piratenpartei
www.piratenpartei.ch

Piratenpartei Schweiz, 3000 Bern

Stellungnahme der Piratenpartei Schweiz zu den Teilrevisionen zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF)

Sehr geehrter Herr Bundesrat Jans

Sehr geehrte Damen und Herren

Bezugnehmend auf Ihre Vernehmlassungseröffnung vom 29.01.2025 nehmen wir gerne Stellung.

Vorab, wir Piraten finden es sehr bedenklich, dass Sie für die Stellungnahme auf eine proprietäre Software verweisen (Word der Firma Microsoft), wo es doch heute zahlreiche offene und freie Dateiformate gibt. Wir entsprechen ihrem Wunsch mit einer docx-Datei, welche auch in neueren Word Versionen geöffnet werden kann.

Die Piratenpartei Schweiz setzt sich seit Jahren für eine humanistische, liberale und progressive Gesellschaft ein. Dazu gehören die Privatsphäre der Bürger, die Transparenz des Staatswesens, inklusive dem Abbau der Bürokratie, Open Government Data, den Diskurs zwischen Bürgern und Behörden, aber auch die Abwicklung alltäglicher Geschäfte im Rahmen eines E-Governments. Jede neue digitale Schnittstelle und Applikation bedingt aber eine umfassende

piratenpartei
www.piratenpartei.ch

Piratenpartei Schweiz, 3000 Bern

Risikoanalyse und Folgeabschätzung.

Gerne nehmen wir wie folgt Stellung:

Allgemein:

Die Piratenpartei lehnt das BÜPF mit den dazugehörigen Verordnungen weiterhin in Gänze ab. Das Gesetz greift unverhältnismässig in das Recht auf Schutz der Privatsphäre ein und trägt zum chilling effect bei der Meinungs- und Informationsfreiheit bei. Es sollte in dieser Form nicht existieren.

Es zeigt sich ausserdem in dieser Vorlage erneut, was seit Beginn gesehen worden ist: Der Überwachungsstaat wird schleichend aber stetig nach mehr Kontrolle verlangen. So haben sich zuletzt die Überwachungen durch den Staat in nur einem Jahr verdoppelt.[1] Die vorliegende Revision der Verordnungen wird diesen Ausbau weiter beschleunigen und ist entsprechend abzulehnen.

Insbesondere und mindestens die automatisierte Abfrage der Daten bei den FDA und AAKD (Art. 18 Abs. 2 u. Abs. 4 VÜPF bzw. VE-VÜPF), die Vorratsdatenspeicherung (Art. 26 Abs. 5 BÜPF) sowie die Entfernung von Verschlüsselungen (Art. 26 Abs. 2 Bst. c BÜPF) sollten aus den schon in Kraft getretenen Texten vollständig gestrichen statt nun weiteren Personen aufgedrängt werden (vgl. unten Art. 16b i.V.m. Art. 16c VE-VÜPF).

Nach dem erläuternden Bericht zu den Teilrevisionen der VÜPF und VD-ÜPF sollen die Änderungen eine Revision des FMG umsetzen, welche dem Bundesrat eine feinere Unterteilung der Mitwirkungspflichtigen (MWP) ermöglichen soll. Ausserdem soll das VÜPF KMU-freundlicher werden, indem klarere Definitionen für die Einstufung der MWP gegeben werden.[2]

[1] Überwachungen durch den Staat haben sich verdoppelt – das sind die Gründe, https://www.tagesanzeiger.ch/ueberwachungen-durch-den-staat-sind-in-einem-jahr-um-das-doppelte-gestiegen-das-sind-die-gruende-165465973955.

[2] Erläuternder Bericht, S. 3f.

Es ist leider leicht zu erkennen, dass vielen Unternehmen das genaue Gegenteil widerfahren wird. Statt einer Vereinfachung oder Minderbelastung ist mit einer massenhaften Mehrbelastung zu rechnen. Ja, der Übergang für Anbieterinnen abgeleiteter Kommunikationsdienste (AAKD) zwischen «ohne weitergehende Auskunftspflichten» und «weitergehenden Auskunftspflichten» (Art. 22 VÜPF) sowie AAKD mit oder ohne «weitergehenden Überwachungspflichten» (Art. 52 VÜPF) wird abgefedert mit einer Zwischenstufe. Aber jene Zwischenstufe ist leicht erreicht – der Anbieter braucht lediglich 5000 «Teilnehmende» -, so dass am Ende mehr in der mittleren Kategorie landen werden, während sie nach den aktuellen Kriterien in der Kategorie ohne weitergehende Pflichten verbleiben würden. Für Unternehmen wird dies zu einem Mehraufwand und für die Bevölkerung zu mehr Überwachung durch die Hintertür führen.

