piratenpartei

piratenpartei

Vernehmlassungsantwort NDV/VIS-NDB

Patrick Stählin patrick.staehlin@piratenpartei.ch 16. April 2017

Sehr geehrte Damen und Herren,

mit dieser Verordnung sind die Bedenken, die wir schon bei der Vernehmlassung zum Nachrichtendienstgesetz (NDG) geäussert haben, übertroffen worden. Nicht nur sind Speicherfristen in der Verordnung über dem Mass dass sich die Parlamentarier während der Debatte vorgestellt haben eingesetzt worden, es ist auch neues Recht eingebaut und Widersprüche zum NDG und geltendem Recht eingebaut worden.
Dazu sind nur die Rechte, nicht aber die Pflichten des NDG präzisiert worden. Wir hätten uns gerade im Bereich der Kabelaufklärung mehr Details erhofft, einerseits um die technische Machbarkeit der Selektionierung der Daten überprüfen zu lassen, andererseits um der rechtschaffenden Bevölkerung einen Ausweg aus der Überwachung anzubieten.

Auch sind keine Statistiken und kaum Pflichten zur Dokumentation eingeflossen welche das Parlament bei einer, in Zukunft sicherlich anstehenden Revision, die Wirksamkeit einzelner Massnahmen belegen könnten.
Ebenso fehlen konkrete Richtlinien in welchen Lagen welche genehmigungspflichtigen Beschaffungsmassnahmen anzuwenden sind. Ist beispielsweise ein IMSI-Catcher Einsatz an einer Demonstration zulässig?

In der Debatte wurde mehrfach darauf hingewiesen dass die Schweiz keine *Mini-NSA* aufstellt, mit Speicherdauern von fünf Jahren muss man jedoch sagen dass wir auf dem besten Weg dazu sind. Gerade wenn man sich die Worte von Ex-NSA und Ex-CIA Direktor Michael Hayden nochmals in Erinnerung ruft: *We kill People based on Metadata*. Metadaten bzw. Randdaten fünf Jahre aufzubewahren, in der Form eine Verordnung, wo die Speicherdauer beim BÜPF auf sechs Monate beschränkt ist, wiederspricht jeglicher Logik und Vernunft.

Inhaltsverzeichnis

1 Verordnung über den Nachrichtendienst (Nachrichtendienstverordnung, NDV) 4
1.1 Kritik an den einzelnen Artikeln/Abschnitte . . . 4
1.1.1 Art. 1 . . . 4
1.1.2 Art. 2 . . . 4
1.1.3 Art. 3 . . . 4
1.1.4 Art. 5 . . . 4
1.1.5 Art. 6 . . . 5
1.1.6 Art. 7 . . . 5
1.1.7 Art. 9 . . . 5
1.1.8 Art. 10 . . . 5
1.1.9 Art. 12 . . . 5
1.1.10 Art. 13 . . . 5
1.1.11 Art. 14 . . . 6
1.1.12 Art. 16 . . . 6
1.1.13 Art. 18 . . . 6
1.1.14 Art. 21 . . . 6
1.1.15 Art. 23 . . . 6
1.1.16 5. Abschnitt: Kabelaufklärung . . . 7
1.1.17 Art. 25 . . . 8
1.1.18 Art. 26 . . . 8
1.1.19 Art. 27 . . . 9
1.1.20 Art. 33 . . . 9
1.1.21 Art. 35 . . . 9
1.1.22 Art. 39 . . . 9
1.1.23 Art. 48 . . . 9
1.1.24 Art. 49 . . . 10
1.1.25 Art. 54 . . . 10
1.1.26 Art. 57a . . . 10
1.1.27 Anhang 2, Ziffer 6 . . . 10
1.2 1. Verordnung vom 4. März 2011 über die Personensicherheitsprüfungen, Art. 28 . . . 10
1.3 2. Verordnung vom 27. Juni über das Sicherheitswesen in der Bundesverantwortung . . . 11
1.3.1 Art 2, Abs. 4 . . . 11
1.3.2 Art. 12a, Abs. 2 . . . 11
1.3.3 Art. 13, Abs. 3 . . . 11

