittstellenbildung vonnöten ist, scheint die Einordnung als Randdatenüberwachung und das Erfordernis der gerichtlichen Genehmigung folgerichtig – was indes auch für die damit verwandten neuen Auskunftstypen ebenfalls zu prüfen wäre (→ Kap. 4.6.2 und 4.6.3). *Der neue Überwachungstyp ist entsprechend rechtmässig, auch er bildet aber selbstredend eine Pflicht zur weitergehenden Mitwirkung der Anbieterinnen.* Die Ausweitung der Pflichten folgt dem Bedürfnis der Behörden, bei einer hohen Anzahl von identifizierten möglichen Nutzer:innen im Falle von dynamischen IP-Adressen, dennoch weitere Ermittlungen anstellen zu können. Vor allem dort, wo IPv4-Adressen verwendet werden, habe die hohe Anzahl möglicher Ergebnisse in der Vergangenheit oft in eine «kriminalistische Sackgasse» geführt.[140]

Bei ***weiteren Überwachungstypen*** sollen mit der Revision des Weiteren gewisse Änderungen vorgenommen werden, die primär die Erweiterung der Möglichkeiten betrifft, auf welche (technische) Art gewisse Informationen geliefert werden können (Art 60 lit. g nVÜPF). Aufgrund technischer Neuerungen überflüssig gewordene Überwachungstypen werden dagegen aufgehoben (Art. 64 und 65 aVÜPF). Zudem wurde beim Antennensuchlauf die Formulierung auf eine Mehrzahl an umfasster Mobilfunkzellen und WLAN-Zugängen erweitert (Art. 66 nVÜPF), damit der Überwachungstyp in Einklang mit der neuen Abrechnungsweise steht.[141]

5. Fazit: Beurteilung der Rechtmässigkeit und Empfehlungen

Die vorangehenden Ausführungen nahmen sich dem Ziel an, die vorgeschlagene VÜPF-Revision unter die Lupe zu nehmen. Die Vorlage ist äusserst komplex, die Materie sowohl technisch als auch juristisch in vielen Belangen schwer verständlich. Zugleich ist die öffentliche Debatte rege und vorwiegend kritisch. Entsprechend rechtfertigte es sich, die Änderungen im Detail zu analysieren. Es zeigte sich dabei, dass die einleitend erwähnte Aussage von Seiten Behörden, es ändere sich am Pflichtenkatalog der Anbieterinnen nichts, nicht zutrifft. Die vom Bundesrat

[138] Vgl. EJPD, VÜPF/VD-ÜPF Erläuternder Bericht, 44.

[139] EJPD, VÜPF/VD-ÜPF Erläuternder Bericht, 45.

[140] EJPD, VÜPF/VD-ÜPF Erläuternder Bericht, 46.

[141] EJPD, VÜPF/VD-ÜPF Erläuternder Bericht, 47.

vorgeschlagene Revision käme einer Ausweitung des Kreises der Verpflichteten sowie einer Ausweitung der Verpflichtungen gleich. Das räumt der Bundesrat eigentlich bereits selbst ein, wenn er in seinem Bericht festhält, dass den Mitwirkungspflichtigen genügend Zeit gegeben werden muss «für die Umsetzung der neuen Auskunfts- und Überwachungspflichten»[142]. Die staatliche Überwachung in der Schweiz würde insofern einen Ausbau erfahren. Allerdings sind viele der öffentlich geäusserten Befürchtungen oder auch pauschalen Aussagen ebenso wenig zutreffend. Viele der Änderungen betreffen technische Details und sind zudem vom geltenden Gesetzesrecht umfasst. Eine Würdigung sollte also differenziert ausfallen. Dennoch konnte die Auseinandersetzung verschiedene Aspekte offenlegen, die aus juristischer Sicht zu beanstanden sind.

