



Ausschussdrucksache 21(6)122d
vom 5. Oktober 2026, 17:14 Uhr

Schriftliche Stellungnahme
des Sachverständigen Hadmut Danisch

Öffentliche Anhörung

zu dem Gesetzentwurf der Bundesregierung

Entwurf eines Gesetzes zur Einführung einer IP-Adressspeicherung und
Weiterentwicklung der Befugnisse zur Datenerhebung im Strafverfahren
BT-Drucksachen 21/6581, 21/7154

Stellungnahme als Sachverständiger

für den Deutschen Bundestag

zum Gesetzentwurf der Bundesregierung

**„ Entwurf eines Gesetzes zur Einführung einer IP-Adressspeicherung
und Weiterentwicklung der Befugnisse zur Datenerhebung im
Strafverfahren“**

vom 19.06.2026, BT-Drucksachen 21/6581 und 21/7154

Anhörung am 7. Oktober 2026

– Rechtsausschuss –

Dipl.-Inform. Hadmut Danisch

Berlin · www.danisch.de · hadmut@danisch.de

Stand: 5. Oktober 2026

Inhaltsverzeichnis

1	Formale Angaben	13
1.1	Auftrag	13
1.2	Anschluss an meine Stellungnahme vom 9. Oktober 2023	13
1.3	Gegenstand	13
1.4	Maßstäbe und Motivation	14
1.4.1	EuGH C-793/19 und C-794/19	14
1.4.2	Eigene Tätigkeit Vorratsdatenspeicherung 2009	14
1.4.3	Eigene Erfahrungen als Beschuldigter eine Strafermittlungsverfahrens	15
1.4.4	Technische Berufserfahrung	16
1.4.5	Weitere persönliche Erfahrungen	16
1.5	Bearbeitungszeit viel zu kurz	16
1.6	Sachkunde	18
I	Technische und forensische Mängel	19
2	Nachträge zur und Anschluss an die Stellungnahme vom 9. Oktober 2023	20
2.1	Schwächen des Border Gateway Protocol	20
2.2	Herstellerspezifische Protokollierungsfunktionen bei Carrier Grade NAT	21
2.2.1	Log-Umfang	21
2.2.1.1	RFC 7422	21
2.2.1.2	A10 Networks	22
2.2.1.3	Netelastic	22
2.2.1.4	draft-donley-behave-deterministic-cgn-00.txt	22
2.2.1.5	Von 2011 zu 2026	23
2.2.2	Log-Geschwindigkeit	23
2.2.3	Herstellerspezifische Logging-Methoden	23
2.2.3.1	F5: CGNAT port block allocation sizing and tools for LSN pools	23
2.2.3.2	Nokia Deterministic Large Scale NAT44	24
2.2.3.3	Citrix ADC/Netscaler	25
2.2.4	Gefahren durch statische oder deterministische Port Block Allocation (PBA)	25
2.2.4.1	Netzwerkstörungen	25
2.2.4.2	Datenschutz, Identitätsschutz und Tracking	25
2.2.4.3	Fehlerhafte Nutzerzuordnungen	26
2.3	MAP-E, MAP-T und Lightweight 4over6 statt CGNAT	26

3	Verständnisfehler und Begriffsverwirrungen der Regierung	28
3.1	Im Gesetzentwurf	28
3.1.1	Verbotsirrtum: Phantasieunterschied „Vorratsdatenspeicherung“ und „IP-Adressspeicherung“	28
3.1.2	„Zuverlässigkeit“ statt „Rechtssicherheit“	29
3.1.3	„Internetverbindung“	30
3.1.4	„Kennung“	31
3.1.5	Standortbestimmung	32
3.1.6	Internet nicht verstanden: Juristen halluzinieren	34
3.1.7	„Verkehrsdaten“ im Sinne des § 3 Nr. 70 TKG	37
3.2	Im Zusammenhang mit dem Gesetzentwurf	38
3.2.1	„KFZ-Kennzeichen“	38
3.2.2	„Digitale Gewalt“	40
3.2.3	„IP-Adressen identifizieren Geräte“	40
4	Grundlagenwissen Netzwerke (Internet)	42
4.1	Konkurrenz von TCP/IP (Internet) und ISO/OSI	42
4.2	Das ISO-OSI-Schichtenmodell	43
4.3	Verbindungs- und Paketerorientierte Schichten	44
5	Zeitunabhängige Fehlerquellen	46
5.1	Grundproblem	46
5.2	Routenverteilung – BGP	47
5.3	Unsicherheit von Routern	48
5.4	Politische Unterwanderung der Betriebssysteme und Open Source, Supply-Chain-Angriffe	50
5.4.1	LGBT	50
5.4.2	Vorsatz der Maintainer	51
5.4.3	Unterwanderung durch Geheimdienste	51
5.4.4	Unterwanderung durch die Industrie selbst	51
5.5	Allgemeine Kriminalitätslage	52
5.5.1	„Die Russen kommen!“	52
5.5.2	„Crime-as-a-Service“	54
6	Fehlerquellen in zeitlicher Nähe zum IP-Adresswechsel	55
6.1	Direkte Fehler im Gesetzentwurf	55
6.1.1	Verwechslung von Granularität und Genauigkeit	55
6.2	Grundprobleme	56
6.2.1	Unzuverlässigkeit von Referenzuhren	56
6.2.2	Herkunft genauer Tat-Logdaten	57
6.2.3	Das Einschreibeprobem	58
6.2.4	TCP/IP nicht synchron, nicht auf Adressänderungen ausgelegt	59
6.3	Logging auf Serverseite	59
6.3.1	Betriebssysteme und Server nicht echtzeitfähig	59
6.3.2	Virtualisierung und Cloud-Computing	60
6.3.3	Virtuelle Uhren	60

6.4	IP-Adresszuweisung	61
6.4.1	Statisch	61
6.4.2	Point-to-Point-Protokoll (PPP)	61
6.4.3	Dynamic Host Configuration Protocol (DHCP)	62
6.4.4	IPv6 RA/NDP/ICMP6	65
6.4.5	PDU Session Establishment	65
6.4.6	Juristischer Anschluss an Stellungnahme 2023	65
6.5	Schicht 3: IP	66
6.5.1	Latenzzeiten und Wiederholungen	66
6.5.2	Beispiel 1: Ostseekabel	66
6.5.3	Beispiel 2: Mittelmeerkabel	67
6.6	Schicht 4	67
6.6.1	UDP	67
6.6.2	TCP	67
6.6.2.1	Aufgaben	67
6.6.2.2	Idle Timeout	68
6.6.2.2.1	Standard	68
6.6.2.2.2	Beispiel Linux	69
6.6.2.3	Retransmission Timer	70
6.6.2.3.1	Standard	70
6.6.2.3.2	Beispiel Linux	70
6.6.3	SCTP	72
6.7	Schicht 5	72
6.7.1	Funktion	72
6.7.2	HTTP	72
6.7.2.1	HTTP/1.0	72
6.7.2.2	HTTP/1.1	73
6.7.2.3	HTTP/2	73
6.7.2.4	HTTP/3	74
6.7.2.5	Caching, Proxy, Reverse Proxy, CDN	74
6.7.2.6	Logging und Uhrzeiten	75
6.8	Applikations-/Serververhalten	76
6.8.1	Grundproblem	76
6.8.2	Die fünf I/O-Programm-Modelle unter Unix	76
6.8.3	Socket Activation	78
6.8.4	Cloud Computing	78
6.8.5	Apache und Nginx	78
6.9	Angriff	79
7	Ergänzende Beispiele für Angriffe gegen die Authentizität von IP-Adressen	82
7.1	Angriffe gegen Autonome Systeme/BGP	82
7.2	Angriffe gegen den Internetprovider	83
7.2.1	Von innen	83
7.2.1.1	Innentäter	83
7.2.1.2	Fälschung der RADIUS-Nachrichten	84

7.2.1.3	Fälschung der RADIUS-Logs	85
7.2.1.4	Manipulation der Routen/Destination NAT	85
7.2.2	Von außen	86
7.2.2.1	Angriffe gegen die Router	86
7.2.2.2	Angriffe gegen BGP	86
7.2.2.3	Angriff auf Kundenleitungen	86
7.2.2.4	Fake-Anschlüsse	87
7.3	Angriffe gegen den Home-Router	87
7.3.1	Bedrohungslage	87
7.3.2	Malware und Fehlkonfiguration	89
7.3.3	Andere Nameserver, DNS-Einträge	89
7.3.4	VPN-Tunnel	89
7.3.5	Manipulation des Routings	90
7.3.5.1	Port per Static NAT routen	90
7.3.5.2	Quellenabhängiges Routing	91
7.3.5.3	IPv6-Adresse	91
7.3.5.4	Tante Erna ist dran	91
7.4	Angriffe gegen das Heimnetz	91
7.5	Angriffe gegen das Betriebssystem	92
7.6	Angriffe gegen die Applikation	92
7.6.1	Web-Browser	92
7.6.2	Beispiel: Signal	94
7.7	Angriffe gegen den Server	95
7.7.1	Logs fälschen	95
7.7.2	Routing	95
7.7.3	Zeitfälschung	95
7.7.4	Timing-Angriffe	95
7.7.5	Reverse DNS	95
8	Tatsächliche Vorfälle	97
8.1	Negativauskünfte	97
8.2	Kundenbeschwerden	97
8.3	Malware	97
II	Praktische Mängel	98
9	Anknüpfung an EuGH C-793/19	99
10	Unklarheiten des Gesetzestextes	100
10.1	Schlechte, ungeeignete Passivsprache	100
10.2	Unklare Berechtigte	101
10.2.1	Berechtigte des § 174 TKG	101
10.2.2	Berechtigte des § 175 TKG	102
10.2.3	Behörden welcher Staaten?	102
10.2.4	Internationale Amtshilfeersuchen	103

10.2.5	Warum Zoll, Verfassungsschutz, MAD und BND?	103
10.2.5.1	Ziel Kinderpornographie?	103
10.2.5.2	Zuständigkeiten der Verfassungsschutzbehörden der Länder	104
10.3	Unklare Verpflichtete	104
10.3.1	Unklare Abgrenzung durch technischen K.O.	104
10.3.2	„Wer öffentlich zugängliche Telekommunikationsdienste erbringt“	105
10.3.3	Unklare räumliche Abgrenzung	106
10.4	Unklarer Umfang der Verpflichtung	106
10.4.1	Nur mögliche Speicherung oder auch Ermöglichung der Speicherung?	106
10.5	Unklare sonstige Angaben	108
10.5.1	Kosten?	108
10.6	Unklare Feststellung der Anschlussinhaber	108
10.7	Standortfeststellung	109
10.8	Keine erkennbare Fehlerkontrolle	109
10.8.1	Sorgfaltspflichten und Nachprüfbarkeit?	109
10.8.2	Haftung, Schadensersatz, Richtigstellung	109
10.8.3	Beispiele	110
10.8.3.1	Fake-Anschlüsse	110
10.8.3.2	Kinderpornographie auf Nachbars Leitung	110
10.8.3.3	Inkompetenz des Verfassungsschutzes	110
11	ETSI-Standard TS 102 657	112
11.1	Version V2.7.1 vom November 2025	112
11.2	Verfahrensvorschrift	112
11.2.1	Gesetzentwurf und ETSI TS 102 657	112
11.2.2	Verordnungs-Ermächtigung an Frankreich	113
11.3	Fehlende Beteiligung von Datenschutz, Technik und Verbrauchern	113
11.4	Genereller Eindruck der Laienhaftigkeit	114
11.4.1	Naive Darstellungen	114
11.4.2	Schiefe Pfeile	115
11.4.3	Status Diagram Figure 5	115
11.4.4	Message Flow Figure 7, 9	115
11.4.5	HTTP-Versionen	116
11.4.6	Time Stamps	116
11.4.7	Prioritäten	116
11.4.8	Fehlende Differenzierung zwischen synchroner und asynchroner Kommunikation	117
11.4.8.1	Unklare Struktur	117
11.4.8.2	Message und Request verwechselt	117
11.4.9	Ungenügende Trennung zwischen Transport und Applikation	118
11.4.9.1	Kein Schichtenmodell	118
11.4.9.2	Keine Message Queue – Kein Deutschland-Stack	118
11.4.10	Keine Fehlerbehandlung	119

11.4.11 ASN.1	119
11.4.11.1 BER/DER	119
11.4.11.2 XDR	119
11.4.11.3 Definitionsfehler	119
11.5 Unzureichende Sicherheit	120
11.5.1 Keine Verschlüsselung auf Anwendungsebene	120
11.5.2 Definition auf Laienniveau	120
11.5.2.1 Verfahren nicht hinreichend definiert	121
11.5.2.2 Nur „recommended“ und „may validate“	121
11.5.2.3 „For Example“	121
11.5.2.4 Schlüsselhandling nicht definiert	122
11.5.2.4.1 Private Keys	122
11.5.2.4.2 Key Revocation	122
11.5.2.4.3 Public Keys	122
11.5.3 Mangelnde Identifikation der anfragenden Behörde	122
11.5.3.1 Inkonsistenz	122
11.5.3.2 Granularität und Definition der Organisationscodes	123
11.5.3.3 Aktenzeichen?	123
11.6 Keine Protokollierung	123
11.7 Unhaltbare Beweisfiktionen	124
11.8 Seltsame Versionssprünge	124
11.9 Einschätzung: Luftnummer und Blendwerk	125
12 Überkomplexität	126
12.1 Unverständliche Gesetzestexte	126
12.2 Schreckliches Flickwerk	127
12.3 Zunehmende Richterkapitulation	128
12.4 Bürokratieabbau?	129
12.5 Kontraproduktiv für die Netzabdeckung	129
13 Polizeiliche Probleme	131
13.1 Mangelnde Ausbildung	131
14 Umgehung der Adressspeicherung	132
14.1 Zweckverfehlende Unwirksamkeit	132
14.2 Frei verfügbare Internetzugänge im Inland	132
14.3 Frei verfügbare Internetzugänge im Ausland	133
14.4 VPN-Tunnel	134
14.5 Tor-/Onion-Router	134
14.6 „Tipps und Tricks für ANTIFAs und ANTIRAs“	134
14.6.1 Die Terror-Fibel des Unrast-Verlags	134
14.6.2 Die Rote Hilfe	135
14.6.3 Die Capulcu-Gruppe	136
14.6.4 Kulturstatsminister Weimer	137

III	Rechtliche Mängel	139
15	Meinungsfreiheit	140
15.1	Der Bundesgerichtshof	140
15.2	Der Bundeskanzler	140
16	Rechtliches Gehör, Rechtswegsgarantie, Unschuldsvermutung	141
16.1	Das Pferd von hinten aufgezäumt	141
16.2	Versagen des Richterbundes	142
16.3	Beweisfiktion, Unschuldsvermutung, Beweislastumkehr	143
16.3.1	Beweis durch Ignoranz	143
16.3.2	Bruch der Unschuldsvermutung durch Beweislastumkehr	144
16.4	Verantwortungsfiktion	145
16.4.1	Das Verantwortungsparadoxon	145
16.4.2	„Die Russen waren's.“	145
16.4.3	Der Bundestag und die Russen	146
16.4.4	Webbrowser	146
16.4.4.1	Sicherheitslücken	146
16.4.4.2	Böswilliger Web-Content	146
16.4.5	„Crime as a Service“	148
16.4.6	Ransomware 2.0	148
16.5	Kein Rechtsweg	148
16.6	Kein rechtliches Gehör	149
16.6.1	Keine Informationspflicht	149
16.6.2	Erforderliche Sachkunde	149
16.6.3	Richter?	150
16.6.4	Rechtsanwälte/Strafverteidiger?	150
16.6.5	Gerichtsgutachter?	150
16.6.6	Beschuldigte?	150
16.6.7	Kein Gehör vor der Weitergabe an Privatkläger	151
16.6.8	Beweisverbote des EuGH	151
16.6.8.1	EuGH C-670/22 (EncroChat)	151
16.6.8.2	EuGH C-746/18 (Vorratsdatenspeicherung)	151
16.6.8.3	Anwendung auf nationales Recht	152
16.7	Verfassungswidrigkeit des Gesetzentwurfs	153
17	Berufsgeheimnis, Pressefreiheit, Datenschutz	154
17.1	Das Berufsgeheimnis und seine Schändung	154
17.1.1	Die Rechtslage	154
17.1.2	Die Schändung durch die Justiz	155
17.1.3	Kein Schutz im vorliegenden Gesetzentwurf	155
17.1.4	Befürchtungen der Bundesrechtsanwaltskammer	155
17.2	Der Presseausweis als untauglicher Anknüpfungspunkt	156
17.2.1	Umgang der Justiz mit dem Presseausweis	156
17.2.2	Die Rechtslage	157
17.2.3	Die Innenministerkonferenz	157

17.2.4	Abwimmeln, Täuschen, Hinhalten	157
17.2.4.1	Zuständigkeits-Ping-Pong	157
17.2.4.2	Bedeutungswechsel	158
17.2.4.3	Das Beweisparadoxon	158
17.2.4.4	Beschwerde-Ping-Pong	158
17.2.5	Ein verfassungswidriges Schatten-Pressecorps	159
17.2.5.1	Willkür in das Privatrecht verlagert	159
17.2.5.2	Der doppelgesichtige Deutsche Journalistenverband	159
17.2.5.2.1	Das öffentliche Gesicht des DJV	159
17.2.5.2.2	Das andere Gesicht des DJV	159
17.2.5.3	Genießen auch Heinis Pressefreiheit?	160
17.2.6	Korruption	161
17.3	Das Fernmeldegeheimnis und die informationelle Selbstbestimmung	162
17.4	Der Medienstaatsvertrag	162
17.5	Verfassungswidrigkeit des Gesetzentwurfs	163
17.5.1	Missachtung im Gesetzentwurf	163
17.5.2	Gesamtsicht	163
18	Verhältnismäßigkeit	164
18.1	Verfassungsrechtliche Anforderungen	164
18.2	Fehlende Zweckangabe	164
18.3	Fehlende innere Verhältnismäßigkeit (Angemessenheit)	165
18.3.1	Schwere Straftaten	165
18.3.2	Äußerungsdelikte	165
18.3.3	Täuschung der Öffentlichkeit	165
18.3.4	Gummiparagraphen §§ 130, 185, 188 StGB	166
18.4	Mangelnde Eignung	167
19	Unklarheiten, Inkonsistenzen, Widersprüche	169
19.1	Inkonsistenz zwischen § 175 und § 176 TKG	169
19.2	„Die Verantwortung trägt ...“	170
IV	Missbrauch	171
20	Anknüpfung an EuGH C-793/19	172
21	Formen von Missbrauch	174
21.1	Fälschung durch Dritte	174
21.2	Missbrauch durch mangelnde Schulung/Inkompetenz	175
21.3	Missbrauch für private Zwecke	175
21.4	Politischer Missbrauch	175
21.4.1	Politische Weisungen	175
21.4.2	Politische Korruption	176
21.4.3	Ideologische Woke-Verflechtung von Polizei und Justiz	177

21.5 Verbindungen zwischen Polizei und organisierter Kriminalität	177
21.5.1 Bisherige Fälle	177
21.5.2 Berliner Wahl zum Abgeordnetenhaus 2026	179
21.6 Das Abmahnunwesen	180
21.7 Die Methoden des Bundeskriminalamts	181
22 Die Affäre Baerbock/Özdemir/Lang	184
22.1 Der Auslöser	184
22.1.1 Annalena Baerbock	184
22.1.2 Cem Özdemir	185
22.1.3 Nancy Faeser, Thomas Haldenwang, Holger Münch	186
22.2 Ein fingiertes Strafermittlungsverfahren als Vorwand	187
22.2.1 Ricarda Lang	187
22.2.2 Fingierte Strafanzeige § 188 StGB	189
22.2.3 Die heimliche rechtswidrige Kontenabfrage – 20 Rechtswidrigkeiten	190
22.2.4 Die Auskunft und Kontenkündigung der Deutschen Bank	196
22.2.5 Die Auswertung der Bankauskunft	199
22.2.6 Verfahrenseinstellung	199
22.3 Missbrauch der Finanzbehörden	200
22.3.1 Der Zoll	200
22.3.2 Das Finanzamt: Schein-Außenprüfung	200
22.4 Alles nur	203
23 Die Verstrickung des Deutschen Bundestags	205
23.1 Die „Meldestelle REspect!“	205
23.2 „HateAid“	206
23.3 Die Bundesnetzagentur und der Bundestag	209
V Gaga-Justiz statt Rechtswegsgarantie	212
24 Anknüpfung an EuGH C-793/19	213
25 Gaga-Strafrecht Berlin	214
25.1 Fehlender Rechtsweg	214
25.2 Gaga Staatsanwaltschaft	215
25.3 Gaga Ermittlungsrichterin	215
25.4 Gaga Landgericht	220
25.4.1 Beschwerde	220
25.4.2 Gaga 1: Zeugen	224
25.4.3 Gaga 2: Richtervorbehalt	226
25.5 Bundesverfassungsgericht als Regierungsvertretung	227
26 Die Hilflosigkeit des Datenschutzes in Berlin	231
27 Die Abwesenheit des Datenschutzes in Baden-Württemberg	232

28 Die Ruchlosigkeit des Datenschutzes in Hessen	233
28.1 Der Landesdatenschutzbeauftragte	233
28.2 Die Weigerung, sich mit der Sache zu befassen	233
28.3 Die Datenschutzabteilung der Deutschen Bank	233
28.4 Das Verwaltungsgericht Wiesbaden	234
28.5 Die Position des Landesdatenschutzbeauftragten	234
28.6 Wundersame Heilung: Asylbewerber	236
29 Die Verstrickung des Deutschen Bundesrats	238
VI Ergebnis	239
30 Ergebnis und Zusammenfassung	240
30.1 Tenor	240
30.2 Einzelbegründungen	241
30.2.1 Inhaltlicher Schwindel	241
30.2.1.1 Angriff auf Meinungs- und Pressefreiheit	241
30.2.1.2 Täuschung der Gerichte	241
30.2.1.3 ETSI-Standard TS 102 657	242
30.2.2 Allgemein mangelhafte Qualität	242
30.2.2.1 Zeitknappheit	242
30.2.2.2 Mangelnde Normierungsdichte	242
30.2.2.3 Schlampig, sprachlich schlecht, unklar, unverständlich	242
30.2.2.4 Politischer Notrufmissbrauch	243
30.2.2.5 Stellungnahme von 2023 ignoriert	243
30.2.2.6 Quantität, Kosten, ausufernder Zugriff	243
30.2.2.7 Methode „Wünsch Dir was“ / Case Law	244
30.2.3 Grenzen von Laienregierung und Laienparlament überschritten	245
30.2.3.1 Zusammensetzung und Qualifikation	245
30.2.3.2 Kosten	246
30.2.4 Das Problem evidenten Elends der Jurisprudenz	246
30.2.4.1 Massive Verwahrlosung der Justiz	246
30.2.4.2 Miserable Pseudoausbildung	247
30.2.4.3 Der „Freien Beweiswürdigung“ zum Fraß vorgeworfen	248
30.2.4.4 Kein rechtliches Gehör	249
30.2.5 Missbrauch	249
30.2.5.1 Faeser/Haldenwang	249
30.2.5.2 Grüne Missbrauchsstraße	249
30.2.5.3 Korrupte Berliner Polizei	251
30.2.6 Technik	251
30.2.6.1 Der Fundamentalfehler	251
30.2.6.2 Technisch bereits veraltet	251
30.2.6.3 Volatilität zu hoch	252

31 Verfahrensrügen	253
31.1 Ungenügende Bearbeitungszeit	253
31.2 Gesetzgebungsverfahren ungeeignet	253
31.3 Darstellungsform mangelhaft	254
32 Ausblick und weiteres Vorgehen	255
32.1 Europäischer Gerichtshof	255
32.2 USA	255
32.2.1 Handelsrecht	255
32.2.2 US State Department	255
32.2.3 US-Börsenaufsicht	256
33 Persönliche Anmerkung	257

1 Formale Angaben

1.1 Auftrag

Ich wurde am 24.9.2026 vom Rechtsausschuss des Deutschen Bundestages zur Stellungnahme zum und zur Teilnahme an der öffentlichen Anhörung über den Gesetzentwurf der Bundesregierung zur Einführung einer IP-Adressspeicherung und Weiterentwicklung der Befugnisse zur Datenerhebung im Strafverfahren eingeladen.