Die Schweiz geniesst bisher, trotz einigen Lädierungen (z.B. das BÜPF an sich), in den Bereichen Privatsphäre und Datenschutz ein positives Ansehen, weil sie jene als hohes Gut verteidigt. Dies nicht nur bei den eigenen Bürgerinnen und Bürgern sondern auch international. Das beschert den direkt involvierten Unternehmen bessere Umsätze und trägt auch zum guten Ruf der Schweiz als Ganzes bei. Dieses vertrauenswürdige Image würde mit der Annahme der VÜPF Vorlage schlicht in Flammen gesetzt. So wird neu selbst der mittleren Kategorie der AAKD die Entschlüsselung nach Art. 50a VE-VÜPF auferlegt, was bisher den grossen Fernmeldedienstanbietern (FDA) und einigen wenigen riesigen AAKD vorbehalten war. Davon wären nicht nur VPN Anbieter betroffen, sondern u.a. auch Cloudspeicher-, E-Mail- oder Messenger-Anbieter.[3] Art. 19 Abs. 1 VE-VÜPF verlangt neu auch die Nutzeridentifikation durch mehr Anbieter, was die Privatsphäre online zusätzlich aushebelt. Jegliches Vertrauen in schweizerische Dienste müsste also schlicht eingestellt werden.

[3] Erläuternder Bericht, S. 19f.

Piratenpartei Schweiz, 3000 Bern

Zu den einzelnen Artikeln:

Art. 16a-h

Grundsätzlich ist eine klarere Auflistung der betroffenen Dienste sowie die Kriterien zur Kategorisierung an einer Stelle zu begrüssen. Aber die neue Kategorie mit reduzierten Pflichten sollte gänzlich gestrichen werden.

Art. 16b

Anregung 1: Streichung von Art. 16 Abs. 1 Bst. b Ziff. 1

Anregung 2: Streichung der Änderung von Umsatz mit Fernmeldediensten und abgeleiteten Kommunikationsdiensten zu Gesamtumsatz

Begründung:

Gemäss Art. 16b Abs. 1 Bst. b VE-VÜPF können sich FDA zu Diensten mit reduzierten Pflichten herunterstufen lassen, wenn sie (Ziff. 1) keine Überwachungsaufträge zu 10 verschiedenen Überwachungszielen in den letzten 12 Monaten hatten und (Ziff. 2) das gesamte Unternehmen in der Schweiz einen geringeren Jahresumsatz als 100 Millionen hat.

1

Das Kriterium in Ziffer 1 lehnen wir ab und die Chance zur Streichung im

Rahmen der Revision sollte genutzt werden. Die Anfragen bzw. Überwachungsmassnahmen nehmen tendenziell zu[4], was i.V.m. Ziffer 1 zu einer automatischen Zunahme von FDA mit vollen Überwachungspflichten führen wird. Dieses Kriterium belohnt geradezu den Ausbau des Überwachungsstaates mit vereinfachter und noch mehr Überwachung.

2

Die bisherige Regelung in Art. 51 VÜPF spricht aber noch von einem «Jahresumsatz in der Schweiz mit Fernmeldediensten und abgeleiteten Kommunikationsdiensten von 100 Millionen». Neu soll also nicht mehr nur der Umsatz mit solchen Diensten sondern der gesamte Umsatz eines Unternehmens zur Hand genommen werden.

Im erläuternden Bericht wird dies mit einer Vereinfachung begründet, da es sich in der Praxis gezeigt habe, dass der gesamte Umsatz viel einfacher zu ermitteln und belegen sei (Bericht S. 16). Wer hätte es gedacht. Man möge es dem Dienst ÜPF bitte zumuten, diese Abgrenzung vorzunehmen oder alternativ die Herunterstufung zur FDA mit reduzierten Pflichten ungesehen zu akzeptieren - diese Variante würde es wesentlich mehr Personen erlauben, die propagierte «Vereinfachung» zu erleben. Denn damit wären nicht nur die Angestellten des Dienstes ÜPF sondern auch die Unternehmen entlastet. Was «Vereinfachung» angeht, ist die ungesehene Herabstufung auch klar der Vorlage überlegen, da die Entlastung der Angestellten beim Dienst ÜPF nochmals höher wäre.