Die ***Ergebnisse*** der Analyse lassen sich im Wesentlichen wie folgt zusammenfassen:

- Die Gesetzesdelegation in Art. 2 Abs. 2 nBÜPF ist im Allgemeinen zulässig, indem sie den Bundesrat zu *Ausführungsbestimmungen* betreffend die Kategorien der Mitwirkungspflichtigen, d.h. der adressierten Anbieterinnen, ermächtigt. Zulässig ist die Delegation, da die Grundzüge der Kategorisierung im Gesetz selbst geregelt sind und sie sich auf eine bestimmte Materie (nähere Umschreibung der Kategorien von Mitwirkungspflichtigen) bezieht.[143] Die gestützt auf die Delegation erlassenen Normen müssen sich aber in den Schranken des Gesetzes bewegen, d.h. sie müssen das Gesetz präzisieren. Über die gesetzlichen Ermächtigungen hinausgehende Verpflichtungen, die nicht mehr der Ratio des BÜPF entsprechen, sind unzulässig und von der Delegation nicht umfasst.
- Die Neuerung, dass bei den Voraussetzungen einer Herunterstufung von FDA der Jahresgesamtumsatz des Unternehmens massgeblich sein soll, steht nicht in Einklang mit Art. 26 Abs. 6 BÜPF und stellt folglich keine rechtmässige Präzisierung dar.
- Dass AAKD ab 5000 Teilnehmende als «AAKD mit reduzierten Pflichten» neu einem erweiterten Pflichtenkatalog unterstehen sollen, ist weder verhältnismässig noch von Art. 22 Abs. 4 und Art. 27 Abs. 3 BÜPF vorgesehen. Das Gesetz schränkt den Bundesrat dahingehend ein, als dass nur «Dienstleistungen von grosser wirtschaftlicher Bedeutung oder für eine grosse Benutzerschaft» eine Hochstufung rechtfertigen können. Das ist bei Anbieterinnen mit 5000 Teilnehmenden nicht zu bejahen. Die entsprechende Neukategorisierung ist demnach keine blosse Auslegung der vom Gesetz vorgesehenen Kategorisierung und folglich unrechtmässig. Das entfaltet Konsequenzen für die Beurteilung der gestützt darauf für diese AAKD-Kategorie vorgesehenen zusätzlichen Pflichten betreffend die Erfassung, Speicherung und Herausgabe von Bestandes- und Randdaten. Sie sind unzulässig, sofern sie nicht ebenso für AAKD ohne erweiterte Pflichten nach Art. 22 Abs. 4 und Art. 27 Abs. 3 BÜPF vorgesehen wären.
- Bei den Voraussetzungen einer Hochstufung zu einer AAKD mit vollen Pflichten ist es zulässig, auf alle von der Anbieterin angebotenen Kommunikationsdienste abzustellen. Nicht jedoch ist das Abstellen auf den Umsatz des Gesamtunternehmens vom Gesetzestext gedeckt. Die diesbezüglich vorgeschlagene Neuerung wäre nicht gesetzeskonform. Die heutige Regelung, dass bei der Hochstufung auf die Anzahl Auskunfts- oder Überwachungsersuchen abgestellt werden soll, ist aber ebenso wenig zulässig. Der

[142] EJPD, VÜPF/VD-ÜPF Erläuternder Bericht, 7.

[143] Vgl. BSK BV-WYTTENBACH/WYSS, Art. 164 N 7.

Gesetzestext lässt keinen Raum für die Einführung zusätzlicher Kriterien. Die «Überwachungsrelevanz» als massgeblich zu erachten, ist vom Gesetzestext folglich nicht gedeckt.