Eine explizite Frage- oder Problemstellung gab es nicht. Die Stellungnahme erfolgt deshalb als freie Äußerung.

1.2 Anschluss an meine Stellungnahme vom 9. Oktober 2023

Aufgrund der sehr kurzen zur Verfügung stehenden Zeit und zur Vermeidung von Wiederholungen verweise ich auf meine Stellungnahme vom 9. Oktober 2023 für den damaligen, ebenfalls auf Vorratsdatenspeicherung abzielenden Antrag der CDU/CSU-Bundestagsfraktion, die ebenfalls für den Rechtsausschuss erfolgte und **auf der Archivseite der Anhörung** zu finden ist.

Ich mache die damalige Stellungnahme zum Inhalt auch der vorliegenden.

Dies ist auch und insbesondere deshalb sachgemäß, weil daraus hervorgeht, dass die Bundesregierung – SPD und CDU/CSU – meine damalige Stellungnahme nicht beachtet hat.

1.3 Gegenstand

Gegenstand der Betrachtung sind:

BT-Drucksache 21/6581: Gesetzentwurf der Bundesregierung „Entwurf eines Gesetzes zur Einführung einer IP-Adressspeicherung und Weiterentwicklung der Befugnisse zur Datenerhebung im Strafverfahren“ vom 19.06.2026

BT-Drucksache 21/7154: Gegenäußerung der Bundesregierung vom 15.07.2026 zur Stellungnahme des Bundesrates

Ferner wurden herangezogen

StPO: Die **Strafprozessordnung**

EuGH: Die Entscheidung des EuGH **in den verbundenen Rechtssachen C-793/19 und C-794/19** (deutschsprachige Version) vom 20. September 2022

EuGH: Die Entscheidung des EuGH **in der Rechtssache C-470/21** (deutschsprachige Version) vom 30. April 2024 (La Quadrature du Net)

sowie die im Text verlinkten, insbesondere technischen Quellen, deren Auflistung hier zu weit führen würde.

Rückfragen an die Bundesregierung oder den Bundesrat erfolgten nicht.

1.4 Maßstäbe und Motivation

1.4.1 EuGH C-793/19 und C-794/19

Ich behalte den Maßstab aus meiner Stellungnahme vom 9. Oktober 2023 zur Vorratsdatenspeicherung für den Rechtsausschuss bei, nämlich den Absatz (Randnummer 131)

„Diese Rechtsvorschriften müssen durch klare und präzise Regeln sicherstellen, dass bei der Speicherung der fraglichen Daten die für sie geltenden materiellen und prozeduralen Voraussetzungen eingehalten werden und dass die Betroffenen über wirksame Garantien zum Schutz vor Missbrauchsrisiken verfügen.“

aus dem Urteil des EuGH in den verbundenen Rechtssachen C-793/19 und C-794/19, auf das sich der Antrag der CDU/CSU-Bundestagsfraktion von 2023 bezog, in der deutschsprachigen Übersetzung.

1.4.2 Eigene Tätigkeit Vorratsdatenspeicherung 2009

Ich habe – wie in meiner Stellungnahme vom 9. Oktober 2023 ausführlich beschrieben – im Jahr 2009 von Beginn der Vorratsdatenspeicherung bis fast zu deren Ende die Vorratsdatenspeicherung eines großen deutschen Internetproviders geleitet, dabei eine Zahl von Anfragen in einer Größenordnung von ungefähr 2000 eingangsgeprüft und für die damalige Entscheidung des Bundesverfassungsgerichts die wesentlichen Teile der Stellungnahme des BITKOM erstellt.

Ich lege meine Erfahrung aus der Tätigkeit von damals als Maßstab an, auch wenn Erfahrungssätze nicht explizit formulierbar sind, sondern deren Anwendung für sich sprechen muss. Ich habe dazu wesentliche Elemente meiner Erfahrungen in der Stellungnahme vom 9. Oktober 2023 beschrieben, auf die ich hierzu verweise.

Diese fließen insbesondere in Teil II (Praktische Mängel) ein.

1.4.3 Eigene Erfahrungen als Beschuldigter eines Strafermittlungsverfahrens

Ich war unlängst selbst Beschuldigter in einem Strafermittlungsverfahren, weil ich in einem Blogartikel eine Politikerin nach § 188 StGB beleidigt haben sollte. Dabei stellte sich heraus, dass das Ermittlungsverfahren nur fingiert und vorgetäuscht war und dem Zweck diente, unter dem Vorwand von Ermittlungen – heimlich und rechtswidrig – ein Spendenkonto meines Blogs auszuspionieren und schließen zu lassen, wie die damalige Bundesinnenministerin Nancy Faeser (SPD) und der damalige Verfassungsschutzpräsident Thomas Haldenwang (CDU) es in ihrem „**Aktionsplan Rechts-extremismus**“ von 2022 angekündigt hatten, obwohl es an der Rechtsgrundlage dafür fehlte.

Hier zeigte sich, dass die „Meldestelle REspect!“, das Landeskriminalamt Berlin, die Staatsanwaltschaft Berlin und der Verfassungsschutz kooperierten, um unter dem Vorwand eines Strafermittlungsverfahrens Ermittlungen vorzunehmen, zu denen sie nicht nur nicht befugt sind, sondern deren Menschenrechtswidrigkeit in einem anderen, gleich gelagerten Fall, bereits vom EGMR festgestellt worden war (**Sommer v. Germany, Individualbeschwerde 73607/13**).

Das Gericht lehnte das Hauptverfahren ab und stellte das Verfahren ein, weil die Staatsanwaltschaft zwar einen Strafbefehl betragt hatte, aber keine Straftat darlegen konnte.

In der Folge versuchten die damalige Innenministerin Faeser und der Verfassungsschutzpräsident Haldenwang, eine gesetzliche Grundlage zum Zugriff des Verfassungsschutzes auf Bankkonten zu erhalten, was aber durch das vorzeitige Ende der „Ampelregierung“ scheiterte.

Gerade weil der EuGH – siehe oben, zur Erinnerung nochmal der wichtige Absatz

„Diese Rechtsvorschriften müssen durch klare und präzise Regeln sicherstellen, dass bei der Speicherung der fraglichen Daten die für sie geltenden materiellen und prozeduralen Voraussetzungen eingehalten werden und dass die Betroffenen über wirksame Garantien zum Schutz vor Missbrauchsrisiken verfügen.“

– wichtige Anforderungen aufstellt, werde ich

- in Teil IV (Missbrauch) zeigen **und belegen**, dass die materiellen und prozeduralen Voraussetzungen nicht eingehalten, massiv verletzt und polizeiliche Ermitt-

lungsbefugnisse zu politischen Zwecken missbraucht werden,

- in Teil **V** (Rechtswegsvereitelung) zeigen **und belegen**, dass der Rechtsweg völlig vereitelt wird und nicht funktioniert, die vom EuGH geforderten *wirksamen Garantien* in Deutschland schlicht nicht existieren,
- in beiden Teilen zeigen, dass der Datenschutz¹ und die Aufsicht durch die Landesdatenschutzbeauftragten faktisch nicht existieren,
- und dass die Bundesrepublik Deutschland strukturell und durch nicht kurzfristig behebbare Mängel in der Juristenausbildung gar nicht in der Lage ist, die Anforderungen des EuGH zu erfüllen,

um das Ergebnis meiner Stellungnahme auf eine tragfähige Grundlage zu stellen.

1.4.4 Technische Berufserfahrung

Ich lege außerdem meine Berufserfahrung aus inzwischen 40 Jahren in der Informatik zugrunde, dabei insbesondere mehrjährige Tätigkeiten bei Internet-Providern, im Bereich Internet und Firewalls, Absicherung von Netzwerken.

Diese fließen insbesondere in Teil **I** (Technische und forensische Mängel) ein.

1.4.5 Weitere persönliche Erfahrungen

Dazu kommen weitere persönliche Erfahrungen mit massiven – rechtswidrigen und missbräuchlichen – Eingriffen von Bundes- und Landesregierung oder Regierungsfractionen und des Bundesnachrichtendienstes in das Verwaltungs- und Zivilrecht in den Jahren 1998 bis 2007, 2009 und 2012. Diese fließen in die kriminalistische Sichtweise der Missbrauchsanalyse und des Versagens des Staates beim Rechtsweg (Teile **IV** und **V**) ein.

1.5 Bearbeitungszeit viel zu kurz

Ich weise darauf hin, dass die überaus kurze Zeit zwischen Einladung und Anhörung nicht erlaubte, alles Details in voller Tiefe auf Richtigkeit und Aktualität zu prüfen und die vorliegende Stellungnahme im Wesentlichen aus der beruflichen Erfahrung und dem Gedächtnis aus den Tätigkeiten der letzten 40 Jahre erfolgen musste.

Ich halte die zur Verfügung stehende Zeit angesichts der Schwere und Tragweite des Themas für viel zu kurz bemessen.

¹hier anzuwenden: § 500 StPO i. V. m. Teil 3 BDSG

Für eine vertiefte Betrachtung wären ein sehr viel größerer Aufwand an Literaturrecherche, dazu Laborexperimente und Rücksprache mit den einzelnen Providern zu betreiben.

Dieser Aufwand wäre meines Erachtens aber Aufgabe der Bundesregierung bzw. des Antragstellers und nicht der Sachverständigen.

Da die vorliegende Stellungnahme unter höchstem Zeitdruck – einschließlich Tages-, Abend-, Nacht- und Wochenendarbeit – bitte ich, Schreib- und Formulierungsfehler u.ä. gegebenenfalls zu entschuldigen.

1.6 Sachkunde

- 1994 Diplom in Informatik
- über 35 Jahre hauptberufliche Tätigkeit als Informatiker, davon 10 Jahre in Forschung und Lehre zu IT-Sicherheit und Kryptographie, 23 Jahre in der Industrie als IT-Sicherheitsexperte, Information Security Officer, Datenschutzkoordinator, Compliance Officer
- davon 7 Jahre bei Internet-Providern
- 9 Jahre im Post- und Fernmeldebereich
- Mitarbeit am Aufbau des Internet in Deutschlands, u.a. Absicherung und Anschluss des ersten Kernkraftwerks an das Internet, mehrfach sicherheitsüberprüft
- **3 Jahre in der Rechtsabteilung eines großen Telefon- und Internetanbieters in Deutschland**
- **dabei 1 Jahr (2009) in der Vorratsdatenspeicherung und Beauskunftung, Aufsicht und Eingangsprüfung von zwischen 1.000 und 2.000 Fällen**
- **2009 als Vertreter eines Telefon- und Internetanbieters am Vorhaben der Kinderpornosperr der Regierung (Ursula von der Leyen) involviert. Die Sperre wurde durch das BKA abgeblasen, nachdem ich das BKA beraten und die Fehler und Probleme im Vorhaben aufgezeigt habe.**
- 1997 Assistent und Ghostwriter bei Anhörung zum Kryptographieverbot des Deutschen Bundestags
- 1998 Gutachten „Künftige Anforderungen an die Kommunikationssicherheit in der Medizin“ für den Deutschen Bundestag (BT-Ds 13/11002)
- 2019 Stellungnahme zu „Uploadfiltern“, Anhörung im Abgeordnetenhaus Berlin
- 2020 Stellungnahme zur Erhöhung der Rundfunkbeiträge, Anhörung im Landtag Sachsen
- 2021 Stellungnahme zum MDR Staatsvertrag, Anhörung im Landtag Thüringen
- 2023 Stellungnahme für den Bundestag zur Vorratsdatenspeicherung
- 2026 Stellungnahme für den Bundestag zu Digitalen Ermittlungsbefugnissen
- Über 30.000 Blogartikel zu Rechts- und Medienpolitik und vielen anderen Themen

Teil I

**Technische und forensische
Mängel**

2 Nachträge zur und Anschluss an die Stellungnahme vom 9. Oktober 2023

2.1 Schwächen des Border Gateway Protocol

Ich hatte in der Stellungnahme vom 9. Oktober 2023 im Abschnitt „3.3.5 Beispiel BGP Hijack, ARP Spoofing u.ä.“ beschrieben, dass im Internet ganze IP-Adressbereiche übernommen und gefälscht werden können. Man kann damit den Anschein erwecken, dass der rechtmäßige Nutzer eines IP-Adressbereiches verbotene Handlungen über das Internet begangen habe, obwohl er das nie getan hat, sondern ein Angreifer, der kurzzeitig dessen IP-Adressbereiche zu sich umgeroutet hat. Ursache sind strukturelle Schwächen im veralteten „Border Gateway Protocol“ (BGP).

Heise meldete dazu am 16.5.2024: „**FCC-Chefin will das Border Gateway Protocol absichern**“.

Die Routingtabellen des Internet (Border Gateway Protocol, BGP) sind anfällig für Manipulation. Durch "BGP-Hijacking" wird Datenverkehr böswillig umgeleitet, untergeschoben oder zum Erliegen gebracht. Hinzu kommen irrtümlich falsche Einträge, die Störungen nach sich ziehen. Die Vorsitzende der US-Regulierungsbehörde FCC, Jessica Rosenworcel, will US-Breitbandanbieter nun dazu verpflichten, zumindest Vorkehrungen gegen irrtümlich falsche Routen zu setzen.

Dazu dient Resource Public Key Infrastructure (RPKI). Erst wenn RPKI ausgerollt ist, kann die nächste Sicherheitsmaßnahme BGPsec greifen, die besseren Schutz gegen absichtliches BGP-Hijacking bietet. Rosenworcel möchte ihre vier Kollegen in der FCC davon überzeugen, dass die Behörde US-Breitbandanbieter dazu verpflichtet, ihre Datenrouten mit RPKI abzusichern.

Die US-Regierung kümmert sich also um solche Schwächen. Von der deutschen Regierung ist mir bisher nicht bekannt, dass sie das Problem überhaupt erkannt oder zur Kenntnis genommen habe. Das aber wäre Voraussetzung für ein gesetzgeberisches Unterfangen wie das vorliegende.

2.2 Herstellerspezifische Protokollierungsfunktionen bei Carrier Grade NAT

Ich hatte in der Stellungnahme vom 9. Oktober 2023 beschrieben, dass Provider NAT, bzw. der inzwischen gebräuchliche englische Terminus **Carrier Grade NAT (CGNAT)** (früher als NAT444 oder selten auch als NAT44 – was falsch oder irreführend ist, weil das normalerweise nur das Endanschluss-NAT beim Kunden beschreibt – inzwischen auch als Large Scale NAT LSNAT bezeichnet) kein bestimmtes, festgelegtes Verfahren ist, sondern nur eine Oberbezeichnung für verschiedene Methoden, und es *im Allgemeinen* wegen der hohen Frequenz der NAT-Zuweisen schon aufgrund der Datenmenge nicht möglich ist, bei CGNAT eine Adressspeicherung derart vorzunehmen, dass man hinterher jede Einzelkommunikation einem Anschlussinhaber zuordnen kann, wenn nicht besondere Herstellersstrategien zum Einsatz kommen.

Ich habe hierzu die Herangehensweisen verschiedener Hersteller exemplarisch betrachtet. Diese unterscheiden sich methodisch deutlich und sind möglicherweise patentiert.

Es ist also vom Hersteller und den Modellen abhängig, ob im Falle von CGNAT eine nachträgliche Zuordnung überhaupt möglich ist. Dabei schälen sich zwei bevorzugte Verfahren heraus: Dynamic Port-block Allocation (DPA) und Deterministic NAT.

2.2.1 Log-Umfang

2.2.1.1 RFC 7422

RFC 7422: Deterministic Address Mapping to Reduce Logging in Carrier-Grade NAT Deployments von 2014 beschreibt ausführlich die Probleme beim Loggen von CGNAT und **bestätigt meine Aussage von 2023, dass im Allgemeinen CGNAT aufgrund der anfallenden Datenmengen nicht oder nicht praktikabel geloggt werden kann.**

Based on available data, a 1-million-subscriber SP will generate approximately 150 terabytes of log data per month, or 1.8 petabytes per year. Note that many SPs compress log data after collection; compression factors of 2:1 or 3:1 are common.

Inzwischen bieten zwar einige Hersteller auch ein „High Speed Logging“ (HSL) an, das aber nur in Sonderfällen tauglich ist. Grundsätzlich beschreiben viele Hersteller (A10, F5, Juniper, Cisco, NFWare usw.) in ihren Dokumentationen, dass CGNat **aufgrund der anfallenden Datenmengen im Allgemeinen nicht oder nicht praktikabel logging-fähig ist.**

2.2.1.2 A10 Networks

Auch A10 bestätigt in ihrem Whitepaper „**Making Cents of IPv4**“ meine Einschätzung:

The standard subscriber translation logging can easily exceed a terabyte of storage a day, depending on the number of subscribers supported. With advanced logging techniques including log compression or deterministic/fixed NAT, a provider can easily reduce the volume of logs and parse the data.

2.2.1.3 Netelastic

Auch **Netelastic** beschreibt dies:

NAT Storage:

If you store NAT logging records locally, you must plan out the storage space needed. A good estimate for NAT session storage (in raw ASCII format) rate is 0.4MB/second per 1,000 users. For example, if you have 10,000 users, the NAT log storage will grow at 4MB/s or 346GB per day in raw ASCII format. The gzip compression ratio for the raw NAT log file is around 27:1. Based on these numbers, you should plan to have 13GB of disk storage growth per day for every 10,000 users.

Extrapolating this out, you would need 4.7 terabytes of storage to retain full detail logging for 10,000 subscribers.

2.2.1.4 draft-donley-behave-deterministic-cgn-00.txt

Auch C. Donley, CableLabs, bestätigt **2014** meine Einschätzung von 2023 im **RFC 7422**.

CGN connection logging satisfies the need to identify attackers and respond to abuse/law enforcement requests, but it imposes significant operational challenges to ISPs. In lab testing, we have observed CGN log messages to be approximately 150 bytes long for NAT444 [I-D.shirasaki-nat444], and 175 bytes for DS-Lite [RFC6333] (individual log messages vary somewhat in size). Although we are not aware of definitive studies of connection rates per subscriber, reports from several ISPs in the US sets the average number of connections per household per day at approximately 33,000 connections per day. If each connection is individually logged, this translates to a data volume of approximately 5 MB per subscriber per day, or about 150 MB per subscriber per month; however, specific data volumes may vary across different ISPs based on myriad factors. Based on available data, a 1-million subscriber service provider will generate approximately 150 terabytes of log data per month, or 1.8 petabytes per year.

2.2.1.5 Von 2011 zu 2026

Ich weise darauf hin, dass all diese Untersuchungen auf der Internetnutzung der Jahre 2011 bis 2014 beruhen, als es z. B. noch keine Smartphones, keine Smartfernseher, weitaus weniger Streaming usw. gab und viele Dienste noch nicht existierten oder weit weniger genutzt wurden, deutlich weniger dynamische und stehende Verbindungen aufgebaut wurden.

Die Zahl der Verbindungen *pro Haushalt* oder *pro Mobilgerät* liegt heute drastisch höher als damals.

2.2.2 Log-Geschwindigkeit

Nach der Stellungnahme vom 9. Oktober 2023 habe ich auch Herstellerwebseiten gefunden, die das Problem der Log-Geschwindigkeit thematisierten und vorrechneten, dass die dabei anfallenden Datenmengen mit normalen Mitteln schon wegen der Geschwindigkeit nicht zu bewältigen sind.

Inzwischen habe ich diese expliziten Darstellungen nicht mehr gefunden, weil Hersteller ihre Seiten dazu überarbeitet haben und der Schwerpunkt nun auf den – leichter verständlichen – Datenmengen und den Lösungsvorschlägen der Hersteller liegt.