Mit dieser neuen Definition erschwert man es ausserdem grösseren Unternehmen, in diesen Bereich zu investieren, wenn sie bisher nichts damit zu tun hatten. Sie würden sofort in die Kategorie mit vollen Pflichten fallen, was

[4] Statistik zur Fernmeldeüberwachung: Mehr Überwachungsmassnahmen, https://www.news.admin.ch/de/nsb?id=94661; Überwachung im Internet: Wen dürfen die Behörden wann überwachen?, https://blog.init7.net/de/ueberwachung-im-internet/ .

den Einstieg erheblich unattraktiver macht. Selbes gilt auch für FDA, die die Schwelle von 100 Millionen noch nicht erreicht haben, aber gerne in andere Bereiche investieren würden.

Nicht zuletzt ist es schlicht nicht akzeptabel, dass eine kompliziertere Abgrenzung dazu benutzt wird, weitere Unternehmen in die Definition der FDA mit vollen Pflichten hereinzuziehen und damit die ständige (automatisierte) Überwachung der Bevölkerung auszubauen.

Art. 16c

Anregung: Streichung von Abs. 3 Bst. a. (sowie Art. 18 Abs. 2, Abs. 3 Bst. c,Abs. 4 1. Satz und Art. 18a Abs. 3 letzter Teilsatz (VE-)VÜPF)

Begründung:

In Art. 16c Abs. 3 Bst. a wird von FDA mit vollen Pflichten verlangt, dass sie verschiedene Auskünfte nach Art. 18 Abs. 2 automatisiert liefern müssen. Art. 17 Abs. 3 Bst. c ermöglicht das gleiche freiwillig für Anbieterinnen mit reduzierten Pflichten. Jegliche Automatisierung sollte vollständig aus der Vorlage gestrichen werden. Die Automatisierung trivialisiert ein Verfahren, das bewusst mühsam sein muss. Es geht hier um schwere Eingriffe in die Grundrechte der betroffenen Personen. Solche Eingriffe sollen sowohl finanziell als auch Aufwand-mässig zu spüren sein, damit sie auch in dieser Hinsicht ein seltenes Mittel bleiben, statt eine Zunahme zu verzeichnen (vgl. Fussnote 1). Ausserdem schadet es mitnichten, wenn die Anfragen durch eine weitere Person genau kontrolliert werden können.

In Kombination mit der Änderung in Art. 16b Abs. 1 Bst. b Ziff. 2 fallen ausserdem noch mehr Anbieter unter die Automatisierung, was das Problem zusätzlich verschärft.

Art. 16d

Anregung: Einschränkung der AAKD Definition

Begründung:

Gemäss Art. 16d Abs. 1 gilt als AAKD «wer für Dritte einen Einweg- oder Mehrwegkommunikationsdienst oder einen indirekten Zugangsdienst zu einem öffentlichen Fernmeldenetz erbringt, der unabhängig vom Netzzugangsdienst funktioniert.»

Man möchte es nicht meinen, aber, wie im allgemeinen Teil erwähnt, zählen laut erläuterndem Bericht auch «Onlinespeicherdienste, wie Cloud Storage, File Hosting, Share Hoster, Online Storage, File Sharing» dazu.[5] Dies, weil man teilweise gemeinsam Dateien bearbeiten könne. Plötzlich fällt unter AAKD also auch etwas, das mit Kommunikation nichts zu tun hat – die private Ablage von Dateien. Damit fallen u.U. iCloud und Google Drive plötzlich darunter. Diese Interpretation von AAKD ist ausufernd und sollte so nicht umgesetzt werden.

Unternehmen wie Proton verlangen zu recht auch die Exklusion von VPNs, deren Sinn gerade darin besteht, ihre Nutzer zu anonymisieren - ein legitimer Anwendungszweck. Diese der Entschlüsselung (Art. 50a VE-VÜPF) und der Vorratsdatenspeicherung (Art. 16g Abs. 3 Bst. a Ziff. 2 VE-VÜPF) zu unterstellen, wäre der Todesstoss für diese Unternehmen in der Schweiz.[6]

Art. 16e

[5] Erläuternder Bericht, S. 19f.

[6] Proton-Chef: «Diese Entscheidung ist wirtschaftlicher Selbstmord für die Schweiz», https://www.watson.ch/digital/wirtschaft/517198902-proton-schweiz-chef-andy-yen-zum-ausbau-der-staatlichen-ueberwachung .