1.4 8. Verordnung vom 8. März 2013 über den nationelen Teil des Schengener Informationsszstems (N-SIS) und das SIRENE-Büro 11
1.4.1 Art. 7 Abs. 1 Bst. h 11
1.5 9. Verordnung vom 17. Oktober 2012 über die elektronische Kriegsführung und die Funkaufklärung 12
1.5.1 Art. 4 Abs. 3 12
1.6 10. Verordnung vom 31. Oktober 2001 über die Überwachung des Post- und Fernmeldeverkehrs 12
1.6.1 Art. 17 Abs. 2 12
1.6.2 Art. 27 Abs. 4 12
1.7 11. Verordnung vom 25. November 2015 über Fernmeldeanlagen 12
1.7.1 Art. 27 Abs. 4 12
1.8 12. Verordnung vom 9. März 2015 über Frequenzmanagement und Funkkonzessionen 13
1.8.1 Art. 51 Abs. 2 und 3 13

2 Verordnung über die Informations- und Speichersysteme des Nachrichtendienstes des Bundes (VIS-NDB) 14
2.1 Generelle Kritik 14
2.2 Kritik an einzelnen Artikel 14
2.2.1 Art. 2 14
2.2.2 Art. 5 15
2.2.3 Art. 8 15
2.2.4 Art. 10 15
2.2.5 Art. 11 15
2.2.6 Art. 14 15
2.2.7 Anhang 1 (Art. 17 Abs 4 und 23 Abs. 4) 16
2.2.8 Anhang 13 (Art. 57 Abs. 4) 16

3 Schlusswort 16

1 Verordnung über den Nachrichtendienst (Nachrichtendienstverordnung, NDV)

1.1 Kritik an den einzelnen Artikeln/Abschnitte

1.1.1 Art. 1

Artikel 1 wiederspricht den Bestimmungen im *2. Abschnitt: Zusammenarbeit* (Art. 9-12 NDG) indem er viel zu lose formuliert ist. Z.B. könnte der NDG mit irgendwelchen Dienststellen der Kantone zusammenarbeiten, die Kantone müssen jedoch einen Ansprechspartner definieren.
Da der Artikel sonst nichts zusätzliches regelt, was nicht schon im NDG enthalten ist, sollte er gestrichen werden.

1.1.2 Art. 2

Auch Artikel 2 widerspricht dem NDG, in dem er das Gesetz erweitert statt präzisiert. Art. 10 NDG regelt bereits die Zusammenarbeit mit den Kantonen und insbesondere den Regierungskonferenzen. Streichen.

1.1.3 Art. 3

Hier fehlt eine Klausel dass über die Anzahl und Art der Nachrichtenbegehren eine Statistik zuhanden der GPDel bereitzustellen ist um die Notwendigkeit dieses Austausches zu dokumentieren.

1.1.4 Art. 5

Der *2. Abschnitt: Zusammenarbeit* im NDG (Art. 9-12 NDG) sieht keine Zusammenarbeit mit dem fedpol vor, das fedpol ist jedoch auskunftspflichtig als Strafverfolgungsbehörde nach Art. 20.

1.1.5 Art. 6

Um nicht alle Kantone anzufragen zu müssen, sollte der Verteilschlüssel wie auch die Höhe der Abgeltungen jährlich publiziert werden.

1.1.6 Art. 7

Abs. 1: Der Antrag ist der GPDel ebenfalls zuzustellen. Zudem sollten bei Kontakten im Einzelfall der Bundesrat wie auch die GPDel informiert werden.

1.1.7 Art. 9

Produkte ist nicht hinreichend spezifiziert, im NDG kommt der Begriff zwei Mal vor ohne ihn zu erklären. Zudem muss festgelegt werden, was mit den Produkten geschieht und an wen sie weitergegeben werden dürfen.

1.1.8 Art. 10

Diese Vereinbarungen bedürfen trotzdem einer regelmässigen Überprüfung durch die GPDel, insbesondere wenn es um den Austausch von Personendaten geht.