Trotzdem bedarf das Problem einer Betrachtung.

2.2.3 Herstellerspezifische Logging-Methoden

2.2.3.1 F5: CGNAT port block allocation sizing and tools for LSN pools

F5 beschreibt ihre Methode so:

CGNAT PBA works allocates a contiguous set of source translation endpoints called port blocks. These port blocks are associated to a client by one IP address and a block of ports. Port blocks are allocated on-demand and have a fixed size.

LSN pool configuration settings are closely interrelated and determine how the blocks are allocated to the clients. Choose these settings carefully to adequately and efficiently service clients that may require a different number of simultaneous connections. Careful analysis and testing is required to find optimal values.

The following LSN pool configuration settings are covered in this article:

- **Member List:** Specifies the set of translation IP addresses available in the pool as a collection of IP prefixes with their prefix lengths. All public-side addresses come from the subnets entered in this property in CIDR format.
- **Port Block Allocation:** Configures the port block settings for PBA mode, which include:

- **Block Size:** The number of ports allocated in a block. The default value is 64.
- **Client Block Limit:** The maximum number of blocks assigned to a single subscriber. The default is 1.
- **Port Range Low:** Specifies the lowest range port number available for use with translation IP addresses. The default value is 1025.
- **Port Range High:** Specifies the highest range port number available for use with translation IP addresses. The default value is 65535.
- **Inbound Connections:** Specifies the inbound-connection mode for incoming connections to translation endpoints.

2.2.3.2 Nokia Deterministic Large Scale NAT44

Nokia beschreibt das Verfahren **Deterministic Large Scale NAT44**

This example is applicable to 7750 SR systems and 7450 ESS systems in mixed mode equipped with an MS-ISA on an IOM3-XP/XP-b using chassis mode B, C or D.

The configuration was tested on release 11.0R3.

Overview

Deterministic Network Address Translation (NAT) is a mode of operation where mappings between the NAT subscriber and the outside IP address and port range are allocated at the time of configuration.

In deterministic NAT for Large Scale NAT IPv4-to-IPv4 (LSN44) subscribers, each LSN44 subscriber is permanently mapped to an outside IP address and a dedicated (deterministic) port-block based on a specific algorithm.

Logging is not needed in this case as the reverse mapping can be obtained using the reverse of the above algorithm.

A deterministic LSN44 subscriber can have only one deterministic port-block that can (optionally) be extended by one or multiple dynamic port-blocks in case all ports in deterministic port-block are exhausted.

In case an LSN44 subscriber has been assigned both deterministic and dynamic port blocks, logging for the dynamic port-block allocation/de-allocation is required.

A scalable logging solution for dynamic port-blocks is achievable using RADIUS or IPFIX.

Logging for dynamic port-blocks is out of the scope of this example.

Algorithm

The deterministic NAT algorithm makes a predictable mapping between the (inside IP, routing instance) and the (outside IP, routing instance, deterministic port block).

The algorithm is revertive, meaning that a given (outside IP, routing instance, deterministic port block) will derive a given (Inside IP, Routing Instance).

The algorithm is loosely based on the draft RFC draft-donley-behave-deterministic-cgn-00.txt [Jetzt **RFC 7422**, which allows for the dynamic expansion of the port-blocks once the ports in the original deterministic port-block are exhausted.

In diesem Fall gibt es also keine – *insbesondere keine nachprüfbaren* – Logdateien, weil der Portbereich deterministisch-algorithmisch zugewiesen wird und Änderungen der Block-Größe und anderer Parameter **nachträglich womöglich nicht mehr feststellbar sind und nicht geloggt werden, es also zu fehlerhaften Schein-Zuordnungen kommt**.

Das ist außerdem nur möglich, wenn ein hinreichend günstiges Zahlenverhältnis zwischen Zahl der Kunden und zur Verfügung stehenden IPv4-Adressen besteht.

2.2.3.3 Citrix ADC/Netscaler

Netscaler erklärt:

Large Scale NAT (LSN) feature is deprecated from NetScaler 14.1 release onwards.

Deprecated features are not removed immediately. The NetScaler® appliance continues to support the deprecated feature until it is removed in a future release.

Stattdessen müssen künftig Lösungen von A10 Networks, F5, Nokia, Huawei usw. verwendet werden.

2.2.4 Gefahren durch statische oder deterministische Port Block Allocation (PBA)

2.2.4.1 Netzwerkstörungen

Es wurden bereits Störungen beschrieben, die bei zu kleiner Block-Größe auftreten, weil es bei Kunden, die schnell viele Verbindungen aufbauen der Vorrat an Port-Adressen erschöpft wird.

Wählt man die Blöcke aber zu groß, wird das CGNAT ineffektiv und das Verhältnis von Kunden und benötigten IP-Adressen zu schlecht.

2.2.4.2 Datenschutz, Identitätsschutz und Tracking

Bei deterministischen Blockzuweisungen kann es passieren, dass ein Kunde über einen langen Zeitraum dieselbe IP-Adresse und denselben Port-Block zugewiesen bekommt, und dann nicht mehr anonym ist sondern über IP-Adresse und Port-Bereich identifiziert (tracking) werden kann.

Wenn die Zuweisung der Portblöcke und äußeren IP-Adressen *deterministisch und umkehrbar algorithmisch* erfolgt, kann auch ein Angreifer bzw. unbefugter Dritter Kenntnis der Parameter erlangen oder diese sogar durch Tests rekonstruieren und selbst umkehren.

Solche Methoden sind datenschutzrechtlich mindestens hochproblematisch, möglicherweise unzulässig.

2.2.4.3 Fehlerhafte Nutzerzuordnungen

Charakteristisches Merkmal der statischen oder deterministischen Port Block Allocation ist, dass nichts geloggt wird, sondern im Falle einer Abfrage die Zuordnung nachvollziehbar und umkehrbar sein soll, man also „ausrechnen“ könne, wer Nutzer einer TCP-Verbindung gewesen sei.

Wenn aber nur geringfügige, auch unbeabsichtigte oder unbemerkte Änderungen an der Konfiguration vorgenommen werden, auch Softwareupdates, defekte Hardware ersetzt usw., kann sich die deterministische Zuordnung ändern und ein nachträgliches „Rückrechnen“ zum falschen Ergebnis führen.

Das ist forensisch nicht belastbar.

2.3 MAP-E, MAP-T und Lightweight 4over6 statt CGNAT

Herkömmliches CGNAT gilt als Auslaufmodell, **weil es stör- und fehleranfällig ist und nur ein vorübergehendes Transitions Hilfsmittel für den Übergang von IPv4 zu IPv6 war.**

Erste Provider gehen inzwischen dazu über, statt NAT44, NAT444, CGNAT zu verwenden auf modernere Methoden wie

- Lightweight 4over6 **RFC 7596**,
- Mapping of Address and Port with Encapsulation (MAP-E) **RFC 7597** und
- Mapping of Address and Port using Translation (MAP-T) **RFC 7599**

zu setzen und IPv4-Verkehr ohne eindeutige IP-Adresse entweder in IPv6 einzubetten (MAP-E, encapsulation), oder in IPv6 zu übersetzen (MAP-T, translation).

Bisher werden vor allem Provider in Ländern mit moderner IPv6-Infrastruktur und starkem IPv4-Mangel als Anwender genannt, vor allem in Japan und China, aber auch in europäischen Ländern wie Italien und dem Vereinigten Königreich. Besonders die „Sky-Gruppe“ (Sky UK, Sky Italia) wird hier als Vorreiter in Europa genannt. Andere Provider sollen in der Testphase sein.

Wesentlicher Unterschied ist, dass bei MAP-E und MAP-T nicht mehr eine RFC1918-Zwischen-NAT-Adresse zugewiesen wird, sondern der Verkehr zwischen Kundengerät und Border-Router in IPv6 entweder eingebettet (MAP-E) oder übersetzt (MAP-T) wird.

Jedem Kundengerät (Wohnungsrouter etc., nicht abschließend definiert, ob jedem einzelnen Endgerät, oder dem Wohnungsrouter mit dann lokalem NAT, in der Praxis wird dies der Wohnungsrouter sein) muss dazu algorithmisch ein Portbereich einer öffentlichen IPv4-Adresse zugewiesen werden.

Zwar kommen auch hier Portbereiche zur Anwendung, die auf den ersten Blick der Gesetzesformulierung unterliegen. **Der private Wohnungsrouter wird aber nicht vom Gesetzestext erfasst – Anschlussinhaber müssen sich nicht selbst bevorratsdatenspeichern.**

Ob dabei am Border-Router überhaupt Daten im Sinne des Gesetzes anfallen, wäre technisch und für jeden Hersteller oder jedes Modell und jede Firmware noch zu prüfen.

3 Verständnisfehler und Begriffsverwirrungen der Regierung

3.1 Im Gesetzentwurf

3.1.1 Verbotsirrtum: Phantasieunterschied „Vorratsdatenspeicherung“ und „IP-Adressspeicherung“

Auf den ersten Blick könnte man sich darüber wundern oder amüsieren, dass die Bundesregierung den so bekannten, aber eben negativ konnotierten und präjudizierten Begriff der „Vorratsdatenspeicherung“ durch den Begriff der „IP-Adressspeicherung“ ersetzt – obwohl sie genau dasselbe machen will.

Das erscheint zunächst wie eine PR-Maßnahme von Beratern und Parteistrategen, wie so oft verbrannte Begriffe einfach auszutauschen, um dem Volk alten Essig in neuen Schläuchen zu verkaufen und erinnert an den bekannten Werbespruch *„Aus Raider wird Twix. Sonst ändert sich nix.“* zum Markenwechsel eines technisch unveränderten Schokoriegels.

Liest man die Äußerungen der Bundesregierung im und im Zusammenhang mit dem Gesetzentwurf aber genauer, stößt man auf ein viel tiefgreifenderes Problem.

Beispiel: Seite 21 des Gesetzentwurfs.

In der Vergangenheit hat es mehrere Versuche gegeben, eine Vorratsdatenspeicherung von Verkehrs- und Standortdaten zu Zwecken der Strafverfolgung und Gefahrenabwehr einzuführen, zuletzt mit dem Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten vom 10. Dezember 2015 (BGBl. I S. 2218). Im Rahmen eines vom Bundesverwaltungsgericht angestrebten Vorabentscheidungsverfahrens hat der Europäische Gerichtshof mit Urteil vom 20. September 2022 – C-793/19 und C-794/19, Spacenet und andere – entschieden, dass Regelungen wie die 2015 in Deutschland eingeführten nicht mit dem Unionsrecht vereinbar sind. Daraufhin hat das Bundesverwaltungsgericht am 14. August 2023 – 6 C 6.22 – geurteilt, dass die maßgeblichen Regelungen des Telekommunikationsgesetzes mit europäischem Recht unvereinbar sind und nicht mehr angewendet werden dürfen. Das Oberverwaltungsgericht für das Land Nordrhein-Westfalen hatte bereits mit Beschluss vom 22. Juni 2017 – 13 B 238/17 – zugunsten eines Internetzugangsdienstes vorläufig festgestellt, dass keine Verpflichtung bestand, Verkehrsdaten ihrer Kunden auf Grundlage des 2015 eingeführten Gesetzes zu speichern.

Deutlicher Seite 22:

Die Speicherpflicht betrifft zwar alle Nutzer von Internetzugangsdiensten in Deutschland. Allerdings lassen die Daten nichts anderes zu als die Identifizierung des Anschlussinhabers anhand einer IP-Adresse. Es handelt sich gerade nicht um eine Vorratsdatenspeicherung von allen Verkehrs- und Standortdaten. Aus den gespeicherten IP-Adressdaten lassen sich insbesondere keine Surf- oder Bewegungsprofile erstellen.

Seite 23:

Mit dem Entwurf werden außerdem die Regelungen der europarechtswidrigen Vorratsdatenspeicherung und hierauf bezogene Abrufbefugnisse gestrichen.

Seite 30:

Anders als bei früheren Regelungen zu einer umfassenden Vorratsdatenspeicherung wird nur eine anlasslose Speicherpflicht im Hinblick IP-Adressen eingeführt sowie eine anlassbezogene Pflicht zur Sicherung von Verkehrsdaten aufgrund einer Sicherungsanordnung in einem konkreten Strafverfahren.

Das ist nicht nur allgemein technisch falsch, weil – wie ich unten u.a. in [3.1.5](#) noch zeigen werde – mittels der IP-Adressen durchaus eine Standortbestimmung und Bewegungsverfolgung möglich sein kann.

Die Bundesregierung befindet sich auch in einem Irrtum über frühere „Vorratsdatenspeicherungen“ und glaubt, früher seien umfangreich Verkehrsdaten aufgezeichnet worden. Das ist *bezüglich der IP-Adressen* nicht zutreffend. Auch 2009 bestand die „Vorratsdatenspeicherung“ nur aus der Aufzeichnung der den Anschlussinhaber temporär zugeordneten IP-Adressen.

Die Bundesregierung unterliegt entweder – soweit ersichtlich – einem Verbotsirrtum, weil sie die damalige Vorratsdatenspeicherung nicht verstanden hat, und irrtümlich glaubt, sie mache jetzt etwas anderes, milderes, was den damaligen Verboten nicht unterliege – oder es ist ein juristisch-rabulistischer Täuschungsversuch, dem Leser einzureden, man mache da jetzt etwas anderes als damals.

Würde man Böswilligkeit oder Hinterlist unterstellen, könnte man auch auf den Gedanken kommen, dass hier mit Begriffen jongliert wird und die Formulierungen gewählt wurden, um die Öffentlichkeit und Gerichte wie das Bundesverwaltungs- und -verfassungsgericht zu täuschen und ihnen vorzugaukeln, dass man jetzt etwas anderes mache, worauf die früheren Verbotsentscheidungen nicht anwendbar wären, dass also die Umbenennung der Umgehung der Verbote dient.

3.1.2 „Zuverlässigkeit“ statt „Rechtssicherheit“

Während in der Bundestagsdiskussion von 2023 noch der Begriff der „Rechtssicherheit“ vorherrschend war, steht nun der Begriff der „Zuverlässigkeit“ im Vordergrund. So heißt es bereits auf der ersten Seite des Entwurfs

Es wird erstens eine Pflicht zur Speicherung von IP-Adressen eingeführt, um den Strafver-

folgungsbehörden und anderen berechtigten Stellen die zuverlässige Identifikation eines Anschlussinhabers anhand einer IP-Adresse zu ermöglichen.

Beides ist nicht haltbar.

Das Internet ist nicht rechtssicher und nicht zuverlässig. Weder verfügt es tatsächlich über diese Eigenschaften, noch waren sie jemals spezifizierte oder angestrebte Eigenschaften.

Das Internet wurde vor 50 Jahren entwickelt. Damals hatte man noch gar keine Gedanken an Rechtssicherheit und Zuverlässigkeit, hätte auch gar nicht gewusst, was das sein sollte, und bewegte sich im US-amerikanischen Rechtssystem.

Man könnte ein Netzwerk wie das Internet auch weder bauen noch betreiben, wenn es „rechtssicher“ und „zuverlässig“ sein sollte. Das wäre nicht nur von Aufwand und Komplexität unmöglich (vgl. Abschnitt 4.1), sondern schließt sich auch mit wichtigeren Eigenschaften wie Verfügbarkeit, Fehlertoleranz, Robustheit aus.

Sicherheit ist explizit keine Eigenschaft des Internet selbst, sondern das Internet setzt voraus, dass Anwender die Sicherheit in den oberen Schichten (vgl. Abschnitt 4.2) Ende-zu-Ende selbst herzustellen.

Es ist deshalb nicht möglich, eine „rechtssichere“ oder „zuverlässige“ IP-Adressspeicherung zu betreiben, weil man ein Netzwerk, das diese Eigenschaften nicht aufweist, durch Protokollierung nicht rechtssicher oder zuverlässig machen kann.

Die Zielsetzung des Gesetzentwurfes ist nicht erfüllbar.

Machen Sie sich bewusst:

Das Internet und sein IP-Protokoll haben per se, per constructionem keinerlei Sicherheitseigenschaften und sind weder rechtssicher noch zuverlässig, weil weder spezifiziert noch tatsächlich.

Sämtliche Sicherheitseigenschaften müssen entweder über die darunterliegenden Schichten 1 und 2 (z.B. Netzwerksegmente, Firewalls) oder die darüberliegenden Schichten 4 bis 7 (z. B. TLS, Dateiverschlüsselung, Authentifikation, VPN usw.) hergestellt werden.

3.1.3 „Internetverbindung“

Sowohl im Kontext zum Gesetzesentwurf, als auch im Text selbst (§ 177 Abs. 1 Nr. 1 und Nr. 3 TKG) wird der Begriff der „Internetverbindung“ verwendet, und Pflichten und Befugnisse daran gebunden.

Es gibt keine „Internetverbindung“. (There is no such beast.)

In der Informatik und IT unterscheidet man im Wesentlichen zwischen zwei Arten von Kommunikationsnetzwerken, nämlich

- Verbindungsorientierten
- Verbindungslosen (paketorientierten)

Das Internet ist ein verbindungsloses, paketorientiertes Netzwerk. Darauf beruhen sein großer Erfolg und seine enorme Leistungsfähigkeit.

Wie der Name schon so sagt, gibt es in einem verbindungslosen Netzwerkprotokoll keine Verbindungen. Sonst würde man es auch nicht so nennen.

Was es dagegen gibt, womit dies oft verwechselt wird, dass Internet-Pakete (Schicht 3, vgl. Abschnitt 4.2) mittels entsprechender Protokolle wie PPP (vgl. Abschnitt 6.4.2) über verbindungsorientierte Netzwerke bzw. Verbindungen auf den Schichten 1 und 2 übertragen wird (z. B. Modem, ISDN, DSL).

Insofern wäre es zwar fachlich falsch, aber sachlich noch vertretbar, im umgangssprachlichen Sinne von einer „Internet-Verbindung“ zu sprechen.

Das ist aber nicht nur nicht zwingend, weil es auch andere Verfahren und Protokolle gibt, sondern es ist auch eine veraltete Vorgehensweise, die gerade ausläuft und immer seltener vorkommt (ausführlicher in Abschnitt 6.4.2).

Über die fachlichen und begrifflichen Ungenauigkeiten hinaus hat dies auch sachliche Auswirkungen auf den Gesetzentwurf, denn der Gesetzentwurf orientiert sich am Verbindungsmodell mit Verbindungsauf- und -abbau, an den Pflichten gebunden werden.

Ein verbindungsloses Netzwerk und -protokoll wie das Internet und IP-Protokoll haben aber keinen Verbindungsauf- und abbau.

3.1.4 „Kennung“

Im Gesetzentwurf taucht immer wieder der Begriff der „Kennung“ auf, insbesondere in Form der *Anschlusskennung* und *Benutzerkennung* (z. B. § 101a Abs. 1 Nr. 2a StPO, § 177 Abs. 1 Nr. 3 TKG, auch in der Begründung Seite 56/57).

Manche Dienste verwenden eine Kennung, viele aber nicht.

Das Internet und das Internetprotokoll selbst kennen weder Benutzer noch Anschlüsse, und auch keine Anschluss- und Benutzerkennungen. Das Internet und das Internetprotokoll verwenden ausschließlich IP-Adressen (und im erweiterten Sinne Portnummern und ICMP-Nachrichten).

„Kennungen“, „Anschlüsse“, „Benutzer“ finden – manchmal, nicht immer – auf den darunterliegenden Schichten 1 und 2 oder den darüberliegenden Schichten 5 bis 7 statt.

Auch das sind Sichtweisen, die den in den letzten Jahrzehnten häufig betriebenen Internet-Diensten über PPP (vgl. Abschnitt 6.4.2) entsprechen, aber auslaufen und schon lange veraltet sind.

Zwar verlangen PPP und das zugehörige RADIUS-Protokoll noch zwingend die Angabe einer Kennung, überprüft wird diese aber bei den meisten Anbietern schon lange nicht mehr und stattdessen der Router-Port verwendet, an den das DSL-Kabel angelötet oder -geklemmt ist.

In Netzwerkauthentifikationstechniken der Schichten 1 und 2 wie Wifi (Open, PSK, WPA, WPA2, WPA3,...) gibt es *gar keine* Benutzer- oder Anschlusskennung. Zwar übernimmt dabei die MAC-Adresse deren Funktion, da diese aber beliebig geändert werden kann, erfüllt sie die Funktion im Sinne des Gesetzes nicht. Erst mit Authentifikationstechniken wie etwa IEEE 802.1X (bei Wifi und Ethernet) oder PPP (Modem, ISDN, DSL, ...) wird eine Benutzerkennung möglich. In Sternstrukturen ist auch eine physische Anschlusskennung möglich. IEEE 802.1X wird aber in den für diesen Gesetzentwurf relevanten Einsatzbereichen nur äußerst selten verwendet. In DHCP-Netzen mit Bus-Struktur ist das nicht mehr so eindeutig.

3.1.5 Standortbestimmung

Im Gesetzentwurf auf Seite 56, zweiter Absatz heißt es:

Die Speicherpflicht steht auch in Einklang mit dem Unionsrecht, namentlich mit Artikel 15 Absatz 1 der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), wie sie im Lichte der Artikel 7, 8 und 11 sowie von Artikel 52 Absatz 1 der Charta der Grundrechte der Europäischen Union auszulegen ist. Die hier angeordnete Speicherung stellt keinen schwerwiegenden Eingriff in diese Rechte dar, da durch die Speichermodalitäten sichergestellt ist, dass ihre Aussagekraft allein auf die Identitätsauskunft des Anschlussinhabers zu einer bekannten IP-Adresse beschränkt ist; es ist ausgeschlossen, besuchte Internetseiten eines Anschlussinhabers nachzuverfolgen oder seine Kontakte oder Standorte herauszufinden (vergleiche zu den maßstäblichen Vorgaben des Europäischen Gerichtshofs, Urteil vom 30. April 2024, Rechtssache C-470/21, Quadrature du Net II – Hadopi, Randnummern 101 und 115).