Piratenpartei Schweiz, 3000 Bern

Anregung 1: Änderung zu AAKD ohne Pflichten

Anregung 2: Ausnahme für nicht-kommerzielle Anbieter, Bildung und Forschung

Begründung:

1

Es fehlt leider eine Kategorie für AAKD (und FDA), die keine Pflichten haben. Eine solche wäre zu begrüssen. Überwachung ist kein Muss.

2

Art. 16e definiert die Kategorie “AAKD mit minimalen Pflichten” mit der Nicht-Erfüllung der Kriterien der anderen Kategorien. Es wäre sinnvoll nicht-kommerzielle Anbieter ebenfalls grundsätzlich in diese Kategorie aufzunehmen. Es gibt in Art. 16b bereits die Herabstufung für FDA, wenn sie ihren Dienst nur im Bereich Bildung und Forschung anbieten. Eine gleiche Ausnahme sollte auch hier geschaffen werden. Im Bereich der AAKD gibt es aber zusätzlich viele Projekte, die nicht-kommerziell sind. Eine plötzliche Überwachungspflicht nach Art. 16f würde diese einer ungebührlichen Mehrbelastung aussetzen und sie in ihrer Existenz bedrohen (siehe Begründung Art. 16f).

Diese Anbieter können auch wichtige Dienste für demokratische Bewegungen weltweit stellen. Tor-Anbieter[7], also Anbieter, die z.B. für Dissidenten in autokratischen Ländern wichtige Zugänge ins freie Internet bereitstellen, könnten plötzlich die Teilnehmer identifizieren und die Verschlüsselung aufheben müssen.

Nicht-kommerzielle Anbieter sollten entsprechend in der Kategorie mit minimalen Pflichten verbleiben können.

[7] https://de.wikipedia.org/wiki/Tor_(Netzwerk).

Piratenpartei Schweiz, 3000 Bern

Art. 16f

Anregung: Streichung

Begründung:

Mit Art. 16f wird die neue mittlere Stufe «AAKD mit reduzierten Pflichten» eingeführt.

Laut Bericht wird «auf diese Weise [...] eine ausgewogenere und dem Grundsatz der

Verhältnismässigkeit besser entsprechende Abstufung der Verpflichtungen der

verschiedenen Unterkategorien der AAKD erreicht.»[8]

Was harmlos klingt, unterstellt in Wirklichkeit die AAKD schon ab 5000 Teilnehmenden z.B. der Pflicht, Verschlüsselungen zu entfernen nach Art. 50a VE-VÜPF. Die Zahl ist klein genug, dass selbst Projekte wie «Freifunk»[9] (gemeinschaftliche WLAN-Zugänge), Tor-Anbieter oder andere gemeinnützige Vereine darunter fallen.

Die Unternehmen und Vereine, die in diese Kategorie fallen, haben von der «ausgewogeneren» Abstufung entsprechend nichts ausser Mehrkosten und Pflichten. Darauf können nicht nur sie gut verzichten.

Die Kategorie «mit reduzierten Pflichten» wird ausserdem in Art. 19 Abs. 1 VE-VÜPF auch der Identifikationspflicht der Nutzer unterstellt, was bisher nicht der Fall war. Das bedeutet u.U. eine starke Steigerung der anfallenden Daten, was dem Grundsatz der Datensparsamkeit direkt zuwiderläuft und angesichts der Grösse kaum verhältnismässig ist (Art. 6 Abs. 2 DSG).

Die mittlere Kategorie dient letztlich lediglich dem Ausbau der Überwachung und der weiteren Einschränkung der Grundrechte der Schweizer Bevölkerung

[8] Erläuternder Bericht, S. 4.

[9] https://freifunk.net/.

und sollte somit gestrichen werden.

Weniger aber dennoch relevant, erhöht die mittlere Stufe «reduzierte Pflichten» auch für kleinere Unternehmen (und Vereine/Einzelpersonen) die Kosten, Anbieter eines abgeleiteten Dienstes zu werden. Das hat eine abschreckende Wirkung auf die Entwicklung in der Schweiz.

Zuletzt wird im BÜPF explizit von AAKD, "die Dienstleistungen von grosser wirtschaftlicher Bedeutung oder für eine grosse Benutzerschaft anbieten" (Art. 22 Abs. 4 u. Art. 27 Abs. 3 BÜPF), gesprochen, welche weiteren Pflichten unterstellt werden können. Das kann mit der Anforderung von lediglich 5000 Teilnehmenden nur leidlich als erfüllt angesehen werden.