1.1.9 Art. 12

Die Beschreibung *zeitlich begrenzt* sollte durch eine konkrete Zeitspanne ersetzt werden. Zudem sollte beim Abschluss der Operation Daten und Berichte (Produkte) möglichst schnell vernichtet oder mit einem Löschdatum versehen werden.

1.1.10 Art. 13

Abs. 2: Umformulierung:

2) Inländische Amtstellen haben *auf Antrag* des NDB gegenüber Dritten über die Zusammenarbeit oder die Beauftragung Stillschweigen zu bewahren.

Abs. 3: Kantonale und Eidgenössische Datenschutzbehörden müssen im Rahmen ihrer Kontrolltätigkeit ebenfalls davon ausgenommen werden.

1.1.11 Art. 14

Wenn ausländische in der Schweiz aktiv werden sollen, bedarf das mehr als ein Hinweis auf geltende Gesetze. Entweder sollten diese überwacht oder begleitet werden. Verstösse gegen die Bestimmungen müssen als verbotener Nachrichtendienst behandelt werden. Zudem sollten die Art und Anzahl solcher Beschaffungen und Beauftragungen dem Bundesrat wie auch der GPDel als Statistik zur Verfügung gestellt werden.

Was ebenfalls fehlt ist ein Abs. 3 wie in Art. 15:

Neu: 3) Die Zusammenarbeit oder Beauftragung ist zu protokollieren.

1.1.12 Art. 16

Hier fehlt der Hinweis auf die Protokollierung wie in Art. 15 Abs. 3:

Neu: 3) Die Zusammenarbeit oder Beauftragung ist zu protokollieren.

1.1.13 Art. 18

Abs. 4) Umkehrung der Schutzklausel:

4) Bei technischen Quellen sind alle Angaben zu schützen, *falls* deren Bekanntgabe die Auftragserfüllung des NDB direkt oder indirekt gefährdet.

1.1.14 Art. 21

Wenn die Dokumentation elektronisch erfolgt muss diese mittels einer qualifizierten elektronischen Unterschrift geschehen um den Eintrag verifizierbar zu machen.

1.1.15 Art. 23

Dieser Artikel Bezieht sich nur auf Abs. 2 des Art. 37 NDG, eine Klarifizierung der Anträge gemäss Art. 37 Abs 2. NDG ist zwingend nötig, da es sich hier je nach Auslegung des internationalen Rechts um einen Angriff auf ein Land handeln kann.

In Abs. 1 Lit. e sollten die Risiken noch etwas genauer erläutert werden da es sich da um unerlaubten Nachrichtendienst aus der Sichtweite des Auslands handelt. Zu den Risiken gehören desshalb auch die Vergeltungsmassnahmen: Die Spanne ist da von nichts bei einer Privatperson (wobei die Kosten Botnetz zu mieten immer weiter sinken) bis zu einem Gegenschlag auf die Schweizer Infrastruktur bei einem Staat oder der Abbruch der diplomatischen Beziehungen.
Deswegen muss klar sein, wem die Computersysteme bzw. Computenetzwerke gehören bevor so eine Massnahme angeordnet wird.

1.1.16 5. Abschnitt: Kabelaufklärung

In diesem Abschnitt fehlen folgende Klarifizierungen zum NDG, welche sehr Relevant für die Umsetzung der Kabelaufklärung unabdingbar sind:

- Wo werden die *Signale* abgelegt? In ISCO sind nur personenbasierte Selektoren enthalten (laut Entwurf VIS-NDB). Die Hauptdatenbank ist IASA bzw. IASA-GEX, dort fehlen aber die entsprechenden Felder (laut Entwurf VIS-NDB). Wird es eine Suchfunktion innerhalb der *Signale* auf den Systemen der ZEO geben? Falls ja, fehlen diese in dieser Verordnung komplett.
- Wie werden *Signale*, bei denen der Sender und der Empfänger in der Schweiz sind, aussortiert? Geschieht dies nur per IP-Adressen oder werden z.B. E-Mails mit *.ch-Domains* als Sender/Empfänger dennoch abgefangen? Wird das an Provider delegiert?
- Wie werden Personen, die einer der in den Artikeln 171–173 StPO genannten Berufsgruppen angehören, von der Datenerfassung ausgenommen? Ohne die Klärung dieser Frage wird das Zeugnisverweigerungsrecht, wie auch der Quellenschutz in Frage gestellt.