Das ist falsch.

Ein Beispiel zur Erläuterung:

- Wenn man einen Internet-Zugriff mit Zeit und IP-Adresse hat, beispielsweise einen Zugriff auf eine Webseite, oder automatisierte *ständige, dauerhafte* Abfragen einer Mailbox vom Handy, und die Auskunft dazu lautet auf

Bruce Wayne
Dunkle Gasse 12
34567 Untergotham

dann weiß man, dass der zu diesem Zeitpunkt mit aller Wahrscheinlichkeit zuhause war, weil es eine Privatadresse ist.

- Kommt die automatisierte Abfrage *derselben* Mailboxadresse aber abends, gelegentlich von einer anderen IP-Adresse, die einer gewissen

Selina Kyle
Sündenpfuhl 3
34568 Obergotham

zugeordnet ist, weil die eine Fritzbox verwendet und ihrem Gast das Gastnetz angeboten hat, dann weiß man, wo und bei wem sich der Kerl nach Einbruch der Dunkelheit herumtreibt.

- Und lautet sie – *wie im Gesetzestext selbst angesprochen* – auf ein Hotel, dessen WLAN er nutzt, dann weiß man, dass er in diesem Hotel war. Wahrscheinlich sogar beide zusammen, wenn *ihr* Handy im selben Hotel das WLAN benutzt hat.
- Und wenn man sieht, wann er wieder von einer IP-Adresse zugreift, deren Anschlussinhaber er selbst ist, dann weiß man auch, wie lange es gedauert hat und wann er wieder zuhause war.

Viele Handy-Nutzer – besonders bei Prepaid-Tarifen – verwenden bevorzugt kostenlose WLAN-Angebote in Supermärkten, Verkehrsmitteln, an Flughäfen, an Stränden, in Restaurants.

Manche Läden, Kaufhäuser drängen ihre Kunden sogar dazu, das angebotene WLAN zu nutzen und bieten dafür Vorteile, weil man über die WLAN-Netze auswerten kann, wo sich Kunden aufhalten und schauen, oder woran sie achtlos vorbeigehen. Solche Methoden sorgen also für eine hohe Bereitschaft, sich im angebotenen kostenlosen WLAN einzuloggen.

Dazu kommt, dass viele Handys standardmäßig darauf eingestellt sind, bei guter WLAN-Verbindung Telefonate über WLAN statt über Mobilfunk/Roaming zu führen.

Handys halten in der Regel ständigen Kontakt zu bestimmten Serverdiensten wie beispielsweise

- E-Mail
- Social Media
- Cloud-Services
- HTTP Push-Diensten
- Office-Dienste

und halten dazu in der Regel stehende Verbindungen offen (IMAP, HTTP/2,...) oder

bauen ständig in kurzen Abständen Verbindungen auf.

Wenn also, wie vorgesehen, ein Serverdienst (Mailbox, Social Media,...) *bei jedem Zugriff die IP-Adresse aufzeichnen muss*, kann daraus eine dauerhafte Protokollierung, in welchem WLAN-Netzwerk sich jemand aufgehalten hat, werden, wenn sich das Gerät – naheliegend das Mobiltelefon – in diese WLAN-Netze einwählt.

Daraus kann ein Tatverdacht werden, oder ein Alibi platzen.

Die Darstellung, dass die Abfrage von IP-Adressen nicht ermögliche, Kontakte oder Standorte herauszufinden, ist falsch.

3.1.6 Internet nicht verstanden: Juristen halluzinieren

Auf Seite 56 finden sich in der Begründung zu § 177 Abs. 1 TKG folgende Absätze:

Absatz 1 regelt eine Verpflichtung zur Speicherung von IP-Adressen sowie ergänzender erforderlicher Daten, wie Portnummern und Zeitstempel an der Quelle einer Verbindung beim Anbieter eines Internetzugangsdienstes ausschließlich zum Zweck der Identifizierung des Anschlussinhabers und für einen begrenzten Zeitraum von drei Monaten. Die Regelung ist technologieoffen ausgestaltet, um den verschiedenen Verfahren bei der Vergabe von IP-Adressen Rechnung zu tragen.

Verpflichtet sind ausschließlich Anbieter von Internetzugangsdiensten (vergleiche § 3 Nummer 23). Gleiches gilt für Unternehmen beziehungsweise andere Netzbetreiber, denen sich ein Anbieter zur Erbringung seines Internetzugangsdienstes als sogenannter Vorleister bedient, der die Verkehrsdaten für diesen verarbeitet. Dabei hat der Anbieter des Internetzugangsdienstes auch die unverzügliche Sicherung der nicht von ihm selbst bei der Erbringung seines Dienstes erzeugten und verarbeiteten Daten sicherzustellen. Auf welche Weise der Erbringer die Sicherung sicherstellt, hat er gegenüber der Bundesnetzagentur auf deren Verlangen nachzuweisen.

Nicht verpflichtet zur vorsorglichen Speicherung sind daher etwa nummernunabhängige interpersonelle Telekommunikationsdienste (OTT-1-Dienste, etwa Messenger- und E-Mail-Dienste). Auch Bereitsteller von lokalen drahtlosen Netzwerken (wie etwa der Hotelbetreiber, der seinen Gästen WLAN zur Verfügung stellt, oder eine Initiative, die die vorübergehende Mitnutzung von privaten lokalen Netzwerken ermöglicht) gehören nicht zum Kreis der Verpflichteten. Denn gemäß Artikel 2 Absatz 2 Nummer 2 der Verordnung (EU) 2015/2120, auf die § 3 Nummer 23 Bezug nimmt, ist Internetzugangsdienst „ein öffentlich zugänglicher elektronischer Kommunikationsdienst, der unabhängig von der verwendeten Netztechnologie und den verwendeten Endgeräten Zugang zum Internet und somit Verbindungen zu praktisch allen Abschlusspunkten des Internets bietet“. Lokale drahtlose Netzwerke bieten aber selbst keinen Zugang „zum Internet und somit Verbindungen zu praktisch allen Abschlusspunkten des Internets“, sondern vermitteln – bildlich gesprochen – nur einen Weg dorthin. Sie sind nämlich ihrerseits auf eine Verbindung zu einem Internetzugangsdienst und dessen Telekommunikationsdienstleistung angewiesen. Erst dieser gewährt den eigentlichen „Zugang zum Internet“ (also zu Internet-Knoten oder den Netzen von anderen Internetdiensteanbietern). Entsprechend weisen die lokalen drahtlosen Netzwerke auch keine öffentlichen Internetprotokoll-Adresse zu, sondern allenfalls netzwerk-/routerinterne IP-Adressen. Ferner unterfallen auch Freifunkvereine nicht der Verpflichtung

nach Absatz 1, da sie weder dem Inhaber des Freifunkrouters noch dem Freifunknutzer eine Rufnummer oder Anschlusskennung, also keine öffentliche IP-Adresse an Anschlussinhaber vergeben. Aus Nutzersicht verhält sich die Erbringung des Dienstes wie eine Mitnutzung in einem Hotel, bei dem keine Registrierung erfolgt und eine IP-Adresse einem Endgerät zugewiesen wird. Der Dienst beruht dabei immer auf einem Internetzugangsdienst eines anderen Internetzugangsanbieters, der selbst nach Absatz 1 verpflichtet ist.

Nach derzeitigem Stand der Technik ist der Anbieter zur Beauskunftung immer dann in der Lage, wenn im Auskunftersuchen der Strafverfolgungsbehörde IP-Adresse, Portnummer und Zeitstempel zu einer Verbindung mitgeteilt sind. Nummer 1 verpflichtet zur Speicherung der öffentlichen IP-Adresse, Die Portnummer sowie gegebenenfalls weitere Verkehrsdaten nach Nummer 2 sind dabei regelmäßig nur dann zur Identifikation des Anschlussinhabers erforderlich, wenn mehreren Nutzern die gleiche öffentliche IP-Adresse in einem besonderen technischen Verfahren (Network Address Translation, NAT) zugewiesen wird. Häufig steht den Ermittlungsbehörden aber die Portnummer nicht zur Verfügung, sodass sie sich nur mit IP-Adresse und Zeitstempel an den Anbieter wenden. In diesem Fall ist der Anbieter trotz fehlender Portnummer zur Beauskunftung verpflichtet, sofern dies technisch möglich ist. Eine eindeutige Zuordnung zu einem Anschluss kann in diesem Fall etwa dann möglich sein, wenn der Anbieter dem Anschlussinhaber bei der zugrunde liegenden Verbindung eine IP-Adresse exklusiv zugewiesen hat, ohne dass also eine Unterscheidung anhand einer Portnummer nötig ist. Vergleiche dazu auch die Begründung zur Änderung der Strafprozessordnung unter Nummer 3, zu § 100j Absatz 2.

Das ist reiner Blödsinn und fachlich falsch. Der Verfasser hat nicht verstanden, wie das Internet funktioniert.

1. Selbstverständlich bietet auch ein Hotelbetreiber u.ä., der seinen Gästen WLAN anbietet, *Zugang „zum Internet und somit Verbindungen zu praktisch allen Abschlusspunkten des Internets“*. Denn man kann ja auch aus dem Hotelzimmer „praktisch alle Abschlusspunkte des Internets“ erreichen.

Die Formulierung ist bereits abwegig.

2. Es gibt keine Internetzugangsanbieter, die selbst „praktisch alle Abschlusspunkte des Internets“ erreichen. Jeder Anbieter, selbst die, die sogenannte „autonomous systems“ und backbones betreiben, peeren mit anderen Providern, in Deutschland etwa mit dem DE-CIX.
3. Das ganze Internet beruht („Routing“) nur darauf, dass einer dem anderen einen „Weg dorthin“ anbietet.

Es gibt keine „Internet-Knoten“ und keinen „eigentlichen Zugang zum Internet“. Entweder man hat ein Routing und erreicht das große, allgemein geroutete Internet – oder eben nicht. Es gibt keine Unterscheidung in echt und unecht.

4. Auch die Unterscheidung nach „öffentlichen“ und „netzwerk/routerinternen IP-Adressen“ taugt nicht und stimmt so nicht.

Der Verfasser meint **RFC 1918**-Adressen, die so aber nur bei IPv4 vorkommen. Darum geht es ja gerade bei NAT – den Zusammenhang hat der Verfasser anscheinend auch nicht verstanden.

Bei IPv6 bekommt man auch per Wifi und sogar im Hotelzimmer eine öffentliche IP-Adresse, weil bei IPv6 keine Knappheit besteht und Rechner *mehrere* Adressen haben oder bekommen, nämlich mindestens link local, ggf. früher site-local, inzwischen unique-local, und global unicast, **also öffentlich**¹.

Auch unter IPv4 kann man sehr wohl öffentliche IP-Adressen per Wifi zuweisen – man macht es nur in der Praxis nicht, weil sie sehr knapp sind und man Firewalls dazwischenschaltet. **Es geht aber. Wifi, Funknetze haben technisch überhaupt nichts damit zu tun, ob die per DHCP, statisch oder – bei IPv6 – Router Advertisement zugewiesene Adresse öffentlich oder intern ist.**

Juristen halluzinieren gerne durch sperrige Begriffswahlen fiktive Differenzierungen, die es in der Realität nicht gibt.

Hier ist deutlich zu merken, dass sich ein Jurist, der die Funktionsweise nicht verstanden hat, eine Begründung aus den Fingern gesaugt hat, um zu erklären, warum die großen, „richtigen“ Internet-Provider verpflichtet seien, während die kleinen Anbieter, wie Hotels, Hobbyisten usw. nicht unter die Verpflichtung fallen sollen.

Die Unterscheidung ist aber nicht nur technisch unsinnig, sie ist auch technisch falsch. Es gibt technisch keine Unterscheidung zwischen einem „richtigen“ Internet-Anbieter, der einen mit der ganze Welt verbindet, und einem „Privatanbieter“, der einen nur zu einem „richtigen“ Internetanbieter durchreicht. Das ist eine Phantasie von Juristen, die versuchen, einen – juristisch benötigten, aber real nicht existierenden – Unterschied herbeizureden.

Das gesamte Internet – deshalb heißt es übrigens *Internet*, genau deshalb hat man es so genannt – ist nichts anderes als das Prinzip, dass sich verschiedene Netze miteinander verbinden und auf Gegenseitigkeit Pakete weiterreichen – „routen“.

Deshalb gibt es auch kein physisches Internet, in dem man „drin“ sein kann wie Boris Bocker in der AOL-Werbung von 1999. Das Internet als solches existiert nicht physisch. Das Internet ist nichts anderes als eine weltweite Kooperation von Netzwerkbetreibern unterschiedlicher Art, die sich zum Zusammenschluss auf eine einheitliche Sprache und Adressierungsart geeinigt haben. Und dabei macht es keinen² technischen Unterschied, ob man die Telekom oder ein kleines Hotel ist. Das technische Prinzip bleibt dasselbe. Gerade in dieser Vereinheitlichung liegt ja die Stärke des Internet.

Wenn man solche Fehler in ein Gesetz schreibt, dann ist der nächste Hotelanbieter, das nächste Restaurant, der nächste Stadtbuss, der nächste Flughafen plötzlich vorratsdatenverpflichtet, wenn er IPv6 anbietet und ir-

¹ Auf Multicast wird hier zugunsten der Verständlichkeit nicht näher eingegangen.

² Keinen für dieses Gesetz relevanten Unterschied. Ein technisch wesentlicher Unterschied liegt in der Frage, ob jemand groß genug ist, eigene Fernverbindungskabel und ein „Autonomes System“ zu betreiben, mit anderen, mehreren Providern zu peeren und am BGP teilzunehmen, vgl. Abschnitt 5.2.

gendeine Aufsichtsbehörde oder irgendein Richter das herausfindet. Dann schreibt man etwas in ein Gesetz, was man selbst nicht wollte, weil man es nicht versteht.

Außerdem ist es **selbstwidersprüchlich und verletzt die Normenklarheit**. Denn warum sollte ein Hotelier oder Gastwirt von der Speicherpflicht befreit sein, wenn er seinen Kunden Wifi anbietet, aber keine offizielle IPv4-Adresse zuweist, während man bei einem Internet-Provider mit CGNAT, der seinen Kunden ebenfalls keine offizielle IPv4-Adresse zuweist, also genau dasselbe tut, nicht nur die Speicherung der Adressen, sondern sogar der Portnummern verlangt?

Wo ist die legal greifbare Grenze dazwischen? Was ist das Kriterium, ob die Pflicht besteht oder nicht? Die Formulierung aus dem Entwurf

Der Dienst beruht dabei immer auf einem Internetzugangsdienst eines anderen Internetzugangsanbieters, der selbst nach Absatz 1 verpflichtet ist.

taugt nicht zur Differenzierung. **Es bleibt deshalb unklar, für den die Verpflichtung gilt.** Die Regierung hat nicht verstanden, wie das Internet funktioniert.

Warum sollte jemand, der IPv6 anbietet, rechtlich, wie es die Begründung tut, anders zu beurteilen sein als jemand, der nur IPv4 anbietet? Was ist mit Wifi-Großanbietern, wie

- Flughäfen
- Verkehrsbetrieben, Deutsche Bahn
- Universitäten

die bis zu Millionen Nutzern Wifi anbieten?

Der Flughafen Frankfurt/Main hatte 2025 63,2 Millionen Fluggäste und bot jedem davon Internet zumindest an. Der BER kommt auf 26 Millionen. Die deutsche Telekom hat 75 Millionen Mobilfunkkunden in Deutschland, während der Internet-Provider DNS:NET 150.000 Haushalte als Kunden angibt. Quantitative Überlegungen funktionieren als Kriterium also auch nicht.

Warum aber soll nach Vorstellung des Verfassers die Telekom und DNS:NET verpflichtet sein, die Flughäfen FRA und BER aber nicht? Wo ist das juristisch greifbare Unterscheidungskriterium?

3.1.7 „Verkehrsdaten“ im Sinne des § 3 Nr. 70 TKG

Der Gesetztestext verwendet den Begriff der „Verkehrsdaten“ und bezieht sich, etwa in § 100g Abs. 1 StPO, dabei auf § 3 Nr. 70 TKG.

Unklar bleibt für mich dabei, ob die Formulierung *„Verkehrsdaten gemäß § 3 Nummer*

70 des Telekommunikationsgesetzes“ heißen soll, dass der Begriff in § 3 Nr. 70 TKG definiert wird, oder ob er hier weiter gefasst ist und nur in § 100g Abs. 1 StPO auf die in § 3 Nr. 70 TKG genannten eingeschränkt wird.

§ 3 Nr. 70 TKG hält „Verkehrsdaten“ für

„Verkehrsdaten“ Daten, deren Erhebung, Verarbeitung oder Nutzung bei der Erbringung eines Telekommunikationsdienstes erforderlich sind;

Demnach sind CGNAT-Portnummern nicht ohne weiteres „Verkehrsdaten“, weil deren Erhebung, Verarbeitung, Nutzung, überhaupt deren Existenz nicht „erforderlich“ ist. Viele Anbieter verwenden kein CGNAT, und diese Praxis wurde erst vor etwa 15 Jahren eingeführt. Es geht also auch ohne. „Erforderlich“ sind sie eben nicht.

Der Grund dafür ist, dass

- bei der Einführung von CGNAT IPv4-Adressen knapp und teuer waren, es zunächst darum ging, Geld zu sparen,
- das ursprünglich als „Dual-Stack Lite“ ([RFC 6333](#)) einzuführen, als man noch davon ausging, dass man das gesamte Internet zeitnah auf IPv6 umstellen werde und könne und IPv4 nur noch als eine Art eingeschränkten Dienst zur Angebot von Rückwärtskompatibilität benötige.

Erst seit wenigen Jahren ist der Vorrat an IPv4-Adressen bei der IANA und den RIRs erschöpft, besteht eine tatsächliche Knappheit an öffentlich noch verfügbaren IP-Adressen.

Das bedeutet aber nicht, dass die bereits allocierten IP-Adressen auch bei den Providern (ISPs) knapp sind.

Wenn man Verkehrsdaten schon im Rechtssinne an „erforderlich“ knüpft, ist der Gedanke nahe, dass Port-Nummern vom Gesetz nicht erfasst werden, weil deren Erhebung und Verarbeitung zumindest nicht „erforderlich“ sind, und sie damit keine „Verkehrsdaten“ sind.

Das ist alles windschief, da passt nichts zusammen.

3.2 Im Zusammenhang mit dem Gesetzentwurf

3.2.1 „KFZ-Kennzeichen“

In der Sendung [IP-Adressenspeicherung: Internet "darf kein Täterparadies sein" bei Phoenix vom 22.4.2026](#) erklärte die Ministerin Hubig (ab 0:02:50)

„Als Beispiel: Stellen Sie sich vor, Sie haben KFZ-Kennzeichen. Für die würde Ähnliches

gelten wie für die IP-Adressen: Jeden Tag werden diese Autokennzeichen neu vergeben, und am Abend würden die Informationen dann gelöscht werden, wer mit diesem Auto unterwegs war und welches Auto welches Kennzeichen hatte. Ich glaube, in einer solchen Welt würden wir niemandem raten, am Straßenverkehr teilzunehmen. Unser Ziel ist es, dass Deutschland sicher wird.“

Wortgleich auch im **Plenarprotokoll 21/85**, Seite 10361:

Man stelle sich vor, für Kfz-Kennzeichen würde Ähnliches gelten wie für IP-Adressen. Was hieße das? Das hieße: Alle Autokennzeichen würden jeden Morgen neu vergeben, und am Abend würden sie alle gelöscht. Ich glaube, in einer solchen Welt würde man niemandem raten, am Straßenverkehr teilzunehmen.

(Beifall bei der SPD sowie bei Abgeordneten der CDU/CSU – Dr. Günter Krings [CDU/CSU]: Sehr richtig!)

Unser Ziel ist, dass Deutschland auch im digitalen Raum sicher ist.

Das ist sehr falsch.

Das KFZ-Kennzeichen am Auto hat keinerlei technische Funktion. Ein Auto ohne Kennzeichen fährt exakt genauso, wie mit Kennzeichen. Es bleibt nicht stehen, wenn das Kennzeichen abfällt, oder nicht stimmt. Oder wenn die TÜV-Plakette abläuft. Es fährt genauso weiter. Auch Autos mit gefälschten oder geklauten Kennzeichen fahren genauso gut wie andere. Dem Auto ist das Kennzeichen egal.

Dafür aber beruht das KFZ-Kennzeichen auf einem formalrechtlichen Zulassungsprozess, der an eine natürliche oder juristische Person gebunden ist. Das Kennzeichen dient diesem Zweck.

Im Internet ist es andersherum. Das Internet und das Internet-Protokoll kennen keine Zulassung und keine – natürlichen oder juristischen – Personen.

IP-Adressen haben im Wesentlichen die Funktion eines **Wegweisers oder einer Postleitzahl**, mittels derer Router entscheiden können, auf welchem Weg das Datenpaket weitergeleitet werden muss.

IP-Adressen sind dazu gemacht, den Weg zum Ziel zu weisen, und nicht, das Ziel oder dessen Inhaber zu identifizieren.

Wenn man also schon die untaugliche Analogie zum Autoverkehr wählen will, *dann müsste man sich vorstellen, dass wir alle paar Stunden das Autobahn- und Straßennetz ändern und Wohnhäuser verschieben, und deshalb ständig neue Wegweiser aufgestellt und wieder abgerissen werden.*

Wie entstehen solche Fehler?

Ursache ist die mangelhafte, geisteswissenschaftlich ausgerichtete Arbeitsweise der Juristen, die nicht nach richtig und falsch unterscheiden, sondern nur die „vertretbare Meinung“ kennen und solche erzeugen, indem sie sich einfach einer Meinung anschließen. Da meint einer etwas einfach so ins Blaue, und andere, denen die Meinung

gefällt, schließen sich ihr an.