- AAKD mit vollen Pflichten können verpflichtet werden, Teilnehmende mit geeigneten Mitteln zu identifizieren. Eine entsprechende Pflicht für AAKD mit reduzierten Pflichten ist aus genannten Gründen nicht zulässig. Sollte dies anders beurteilt werden, wäre allerdings die Vorgabe, dass Dienste wie z.B. E-Mail-Dienste, die Identifikation durch die Speicherung von IP-Histories bzw. Logfiles, d.h. Randdaten, ermöglichen, unzulässig. Dies käme einer Vorratsdatenspeicherung von Randdaten über Umwege, genauer über die Statuierung von Identifikationspflichten, gleich.
- Die genauen Pflichten betreffend die Aufbewahrung und Herausgabe von Bestandes- und Randdaten lassen sich für die Mitwirkungspflichtigen im Geflecht von BÜPF und VÜPF nur mit viel Mühe und auch dann nur unzureichend erkennen. Unklare Vorgaben wie diese zu Daten betreffend die «benachbarten Netze», aber ebenso keine klare Auflistung der zu speichernden Randdaten zum Zwecke der Überwachungen sind der Voraussehbarkeit der Massnahmen und der Rechtssicherheit nicht zuträglich. Die hohe Invasivität insbesondere der Vorratsdatenspeicherung, aber auch der Inhalts- und Randdatenerhebung im Allgemeinen verlangt nach einer klaren und differenzierten Regelung. Nur so kann auch die Verhältnismässigkeit der Massnahmen gewahrt und überhaupt beurteilt werden. Die genauen Pflichten ergeben sich oftmals erst über Umwege (z.B. über die Pflicht, gewisse Überwachungstypen durchführen zu können, ergibt sich die Pflicht zur Vorratsspeicherung der zugehörigen Informationen). Das ist zu kritisieren. Ebenfalls wäre es adäquater, wenn sich die Grundzüge der Aufbewahrungs- und Herausgabepflichten (gerade eben etwa in Bezug auf Logfiles) aus dem Gesetz ergeben würden. Da die Pflichten nicht nur schwer erkennbar, sondern darüber hinaus wenig differenziert ausfallen, ist folglich generell zweifelhaft, ob sie einer Verhältnismässigkeitsprüfung standhalten würden und Anbieterinnen – auch die voll Verpflichteten – gestützt darauf rechtmässig zur entsprechenden Mitwirkung angehalten werden könnten.
- FDA mit vollen Pflichten könnten weiterhin, AAKD mit vollen Pflichten könnten neu dazu angehalten werden, serverseitige Verschlüsselungen sowie Transportverschlüsselungen aufzuheben, sofern sie über den Schlüssel verfügen und ihn nutzen können. Dies ist als rechtmässig zu beurteilen. Von der vorgeschlagenen (eher unbestimmten) Regelung lässt sich hingegen keine Pflicht ableiten, gewisse Verschlüsselungsarten zu unterlassen oder Schlüssel per se durch die Anbieterin zur Verfügung zu halten.
- Die vorgeschlagene Pflicht, bei Auskünften zu statischen IP-Adressen bei Mehrfachergebnissen die Anzahl der Ergebnisse bekanntzugeben, ist nicht zu beanstanden. Dass bei dynamischen IP-Adressen im Falle von Mehrfachergebnissen nicht nur die Anzahl, sondern auch die Ergebnisse selbst geliefert werden müssen, ist weitreichender. Insbesondere sind unbeteiligte Dritte von dieser Massnahme berührt. Für die Rechtmässigkeit dieser Massnahme wird es entscheidend darauf ankommen, wie hoch die Zahl der gelieferten Teilnehmerdaten sind und welchem Ermittlungszweck sie dienen. Bei zurückhaltender Auslegung und Praxis kann die Massnahme jedoch zulässig sein.
- Ein neuer Auskunftstyp soll die Schnittmengenbildung bei IP-Adressen zum Zwecke der Teilnehmeridentifikation ermöglichen. Die Massnahme verlangt den Anbieterinnen die

Teilnehmeridentifikationen zu Randdaten im grösseren Stil (Massenabfragen) ab. Den Behörden wird zwar nur die Schnittmenge zum Zwecke der Identifikation geliefert, als Zwischenschritt ist jedoch eine Bearbeitung von Daten zahlreicher Nutzer:innen nötig, womit die Massnahme eine grosse Streubreite erhält und die Anbieterinnen zu weitgehenden Analysen verpflichtet. Es ist mindestens als fraglich zu werten, ob dieser neue Auskunftstyp bei allen Delikten und ohne staatsanwaltliche oder richterliche Überprüfung als verhältnismässig gelten kann.

- Eine ähnliche, wenn auch weitergehende Problematik zeigt sich bei den neuen Auskunftstypen, die E-Mail-Dienste und andere Kommunikationsdienste verpflichten, Auskunft über die IP-Adresse des letzten Zugriffs auf den Dienst zu erteilen. Der letzte Zugriff auf einen Kommunikationsdienst muss zwar nicht zwingend, wird aber sehr oft einen Bezug zu einer Kommunikation aufweisen. Diese Abfrage hat also das Potenzial, das Fernmeldegeheimnis unmittelbar zu berühren. Darüber hinaus verlangt diese Analyse, dass Anbieterinnen Randdaten (IP-Adressen) fortlaufend erheben und auf Vorrat (mindestens 6 Monate) speichern. Im Falle eines Auskunftsbegehrens nach diesen Typen müssen sie diese Randdaten dann bearbeiten. Es ist zu bestreiten, dass die Einordnung dieser Massnahme als das Fernmeldegeheimnis nicht berührende, nach dem vereinfachten Verfahren durchzuführende Bestandesdatenabfrage qualifiziert. Die Anbieterinnen werden zur Bearbeitung von Randdaten der Kommunikation verpflichtet und zu Auskünften gestützt auf eine Vorratsdatenspeicherung. Das ist invasiv. Der Grundrechtsschutz und die gesetzlichen Vorgaben müssten damit in Einklang stehen.
- Auch die neue Pflicht von Kommunikationsdiensten, Angaben zu getätigten Zahlungen und Transaktionen, Zahlungsmitteln usw. zu machen, betrifft das Verhalten von Online-Nutzer:innen und nicht bloss «beständig» bei den Anbieterinnen vorliegende Daten. Die entsprechende Qualifikation als Bestandesdaten und mit ihr als Auskunft in der Terminologie der VÜPF überzeugt folglich nicht.