Zudem ist die Speicherdauer von 5 Jahren auf Verbindungsdaten unerklärbar hoch, hat sich doch das Parlament bei der BÜPF Revision auf sechs Monate beschränkt. Es weckt den Verdacht als ob die Daten für einen Tauschhandel mit anderen Staaten gespeichert werden. In der Debatte sind diese Zahlen, wohl des Referendums bewusst, nie gefallen. Auch die Speicherdauer der Inhalte von 18 Monaten ist in unserer schnellebigen Zeit nicht angebracht. Entweder werden die Daten direkt ausgewertet oder sie sollten vernichtet werden. Dies gilt sowohl für die Verbindungsdaten wie auch die gesammelnten *Signale*.
Ganz zu schweigen davon, dass die Kabelaufklärung durch die Nutzung von VPN, Tor

oder immer mehr Sender-Empfänger Verschlüsselung (auch bei weit verbreiteten Chat-Systemen wie Facebook oder WhatsApp) ad absurdum getrieben wird.

Auch zum Schutz der gesammelten Daten wird kein Wort verloren.

Es muss verhindert werden, dass nicht-Berufssoldaten im ZEO Zugriff auf die Daten bekommen. Bei der Funkaufklärung werden im Moment, nach unseren Informationen, sowohl WK-Soldaten wie Durchdiener eingesetzt.
Zudem sind die Räumlichkeiten besonders zu sichern sowie rund um die Uhr zu Bewachen.

Unser Vorschlag, ist die Kabelaufklärung komplett zu verbieten, bis die Frage der Datenhaltung geklärt ist. Sobald die Datenhaltung geklärt ist braucht es unserer Meinung nach eine Anpassung der Verordnung und auch des NDGs. Gerade weil die Kabelaufklärung wie Funkaufklärung *Massenüberwachung von Kommunikationen* (Bericht GPDel 2003) zulässt, ist es wichtig diese Detailfragen zu klären, bevor auch nur ein Test mit einem solchen System stattfindet.

1.1.17 Art. 25

Abs. 2: Die Grundsätze der Zusammenarbeit sollten Teil dieser Verordnung sein, da gerade die Details der Datenbeschaffung und Verarbeitung die korrekte Speicherung und der Zugriff auf die Daten für den Datenschutz relevant sind.

1.1.18 Art. 26

Abs. 4: Streichen, das ZEO soll nur ausführen und die Daten nicht durchsuchen (siehe Art. 42 Abs. 5 NDG). Dadurch wird wie beim Strafrecht (Dienst ÜPF) die Trennung zwischen den Anbieter von Telekommunikationsdienstleistungen und den NDB wahrgenommen.
Das ZEO ist als Blackbox zu betrachen bei der Befehle am einen Ende entegengenommen und *Signale* am anderen Ende abgeliefert werden. Die Auswertung der *Signale* am anderen Ende hat durch Personen zu erfolgen, welche sich das ganze Jahr damit befassen und auch ständig in Kontakt mit Leuten aus der Nachrichtendienstszene sind. Dies erhöht die soziale Kontrolle und macht die Früherkennung von personellen Problemen möglich.

1.1.19 Art. 27

Die Speicherdauer von sowohl Inhalten wie auch von Verbindungsdaten sind zu lang. Bei der einzigen Studie zum Thema speichern von Verbindungsdaten (Vorratsdaten) im Europäischen Raum, gibt keine messbaren Steigerung der Aufklärungsraten. Von daher ist die langfristige Speicherung ein Unsinn. Laut dem Dienst ÜPF betreffen die meisten Abfragen nach Verbindungsdaten den Zeitraum einer Woche nach einem Ereignis.