Eventualiter sollte mindestens die Einstufung an massiv höhere Anforderungen als 5000 Teilnehmende geknüpft werden. 5000 ist eine auffällig kleine Zahl, wenn die nächste Stufe bei 1 Million angesetzt wird.

Art. 16g

Anregung 1: Streichung als Kriterium oder Erhöhung der Teilnehmendenzahl

Anregung 2: Streichung der Änderung von 100 Millionen Umsatz, «wobei grosser Teil ihrer Geschäftstätigkeit im Anbieten abgeleiteter Kommunikationsdienste besteht» zu Gesamtumsatz

Anregung 3: Streichung der Vorratsdatenspeicherung

Anregung 4: Streichung der Automatisierung

Begründung:

1

Zunächst begrüssen wir die Änderung, dass neu die Einstufung «mit vollen Pflichten» bei den AAKD nicht mehr auf die Anzahl der Überwachungsaufträge bzw. Auskunftsgesuche (Art. 22 Abs. 1 Bst. a bzw. Art. 52 Abs. 1 Bst. a VÜPF) abgestellt wird. Siehe Begründung Art. 16b.

Aber die neue Anforderung von 1 Million Nutzer darf gerne massiv erhöht werden. Der Erfolg eines Anbieters bzw. eines Angebots, viele Personen anzusprechen, sollte nicht allein als Begründung reichen, mehr Teilnehmende der automatisierten und erweiterten Überwachung auszusetzen.

2

Analog Begründung Art. 16b 2: Der Dienst ÜPF soll sich diese Arbeit gerne machen oder ganz bleiben lassen und nicht hochstufen, statt die Anzahl AAKD mit vollen Pflichten mit fragwürdiger Begründung zu erhöhen.

Eventualiter sollte der erforderliche (Gesamt-)Umsatz massiv erhöht werden.

3

Gemäss Art. 16g Abs. 3 Bst. a Ziff. 2 sollen die AAKD mit vollen Pflichten neu ebenfalls zur Vorratsdatenspeicherung verpflichtet werden, wie es die FDA bereits sind. Es sollen also Daten wie die IP und andere Randdaten für 6 Monate aufbewahrt werden müssen. Die Vorratsdatenspeicherung im Falle der FDA ist bereits äusserst bedenklich, diese aber auf AAKD auszuweiten geht weit über das Mass anderer Staaten hinaus. Die anhaltslose Massenüberwachung und Speicherung der Daten aller ist ein extremer Eingriff in die garantierten Rechte und wurde entsprechend auch schon vom EuGH abgewiesen.[10] Für die Schweiz hat dies natürlich keinen direkten Einfluss, aber

[10] Vgl. z.B. EuGH Pressemitteilung Nr. 58/22; NLMR 5/2018-EGMR.

es darf festgehalten werden, dass unsere Menschenrechte in unseren Nachbarländern bereits als verletzt gelten würden.

Die Aufbewahrung von Randdaten auf AAKD auszuweiten, ist allerdings eine Eskalationsstufe die schlicht nicht mehr akzeptabel ist. Es wäre praktisch nicht mehr möglich, online sein Recht auf Privatsphäre wahrzunehmen, ohne auf ausländische Dienste zurückzugreifen. Die Rechte der eigenen Bürgerinnen und Bürger nur noch durch Dienste im Ausland gewährleisten zu können, kann nicht Ziel dieser Revision sein.

Ironischerweise könnte dies auch dazu führen, dass die Überwachungspflichten nutzloser werden, weil die zu Überwachenden alle schweizerischen AAKD meiden werden.

Wirtschaftlich betrachtet, wird das von Proton-Chef Andy Yen vollkommen zurecht als «Selbstmord für die Schweiz» bezeichnet.[11] Wird dieser Vorschlag umgesetzt, wird die Schweiz das letzte Land sein, in dem eine AAKD ihren Sitz haben wollen wird. Der Nachteil ist zu gross für Unternehmen, die darauf angewiesen sind, dass ihre Kunden ihnen vertrauen können, ihre Rechte ernstzunehmen – fast jedes andere Land wäre fortan besser dafür geeignet. Von den zusätzlichen Kosten gar nicht zu sprechen.

Nicht zuletzt muss für die Vorratsdatenspeicherung auch ein System her, welches diese Funktion sicherstellt. Die Speicherung setzt die Daten jedoch nicht nur den Behörden aus, sondern erhöht auch das Risiko, dass andere Zugriff erlangen können. Damit schafft man bei den betroffenen Anbieterinnen unnötig Angriffspunkte, die statt zur Bekämpfung zur Förderung von Delikten u.ä. beitragen können.