Dem Bundesrat ist gestützt auf diese Ergebnisse zu empfehlen, die Vorlage erneut zu überarbeiten. Die Gesetzesdelegation in Art. 2 Abs. 2 nBÜPF ermächtigt zur Präzisierung, weshalb sich der Bundesrat – auch aus demokratiepolitischen Überlegungen – wirklich auf Präzisierungen beschränken sollte. Es ist dem Bundesrat in diesem Sinne zu empfehlen, (1.) davon abzusehen, AAKD mit über 5000 Teilnehmenden bereits einem erweiterten Pflichtenkatalog zu unterstellen. Die Pflichten des BÜPF adressieren private Unternehmen und schränken diese in ihren Freiheiten ein. Diese Einschränkung hat sich an enge gesetzliche Vorgaben zu halten. Sie muss allem voran verhältnismässig sein, was bei grossen wirtschaftlichen Akteuren anders zu beurteilen ist als bei kleinen und mittelgrossen. Das gilt nicht zuletzt für die Identifikationspflichten, die sich neu auch für kleinere Anbieterinnen ergeben würden. Da mit der vollen Verpflichtung von AAKD sehr weitgehende Pflichten einhergehen, ist dem Bundesrat (2.) zu empfehlen, dass er die Kriterien, welche zu einer Hochstufung führen, erneut überprüft. Das Abstellen auf den Gesamtumsatz ist zu kritisieren und wird – in Anbetracht der Konsequenzen, die mit dem Upgrade einhergehen – mutmasslich zu Beschwerdeverfahren führen, die in Aufhebungen von Normen resultieren könnten.[144]

[144] In diese Richtung auch WEBER, 11.

Aufgrund der hohen Invasivität und Brisanz der Vorratsdatenspeicherung ist (3.) das System und das komplexe Zusammenspiel der VÜPF- und BÜPF-Normen diesbezüglich erneut zu überprüfen. Voll verpflichtete FDA und AAKD müssen grundsätzlich Bestandes- und Randdaten auf Vorrat speichern, solche mit reduzierten Pflichten dagegen nur die Daten zur Teilnehmeridentifikation. Die Zulässigkeit Letzteres wird vorliegend generell bestritten, da die entsprechende Gesetzesdelegation nicht ausreicht. Unabhängig davon lassen jedoch neue Auskunftstypen, welche die Analyse von Mehrfachergebnissen, die Schnittmengenbildung und die Auskünfte über den letzten Zugriff auf Kommunikationsdienste betreffen, die Frage aufkommen, inwieweit es rechtmässig ist, dass gestützt auf vereinfachte Bestandesdatenabfragen, d.h. ohne gerichtliche Überprüfung, auch die massenweise Nutzung sowie die Bearbeitung von Randdaten verlangt werden kann. Das ist besonders heikel, da die entsprechenden Randdaten von den voll verpflichteten Anbieterinnen auf Vorrat gespeichert werden müssen. Diese auf Vorrat gespeicherten Daten können dann faktisch ohne massgebliche Einschränkung via Bestandesdatenabfragen genutzt werden, was in vielen Fällen zu einem Missverhältnis zwischen Eingriffsintensität und Rechtsschutz führen wird. Es ist deshalb sinnvoll, Auskünfte und Überwachungen klarer zu trennen und Auskünfte, die implizit eine Bearbeitung vorrätig gespeicherter Randdaten (insbesondere Logfiles) involviert, dem Rechtsschutz der Randdatenerhebung zu unterstellen. Alternativ könnte im Sinne einer Weiterentwicklung zukünftig eine Zwischenstufe – vergleichbar mit der angesprochenen E-Evidence-Verordnung der EU (→ Kap. 4.6.4) – geschaffen werden, um den Umgang mit IP-Adressen zu flexibilisieren und vor allem zu klären. Das würde für Abfragen gelten, die zwar letztlich der Identifikation dienen, als Zwischenschritt aber die Bearbeitung von Internetverhaltensdaten, d.h. Überwachungsdaten, erfordern und deshalb das Fernmeldegeheimnis in erhöhtem Masse berühren. Um die Verhältnismässigkeit der für voll verpflichtete Anbieterinnen vorgeschriebenen Vorratsdatenspeicherung sicherzustellen, ist jedenfalls eine Überprüfung des Zusammenspiels von StPO, BÜPF und VÜPF angezeigt.