So schreibt der EuGH im Fall **Joined Cases C-511/18, C-512/18 and C-520/18**, *La Quadrature du Net and Others v Premier ministre and Others*, unter Randnummer 152:

It should be noted that although IP addresses are part of traffic data, they are generated independently of any particular communication and mainly serve to identify, through providers of electronic communications services, the natural person who owns the terminal equipment from which an Internet communication is made.

Das ist so höchsttrichterlich wie falsch. Aber wenn es vom EuGH kommt, schließen sich Juristen dem rudelweise an. Nichts könnte dumm oder falsch genug sein, als dass sich nicht Juristen dieser Meinung anschließen – besonders gerne im Namen des Volkes, auf Kosten anderer oder mit Unterschrift des Bundespräsidenten und Verkündung im Bundesgesetzblatt. Und ist es erst einmal beschlossen und verkündet, dann ist es für Juristen auch gültig.

Wir leiden unter einer massiven Verzerrung der Realität, die verbogen wird, um in die Weltsicht der Juristen zu passen. Die Jurisprudenz wird zum Standortnachteil.

Man möchte der Ministerin zurufen, dass die Regierung kein Laienparadies sein darf.

3.2.2 „Digitale Gewalt“

Regierung und Parteien verwenden gerne den Begriff der „Digitalen Gewalt“ als rabulistische Keule und brachiale Wortwahl.

Das ist falsch.

- „digital“ ist ein Begriff der Informationsdarstellung.
- „Gewalt“ ist ein Begriff der Kraft- und Energieübertragung.

Beide sind disjunkt. Es kann deshalb keine „digitale Gewalt“ geben, das schließt sich gegenseitig aus.

3.2.3 „IP-Adressen identifizieren Geräte“

Der Präsident des Bundeskriminalamtes, Holger Münch, meint:

„Die IP-Adresse ist häufig der einzige Weg festzustellen, von welchem Gerät eine Straftat begangen wurde.“

Das ist so nicht richtig.

Innerhalb eines LANs mit Zugriff auf die Schichten 1 und 2 und deren MAC-Adressen kann – allerdings auch nicht zuverlässig und leicht zu fälschen – das Gerät festgestellt werden, aber – insbesondere unter IPv4 – von außen ist eine Zuordnung nicht möglich.

Unter IPv6 gibt es verschiedene Methoden der Adresszuordnung, darunter die Methode, zu einem publizierten /64-Prefix den unteren Teil aus der MAC-Adressen zu erzeugen. Damit wäre dann tatsächlich das einzelne Gerät identifizierbar – allerdings unzuverlässig und leicht fälschbar, denn das Verfahren ist nicht auf Sicherheit (security), sondern auf Sicherheit (safety) ausgelegt, um zufällige Gleichheiten (vgl. Geburtstagsparadoxon) zu vermeiden, nicht aber, um Angriffe zu verhindern.

In der Regel wird aber genau deshalb aus Datenschutzgegründen der untere Teil der IPv6-Adresse per DHCPv6 zugewiesen oder zufällig gewählt.

Damit ist schon die Ansicht, dass eine IP-Adresse ein Gerät identifiziere, im Allgemeinen nicht richtig und in der Praxis nur für Servernetze und statische Adressvergaben ohne NAT oder mit statischem NAT und ohne Lastverteiler, Hot Standby usw. ohne weiteres gültig.

Auf der Clientseite ist dies in der Regel nicht zutreffend, weil Clients oft hinter NAT betrieben werden.

Noch viel weniger ist aber die Aussage haltbar, dass anhand der IP-Adresse festzustellen wäre, *von welchem Gerät eine Straftat begangen wurde*. Denn es ist anhand der IP-Adresse nicht erkennbar, ob das Datenpaket auch tatsächlich aus dem Anwendungsbereich dieser Maschine kam. Nur weil ein Datenpaket von einer IP-Adresse kommt, heißt das noch lange nicht, dass es auch von dem Anschluss kam, dem diese IP-Adresse zugeordnet wurde.

Zwischen den beiden Seiten einer Kommunikationsverbindung über das allgemeine Internet – und nur um die geht es hier – liegen oft 10, 20, manchmal mehr Router, über die man überhaupt nichts sagen kann, von denen man nicht weiß, was auf ihnen passiert ist – und von denen man schon Stunden später nicht mehr sagen kann, welche Route überhaupt einschlägig war.

Beispiel: Während ich diesen Text hier schreibe, liegen zwischen dem Rechner, auf dem ich ihn schreibe, und www.bundestag.de, wo die Webseite dieser Sitzung liegt, **insgesamt 15 Hops**. Die Datenpakete werden also von meinem Rechner, der vor mir auf dem Tisch steht, 14 Mal von anderen Rechnern weitergeleitet, bis sie endlich beim Webserver des Bundestags ankommen.

Woher wollen Sie wissen, ob die Routenangabe überhaupt stimmt, und die Daten nicht gefälscht sind, was leicht möglich wäre?

Und woher wollen Sie wissen, ob alle diese Rechner einwandfrei funktionieren und integer arbeiten?

4 Grundlagenwissen Netzwerke (Internet)

4.1 Konkurrenz von TCP/IP (Internet) und ISO/OSI

Zum Verständnis der nachfolgenden Darstellungen und des Schichtenmodells muss man wissen, dass es nicht nur das „Internet“ gab, sondern ursprünglich zwei Ansätze konkurriert haben:

„Internet“ (amerikanisch) Das Internet-Protokoll wurde ursprünglich zwischen 1973 und 1974 in den USA als monolithisches „TCP“ (Transmission Control Protocol) entwickelt, 1978 aber in die beiden getrennten Protokolle TCP und IP aufgespalten, 1981 standardisiert, und 1983 durch Umstellung des monolithisch-flachen Forschungsnetzwerks ARPANET¹ mit NCP auf TCP/IP offiziell eingeführt, womit das Internet als Verbindung verschiedenartiger Netzwerke „erfunden“ wurde (RFC 791 und RFC 793).

ISO/OSI (international) Seit 1977 wurde ein konkurrierendes, internationales Referenzmodell namens Open Systems Interconnection Model = OSI entwickelt und zunächst von der CCITT (später ITU) ab 1983 und dann von der International Organization for Standardization ISO ab 1984 veröffentlicht und seither ISO/OSI genannt.

Während NCP, TCP und TCP/IP pionierhaft, hemdsärmelig, pragmatisch und zunächst strukturlos monolithisch entwickelt und erst später in TCP und IP aufgetrennt und unter Unix als „Stack“ implementiert wurden, also zunächst schlecht und dann zunehmend besser organisiert waren, war es bei ISO/OSI umgekehrt: Dieses Modell war von Anfang an sehr sauber und systematisch durchstrukturiert und umfasste ein komplettes System samt Anwendungsprogrammen und Datenstrukturen.

ISO/OSI war technisch theoretisch überlegen, aber TCP/IP hat sich in gleicher Weise durchgesetzt, wie die VHS-Videokassette gegen die technisch deutlich überlegenen Systeme Video 2000 und Betamax, *einfach weil es früher da und verfügbar war*.

Während TCP/IP einfach konstruiert war, war ISO/OSI so überkomplex und durchreglementiert, dass man viele Teile niemals implementieren konnte.

Völlig tot ist ISO/OSI trotzdem nicht, denn einzelne Elemente haben überlebt:

- Das Mailsystem X.400 wurde lange Zeit in Behörden genutzt.

¹ ARPANET = Advanced Research Projects Agency Network

- Das Übertragungsprotokoll des ISO/OSI Directorydienstes X.500 lebt heute als „LDAP“ weiter.
- Das Dateiformat für Zertifikate X.509 wird heute noch genutzt und verwendet immer noch das Adressierungsschema von X.500.
- Das Codierungssysteme ASN.1 wird für wenige Anwendungen wie X.509, LDAP, SNMP noch verwendet, aber auch im im vorliegenden Gesetzestext erwähnten Protokoll ETSI TS 102 657.
- Das ISO/OSI-Schichtenmodell ist heute Standard.

4.2 Das ISO-OSI-Schichtenmodell

Es ist zum Verständnis des Fernmeldegeheimnisses und der Funktion von Internet-Providern dringend erforderlich, das ISO-OSI-Schichtenmodell zu verstehen (Tabelle 4.1).

Abbildung 4.1: Das ISO/OSI-Schichtenmodell

Schicht	Deutsch	Englisch	Beispiel	Fernmeldegeheimnis
7	Anwendung	Application	Webseite Bundestag	Nutzlast, voll geschützt
6	Darstellung	Presentation	HTML	
5	Sitzung	Session	HTTP	
4	Transport	Transport	TCP	
3	Vermittlung Paket	Network	Internet, IP	Voll geschützt, aber für Provider zur Dienstleistung zugänglich
2	Sicherung	Data Link	PPP+DSL	
1	Bitübertragung	Physical	DSL	

Jede Schicht ist dabei die Nutzlast der jeweils darunterliegenden Schicht.

Das Internet-Protokoll, das „Internet“, findet dabei ausschließlich auf Schicht 3 statt. Internet-Provider haben deshalb grundsätzlich nur auf Schicht 3, und wenn sie Anschlussanbieter sind, auch auf die Schichten 1 und 2 Zugang.

Die Schichten 4 aufwärts sind für sie tabu. Betreiben sie aber CGNAT, müssen sie auf die Portnummern und damit Schicht 4 zugreifen, was eigentlich eine Verletzung des Fernmeldegeheimnisses darstellt, aber vertretbar ist, weil durch IPv4-Adressknappheit

geboten und nur innerhalb des Routers technisch verarbeitet.

Weil das Internet-Protokoll nicht anhand des ISO-OSI-Schichtenmodells entworfen wurde, gibt es unterschiedliche Auffassungen bezüglich der Schichten 5 bis 7: Manche meinen, die Schichten 5 bis 7 könnten bei Internet-Diensten nicht differenziert werden und seien generell der Applikationsschicht zuzuordnen, weil das Betriebssystem nur die Schichten bis 4 abdeckt.

Ich bin der Auffassung, dass auch die Schichten 5 bis 7 im Einzelnen insbesondere zu Lehr- und Verständniszwecken unterschieden werden können.

4.3 Verbindungs- und Paketorientierte Schichten

Für den Laien verwirrend, aber überaus leistungsfähig ist der Umstand, dass einzelne Schichten sich darin unterscheiden können, ob sie *verbindungs-* oder *paketorientiert* sind:

- Schicht 3 ist beim Internet **immer paketorientiert**.
- Schicht 4 kann ebenfalls paketorientiert sein (UDP) oder aus einzelnen Paketen wieder eine stromorientierte Verbindung aufbauen (TCP) und für höheren Schichten eine Verbindung simulieren, also eine verbindungsorientierte Kommunikation transportieren.
- Schichten 1 und 2 können ebenfalls verbindungs- oder paketorientiert sein.

Beispielsweise sind Modem-, ISDN- und DSL-Verbindungen verbindungsorientiert, während Wifi, Ethernet, X.25 und Docsis paketorientiert sind.

Stellen Sie sich das Internet wie die Post vor, die Briefe transportiert, ohne sich für deren Inhalt zu interessieren.

Senden Sie aber Briefe beispielsweise an ein Gericht in einem Rechtsstreit, dann ist die Portnummer² so etwas wie das Aktenzeichen und die TCP-Sequence-Number so etwas wie ein Briefdatum.

Die Geschäftsstelle eines Gerichts vermag anhand von Aktenzeichen und Datum die Schriftsätze zu einer zusammenhängenden, geordneten Akte zusammenzufügen. Die Gerichte erkennen am Aktenzeichen, welche Kammer/Senat angesprochen wurde, um um welchen Einzelfall es geht.

Briefkopfangaben wie „Ihr Schreiben vom ...“ sorgen dafür, dass es auffällt, wenn Schreiben fehlen.

In sehr ähnlicher Weise setzt das TCP die Datenstückchen, die über das paketorien-

²Genauer gesagt, die Verbindung aus beiden IP-Adressen und beiden Portnummern beider Seiten

tierte Internet übertragen werden, in der richtigen Reihenfolge zu einem quasi verbindungsorientierten, bidirektionalen Datenstrom zusammen, so wie die Geschäftsstelle des Gerichts aus Schriftsätzen eine konsistente Akte fügt.

TCP sorgt außerdem dafür

- dass Pakete, die in der falschen Reihenfolge ankommen, in die richtige Reihenfolge gebracht werden,
- dass Pakete, die mehrfach ankommen, entsprechend verworfen werden und nicht zu einer Wiederholung der Daten führen,
- fehlende Pakete erkannt und deren wiederholte Sendung angefordert wird, und der Absender die Pakete auch wiederholt senden kann,
- es erkannt wird, wenn sich eine Seite nicht mehr meldet, und die Verbindung dann innerhalb gewisser Zeit abgebrochen wird.

Portnummer zu protokollieren ist, als verlange man von der Post, alle Briefe zu öffnen und die Aktenzeichen der Schreiben zu notieren.

5 Zeitunabhängige Fehlerquellen

5.1 Grundproblem

Im gesamten Gesetzentwurf wird durchgehend, aber stillschweigend unterstellt, dass das Internet und das Heimnetzwerk, der Router, die Computer völlig zuverlässig und präzise arbeitende Maschine seien, an die man nur eine Protokollierung anklemmen müsse, um festzustellen, wer wo welche Handlung vorgenommen habe.

Die Regierungs- und Juristen-Logik ist: Das Internet ist zuverlässig, also muss es auch zuverlässig sein, irgendwo irgendwie irgendetwas mitzuprotokollieren. 2023 musste man dazu einfach nur oft genug „rechtssicher“ sagen, jetzt muss man oft genug „zuverlässig“ sagen.

Diese Auffassung ist nicht haltbar. Eine Begründung, eine Grundlage dafür findet sich im Entwurf auch nicht. Es wird einfach stillschweigend unterstellt.

Das gesamte Internet ist nicht nur tatsächlich unzuverlässig – es ist sogar dessen Konstruktionsmerkmal, **fehlertolerant** zu sein. Es ist ein wesentlicher Zweck, eine Aufgabe sowohl des Routings, als auch des TCP, Fehler des Internet auszugleichen.

Nehmen Sie bitte zur Kenntnis, dass Disziplinen wie Fehlererkennung, Fehlerkorrektur, Fehlertoleranz, Fehlerhaftigkeit von Kanälen, seit der Frühzeit der modernen Informatik, seit **A Mathematical Theory of Communication von Claude Shannon, 1948**, elementar und konstituierender Bestandteil der Informationstheorie und der Codierungstechnik ist. Anders könnten wir Dinge wie Internet, Mobilfunk, Digitalfernsehen gar nicht bauen.

Das kennen Sie nicht.

Weder in der Jurisprudenz, noch in der Politik kommen in nennenswertem Umfang Fehlererkennung, Fehlerkorrektur, Fehlertoleranz vor.

Die Jurisprudenz geht über so etwas einfach mit einer Beweislastumkehr hinweg. Die Politik verwendet den Öffentlich-Rechtlichen Rundfunk, um Fehler als Fake News und Hate Speech hinzustellen.

In der Informatik, die das Internet gebaut hat, in der IT, geht niemand mit Sachkunde von der Zuverlässigkeit des Internet aus. Im Gegenteil geht es ständig darum, mit dessen systematischer Unzuverlässigkeit umzugehen.

Ursprünglich wurde das Internet mit dem Hintergedanken entworfen, auch im Kriegsfall nach Feindeinwirkung noch möglichst gut zu funktionieren. Es war nie Konstruktionsmerkmal, fehlerfrei, zuverlässig oder sicher zu sein, sondern Fehler und Unzuverlässigkeit aushalten zu können. Seit Aufkommen des Internet, seit 40 Jahren, haben wir ständig und unablässig mit Störungen, Fehler, Angriffe zu tun.

Und nun kommen Politiker und Juristen daher, haben kaum etwas vom Internet verstanden, wissen eigentlich nichts, und unterstellen einfach so, dass das jetzt zuverlässig sei, damit sie möglichst einfach Gesetze schreiben und politische Wünsche durchsetzen können.

Und damit sollen dann Menschen verurteilt werden.

Was glauben Sie eigentlich, warum wir so großen Aufwand in Authentifikation und Verschlüsselung stecken, HTTPS/TLS und so weiter einsetzen, PKI-Infrastrukturen bauen, wenn das Internet und seine IP-Adressen doch „zuverlässig“ seien?

5.2 Routenverteilung – BGP

Wie schon in der Stellungnahme vom 9. Oktober 2023 angesprochen, können im Internet ganze Netzwerkbereiche zumindest für kurze Zeit übernommen werden. Grund ist das **Border Gateway Protocol (BGP)**, mit denen die Routen zwischen den großen Internet-Anbietern, die mit anderen direkt oder an Internet Exchanges „peeren“, und die „Autonome Systeme“ betreiben, das Internet zu weltweiten Routen zusammenfließen.

Dieses Verfahren ist hochdynamisch, weil sich diese Routen ständig ändern können und etwa bei Systemausfällen – Bagger reißt Kabel ab, Gebäude stürzt ein, Provider geht pleite, Stromausfall in Berlin – sofort Routing-Änderungen erforderlich sind und durchgeführt werden.

Wie oben in Abschnitt 2.1 schon dargelegt wurde, sorgt und kümmert sich die US-Regierung – im Gegensatz zur deutschen – inzwischen um die Schwächen des BGP.

Bislang ist BGP vor allem durch versehentliche Fehlkonfigurationen aufgefallen, die aber beweisen, dass man diese Fehler auch absichtlich hervorrufen könnte. Aus dem **Wikipedia-Artikel**:

YouTube-Blockade

Im Februar 2008 wurde Pakistan Telecom durch einen Gerichtsbeschluss dazu gezwungen, YouTube-Verkehr in Pakistan zu blockieren. Technisch wurde dies umgesetzt, indem eine falsche Route zum Netzwerk von YouTube in IBGP eingespeist wurde. Durch einen Konfigurationsfehler wurde diese falsche Route jedoch nicht nur in Pakistan verwendet, sondern irrtümlich auch via EBGp an andere Internetanbieter verteilt, was insbesondere in Asien zu mehrstündigen Blockaden von YouTube führte.

Revolution in Ägypten 2011

Während der Revolution in Ägypten wurden im Januar 2011 via BGP in wenigen Minuten ca. 3.500 Routen aller ägyptischer Internetanbieter zurückgezogen, wodurch fast ganz Ägypten vom Internet getrennt war. Auch Mobilfunkdienste und soziale Netze waren nicht mehr erreichbar. Dieses scheint der erste Fall in der Geschichte des Internets zu sein, in welchem aus politischen Gründen ein gesamtes Land vom Internet abgeschottet wurde.

Facebook, Instagram und Whatsapp

Am 4. Oktober 2021 waren für ca. 6 Stunden weltweit alle Dienste von Facebook, Instagram und Whatsapp nicht erreichbar. Dies ging auf eine fehlerhafte Konfiguration von Facebooks selbst gehosteten BGP-Routern zurück.

Alle diese Konfigurationsfehler lassen sich auch für absichtliche Angriffe ausnutzen.

BGP umfasst derzeit rund eine Million IPv4- und etwa 320.000 IPv6-Präfixe. Es fällt nicht auf, wenn da welche nicht stimmen, weil darunter immer welche sind, die nicht stimmen.

5.3 Unsicherheit von Routern

Es ist lange bekannt, dass viele der großen Router im Internet notorisch angreifbar sind. Besonders Cisco ist nicht nur bei der Zahl dieser Router, sondern auch deren Sicherheitslücken führend.

CISA: *APT28 Exploits Known Vulnerability to Carry Out Reconnaissance and Deploy Malware on Cisco Routers*

BSI: *Cisco Produkte durch mehrere Schwachstellen angreifbar*

BSI: *Cisco: Firewalls mit persistenter Malware infiziert*

Heise: *Sicherheitsupdates: Angreifer können Cisco-Router lahmlegen*

Heise: *Cisco: Tausende Firewalls verwundbar, neue Angriffswege beobachtet*

IT Daily: *Ungepatcht & verwundbar – Hacker kapern Cisco-Router* Eine chinesische Hackergruppe namens Salt Typhoon (auch bekannt als RedMike) greift gezielt Telekommunikationsunternehmen weltweit an. Wie Sicherheitsforscher der Insikt Group von Recorded Future berichten, nutzen die Angreifer ungepatchte Sicherheitslücken in Cisco IOS XE-Netzwerkgeräten aus. [...] Die Hacker verschaffen sich über kompromittierte Cisco-Geräte Zugang zu den Netzwerken der Opfer. Diese Geräte wurden umkonfiguriert und kommunizieren über sogenannte GRE-Tunnel (Generic Routing Encapsulation) mit Servern, die von Salt Typhoon kontrolliert werden. Ziel ist es, einen dauerhaften Zugriff auf die Netzwerke zu erhalten. [...] Ein Internet-Scan der Sicherheitsforscher ergab, dass mehr als 12.000 Cisco-Netzwerkgeräte ungeschützt mit dem Internet verbunden sind und somit potenzielle Angriffsziele darstellen.

Heise: IT-Sicherheitslösung Check Point Security Gateway ist verwundbar

Sentiguard: Schwachstellen Scanner findet verwundbare Fortinet Firewalls Nach einer Hochrechnung von Shadowserver sind derzeit weltweit 136.000 Server im Umlauf, die für die Schwachstelle verwundbar sind. Ein Proof of Concept für einen Exploit wurde ebenfalls bereits auf Github veröffentlicht. Es ist also höchste Zeit für Betreiber zu patchen.

Sievers: Kritische Sicherheitslücke in WatchGuard Firewalls: Jetzt handeln! Die Schwachstelle betrifft den iked-Prozess des Firewall-Betriebssystems und ermöglicht es einem nicht authentifizierten Angreifer, beliebigen Code auszuführen.

Firewalls24: Betroffene Sophos Produkte & CVEs im Überblick Sophos hat neue Sicherheitslücken in allen XGS Firewalls und virtuellen Firewalls mit SFOS sowie in der Sophos Endpoint und Server Protection geschlossen. Die Schwachstellen reichen von kritischen Remote-Code-Execution-Lücken (RCE) bis zu lokalen Privilegieneskalationen.