Die Speicherung wiederspricht zudem dem Artikel 8 der EMRK *SR 0.101*.

1.1.20 Art. 33

Da Nachrichtendienstliche Sammlungen ohne strafrechtliche Anfangsverdachtsmomente stattfinden, ist entweder die Weitergabe zu untersagen oder die Weitergabe den betroffenen Personen, Organisationen oder Gruppierungen mitzuteilen. Ohne Mitteilungspflicht werden diesen ihr Menschenrecht bzw. das in der Bundesverfassung verankertes Recht auf ein faires Verfahren genommen.

1.1.21 Art. 35

Abs. b & c) Wie ein Dienst operiert sowie welche Mittel er einsetzt, sollten nicht vom Öffentlichkeitsgesetz ausgenommen sein, gerade Abhängigkeiten zu bestimmten Hersteller sollen dem Volk, welche diese bezahlt, publik gemacht werden.

1.1.22 Art. 39

Wir schlagen einen neuen Absatz 3 vor:

3) Nach der Einstellung des Prüfverfahrens werden die betroffenen Personen, Organisationen oder Gruppierungen benachrichtigt. Die während der Überprüfung angefallenen Daten werden vernichtet.

1.1.23 Art. 48

Ergänzung zu Absatz 3:

Datenträger und Telefone welche nicht entschlüsselt werden können, werden der sicheren Vernichtung zugeführt.

Ergänzung zu Absatz 5:

Die Behältnisse sind vor den Sicherheits- und Kontrollmassnahmen anzubringen.

1.1.24 Art. 49

Hier muss in Abs. 2 zwingend ein Bezug zu Art. 48 Abs. 5 hergestellt werden. Zudem sollte der Teil mit den privaten Gegenständen gestrichen werden, sonst werden Daten in Sporttaschen herausgetragen.

1.1.25 Art. 54

Abs. b): Streichen. Munition mit Expansionswirkung (sog. Dum-Dum-Geschosse) sind gemäss internationalem Kriegsrecht sowie der Bestimmungen des Humanitären Völkerrechts verboten.

1.1.26 Art. 57a

Streichen. Es gibt keinen Grund die Schutzfrist zu verlängern nur weil ein neues Gesetz in Kraft tritt, eher sollte sie verkürzt werden. Gerade in dieser Zeit sind innenpolitisch und historisch signifikante Ereignisse geschehen, zu welchen die Akten nicht in Archiven verstauben sollen.

1.1.27 Anhang 2, Ziffer 6

Dass der Auftraggeber die Schlichtungsstelle ist, kann nicht im Sinne der verpflichteten Unternehmen sein. Da sollte das Verwaltungsgericht im Streitfall zuständig sein.

1.2 1. Verordnung vom 4. März 2011 über die Personensicherheitsprüfungen, Art. 28

Alte Fassung beibehalten, weder im NDG noch in der NDV gibt es einen zwingenden Grund für diese Verschärfung.

1.3 2. Verordnung vom 27. Juni über das Sicherheitswesen in der Bundesverantwortung

1.3.1 Art 2, Abs. 4

Auch hier gibt es keine Indikation warum das geändert werden, oder so breit gefasst werden soll. Falls zu wenig Personal da ist, soll solches eingestellt werden oder die Militärische Sicherheit für kurzfristige Überbrückungen eingesetzt werden.

Sollte dieser Absatz unverändert übernommen werden, beantragen wir den alten Art. 3, Abs. 3 (Fassung 2001) als Abs. 4 in die Verordnung wieder aufzunehmen:

3) Das Eidgenössische Justiz- und Polizeidepartement (Departement) legt die Anforderungen an die privaten Schutzdienste fest, die diese für einen Einsatz beim Bund erfüllen müssen.

1.3.2 Art. 12a, Abs. 2

Nach unserer Leseweise will der Bund hier für 100% nur 80% bezahlen. Falls dies nicht der Fall ist, sollte die Formulierung nochmals übedacht werden.