Ein weiterer Blick ist auch die Frage des Zusammenspiels zwischen

[11] Proton-Chef: «Diese Entscheidung ist wirtschaftlicher Selbstmord für die Schweiz», https://www.watson.ch/digital/wirtschaft/517198902-proton-schweiz-chef-andy-yen-zum-ausbau-der-staatlichen-ueberwachung.

Vorratsdatenspeicherung und legitimer Geheimnisbewahrung wert. Arzt- und Anwaltsgeheimnis sowie Quellenschutz und Whistleblower sind alle gleichsam von der ausgeweiteten massenhaften Überwachung betroffen. Es ist wohlbekannt, dass der Inhalt häufig gar nicht so wichtig ist, weswegen die Randdaten genügen, um relevante Einsichten bekommen zu können. Mit der Vorratsdatenspeicherung setzt man diese Daten zusätzlichem Risiko aus.

4

Siehe Begründung Art. 16c.

Art. 16h

Anregung: Änderung der Voraussetzung bzgl. professionellem Betrieb

Begründung:

Nach Art. 16h Abs. 2 VE-VÜPF soll ein öffentlicher WLAN-Zugang als professionell betrieben gelten, «wenn kumuliert maximal mehr als 1000 Endbenutzerinnen und -benutzer alle von der gleichen Person gemäss Absatz 1 zur Verfügung gestellten öffentlichen WLAN-Zugänge nutzen können.» Im Bericht steht dazu, dass die Kapazität für tausend Zugänge schon genüge und nicht auch tatsächlich tausend Nutzer (gleichzeitig) vorhanden sein müssen.[12] Wenn also jemand schon nur 1-2 «Prosumer» Produkte - beispielsweise bietet Ubiquiti APs an, die 500+ Connections versprechen - öffentlich zugänglich macht, gilt das WLAN dieser Person als professionell betrieben. Der Bericht geht davon aus, dass dies der Verhältnismässigkeit genüge tue, was definitiv bezweifelt werden muss.

Ebenfalls davon betroffen wären z.B. Konferenzen. Wenn normale Konsumenten-Hardware schon die Voraussetzungen erfüllen kann, gilt dies umso mehr für die Hardware, die für Konferenzen bereitgestellt wird.

[12] Erläuternder Bericht, S. 26.

Die FDA, die die Zugänge sowohl hinter den Privatpersonen als auch hinter Konferenzen stellt, müsste dann bei einer solchen Konstellation gemäss Art. 19 Abs. 2 VÜPF alle Nutzer des WLANs identifizieren können. Wie sie dies anstellen soll, ist gänzlich unklar, wird aber verlangt – absurd. Angesichts dessen wäre es sinnvoll, wesentlich höhere Hürden anzusetzen oder den Absatz gleich zu streichen.

Alternativ könnte die Identifikationspflicht davon abhängig gemacht werden, ob die Nutzer separat für das WLAN bezahlen müssen oder nicht.

Art. 18

Anregung: Streichung der Automatisierung

Begründung: Siehe Begründung Art. 16c

Art. 18a

Anregung: Streichung der Automatisierung

Begründung: Siehe Begründung Art. 16c

Art. 19

Anregung 1: Streichung der Identifikationspflicht durch die AAKD

Anregung 2: Streichung der Endbenutzeridentifikation bei professionell betriebenen öffentlichen WLAN-Zugängen

Begründung:

1

Gemäss Art. 19 Abs. 1 VE-VÜPF sollen neu auch die AAKD mit reduzierten

Pflichten ihre Nutzer mit geeigneten Mitteln identifizieren. Wie bei Art. 16f bereits erwähnt, läuft dieses Vorhaben direkt wichtigen Prinzipien wie der Datensparsamkeit entgegen. Durch die Erweiterung um AAKD mit reduzierten Pflichten, bzw. der Inklusion von AAKD überhaupt, wird es der eigenen Bevölkerung praktisch unmöglich sein, schweizerische Unternehmen zu nutzen, wenn sie auf ihre Daten und ihr Recht auf Privatsphäre acht geben wollen. Personen von ausserhalb werden selbstverständlich schweizerische Anbieter sowieso meiden. Beide Umstände sollten nicht wünschenswerte Auswirkungen einer Verordnungsrevision sein.