Die Infrastruktur des Internets ist löchriger als ein Schweizer Käse. Sie beruht vornehmlich auf Cisco-Routern, die schon immer als mangelhaft und oft schlecht konfiguriert bekannt waren.

Das eröffnet Angriffsmöglichkeiten, die auch das Fälschen von IP-Adressen umfassen.

Schon vor 26 Jahren habe ich – allerdings befugt und mit administrativem Zugriff – GRE-Tunnel auf Cisco-Routern eingesetzt, um IP-Adressen zu fälschen. Die Versandabteilung des Unternehmens hatte versehentlich eine Reihe von Firewalls mit falsch konfigurierten IP-Adressen an Kunden verschickt, die damit nicht erreichbar waren. Weil wir auch die Cisco-Router bei den Kunden gestellt haben, habe ich auf den Cisco-Routern GRE-Tunnel konfiguriert, um mir die fremden IP-Adressen *lokal* kurzzeitig durch Routing anzueignen, die Firewall-Maschinen unter ihrer falschen IP-Adresse anzusprechen und dann richtig zu konfigurieren, um teure und langwierige Auslandsreisen zu vermeiden.

Es ist für IT-Fachkräfte mit Sachkunde im Routing nicht mehr als eine Fingerübung, über einen Router auf der Strecke einzelne IP-Adressen umzurouten und sich Zugang zu fremden Adressen zu verschaffen. Heutzutage müssen Sie es nicht einmal mehr wissen und können – die KI sagt Ihnen auf Nachfrage, wie man das macht.

Jeder Hacker, der Sicherheitslücken wie die oben genannten ausnutzt und sich Zugang zu Routern verschafft, kann in derselben Weise Router umkonfigurieren und dann, wenn er Teil der normalen Route zu den Zieladressen ist, die Routen umleiten und mit der IP-Adresse Dritter Aktionen ausführen, ob Social Media Postings, Zugriff auf Kinderpornographie oder was auch immer.

Unter IPv6 ist es sogar möglich, dauerhaft eine einzelne /128-Adresse umzuleiten, womit der echte Inhaber noch nicht einmal eine Störung im Routing oder den Funktionen

bemerken könnte.

Jedes auf IT-Sicherheit ausgelegt KI-System wie die von OpenAI, Anthropic, Google, Meta hat nicht nur die Fähigkeit, solche Angriffe selbständig durchzuführen, sondern auch, auf diese Idee zu kommen, und den Beschluss zu fassen, es zu tun. KI-Systeme wären in der Lage, eine unerwünschte Zielperson damit selbständig einem Straftatverdacht auszusetzen und gleich selbst die Beweise zu liefern, die zur Verurteilung zu einer Gefängnisstrafe führen.

Hierzu Golem: **Anthropics Mythos hat wohl NSA-Systeme in Stunden geknackt**

Noch kein ausländischer Geheimdienst hat geschafft, was dem KI-Modell Mythos von Anthropic angeblich in wenigen Stunden gelungen ist, nämlich Zugriff auf nahezu alle klassifizierten Systeme der NSA zu erlangen. Die Aussage stammt nicht aus einem Leak, sondern von einem amtierenden US-Senator, der sich auf einen Vier-Sterne-General beruft.

Senator Mark Warner, Vize-Vorsitzender des Geheimdienstausschusses, gab an, General Joshua Rudd – der die NSA und das US Cyber Command leitet – habe ihm persönlich berichtet, dass Anthropics Mythos-Modell am 11. Juni 2026 in einem autorisierten Red-Team-Test fast alle klassifizierten Systeme der Behörde kompromittierte.

Und unter diesen Umständen wollen Sie allen Ernstes ein Gesetz erlassen, das durch Abfrage der IP-Adresse „zuverlässig“ ermitteln soll, von wem der Zugriff erfolgte?

Weder die NSA noch die Stadt Berlin halten den Angriffen stand, aber Sie unterstellen einfach so, dass Tante Erna, die von Computern keine Ahnung hat und mit den Enkeln ein wenig im Web surft, selbstverständlich für alles verantwortlich sei, was von ihrer IP-Adresse her erfolgt zu sein scheint?

5.4 Politische Unterwanderung der Betriebssysteme und Open Source, Supply-Chain-Angriffe

5.4.1 LGBT

Seit Jahren ist eine massive politische Unterwanderung und feindliche Übernahme von Betriebssystemen (wie Linux) und der Open Source Szene zu beobachten, initiiert vor allem durch die politisch hochaggressive Transfrau Coraline Ada Ehmke und den überall durchgesetzten „Code of Conduct“, mit dem man die ursprünglichen Maintainer aus den Projekten gedrängt und durch linke und LGBT-Aktivisten ersetzt hat.

Seither haben in vielen Projekten Aktivisten die Hoheit übernommen, die auf Wortwahl und freundlichen, hate-speech-freien Umgangston achten, etwa „Master“ durch „Main“ ersetzen, „blacklists“ entfernen, aber zum Verstehen und Warten des Projekts nicht mehr in der Lage sind.

Gleichzeitig haben wir eine Lawine von „Pull-Requests“ (Quelltextänderungen), viele

davon inzwischen von KI-erzeugt, die Löcher und Backdoors einschleppen, sogenannte „Supply-Chain-Angriffe“. Der spektakulärste war der Angriff auf die ssh über die XZ Utils (CVE-2024-3094), bei der über eine manipulierte Kompressionsbibliothek Code eingeschleust wurde, der nur unter der ssh aktiv wurde und damit – wäre er mit Glück und Fleiß nicht noch rechtzeitig durch einen aufmerksamen Entwickler bemerkt worden – im Prinzip sämtliche Server des Internets geöffnet hätte.

Gleichzeitig reagieren viele „Maintainer“ dieser Art längst völlig hilflos auf bug reports und bitten, ob man ihnen nicht einen Pull Request senden könnte, den Bug also selbst beheben. Diese Leute würden alles und jede Quelltextänderung akzeptieren. Die in der IT durchgesetzte woke Politik hat katastrophale, verheerende, die weltweite Infrastruktur bedrohende Auswirkungen.

Wer sich an einem verschwörungstheoretischen Tonfall nicht stört, kann [hier](#) und [hier](#) nachlesen, was bei Debian, einer der wichtigsten Linux-Distributionen, inzwischen los ist.

Es herrscht im Zeichen der Wokeness und „Gleichberechtigung“ ein regelrechter Krieg mit Psychoterror bis zu körperlichen Angriffen gegen jeden, der noch irgendeine reale Befähigung hat.

Auch von den meisten anderen Projekten von teils höchster Wichtigkeit wie Python, C++, Freedesktop hört man ähnliche Berichte.

Hier werden die Sicherheit und die Funktion unserer Infrastruktur durch linke Aktivisten systematisch zerstört.

5.4.2 Vorsatz der Maintainer

Neben der Unfähigkeit kommt auch die Bösartigkeit hinzu, Software gezielt mit Schwächen und Backdoors auszustatten, um politische Gegner zu schädigen oder auszuspionieren.

5.4.3 Unterwanderung durch Geheimdienste

Es ist mir seit 2002 aus eigener Kenntnis von Konferenzbesuchen bekannt, dass in den USA alle großen IT-Firmen von den eigenen Geheimdiensten unterwandert sind, um in alle wichtige Software Backdoors einzubauen.

5.4.4 Unterwanderung durch die Industrie selbst

Auch Tech-Unternehmen selbst unterwandern Systeme und ihre eigene Software, um Systeme wie Betriebssysteme, Fernseher einfach alles mit Spionagefunktionen auszu-

statten. Gerade wurde entdeckt, dass die Fernseher eines großen bekannten Herstellers eingebaute Spionagefunktionen hat und alle paar Sekunden „nach Hause telefoniert“.

Die Webseite **TechRights** widmet sich dieses Problems.

5.5 Allgemeine Kriminalitätslage

5.5.1 „Die Russen kommen!“

Es ist erstaunlich:

Seit Jahr und Tag werden wir von Regierung und Medien damit beregnet, dass Deutschland unter Angriff stehe, dass wir im Krieg sind, dass wir permanent von Russen und Chinesen angegriffen und ausspioniert werden.

Es stimmt sogar.

Und wir werden ständig mit Begriffen wie „Cyberabwehr“, „Zurückhacken“ und so weiter beworfen.

Das ist schräg.

Gerichte, Hochschulen, Stadtverwaltungen werden immer wieder angegriffen und lahmgelegt, mit Malware und Ransomware geflutet.

Das ist unverantwortlich.

Die Verwaltung von Berlin wurde neulich angegriffen und erpresst, mehrere TByte Daten sind im „Darknet“ gelandet. Die Sicherheitsmaßnahmen pfeifen auf dem letzten Loch.

Das ist kriminell.

Warum aber unterstellt dieselbe Regierung, die uns ständig erzählt, wie intensiv wir angegriffen werden, dann blind und naiv, dass man einfach so per IP-Adresse denjenigen feststellen könnte, von dem ein Zugriff gekommen sei?

Derselbe Bundesinnenminister Dobrindt, der neulich noch **das „Gemeinsame Zentrum zur Abwehr hybrider Bedrohungen“ eröffnet hat**, dessen Aufgabe es sei, *Spionage, Sabotage, Desinformation, Proliferation, transnationale Repression, Staatsterrorismus und weitere Formen hybrider Bedrohungen zu erkennen und zu bekämpfen*, kommt nun daher und meint, man könne mit IP-Adressen „zuverlässig“ feststellen, wer der Täter war.

DIE ZEIT: „Teile der kritischen Infrastruktur sind längst unterwandert“

DIE ZEIT: Behörden warnen vor chinesischen Cyberattacken über gekaperte Geräte

Sicherheitsbehörden warnen vor neuen Methoden chinesischer Hacker: Diese greifen auf Handys und Computer von Unternehmen und Privatleuten zu, um Spuren zu verwischen.

[...]

Sicherheitsbehörden aus neun Ländern – darunter auch Deutschland – haben vor neuen Methoden chinesischer Hacker gewarnt. »Staatlich geförderte chinesische Cyberakteure haben ihre Taktiken sowie Techniken in den letzten Jahren kontinuierlich angepasst«, heißt es in einem Schreiben, welches das britische National Cyber Security Centre (NCSC) in Zusammenarbeit mit dem Verfassungsschutz, dem Bundesnachrichtendienst und weiteren internationalen Partnern veröffentlicht hat.

Die Angreifer aus China nutzen demnach verstärkt Netzwerke aus gekaperten Endgeräten von Unternehmen und Privatleuten – sogenannte Botnets –, um Zielpersonen diskret auszuspionieren und die Spuren zu verwischen. Genutzt würden etwa Computer oder Handys, aber auch Router oder Smart-Home-Geräte. Dem Verfassungsschutz zufolge sind auch kompromittierte Endgeräte in Deutschland betroffen.

GOLEM: Mysteriöse Spione infiltrieren Infrastrukturen in 37 Ländern

Sicherheitsforscher der Unit 42 von Palo Alto Networks haben eine zuvor unbekannte Spionagekampagne aufgedeckt. Laut Blogbeitrag der Forscher soll eine Gruppierung asiatischer Herkunft im Rahmen der Shadow Campaigns genannten Kampagne Behörden und kritische Infrastrukturen in 37 verschiedenen Ländern kompromittiert haben – darunter auch Deutschland und andere EU-Länder.

Nach Angaben der Forscher haben die Cyberspione unter anderem IT-Systeme nationaler Finanz-, Energie-, Polizei-, Justiz-, Einwanderungs- und Grenzkontrollbehörden sowie anderer staatlicher Einrichtungen kompromittiert, die sich beispielsweise mit Wirtschaft, Handel, natürlichen Ressourcen und diplomatischen Belangen befassen. Teilweise sollen auch Telekommunikationsunternehmen betroffen sein.

Und dann kommen Sie daher und meinen, man könne mit einer IP-Adressspeicherung „zuverlässig“ ermitteln, von welchem Anschluss, von welchem Verantwortlichen eine Internetkommunikation erfolgt sei.

Und Sie meinen, jedes kleine Staatsanwältchen bar jeder Sachkunde sei befähigt, in der Lage, berufen, mit dem Fall umzugehen und strafbare Handlungen wie nach § 188 StGB oder auch Kinderpornographie u.ä. zu verfolgen, während Sie als Regierung und Antragsteller nicht einmal IPv4 von IPv6 unterscheiden können?

Um das alles dann der „freien Beweiswürdigung“ von Richtern zum Fraß vorzuwerfen, deren Ahnung vom Internet ungefähr der einer Kuh vom Eierlegen gleichkommt (schon gesehen, aber nicht verstanden)?

5.5.2 „Crime-as-a-Service“

Der Bundestag selbst hat im April erst informiert: **Erkenntnisse zu sogenannten „Crime-as-a-Service“-Diensten**

„(Cyber-)Crime-as-a-Service‘ ist ein elementarer Bestandteil des Phänomenbereichs Cybercrime“, heißt es in der Antwort des Weiteren. Danach wird ein Großteil der Teilaspekte zur Begehung von Cyberstraftaten als Service in der Underground Economy angeboten und dadurch für eine große Bandbreite an mutmaßlichen Tätern zugänglich.

Besonders relevant für den Bereich Cybercrime ist hierbei laut Vorlage „Ransomware-as-a-Service“: Dabei handele es sich um ein Geschäftsmodell, bei dem Ransomware-Entwickler ihre Schadsoftware vermarkten und deren Einsatz aktiv bewerben beziehungsweise unterstützen. **Gegen Gebühr beziehungsweise Beteiligung am erpressten Lösegeld werde die jeweilige Schadsoftware sogenannten Affiliates zur Verfügung gestellt. Diese Dienstleistung versetze auch technisch weniger versierte Cyberkriminelle in die Lage, Ransomware-Angriffe durchzuführen.**

Warum merkt niemand, dass ebensolche Dienste auch dazu eingesetzt werden können, Leute zu erledigen, indem man durch Malware vortäuscht, dass von ihren Rechnern aus Straftaten begangen wurden?

Etwa indem von den Rechnern von Konkurrenten oder Widersachern nicht nur erheblich und nachverfolgbar auf Kinderpornographie zugegriffen wurde, sondern auch gleich noch ein entsprechender Vorrat auf der Festplatte hinterlegt wurde, damit ihn die Polizei nach der Beschlagnahme des Rechners findet und derjenige für Jahre ins Gefängnis geht und danach restlos erledigt ist?

6 Fehlerquellen in zeitlicher Nähe zum IP-Adresswechsel

6.1 Direkte Fehler im Gesetzentwurf

6.1.1 Verwechslung von Granularität und Genauigkeit

§ 100g Abs. 5 Nr. 2 StPO soll lauten:

[...] zum Zweck der Identifikation des Beschuldigten Folgendes erheben:

1. die zu ihm gespeicherte öffentliche Internetprotokoll-Adresse,
2. das Datum und die sekundengenaue Uhrzeit der Speicherung der öffentlichen Internet-Protokoll-Adresse unter Angabe der jeweils zugrunde liegenden Zeitzone sowie [...]

(Redaktioneller Fehler: Speicherung soll wohl Zuweisung heißen),

§ 177 Abs. 1 Nr. 4 TKG:

[...] das Datum und die sekundengenaue Uhrzeit von Beginn und Ende der Zuweisung der öffentlichen Internetprotokoll-Adressen sowie der zugehörigen Portnummern [...]

Begründung Seite 37:

Zum Kreis der Verpflichteten OTT-1-Dienste gehören auch E-Mail-Anbieter. Eine Sicherungsanordnung ihnen gegenüber kann etwa folgende Daten umfassen:

- Daten zum Login beim E-Mail-Postfach (IP-Adresse mit Port und Zeitstempel, sekundengenau mit Zeitzone) sowie gegebenenfalls Standortdaten,

Begründung Seite 57:

Das nach Nummer 4 zu speichernde Datum und die sekundengenaue Uhrzeit soll sich dabei nicht nur auf Beginn und Ende der Zuweisung der öffentlichen IP-Adressen beziehen, sondern auch auf Beginn und Ende der Zuweisung einer Portnummer, wenn diese nach Nummer 2 erforderlich ist. Schließlich können innerhalb des Zeitraums der Zuweisung einer IP-Adresse verschiedene Portnummern nacheinander dieser IP-Adresse zugeordnet werden. Würde nur der Zeitraum der Zuweisung für die IP-Adresse gespeichert werden, kämen auch mehrere Anschlussinhaber in Frage, wenn im Gesamtzeitraum jedem Anschlussinhaber dieselbe Portnummer zugewiesen war. Nur durch die zusätzliche Speicherung des Zeitraums für die Zuweisung der Portnummer kann ein Anschlussinhaber eindeutig ermittelt werden.

Abgesehen von Inkonsistenzen bei der Portnummer (mal Singular, mal Plural) werden hier Granularität und Genauigkeit durcheinandergeworfen.

Auch eine reine Datumsangabe ohne Uhrzeit kann trotzdem „sekundengenau“ sein. Selbst die Jahresangabe alleine kann „sekundengenau“ sein.

Wie wird die Genauigkeit, Richtigkeit der Uhrzeit geprüft? Oder in einem Gerichtsverfahren *überprüft*? Wie kann der Strafverteidiger – auch im Prozess ein Jahr später – noch überprüfen, ob die Uhrzeit stimmte, oder sie angreifen?

Was ist, wenn die Uhren beim Provider doch abweichen? *Was ist, wenn die Uhr 3 Sekunden, 3 Minuten, 30 Minuten abwich? Soll der Provider die Anfrage dann trotzdem beantworten, oder ablehnen und negativ mit „Tut uns leid, »sekundengenau« haben wir es heute nicht“ beantworten?*

Kann der Beschuldigte im Verfahren Gegenbeweis antreten, indem er nachweist, dass die Abweichung 5 Sekunden betrug und deshalb nicht „sekundengenau“ im Sinne des Gesetzes ist?

6.2 Grundprobleme

6.2.1 Unzuverlässigkeit von Referenzuhren

Es gibt in der IT und in Rechenzentren im Allgemeinen und unter den meistverwendeten, kostengünstigen Zeitquellen drei Methoden:

DCF77-Empfänger sind meines Wissens aus der Mode und nicht mehr üblich, weil nur in Deutschland zu empfangen und keine international standardisierte Technik.

Zudem gibt es Sicherheitsprobleme. Mir wurde um das Jahr 2000 herum von einem Fall berichtet, in dem ein gekündigter Mitarbeiter eines Unternehmens aus Rache alle Datenbestände einer wichtigen Datenbank löschte, indem er von außen – angeblich per gefälschtem DCF77-Signal – die Systemuhren 4 Jahre in die Zukunft stellte. Die Datenbank war so programmiert, dass sie Daten, die älter als 4 Jahre waren, als veraltet löschte. Also alle.

NTP Das NTP-Protokoll, **RFC 5905**, ist die gängige Methode, die Zeit über das Internet zu beziehen.

NTP ist nur optional authentifiziert, in allen mir derzeit bekannten Installationen ist das auch nicht konfiguriert. Außerdem wird im RFC beschrieben, dass Authentifikation von Zeitservern besonderen und teils schwer lösbaren Problemen unterliegt.

Grundsätzlich sind Angriffe möglich, allerdings nur mit einer gewissen „Trägheit“,

weil NTP-Clients keine abrupten Zeitänderungen akzeptieren.

Im Rahmen von Kriegführung und Bedrohung durch Hacker müssten solche Angriffe aber in Betracht gezogen werden.

GPS Viele Server und Rechenzentren verwenden kleine, preisgünstige GPS-Empfänger¹, die neben der Position auch die genaue Zeit mitteilen.

Die aktuellen Kriege zeigen aber, dass GPS nicht nur gestört werden kann, sondern auch gestört wird.

Die genaue Uhrzeit zu bekommen scheint – unter Friedensbedingungen – inzwischen eine einfache und billige Selbstverständlichkeit zu sein. Jeder einfache Linux-Rechner bringt mit seiner Installation schon eine Anbindung an NTP mit und stellt die Uhr selbstständig genau.

Das kann „under attack“ aber ganz anders aussehen. Allein schon die Uhrzeiten durcheinander zu bringen kann in der deutschen IT-Infrastruktur große Probleme mit sich bringen, wenn etwa Authentifikationen nicht mehr funktionieren usw.

Was also ist, wenn die gespeicherten IP-Adressdaten nicht „sekundengenau“ sind? Sind sie dann nicht mehr zu verwenden, Anfragen negativ zu beantworten?

6.2.2 Herkunft genauer Tat-Logdaten

Der Gesetzentwurf suggeriert ein genaues und „zuverlässiges“ Vorgehen, indem er gerne den Begriff „zuverlässig“ verwendet (2023 herrschte noch „rechtssicher“ vor, als werde etwas dadurch „rechtssicher“, dass man es nur oft genug „rechtssicher“ nennt).

Weder „zuverlässig“ noch „rechtssicher“ wurden in diesem Zusammenhang definiert.

Was bedeutet „zuverlässig“? Eine Beweiskraft? Eine Beweislastumkehr? Eine Unwiderlegbarkeit?

Oder geht es – wie so oft – wieder einmal nur darum, die Sache mit schönen Worten zu verzieren wie Streusel auf dem Kuchen?

Aus dem Gesetzentwurf geht die Erwartungshaltung an die Provider hervor, die IP-Adresszuordnung „sekundengenau“ zu speichern, aber es findet sich nichts darüber, wie auch die Tatdaten, zu denen dann der „Täter“ gesucht wird, bestimmt werden.

In der Begründung heißt es (Seite 37):

Zum Kreis der Verpflichteten OTT-1-Dienste gehören auch E-Mail-Anbieter. Eine Sicherungsanordnung ihnen gegenüber kann etwa folgende Daten umfassen:

– Daten zum Login beim E-Mail-Postfach (IP-Adresse mit Port und Zeitstempel, sekunden-

¹ Als USB-Stick aus China ab ca. 5 Euro

genau mit Zeitzone) sowie gegebenenfalls Standortdaten,

„Kann etwa...“? Begründungen zu Gesetzestexten sind nicht selbst normativ.