In der Summe zeigt die Analyse, möge es bei der Revision auf den ersten Blick noch so sehr um Details gehen, dass das Schweizer Überwachungsrecht aufgrund seiner historisch bedingten Ausrichtung auf Post- und Fernmeldedienste allgemein Schwächen aufweist. Überwachungen und die Ermittlungsarbeit im Allgemeinen betreffen heute zu einem sehr wesentlichen Teil Internetdienste. Sie weisen oft, aber nicht immer einen Bezug zu einer konkreten Kommunikation auf. Der Fokus des BÜPF auf Eingriffe in das Fernmeldegeheimnis schmälert den Anwendungsbereich von vornherein. Allgemeine Internetüberwachungen oder Dienste, die nicht per se einen Kommunikationsbezug aufweisen, sind nicht umfasst. Elektronische Beweismittel können sie aber ebenso betreffen. Dass sie heute auf gänzlich andere Weise, über die Beschlagnahme samt Siegelung beschafft werden müssen, schafft ein Ungleichgewicht, sind doch so teilweise Inhaltsdaten einfacher zu erlangen als Randdaten. Umgekehrt werden durch die Neuerungen im BÜPF zunehmend Online-Dienste verpflichtet gestützt auf Normen, die ursprünglich auf Fernmeldedienste zugeschnitten waren. Das führt zu einem sehr komplexen Normengeflecht, was wiederum den rechtspolitischen Diskurs deutlich erschwert.

Der Bundesrat hat im April dieses Jahres entschieden, die Schaffung einer Gesetzesgrundlage zu prüfen, um den grenzüberschreitenden Zugriff auf elektronische Beweismittel mit einem allfälligen Anschluss an das System der EU zu prüfen.[145] Das weist insoweit einen Zusammenhang mit

[145] Medienmitteilung des Bundesrats v. 9.4.2025, <https://www.news.admin.ch/de/nsb?id=105595> (Abruf: 1.11.2025).

der vorliegenden Diskussion auf, als dass alle Informationen, die Anbieterinnen in der Schweiz speichern müssen, gestützt auf die Regelung der EU auch grenzüberschreitend zugänglich gemacht werden können. Kurz: «Was da ist, kann auch geholt werden». Die Regelung der EU sieht darüber hinaus aber auch andere Datenkategorien, ein anderes Zwangsmassnahmensystem samt Rechtsschutz und vor allem den bereits erwähnten weiteren Anwendungsbereich auf alle Internetdienste («Dienste der Informationsgesellschaft») vor.[146] Im Zuge eines allfälligen Anschlusses wäre deshalb zu prüfen, ob auch das Schweizerische Zusammenspiel zwischen den Zwangsmassnahmen der StPO und den Mitwirkungspflichten der BÜPF einer grundlegenden Überprüfung unterzogen werden sollte. Dies wäre zu empfehlen, soll einerseits die Ermittlungsarbeit der Behörden mit den Gegebenheiten des digitalen Zeitalters Schritt halten können. Eine Modernisierung wäre angezeigt. Andererseits wäre eine übersichtlichere, kohärentere Regelung auch dem rechtspolitischen Diskurs zuträglicher. Die Balance zwischen Sicherheits- sowie Strafverfolgungsinteressen auf der einen und Grundrechtsschutz auf der anderen Seite könnte so transparenter ausgehandelt werden, Befürchtungen aber auch entgegengewirkt werden. Es handelt sich bei den Regelungen de lege lata und de lege ferenda – anders als in den Medien kolportiert – sicherlich nicht um etwas, was «autoritäre Überwachungsstaaten kopiert».[147] Dennoch hat die Vorlage rechtliche Schwächen und wäre in der vorliegenden Form in mehreren Belangen unrechtmässig. Dies zu beheben, würde unserem demokratischen Rechtsstaat gut anstehen.