Wie Alexis Roussel, COO von NymVPN, ausserdem zu bedenken gibt, bedeuten mehr verfügbare Daten und weniger Anonymität online auch automatisch mehr Daten, die ausgenutzt werden können:

«For example, enforcing identification of all these small services will eventually push to leaks, more data theft, and more attacks on people.»[13] Was man sich hier vielleicht an besserer Überwachungsmöglichkeit und damit (vermeintlich) besserer Bekämpfung von Verbrechen etc. erhofft, könnte in Wirklichkeit zu mehr erfolgreichen Delikten dank mehr stehlbaren Daten führen – Hacker, Personen mit kriminellen Absichten (z.B. Erpresser) oder gar vereinzelte Mitarbeiter könnten sich den neuen Daten ermächtigen und diese ausnutzen.

2

Wie schon bei Art. 16h beschrieben, ist es äusserst leicht, als Person mit professionell betriebenem öffentlichem WLAN-Zugang eingestuft zu werden. Art. 19 Abs. 2 VE-VÜPF verlangt nun die Nutzeridentifikation durch die FDA. Es ist absolut korrekt, dass der Betreiber selbst nicht identifizieren muss, aber dies den FDA aufzubürden ist keine Lösung. Um die Kontrolle sicherzustellen, müssten diese entweder einen enormen Aufwand betreiben oder starke

[13] Secure encryption and online anonymity are now at risk in Switzerland – here's what you need to know, 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.

Einschränkungen bei ihren Kunden vornehmen. Beides ist unverhältnismässig angesichts der sehr tiefen Hürde, als professionell zu gelten.

Art. 21

Anregung 1: Streichung AAKD in Abs. 1 Bst. a.

Anregung 2: Streichung der Vorratsdatenspeicherung, besonders für AAKD in Abs. 6

Begründung:

1

Siehe Begründung Art. 19, Anregung 1

2

Siehe Begründung Art. 16g, Anregung 3

Art. 42a, Art. 43a

Anregung: Streichung

Begründung:

Die verschiedenen Auskunfts- und Überwachungstypen sind leider reichlich unübersichtlich. Aber, sofern richtig interpretiert, gibt es bei AAKD bisher, ausser im Rahmen als Netzzugangsdienst i.S.v. Art. 35 VÜPF, keine «Information Requests» (IR-Abfragen), also die Stufe mit den niedrigsten Anforderungen, die die Herausgabe des «verwendeten Protokolls sowie IP-Adresse und Portnummer» (Art. 42a Abs. 1 Bst. c und Art. 43a Abs. 1 Bst. c) verlangen. Jetzt hingegen sollen plötzlich auch andere AAKD (ohne Netzzugangsdienst), wie Messenger oder E-Mail-Dienste die IPs, Protokolle und Ports mit einer IR-Abfrage (automatisch) herausgeben. Dies war bisher sonst scheinbar nur als Teil der «Historical Data» (HD) Abfragen und der «Real Time»

(RT) Überwachung der Fall, welche höheren Anforderungen zur Ausführung unterliegen.

Da auch die AAKD mit reduzierten Pflichten darunterfallen, wird die Abfrage auch noch massiv ausgeweitet, was schlicht insgesamt unverhältnismässig und damit abzulehnen ist.

Die Schaffung dieser neuen Auskunftstypen schafft für die AAKD ausserdem einen unnötigen Mehraufwand. Mit der für viele AAKD bevorstehenden Einstufung zu AAKD mit reduzierten Pflichten (oder gar vollen Pflichten) wird die Belastung weiter erhöht.

Art. 50a

Anregung: Streichung (auch im BÜPF)

Begründung:

Nach Art. 50a VE-VÜPF soll die Entfernung von Verschlüsselungen nach Art. 26 Abs. 2 Bst. c BÜPF konkretisiert werden. Die Regelung schliesst die Ende-zu-Ende-Verschlüsselung von der Entfernung aus, da dies zu schwerer Kritik geführt hatte und Befürchtungen wie Chatkontrolle hochkommen liess.[14] Das ist sicherlich eine begrüssenswerte Konkretisierung. Aber umgekehrt legt der Artikel immer noch fest, dass alle Anbieterinnen mit reduzierten und vollen Pflichten alle anderen von ihnen oder für sie angebrachten Verschlüsselungen entfernen müssen, um die unverschlüsselte Daten liefern zu können. «Wenn [...] ein Schlüssel der Anbieterin bei der Verschlüsselung verwendet wird, das heisst wenn die Anbieterin in der Lage ist, verschlüsselten Fernmeldeverkehr der überwachten Person zu entschlüsseln, dann muss sie dies auch tun.»[15]

Das bedeutet, dass jegliche Verschlüsselung, die eine Person nicht selbst

[14] Oberster Schweizer Datenschützer spricht sich gegen Aufweichung der Verschlüsselung aus, https://www.watson.ch/digital/schweiz/528820964-schweizer-datenschuetzer-ist-gegen-aufweichung-der- verschluesselung.