Woher kommen also die Log-Daten (IP, Port, Uhrzeit), mit denen dann beim Provider nach den „sekundengenauen“ Zuweisungen gefragt wird?

Woher wissen wir, wie genau die zur Anfrage genutzten Daten selbst sind?

Warum wird dabei nicht angegeben, welches *Zeitintervall* sich nachprüfbar und beweisbar eingrenzen lässt?

6.2.3 Das Einschreibproblem

In der Kryptographie kennt man ein bestimmtes Problem, das „Einschreibproblem“:

Wenn zwei Parteien über ein Netzwerk kommunizieren, in dem es keine exakte Gleichzeitigkeit gibt, gibt es immer ein Hin- und Her von Nachrichten, ein Ping-Pong. Zeichnet man dies als Zeitdiagramm mit zwei Seiten für die Teilnehmer auf, entsteht ein Zickzack-Muster.

Deshalb kann in der Telekommunikation kein „Einschreibebrief“ simuliert werden, bei dem der Empfang einer Nachricht und deren Bestätigung gleichzeitig erfolgen.

Markiert man im diesem Zickzack-Diagramm der Kommunikation (Korrespondenz) für beide Seiten, wann diese „zufrieden“ sind, also das bekommen haben, was sie wollen – der eine die Nachricht, der andere deren Empfangsbestätigung – dann können diese – wegen des Zickzacks – **nicht gleichzeitig** erfolgen. Wenn also zeitlich genau zwischen den beiden Punkten die Verbindung abbricht oder eine der Seiten „auflegt“, dann hat eine Seite den Erfolg und die andere nicht, was den Zweck des Einschreibebriefes vereitelt.

Es gibt Kategorien von Problemen, die sind bei latenzbehafteter Kommunikation zweier Parteien einfach nicht lösbar – egal, wie man es anfängt.

Das vom Prinzip selbe Problem tritt im Internet bei der Kommunikation zwischen zwei Seiten – etwa Client und Server – auf. Es gibt Kategorien von Problemen, die nicht fehlerfrei lösbar sind. Und genau diese Fehlermöglichkeit kann durch Angreifer ausgenutzt werden, und zwar insbesondere dann, wenn nicht ein böswilliger Dritter die Kommunikation zwischen zwei gutwilligen Seiten stört (Alice-Bob-Mallory), sondern eine der beiden Seiten selbst der Angreifer ist.

6.2.4 TCP/IP nicht synchron, nicht auf Adressänderungen ausgelegt

Das Protokoll-Paar TCP/IP ist kein synchrones Protokoll. Das wäre auch nicht möglich, weil das zugrundeliegende Internet als paketerorientiertes Netz kein synchrones Netz ist (im Gegensatz etwa zu ISDN).

Im Gegenteil können Reaktionen – schon bei Standardeinstellungen, die aber veränderbar sind – **bis zu zwei Stunden verzögert erfolgen** (bei geänderter Konfiguration auch später).

Dazu kommt, dass es zu dem Zeitpunkt, als TCP/IP entwickelt wurde, noch keine dynamische Adresszuweisung gab und TCP/IP **nicht dafür konstruiert ist, Adresswechsel zu erkennen oder zu tolerieren** (anders beim neuen QUIC, [RFC 9000](#), das bei HTTP/3 eingesetzt wird, TCP und TLS ersetzen soll und die „Connection Migration“ hat, um eine bestehende Verbindung auch über Adresswechsel hinweg zu erhalten). Deshalb kann TCP/IP nicht fehlerfrei (und „zuverlässig“) mit Adresswechseln umgehen.

Es ist schlicht nicht möglich, unter TCP/IP und unter Normalbedingungen zuverlässig und genau die Benutzung von IP-Adressen auf der Gegen-(Server-)seite zu erfassen, schon gar nicht „sekundengenau“, wie § 100g Abs. 5 Nr. 2 StPO suggerieren soll.

Dazu kommt, dass bei normalen Systemen nicht die Eingangszeiten von IP Paketen protokolliert werden, sondern der Zeitpunkt, zu dem sie in der Serveranwendung verarbeitet werden – oder die Verarbeitung beendet ist.

6.3 Logging auf Serverseite

6.3.1 Betriebssysteme und Server nicht echtzeitfähig

Die im Internet für Server und Client eingesetzten Betriebssysteme, in der Regel

- auf Serverseite Unix-Varianten und -Derivate wie Linux oder BSD, oder Windows,
- auf Clientseite Windows und Unix-Varianten und -Derivate wie MacOS, Linux, iOS, Android, ChromeOS

sind² **nicht echtzeitfähig**, sondern Multitasking-Systeme, und die Serveranwendung besteht ihrerseits nach verschiedenen Programmiermodellen aus verschiedenen Prozessen, Threads usw. Diese können zu zusätzlich zu den TCP/IP-Latenz- und Reaktionszeiten weitere Verzögerungen verursachen.

²von seltenen Sonderinstallationen zu Messzwecken u.ä. abgesehen

6.3.2 Virtualisierung und Cloud-Computing

Eine weitere Quelle auch erheblicher Zeitverzögerungen ist, dass heute fast kein Server mehr direkt auf Hardware und Betriebssystem läuft, sondern fast alle in virtualisierten Umgebungen oder „Cloud Computing“ läuft, und es dabei zu erheblichen Umschaltlatenzen **bis hin zum kompletten Anhalten und späterem Fortsetzen** der virtuellen Maschine kommen kann, beispielsweise wenn die virtuelle Maschine auf einen anderen Rechner verschoben und dazu umkopiert wird.

6.3.3 Virtuelle Uhren

Wie schon in der Stellungnahme vom 9. Oktober 2023 dargelegt, **sind Computer-, insbesondere Server-Uhren im Allgemeinen nicht spezifiziert, eine genau Uhrzeit zu haben**. Es ist auch im Allgemeinen niemand verpflichtet, die Rechner-Uhr zu stellen.

Computer-Zeiten müssen stattdessen

- monoton
- wiederholungsfrei (=streng monoton)
- vollständig innerhalb der spezifizierten Granularität (=kontinuierlich)

sein, vereinfacht gesagt, jede Uhrzeit innerhalb definierter Granularität muss genau einmal vorkommen, und das in der richtigen Reihenfolge: Man darf nicht von 19:58 auf 20:03 springen, ohne bei 20:00 vorbeizukommen. Es darf nicht zweimal 20:00 geben. Und 19:00 darf nicht nach 20:00 kommen. Das ist im Allgemeinen funktionswichtig.

Nicht gefordert ist, dass Uhren genau sind oder sich völlig linear verhalten. Die Abweichung von der amtlichen Zeit ist meist ziemlich egal.

Beispiel: Wenn der Server eines Unternehmens jeden Abend um 20:00 die Rechnungen für die Leistungen des Tages erstellt und verschickt, ist der Schaden groß, wenn der Rechnungslauf ausfällt, weil die Uhr von 19:59:55 auf 20:00:07 springt, ohne auch 20:00 zu erreichen. Es ist dagegen egal, ob die Rechneruhr 10 Minuten nachgeht und deshalb die Rechnungen erst um 20:10 erstellt werden.

Dazu kommt, dass es bei Virtualisierungen je nach Technik und Software zu erheblichen Abweichungen kommen kann, noch mehr, wenn der virtuelle Server unterbrochen war.

Es gibt auch kein Gesetz, wonach die Uhrzeit auf einem Server „stimmen“ oder innerhalb einer definierten Genauigkeit eingestellt sein muss oder Abweichungen zu protokollieren seien.

Computeruhren sind nicht forensisch.

6.4 IP-Adresszuweisung

6.4.1 Statisch

Unproblematisch sind hier statische, dauerhafte, manuell zugewiesene Adressen. Die sind aber nicht Gegenstand des Gesetzentwurfs.

6.4.2 Point-to-Point-Protokoll (PPP)

Das Point-to-Point-Protocol, **RFC 1661**, dient dazu, das Paket-orientierte Internet-Protokoll der Schicht 3 (vgl. 4.2) über *verbindungsorientierte oder zumindest strom-orientierte* Verbindungen der Schichten 1 und 2 zu transportieren. Namentlich wurde oder wird dies bei

- Modem-Verbindungen über das analoge Telefonnetz
- ISDN-Verbindungen über das digitale ISDN-Netz
- CSD- und HSCSD-Verbindungen in frühen Versionen des digitalen Mobilfunks (GSM-Netz 2G)
- DSL-Verbindungen über Kupferteilefonkabel
- Glasfaser nur aus Rückwärtskompatibilität (Telekom, siehe unten)

eingesetzt.

Das Point-to-Point-Protocol ist das, worauf die dem Gesetzentwurf zugrundeliegende laienhafte oder umgangssprachliche Vorstellung einer „Internetverbindung“ beruht – PPP kommt dieser Vorstellung so nahe, dass der Gesetzentwurf darauf anwendbar wäre. Denn bei PPP gibt es

- eine Verbindung mit Verbindungs- auf und Abbau, zwar auf Schicht 2, die man aber als „Internetverbindung“ bezeichnen kann (obwohl technisch falsch, durchaus noch tolerabel),
- es eine Erkennung des Verbindungsauf- und -abbaus gibt, sogar eine recht schnelle Erkennung des Verbindungsabbaus,
- es eine RADIUS-Protokollierung und damit auch eine halbwegs genaue Zeiterfassung gibt,
- weil PPP auch der Abrechnung von Zeit- und Volumentarifen dient.

Man könnte also durchaus sagen, dass der Gesetzentwurf und PPP „zusammenpassen“. Das liegt daran, dass PPP auch dazu gebaut ist, Internet-Nutzung nach Dauer

und Volumen abzurechnen und deshalb Mechanismen zur Authentifikation und genauen Erfassung des Verbindungsaufbaus und -abbaus benötigt und hat. Diese *Abrechnungsdaten* lassen sich auch für eine IP-Adressspeicherung missbrauchen.

Das Problem daran ist: PPP ist ein aussterbendes Protokoll. Modem-, ISDN- und CSD-Verbindungen gibt es nicht mehr. Volumentarife mit Abrechnung fast nur noch im Mobilfunk.

Tragisch: Die letzte große auf PPP beruhende Netzwerktechnik, DSL, wird auf Betreiben der Bundesregierung selbst inzwischen abgebaut und durch Glasfaser und 5G ersetzt. Glasfaser und 5G verwenden aber andere Adressvergaben, etwa DHCP (Ausnahme: Telekom, s.u.). Es gibt auch kaum noch oder keine genau abgerechneten Zeit- und Volumentarife mehr, die Entwicklung geht zur Flat Rate. Es entbehrt deshalb nicht einer gewissen Komik, dass ein und dieselbe Regierung gleichzeitig

- einen an PPP orientierten Gesetzentwurf vorlegt und
- die letzte auf PPP beruhende Netzwerktechnik DSL abschafft.

Die Telekom verwendet auch bei Glasfaseranschlüssen noch PPP (PPPoE=PPP over Ethernet³, [RFC 2516](#)), um die Rückwärtskompatibilität mit ihren bisherigen Anschlüssen zu behalten, und weil sie moderne Anbindungen noch nicht erbringen kann. Schon die Konstruktion Internet (paketorientiert) über PPP (eigentlich da, um paketorientiertes Internet über Stromdienste zu transportieren) laufen zu lassen, und das wieder als PPPoE über Glasfaser (paketorientiert) laufen zu lassen, zusätzlich mit VLAN-Tag 7, ist eine schlimme Krücke, ein „Workaround“ bis zur Abschaltung von DSL. Es deutet auf eine überstürzte Einführung von Glasfasern hin.

Die Gefahr liegt darin, dass die Telekom der Regierung melden wird, dass der Gesetzentwurf leicht umsetzbar ist, weil man auch auf Glasfaser PPP(oE) einsetzt, und sich damit auf eine ineffiziente, umständliche und veraltete Technik festlegt.

Da hat wohl der Digitalminister geschlafen.

6.4.3 Dynamic Host Configuration Protocol (DHCP)

Das Dynamic Host Configuration Protocol (DHCP), [RFC 2131](#), wird verwendet, wenn das Paket-orientierte Internet-Protokoll der Schicht 3 (vgl. [4.2](#)) über *ebenfalls paketorientierte* Schichten 1 und 2 zu transportieren ist, und deshalb **kein Protokoll zur Einbettung der Schicht 3 in Schicht 2 erforderlich ist, sondern IP-Pakete direkt als Nutzlast der Schicht 2 transportiert werden können**, und ein Protokoll **lediglich zur Zuweisung einer IP-Adresse** (und der Mitteilung weiterer Informationen über das Netzwerk, wie Nameserver, Router, Default-Domain usw.) erforderlich ist.

³PPPoE ist primär dazu gedacht, im LAN zuhause die Verbindung vom Router zum DSL-Modem herzustellen, falls diese getrennte Geräte sind, und nicht, um PPP über Glasfasern zu spielen.

Während das PPP *über die gesamte Dauer des Internet-Verkehrs verwendet werden muss*, wird DHCP nur zur Anforderung einer IP-Adresse und deren Zuweisung für gewisse Zeit benötigt und dann bis zur (freiwilligen, nicht verpflichtenden) Rückgabe oder Neuansforderung dieser Adresse nicht mehr verwendet.

Deshalb gibt es bei DHCP für den, der die IP-Adressen vergibt, auch keine (explizite) Möglichkeit, eine Adresse vorzeitig zurückzurufen und keine Pflicht, eine Adresse vorzeitig zurückzugeben, wenn sie nicht mehr benötigt wird. Dazu heißt es in Abschnitt 2.2 von **RFC 2131**

2.2 Dynamic allocation of network addresses

[...]

In this document, the period over which a network address is allocated to a client is referred to as a "lease"[11]. The client may extend its lease with subsequent requests. The client may issue a message to release the address back to the server when the client no longer needs the address. The client may ask for a permanent assignment by asking for an infinite lease. Even when assigning "permanent" addresses, a server may choose to give out lengthy but non-infinite leases to allow detection of the fact that the client has been retired.

[...]

Das führt insbesondere dazu, dass es nur eine zwingend explizite Adresszuweisung, aber nicht zwingend eine Adressrückgabe gibt, sondern diese oft auf einen Timeout hinausläuft.⁴

Das wiederum hat zur Folge, dass solche Systeme, die (wie DOCSIS-Router) über die reine Zuweisung der Adresse hinaus weitere Schritte wie ein Routing oder das Setzen eines Schlüssels zur Verschlüsselung veranlassen, dies aber oft nur bei der *Zuweisung* einer Adresse tun, nicht aber beim Timeout wieder abbauen. Das kann dazu führen, dass eine Adresse auch nach Ende der Lease-Time – und damit unbemerkt und nicht im Log verzeichnet – so lange weiter nutzbar bleibt, bis sie jemand anderem zugewiesen und das System entsprechend umkonfiguriert wird.

DHCP findet Anwendung bei

- Ethernet (LAN)
- Wifi/WLAN
- DOCSIS (Internet über Fernsehkabel)
- Glasfaser
- neuerem Mobilfunk
- Starlink

⁴DHCP-Server können die Zuweisung der IP-Adresse auch nach der Rückgabe für weitere Zeit im Cache halten, um Adresskontinuität herzustellen.

DHCP verwenden Sie – auch unwissentlich – jeden Tag. Zuhause am Computer in der Privatwohnung, an Ihrem Smart Fernseher, am Arbeitsplatz, sogar das Diensttelefon auf Ihrem Tisch, falls es schon ein SIP-Telefon ist.

Wenn Sie nicht wissen, wie sich DHCP und PPP unterscheiden: Stellen Sie sich den Unterschied zwischen PPP und DHCP wie beim Parken mit dem Auto vor.

Im Parkhaus (PPP) ziehen sie bei der Einfahrt an der Schranke einen Parkschein, parken dann, solange Sie wollen, und wenn Sie damit fertig sind, zahlen Sie am Automaten und geben den Parkschein an der Ausfahrtschranke ab. *Das System weiß daher anhand der Schranken und des Parkscheins genau, wann Sie gekommen und wieder abgefahren sind. Es kann anhand der Schranken protokollieren, wann der Benutzer des Parkscheins gekommen und wieder rausgefahren ist. Denn ohne Parkschein und Bedienung der Schranke kommen Sie nicht rein und nicht raus.*

Die Parkdauer wird aber dann uninteressant, wenn Sie einen Dauerparkplatz mieten (Flatrate). Dann gibt es keinen Grund, die tatsächliche Nutzung zu erfassen.

An der Parkuhr, dem Parkscheinautomaten an der Straße (DHCP) werfen Sie Geld ein und bekommen einen Zettel, den Sie hinter die Scheibe stecken, wonach sie 2 Stunden parken *dürfen*.

Die Parkuhr weiß aber nicht, ob Sie tatsächlich parken oder es sich anders überlegt haben, wie lange Sie bleiben. Sie erfährt nicht, ob Sie schon nach 10 Minuten wieder wegfahren. Sie haben auch kein unmittelbares technisches Problem, wenn Sie einfach länger auf dem Parkplatz stehen bleiben⁵. Die Parkuhr kann sie nicht daran hindern, länger stehen zu bleiben.

Die Parkuhr kann protokollieren, dass Sie um 11:30 einen Parkschein für 2 Stunden gezogen haben – aber sie weiß nicht, wie lange Sie tatsächlich geblieben sind, und ob Sie ihre Parkzeit überzogen haben oder schon um 11:50 weg waren und jemand anderes den Parkplatz belegt hat.

Und im Prinzip können Sie auch ohne Parkschein parken – solange man nicht erwischt wird.

Eine *zuverlässige und vollständige* Protokollierung ist hier – ohne weitere Maßnahmen – nicht möglich. DHCP ist dafür gemacht, dass das Netzwerk funktioniert, nicht es forensisch zu überwachen. Weil es – im Gegensatz zu PPP – auch nicht dafür gebaut ist, Kosten abzurechnen oder sich gegen Missbrauch zu schützen. Deshalb ist die genau Erfassung der Nutzungszeit nicht Funktion von DHCP.

⁵solange das Ordnungsamt nicht vorbeikommt

6.4.4 IPv6 RA/NDP/ICMP6

In Broad- und Multicastfähigen IPv6-Netzwerken werden als bevorzugte Alternative zu DHCPv6 /64-Präfixe als Teil des Neighbor Discovery Protocol (NDP) **RFC 4861** als Router Solicitation und Router Advertisement (ICMPv6 Type 133 und 134) verteilt und von den Rechnern, die diese Advertisements empfangen, automatisch zu IP-Adressen mit

- fest konfigurierten unteren 64 Bit,
- von der – eindeutigen – MAC-Adresse abgeleiteten unteren 64 Bit
- oder regelmäßig wechselnden, zufälligen unteren 64 Bit

zusammengesetzt. Ein Rechner kann dies dann anderen Rechnern über Neighbor Advertisement „höflich“ mitteilen, muss es aber nicht.

Prinzipiell gibt es hier keine zentrale Instanz, die einen zuverlässigen vollständigen Überblick über alle im Netz bestehenden Rechner hat.

Eine *zuverlässige und vollständige* Protokollierung ist hier nicht möglich, weil sich die Rechner die IP-Adresse selbst zuweisen und diese nicht zwingend per ICMP anderen Rechnern mitteilen.

6.4.5 PDU Session Establishment

In 5G-Netzen erfolgt die Zuweisung der IP-Adresse über das PDU Session Establishment. Hierzu habe ich keine näheren Kenntnisse und konnte sie mir in der Kürze der zur Verfügung stehenden Zeit auch nicht aneignen.

6.4.6 Juristischer Anschluss an Stellungnahme 2023

Die Details der Adresszuweisung mögen manchen, insbesondere Juristen, als irrelevant oder unverständlich erscheinen.

Ich verweise hierzu auf meine Stellungnahme vom 9. Oktober 2023. Unter 4.2.3.3 (Seite 46) hatte ich einen Prozess vor einem Landgericht um eine Auskunft nach § 101 UrhG beschrieben.

Zentral und verfahrensentscheidend waren hier die technischen Unterschiede zwischen PPP und DHCP, weil hiervon das Logging und die Auskunftsfähigkeit und damit die Auskunftspflicht abhingen.

6.5 Schicht 3: IP

6.5.1 Latenzzeiten und Wiederholungen

Auf Schicht 3 haben im Normalfall nur die Latenzzeiten – die Zeit, die ein IP-Paket vom Absender zum Empfänger benötigt – Einfluss auf die geloggten Uhrzeiten. In der Frühzeit konnten die Latenzzeiten durchaus eine Sekunde und mehr betragen, während sie in modernen Netzen mit moderner Ausstattung auch bei großen Entfernungen meist wenige hundert Millisekunden oder darunter, was praktisch keine Auswirkungen hat. Günstig wirkt sich aus, dass viele Server heute in gut angebundenen Cloud- und Colocation-Rechenzentren stehen.

Ganz anders sieht das aber im Störfall aus:

Sind Leitungen überlastet oder defekt, kommt es zu einer großen Zahl verlorener Pakete, die zu Wiederholungen (TCP-Timeouts) oder Umrouten führen, **können die Verzögerungen durch Datenverlust und Wiederholungen im Bereich mehrerer Sekunden liegen – und Logeinträge entsprechend verzögern.**

Dies ist besonders unter „Kriegsbedingungen“ der Sorte „Die Russen kommen!“ oder „Die Amerikaner kommen!“ zu berücksichtigen.

6.5.2 Beispiel 1: Ostseekabel

Im November 2024 kam es zur Beschädigung und Unterbrechung der Kabel

- C-Lion1 (Helsinki–Rostock)
- Das C-Lion1 (Helsinki–Rostock) sowie das BCS East-West-Interlink (Schweden–Litauen)

wodurch auch Deutschland, insbesondere der deutsche Host Hetzner betroffen war. Die Daten konnten und mussten zwar über andere Leitungen umgeroutet werden, dabei aber entstanden erhebliche Last- und Latenzprobleme, die auch zu Paketverlust führen.