1.3.3 Art. 13, Abs. 3

Listen in Gesetzen sollen Abschliessend sein und nicht durch Verordnungen wieder aufgebrochen werden. Falls dieser Absatz so bestehen bleibt, fordern wir auch hier eine Informationspflicht zuhanden der kantonalen Datenschutzbehörde wie auch den betroffenen Personen, da die Daten nicht anhand geltendem Gesetz bearbeitet wurden.

1.4 8. Verordnung vom 8. März 2013 über den nationelen Teil des Schengener Informationsszstems (N-SIS) und das SIRENE-Büro

1.4.1 Art. 7 Abs. 1 Bst. h

Buchstabe h ist zu streichen da diese Informationen über das fedpol angefordert werden können. Bleibt dieser Buchstabe drin, sind auch die Schnittstellen zum fedpol in dieser Verordnung grösstenteils zu entfernen.

1.5 9. Verordnung vom 17. Oktober 2012 über die elektronische Kriegsführung und die Funkaufklärung

1.5.1 Art. 4 Abs. 3

Da der NDB mit neuen Aufträgen im Bereich der Wirtschaftsspionage beglückt wurde, sollte da evtl. auch noch ein Buchstabe zu dem Thema rein.
Zudem sind wir der Meinung, dass die Kräfte der EKF/Fk Aufkl. nicht dazu geeignet sind die Herkunft oder die technische Beschaffenheit der Cyber-Angriffsmittel zu bestimmen oder oder der Gestaltung von wirksamer Abwehrmassnahmen (ausser Internet abschalten) fähig sind.
Diese Kräfte sind regelmässig mit Durchdiener und WK-Soldaten besetzt, die Cyber-Abwehr eines Landes sollte sich nicht auf Teilzeitkräfte mit maximal 300 Tagen Erfahrung verlassen. Dazu ist unser Land, unsere Infrastruktur, die Einwohner sowie unsere Wirtschaft zu wertvoll.

1.6 10. Verordnung vom 31. Oktober 2001 über die Überwachung des Post- und Fernmeldeverkehrs

1.6.1 Art. 17 Abs. 2

Die Bestimmung für den NDB aufzuheben ist falsch. Der NDB muss benachrichtigt werden damit er nach Art. 58 Abs. 3 NDG die Aussonderung beim Bundesverwaltungsgericht anordnen kann.

1.6.2 Art. 27 Abs. 4

Siehe Kommentar zu Art. 17 Abs. 2.

1.7 11. Verordnung vom 25. November 2015 über Fernmeldeanlagen

1.7.1 Art. 27 Abs. 4

Wir sehen keine Veranlassung dazu diese Verordnung zu ändern. Streichen.

1.8 12. Verordnung vom 9. März 2015 über Frequenzmanagement und Funkkonzessionen

1.8.1 Art. 51 Abs. 2 und 3

Wir sehen keine Veranlassung dazu diese Verordnung zu ändern. Streichen.
Was wir als zynisch empfinden ist, dass sich der Nachrichtendienst mittels Störsender vor Überwachungssystemen schützen will, gleichzeitig aber diese Massnahme aber übers neue BÜPF anordnen kann (IMSI-Catcher).

2 Verordnung über die Informations- und Speichersysteme des Nachrichtendienstes des Bundes (VIS-NDB)

2.1 Generelle Kritik

Was in dieser Verordnung generell fehlt, sind nicht nur die Personenbezogenen Daten sondern auch das Aufzeigen von Möglichkeiten zur Verknüpfung und Suche über verschiedene Systeme. Zur Suche (SIDRED) befindet sich nur der Name in dieser Verordnung, zum Betrieb eines solchen Systemes fehlen die rechtlichen Grundlagen.
Was ebenfalls fehlt sind Angaben ob pro Datensatz ein Löschdatum gespeichert wird, oder nur das Datum der letzten Überprüfung.
Zudem fehlt die Protokollierung jedes Zugiffs auf die Daten, selbst wenn Kopien abgerufen werden. Dies muss beim Original-Dokument annotiert werden, da Kopien jederzeit vernichtet werden können. Werden Daten an Partnerdienste weitergegeben, soll das ebenfalls annotiert werden, insbesondere bei Personendaten.
Ebenfalls nicht geregelt ist die Anmeldung an den Systemen, z.B. bei Systemen auf die von den Kantonen zugegriffen werden können. Diese befinden sich unter Umständen nicht in besonders gesicherten Räumlichkeiten.