[146] Die Verordnung gilt für drei verschiedene Kategorien von Diensteanbietern, namentlich (1.) elektronische Kommunikationsdienste, (2.) Internetdomänenamen- und IP-Nummerierungsdienste, sowie (3.) Dienste der Informationsgesellschaft (Art. 3 Ziff. 3 E-Evidence-Verordnung). Insbesondere die letzte Kategorie ist sehr weit.

[147] Republik v. 7.5.2025, <https://www.republik.ch/2025/05/07/die-schweiz-ist-drauf-und-dran-autoritaere-ueberwachungsstaaten-zu-kopieren> (Abruf: 1.11.2025).

.

Materialienverzeichnis

Botschaft zum Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) vom 27. Februar 2013, BBl 2013 2683 (zit. Botschaft BÜPF).

Botschaft zur Revision des Fernmeldegesetzes vom 6. September 2017, BBl 2017 6559 (zit. Botschaft FMG).

EJPD, Teilrevisionen von Ausführungserlassen des Bundesgesetzes über die Überwachung des Post- und Fernmeldeverkehrs (BÜPF), Erläuterungen vom 15. November 2023 (zit. EJPD, BÜPF Erläuterungen).

EJPD, Teilrevisionen zweier Ausführungserlasse zur Überwachung des Post-und Fernmeldeverkehrs (VÜPF, VD-ÜPF), Erläuternder Bericht zur Eröffnung des Vernehmlassungsverfahrens vom 8. Januar 2025 (zit. EJPD, VÜPF/VD-ÜPF Erläuternder Bericht).

EJPD, Teilrevisionen zweier Ausführungserlasse zur Überwachung des Post-und Fernmeldeverkehrs (VÜPF, VD-ÜPF), Stellungnahmen Vernehmlassung (zit. EJPD, VÜPF/VD-ÜPF Stellungnahmen).

Literaturverzeichnis

BETSCHMANN SIMON, Randdatenerhebung im Fernmeldeverkehr gemäss Art. 273 StPO, in: AJP, Heft 3, 2019, 358 ff.

DEUSCH FLORIAN/EGGENDORFER TOBIAS, Beauftragte für IT-Sicherheit und Informationssicherheit, Frankfurt a.M. 2024.

HANSJAKOB THOMAS, Überwachungsrecht der Schweiz, Zürich 2018.

HERFERT MICHAEL/LANGE BENJAMIN/SPYCHALSKI DOMINIK, Verschlüsselung in der Cloud, in: digma, Heft 3, 2019, 128 ff.

KNEUPER RALF, Rolle der Transportverschlüsselung für die sichere E-Mail-Kommunikation, in: DuD, Heft 2, 2019, 76 ff.

NIGGLI MARCEL ALEXANDER/HEER MARIANNE/WIPRÄCHTIGER HANS (Hrsg), Basler Kommentar Schweizerische Strafprozessordnung/Jugendstrafprozessordnung (StPO/JStPO), Bd. II, 3. Aufl., Basel 2023 (zit. BSK StPO-Bearbeiter).

PETERS ANNE/ALTWICKER TILMANN, Europäische Menschenrechtskonvention, 2. Aufl., München 2012.

REINDL-KRAUSKOPF SUSANNE/SALIMI FARSAM/STRICKER MARTIN, IT-Strafrecht, Wien 2018.

RINGLAND KRISTINA, The European Union's Data Retention Directive and the United States's Data Preservation Laws: Finding the Better Model, in: Washington Journal of Law, Technology & Arts, Vol. 5(3), 2009, 13 ff.

SIMMLER MONIKA, Gegenüberstellung des Schweizer Rechts und der E-Evidence-Gesetzgebung der EU – eine Auslegeordnung, in: forumpoenale, Heft 2, 2025, 132 ff.

WALDMANN BERNHARD/BELSER EVA MARIA/EPINEY ASTRID, Basler Kommentar Bundesverfassung, 2. Aufl., Basel 2025 (zit. BSK BV-Bearbeiter).

WEBER ROLF H., Kurzgutachten: Teilrevision der Post- und Fernmeldeverkehrsordnung, Zürich 2025.

Kompetenzzentrum für Strafrecht und Kriminologie
Universität St. Gallen (SK-HSG)
Bodanstrasse 3
9000 St. Gallen
+41 71 224 31 96
strafrecht@unisg.ch
strafrecht.unisg.ch