[15] Erläuternder Bericht, S. 43.

angebracht hat (ausser z.B. E2EE in Messengern) muss auch entfernt werden.

Es ist unklar, ob davon selbst Dienste wie iCloud betroffen sein werden, aber Cloudspeicher-Anbieter gehören zu den AAKD, womit sie grundsätzlich dazu zählen. Und jede AAKD, die bisher im Auftrag eines Nutzers, Daten verschlüsselt hat, muss denselben Schlüssel nun benutzen, um die Daten herauszugeben. Theoretisch könnte dies selbst die Ausnahme der Ende-zu-Ende-Verschlüsselung umgehen, da die Verschlüsselung quasi vom Anbieter angebracht wird.

Das alles gilt, wie gesagt, schon ab 5000 Teilnehmenden. Die Zahl der Dienste, die von der Entschlüsselung betroffen sind, springt also zusätzlich massiv an.

Damit die Verschlüsselung jederzeit aufgehoben werden kann, muss zudem wiederum ein System her, welches diese Funktion sicherstellt. Diese Vereinfachung der Entschlüsselung setzt die Daten dahinter jedoch nicht nur den Behörden aus, sondern erhöht auch das Risiko, dass andere Zugriff erlangen können. Wie schon bei der Nutzeridentifikation schafft man damit unnötig Angriffspunkte, die statt zur Bekämpfung zur Förderung von Delikten u.ä. beitragen können. Zusätzlich könnte auch hier die Sicherheit des Arzt- und Anwaltsgeheimnisses sowie der Schutz von Quellen und Whistleblowern in Gefahr sein, insbesondere da eben auch kleine Anbieter in die Pflicht genommen werden.

Der Schaden für Wirtschaft, Image, Sicherheit und Privatsphäre ist schlicht unverhältnismässig im Vergleich zum fraglichen Nutzen.

Art. 60a

Anregung: Streichung

Begründung:

Gemäss Art. 60a Abs. 1 soll eine rückwirkende Überwachung (HD-Abfrage) zum Zweck der Teilnehmeridentifikation stattfinden und dafür a. «alle Angaben über die mutmassliche Urheberschaft oder Herkunft einer Internetverbindung» und b. «die Schnittmenge aus allen Angaben über die mutmassliche Herkunft von zwei oder mehreren Internetverbindungen im Falle von zu vielen Ergebnissen (Art. 38a Abs. 4)» übermittelt werden.

Im erwähnten Art. 38a VE-VÜPF wird kein Ergebnis geliefert, wenn mehr als ein einziger Treffer vorliegt, weil dies Daten unbeteiligter Dritter liefern würde. Hier soll dies nun akzeptabel sein, weil die rückwirkende Überwachung (zu recht) höheren Anforderungen unterliege.[16] Die Kombination aus der extrem fragwürdigen Praxis der Vorratsdatenspeicherung und der Lieferung von «falsch-positiven Ergebnissen» scheint allerdings generell unverhältnismässig.

Auf die Massenüberwachung aufbauend werden damit plötzlich Daten zu unbescholtenen Usern ausgelesen - eine klare Verletzung der Privatsphäre, die kaum mit dem Nutzen abgewogen werden kann. Da es sich eben genau um Mehrfachtreffer handelt, die keine eindeutige Zuteilung erlauben, ist der Nutzen der Auskunft gering, die Gefahr für Fehler in der Folge eher hoch.

% Schlussbemerkungen

Wir beschränken uns in dieser Stellungnahme auf unsere Kernanliegen. Bei Verzicht unsererseits auf umfassende allgemeine Anmerkungen oder auf Anmerkungen zu einzelnen Regelungen, ist damit keine Zustimmung durch die Piraten zu solchen Regelungen verbunden.

[16] Erläuternder Bericht, S. 45.

piratenpartei
www.piratenpartei.ch

Piratenpartei Schweiz, 3000 Bern

Kontaktdetails für Rückfragen finden Sie in der Begleit-E-Mail.

_____

Piratenpartei Schweiz, Arbeitsgruppe Vernehmlassungen, 05. Mai 2025