Personendaten sollten keine Angaben wie Ethnische Zugehörigkeit oder Religion enthalten, diese Daten sind besonders schützenswert. Zumindest sollte die Suche auf gewissen Felder eingeschränkt werden um ein Profil nach Ethnie oder Religion über alle Datensätze zu erstellen. Ebenfalls nicht spezifiziert ist, welche Felder immer ausgefüllt werden. Zudem fehlen in allen Katalogen die möglichen Werte (z.B. bei der Haarfarbe blond, braun, etc.). Was auch nicht ersichtlich ist, ob in gewissen Feldern Daten wie Berichte (bei der Religion z.B. besucht immer am Sonntag die Ref. Kirche in Adliswil) eingefüllt werden können.

2.2 Kritik an einzelnen Artikel

2.2.1 Art. 2

In der *NDV* und im *NDG* werden Produkte erwähnt, die sollten hier wohl auch definiert werden.

2.2.2 Art. 5

Abs. 4) Die Zugriffsrechte müssen entzogen werden, wenn sie nicht gebraucht wurden. Daten auf die man nicht zugreifen kann, landen nicht auf Festplatten zu Hause.

2.2.3 Art. 8

Abs. 1) Dass die Daten erst drei Monate nach dem Ablauf der Aufbewahrungsdauer gelöscht werden sollen, ist technisch oder organisatorisch zu begründen. Zudem sind die Daten während dieser drei Monate für alle Benutzer unwiederrufbar zu sperren und auch nicht wiederherstellbar zu machen.

2.2.4 Art. 10

Betroffene Personen, welche nach Art. 63 ein Auskunftsbegehren gestellt haben, sollen schnellstmöglich informiert werden.

2.2.5 Art. 11

Abs. 5) Missbräuche müssen in jedem Fall der Direktion sowie der GPDel gemeldet werden.

2.2.6 Art. 14

Abs. 1) Weder in der *NDV* noch im *NDG* (insbesondere Art. 47 NDG) wird SIDRED erwähnt. Wir sind daher der Meinung, dass es keine Grundlagen zum Betrieb dieses Informationssystems gibt. Die Aufzählung in Art. 47 NDG ist abschliessend.
Zudem fehlen Angaben über welche Felder gesucht und kombiniert werden kann. Z.B. kann man innerhalb von ISCO nach E-Mails mit einem bestimmten Absender suchen? Kann nach verschiedenen Kriterien aggregiert werden wie z.B. nach Personen, die E-Mails Verschlüsselt verschicken und deren IP-Adressen über die Zeit gruppiert?

Abs. 2) Gleiches Problem wie in Abs. 1, SiLAN fehlt in Art. 47 NDG.

Abs. 3) Die Daten müssen von SiLAN zusätzlich mit einem Löschdatum versehen werden, damit das Löschen nicht vergessen geht.

2.2.7 Anhang 1 (Art. 17 Abs 4 und 23 Abs. 4)

Hier fehlen die Felder welche nicht Personendaten betreffen, gerade bei der Kabelaufklärung bei der wir vermuten, dass die Daten hier gespeichert werden.

2.2.8 Anhang 13 (Art. 57 Abs. 4)

Das Feld *Daten über Kommunikationsmittel und Fernmeldeanschlüsse* ist unterspezifiziert.

3 Schlusswort

Wir hoffen dass, die eine oder andere Anregung in der überarbeiteten Vernehmlassung Einfluss nehmen wird.

Für die Piratenpartei Schweiz

Patrick Stählin