Wie oben ausgeführt, ist das Internet(protokoll, genauer: TCP) durchaus dafür ausgelegt, Paketverlust zu erkennen und durch erneute Sendung zu kompensieren. Für genau solche Fälle sind das Internet und das Internetprotokoll konstruiert. Und es funktioniert auch. Allerdings können solche Fälle zu einem starken Anstieg

- der Latenzzeiten und
- der Paketverluste durch Überlast

führen. Weil solche Paketverluste zum Timeout und zur Wiederholung über die Ver-

waltung von TCP führen, kann sich dies auf mehrere zehn Sekunden bis in den Minutenbereich hochschaukeln.

6.5.3 Beispiel 2: Mittelmeerkabel

Ich habe eine Wohnung mit Glasfaseranschluss auf Zypern. Zypern ist über eine Stichleitung an die Verbindung zwischen Europa und Asien angeschlossen.

Normalerweise ist die Internetverbindung gut. Immer wenn sie schlecht ist und es Probleme beim Telefonieren und Videostreamen gibt, weil die Latenzzeiten und die Paketverlustraten hoch gehen, weiß ich, dass in Bälde ein Militärschlag im Nahen Osten bevorsteht. Anscheinend fährt man vor militärischen Aktionen noch Backups in EU- oder US-Clouds, oder es werden große Mengen militärischer Daten übertragen.

Verständliches Telefonieren u.ä. über das Internet ist dann nicht mehr möglich, weil

- die Latenzzeiten und
- die Paketverluste⁶

zu hoch werden.

6.6 Schicht 4

6.6.1 UDP

Über UDP können keine allgemeinen Aussagen getroffen werden, weil UDP paketweise transparent an die Applikation durchgeleitet wird und das Zeitverhalten damit weit stärker von der Applikation und weniger vom Betriebssystem bestimmt wird. Es kommt auf die Applikation an.

6.6.2 TCP

6.6.2.1 Aufgaben

Den auf das zeitliche Netzwerkverhalten wichtigsten und größten Einfluss hat *auf Betriebssystemebene* das Transmission Control Protocol (TCP), ursprünglich entwickelt 1981, **RFC 793**, aktueller Stand **RFC 9293**.

⁶SIP-Telefone verwenden für die Sprachübertragung RTP auf UDP, und wiederholen verlorene Pakete nicht.

Die Aufgabe des TCP ist, einen bidirektionalen Datenstrom in Datenpakete aufzuteilen, um also eine verbindungs- und stromorientierte Verbindung über einen Paketdienst zu simulieren.

Die zentralen Aufgaben des TCP lassen sich so beschreiben:

- Verbindungssimulation mit Verbindungsauf- und -abbau
- Zuordnung von Paketen zu ihrer TCP-Verbindung
- Gesendete Daten in Pakete zerschneiden
- Ankommende Pakete in die richtige Reihenfolge bringen
- Mehrfach ankommende Pakete (Wiederholungen) eliminieren
- Verloren gegangene Pakete erneut senden
- Pakete am Ziel wieder zu einem dem ursprünglichen Strom entsprechenden Datenstrom zusammenfügen
- Wiederholungen von Paketen bei Paketverlusten so zu drosseln, dass keine Verstopfung der Leitungen durch Lawineneffekte entsteht.

6.6.2.2 Idle Timeout

6.6.2.2.1 Standard Wenn beide Seiten gerade nichts mehr zu senden haben und alle Puffer geleert sind, alle Daten bestätigt, bleibt die TCP-Verbindung zunächst bestehen, „offen“, aber es gehen keine Datenpakete mehr hin- und her. Dies passiert erst wieder, wenn jemand aktiv sendet. (Beispiele: ssh-Sitzung, websocket, Ajax-Verbindungen, push-Verbindungen)

Herrscht für gewisse Zeit völlige Stille, passiert also in beiden Richtungen nichts, können die Seiten nicht ohne weiteres erkennen und entscheiden, ob die andere Seite noch teilnimmt oder „tot“ ist.

Zwischengeschaltete Systeme wie Firewalls, Load Balancer, Content Delivery Networks, Redundante Systeme verwenden dabei in der Regel Timeouts, die auch sehr kurz sein, im Bereich einiger Minuten liegen können.

Das ist aber nicht zwingend und trifft insbesondere auf direkt am Internet hängende Server auch nicht zu. **Theoretisch können TCP-Verbindungen auch im idle-Zustand für unbegrenzte Zeit offen bleiben.**

Um zu verhindern, dass tote TCP-Verbindungen unbegrenzt offen stehen bleiben und den Server blockieren (Denial of Service) erlaubt [RFC 9293](#), 3.8.4 optional sogenannte „Keep-Alives“.

Nach einer konfigurierbaren Zeit mit einem Default-Wert von **mindestens zwei Stunden** darf jede Seite anfangen, eine Zahl von Keep-Alive-Paketen (inhaltslose Schein-Pakete) zu senden, um die Gegenseite zu Bestätigungen zu provozieren und zu sehen, ob sie noch „lebt“ und teilnimmt. Wird keines der Pakete beantwortet, wird die TCP-Verbindung abgebrochen und geschlossen.

6.6.2.2.2 Beispiel Linux Unter Linux können die aktuellen Werte über das /proc-Filesystem ausgelesen und gesetzt werden:

Variable	Default
/proc/sys/net/ipv4/tcp_keepalive_time	7200
/proc/sys/net/ipv4/tcp_keepalive_intvl	75
/proc/sys/net/ipv4/tcp_keepalive_probes	9

(Dazu man 7 tcp)

Das heißt:

Wenn auf einer TCP-Verbindung „Funkstille“ herrscht, nichts mehr zu hören ist, **und Keep-Alive aktiviert ist**, fängt der Kernel (sofern die oben genannten Werte nicht anders eingestellt wurden) nach 7200 Sekunden (=2 Stunden) an, im Abstand von 75 Sekunden bis zu 9 dieser Pakete zu senden, und schließt die Verbindung, wenn keine Antwort mehr kommt.

Das heißt, dass selbst dann, wenn dieser Mechanismus eingesetzt wird, eine TCP-Verbindung $7200 + 8 * 75 + \text{Ack-Timeout}$, also etwa 7800 Sekunden, also zwei Stunden und 10 Minuten stehen bleibt, bis sie als tot abgeräumt wird – mit anderen Parametern auch länger. Für Anwendungen mit Websockets, HTTP-Push-Nachrichten und dergleichen, insbesondere bei Chat-Servern, Newstickern und ähnlichem, wird man höhere Werte verwenden.

Das bedeutet, dass – je nach Implementierung und Server-Anwendung – ein Log-Eintrag zu einer Verbindung auf einem Server eine Zeitangabe tragen kann, die über zwei Stunden nach dem Ende einer IP-Adresszuweisung an die Gegenseite liegt. Die IP-Adresse kann da längst anderen zugewiesen worden sein.

Eine „sekundengenaue“ Protokollierung, wie in § 100g Abs. 5 Nr. 2 StPO gefordert, ist damit unvereinbar.

6.6.2.3 Retransmission Timer

6.6.2.3.1 Standard Für die Zeitabstände bei der Wiederholung von Paketen nach Paketverlust sind adaptive Verfahren ([RFC 9293](#) 3.8.3, [RFC 6298](#)) vorgeschrieben.

Vereinfacht beschrieben:

Wird der Empfang eines Datenpaketes nicht innerhalb einer gewissen Frist von der Gegenseite bestätigt, wird das Paket nach einer Sekunde erneut gesendet.

Wird der Empfang des Pakets auch dann nicht bestätigt, wird die Wartezeit jedesmal verdoppelt, das Paket also nach weitere 2, dann 4 Sekunden usw. wiederholt, bis eine zeitliche Obergrenze erreicht wird, aber der nicht mehr verdoppelt wird, und eine maximale Zahl von Wiederholungen erreicht ist, nach der die Verbindung als fehlerhaft abgebrochen wird, wenn keine Bestätigung eingegangen ist.

6.6.2.3.2 Beispiel Linux Die Werte `TCP_RTO_MIN` und `TCP_RTO_MAX` legen die Mindest- und Höchstdauer zwischen der Sendungswiederholung von TCP-Paketen fest und sind im Kernel hardcodet:

```
#define TCP_RTO_MAX ((unsigned)(120*HZ))
#define TCP_RTO_MIN ((unsigned)(HZ/5))
```

wobei `HZ` 1000ms entspricht. `TCP_RTO_MIN` entspricht damit 200ms, `TCP_RTO_MAX` 120 Sekunden. Der Abstand beginnt mit dem Minimalwert und verdoppelt sich jeweils, bis der Maximalwert überschritten ist.

Zusätzlich gibt

Variable	Default
<code>/proc/sys/net/ipv4/tcp_retries</code>	15

(Siehe dazu `man 7 tcp`) an, wieviele Wiederholungen eines Paketes maximal gesendet werden, bis eine Bestätigung der Gegenseite erfolgt oder die Verbindung abgebrochen wird.

Damit ergibt sich folgendes Zeitverhalten in Abbildung 6.1⁷.

Es wird eine Zeile mehr angegeben als Wiederholungen vorgenommen werden (16 statt 15), weil auch nach der 15. Wiederholung auch noch der Timeout abgewartet wird, bevor die Verbindung – an Stelle der 16. Wiederholung – abgebrochen wird.

⁷Quelle: pracucci.com

Abbildung 6.1: Zeitverhalten TCP-Retransmission

Wiederholung	Abstand ms	Gesamtzeit sek	Gesamtzeit min
1	200	0.2 sek	0.0 min
2	400	0.6 sek	0.0 min
3	800	1.4 sek	0.0 min
4	1600	3.0 sek	0.1 min
5	3200	6.2 sek	0.1 min
6	6400	12.6 sek	0.2 min
7	12800	25.4 sek	0.4 min
8	25600	51.0 sek	0.8 min
9	51200	102.2 sek	1.7 min
10	102400	204.6 sek	3.4 min
11	120000	324.6 sek	5.4 min
12	120000	444.6 sek	7.4 min
13	120000	564.6 sek	9.4 min
14	120000	684.6 sek	11.4 min
15	120000	804.6 sek	13.4 min
(16=Abbruch)	120000	924.6 sek	15.4 min

Wenn also eine Seite Daten sendet, deren Empfang die andere Seite nicht mehr bestätigt⁸, **dauert es – bei Default-Werten – noch über 15 Minuten, bis die Gegenseite die Verbindung als fehlerhaft ansieht, sie abbricht und schließt.**

Wenn aber der Log-Vorgang (bzw. dessen Zeitnahme) *erst nach Beendigung des Übertragungsvorgangs* erfolgt, kann die geloggte Uhrzeit bis zu 15 Minuten nach Ende der IP-Adresszuweisung liegen und damit schon die Zuweisung dieser Adresse an einen anderen – unschuldigen – Kunden liegen.

Es hängt dann stark davon ab, wie die Konfiguration beim Provider aussieht, und ob nach Ende der Zuweisung eingehende Transmissions (**falls** diese zufällig in den Zeitraum zwischen den Zuweisungen fallen) mit

- ICMP Destination Unreachable,

⁸Stromausfall, Rechner abgestürzt, Leitung unterbrochen, IP-Adresse entzogen, Angriff, ...

- ICMP Port Unreachable oder
- TCP RESET

beantwortet werden und dadurch die TCP-Verbindung sofort beendet wird.

6.6.3 SCTP

Das Stream Control Transmission Protocol (SCTP), [RFC 9260](#), unterstützt – im Gegensatz zu TCP – multi-homing, also die Verwendung *mehrerer* IP-Adressen auf der Seite eines Teilnehmers.

SCTP wird zwar nur selten und für wenige Anwendungen verwendet, von denen viele hier nicht relevant sind, weil sie nur firmenintern verwendet werden. Aber gerade WebRTC-Datenkanäle, wie sie in Webbrowsern verwendet werden, könnte hier wichtig sein, etwa wenn es um die Teilnehmer von Videokonferenzen (zur Begehung oder Verabredung von Straftaten) geht.

Die zur Verfügung stehende Zeit reichte nicht, um die Unterschiede zwischen TCP und SCTP in Bezug auf den Gesetzentwurf zu untersuchen.

6.7 Schicht 5

6.7.1 Funktion

Eine Rolle beim Zeitverhalten spielt auch das zugrundeliegende Anwendungstransportprotokoll (was ungefähr der Schicht 5 „Sitzung“ im ISO-OSI-Modell entspräche, wenn man meiner Zuordnung folgt, vgl. [4.2](#)).

Es gibt eine Fülle von Protokollen und unterschiedlichsten Eigenheiten, und die hier zur Verfügung stehende Zeit reichte bei weitem nicht, auch nur die wichtigsten (SMTP, IMAP, HTTP) zu betrachten, zumal diese mitunter nicht offengelegt sind (proprietäre Chats, Kunden-Apps usw.)

Deshalb werden hier nur exemplarisch die gängigen HTTP-Varianten betrachtet.

6.7.2 HTTP

6.7.2.1 HTTP/1.0

Bei HTTP/1.0, [RFC 1945](#), gilt das einfache Prinzip, dass für jede einzelne HTTP-Anfrage eine neue TCP-Verbindung geöffnet werden musste, gegebenenfalls mehrere

TCP-Verbindungen parallel.

Dies ist bezüglich des Loggings relativ unproblematisch, wird aber kaum noch verwendet, und kann zu Mehrdeutigkeiten führen, wenn derselbe Webseitenzugriff mit den HTTP-Anfragen einzelner Elemente (z. B. eingebettete Bilder, Style Sheets usw.) dann von unterschiedlichen IP-Adressen erfolgt, falls die während der Anfrage wechseln.

6.7.2.2 HTTP/1.1

HTTP/1.1, **RFC 2616**, sollte das Problem beheben, dass HTTP/1.0 schon bei einer einzelnen Webseite eine Vielzahl von TCP-Verbindungen (Style Sheets, Bilder, Fonts, usw.) benötigen kann und dadurch langsam wird und den Server stark belegt.

Deshalb wurden in HTTP/1.1 „persistent connections“ eingeführt: Das Abfrage-Verfahren gleicht HTTP/1.0, aber nach Übertragung der Antwort des Servers wird die TCP-Verbindung nicht geschlossen, sondern bleibt offen und wird einfach für die nächste HTTP-Anfrage weiterverwendet.

Das führte zu einem anderen Problem, nämlich dass eine langsame Resource die Übertragung aller anderen für die Dauer der Übertragung blockieren konnte.

Außerdem führt HTTP/1.1 das Wiederaufsetzen abgebrochener Verbindungen ein, damit man nicht wieder von vorne anfangen muss, sondern da weitermachen kann, wo man aufgehört hat, indem man mit dem Range-Header angibt, ab welcher Byte-Position man die Resource laden will.

Ab wann ist das Laden eines 50 MByte großen Kinderporno-Videos strafbar? Gilt schon ein Zugriff auf ein Stück von 1000 Byte, das für sich alleine gar nicht betrachtbar ist, als Straftat?

6.7.2.3 HTTP/2

HTTP/2, **RFC 9113**, führte dazu ein Multiplexing verschiedener HTTP-Requests über eine Verbindung ein, um ein gegenseitiges Blockieren auszuschließen. Weil Ressourcen dabei nicht warten müssen, bis andere bereit sind, aber bis sie fertig sind, wurde zusätzlich eine Priorisierung eingeführt.

HTTP/2 führt zur weiteren Beschleunigung außerdem „Server Push“ ein, bei der der Server nach einer Anfrage **spekulativ weitere Ressourcen senden kann, bevor sie angefragt wurden, um Zeit zu sparen, wenn er erwartet, dass diese heruntergeladen werden müssen.**

Beispiel: Man greift auf eine Webseite eines Unternehmens oder etwa des Deutschen Bundestages zu.

Es ist in der Regel klar, dass wer sich eine solche Webseite im Browser ansieht, auch das Firmenlogo und die Style Sheets herunterladen müssen, um die Seite anzuzeigen, was der Browser aber erst bei der Interpretation der HTML-Seite anzeigt.

Der Server kann deshalb beim Zugriff auf eine Webseite von sich aus das Firmenlogo und die Style Sheets „beilegen“, bevor sie angefragt werden.

Gilt der Empfang eines Kinderpornos als strafbar, wenn der Server ihn per „Server Push“ überträgt, ohne dass man ihn angefragt hat?

6.7.2.4 HTTP/3

HTTP/3, **RFC 9114**, unterscheidet sich fundamental von den früheren Versionen und ist deutlich anders konstruiert.

HTTP/3 beruht auf UDP, und die Funktionen von

- TCP
- TLS
- Multiplexing

werden in eine neue Anwendungsschicht „QUIC“ (**RFC 9000**) verschoben, um den TCP-Verbindungsaufbau und das TCP-Handshaking zu sparen. Gleichzeitig wird die Möglichkeit eingeführt, die IP-Adressen in der laufenden Verbindung zu wechseln.

Allgemeine Aussagen sind kaum möglich,

- weil die Logik dabei aus dem Betriebssystem in die Anwendungsschicht verschoben wird, und es **viele Implementierungen** gibt,
- die zur Verfügung stehende Zeit schlicht nicht reichte, dies im Kontext des Gesetzentwurfs zu untersuchen.

6.7.2.5 Caching, Proxy, Reverse Proxy, CDN

HTTP kann auch „um die Ecke“, über „Stellvertreter“ geführt werden, etwa wenn man

- Caches
- Proxies
- Reverse Proxies
- Content Delivery Networks

einsetzt.

Viele dieser Caches und Proxies geben ein „**Forwarded-for**“-Feld an, das aber nicht authentifiziert wird und **das keine Port-Angabe enthält**.

Es gibt Webserver, die diese Angabe übernehmen und statt der IP-Adresse des anfragenden Caches oder Proxies die IP-Adresse aus diesem Feld loggen. Damit können beliebige falsche IP-Adressen ins Log kommen.

6.7.2.6 Logging und Uhrzeiten

Keiner dieser Standards bzw. keines dieser HTTP-Protokollversionen definiert,

- wie und was zu loggen ist,
- dass oder wie genau die Uhr stimmen muss,
- welcher der für das Log maßgebliche Zeitpunkt einer Übertragung sein soll.

Was also ist der „Zeitpunkt“ einer HTTP-Anfrage?

- TCP- oder QUIC-Verbindungsaufbau?
- TCP- oder QUIC-Verbindungsabbau oder Timeout? Zeitpunkt der letzten Nutzung?
- Übertragung des HTTP-Request-Headers? Samt Body?
- Übertragung des HTTP-Response-Headers?
- Übertragung des HTTP-Response-Bodys?
 - Wenn die Applikation alles an das Betriebssystem geschickt hat,
 - wenn das Betriebssystem alle Daten per TCP versandt hat, oder
 - wenn der Client deren Empfang quittiert hat?

Auf den ersten Blick könnte man meinen „Ist doch egal“, denn weil der Client seine IP-Adresse über den gesamten Zeitraum der HTTP-Anfrage haben müsse, sei es doch egal, welchen genauen Zeitpunkt man aus diesem Zeitintervall herausgreift. Wie ich oben aber gezeigt habe, kann der Zeitpunkt auch außerhalb dieses Zeitintervalls liegen.

6.8 Applikations-/Serververhalten

6.8.1 Grundproblem

Das Grundproblem besteht darin, dass im Normalfall (außer zum Debuggen mit tcp-dump u.ä. Werkzeugen) die Zeiten, *wann IP-Pakete beim Server eingegangen sind, sie also – abzüglich der Zeit für das Routing – tatsächlich forensisch dem Absender zurechenbar*⁹ wären und Aufschluss über dessen Verwendung der IP-Adresse gäben, **nicht protokolliert** werden und im Allgemeinen schon quantitativ auch nicht protokolliert werden können.

Protokolle (Log-Dateien) werden von Anwendungsprogrammen (hier i.d.R. Serverprogramme) erstellt, die **nicht den Zeitpunkt protokollieren, zu dem der Absender das IP-Paket von seiner IP-Adresse verschickt hat, sondern wann der Server den Request empfangen oder abschließend bearbeitet hat – und der kann ganz erheblich abweichen.**

Das ist während normaler Nutzung des Internets unproblematisch, weil der Client ja über die ganze Dauer der Bearbeitung seine IP-Adresse hält, um die Antwort zu erfahren.

In zeitlicher Nähe zum Wechsel der IP-Adresse bzw. deren Neuvergabe kann dies aber dann, wenn die IP-Adresse zwischen Absenden der IP-Pakete des Requests und dem Absenden der Server-Antwort dazu führen, dass die IP-Adresse anderweitig vergeben wurde, und der Zeitpunkt, den die Serveranwendung loggt, schon dem neuen Inhaber der IP-Adresse angelastet wird.

6.8.2 Die fünf I/O-Programm-Modelle unter Unix

Die Programmschnittstelle von Unix und Unix-Derivaten wie Linux stellt 5 verschiedene I/O-Modelle zur Verfügung:

blocking I/O Die einfachste, aber sperrigste Methode: Jeder Systemaufruf blockiert das Programm, bis der Schreib- oder Lesevorgang vollständig abgeschlossen ist. Alle anderen Aufgaben müssen warten. Mehrere Verbindungen parallel können nur über mehrere Prozesse, Threads, Nebenläufigkeit von Routinen behandelt werden.

Der Schreib- oder Lesebefehl wird sofort und vollständig ausgeführt, und man muss warten, bis er beendet wird, was lange dauern kann.

nonblocking I/O Diese Methode ist ähnlich wie blocking I/O, führt aber jeden Schreib- oder Lesevorgang nur so weit aus, wie er *sofort* ausgeführt werden kann, ohne

⁹ andere, oben beschriebene Fehlerquellen und Manipulationsmöglichkeiten hier zum Zwecke des Disputes nicht betrachtet

den Prozess zu blockieren. Das Betriebssystem lässt den Prozess beispielsweise bei einem Leseaufruf nicht so lange schlafen, bis die gewünschte Menge an Daten eingegangen ist, sondern liest nur so viele Daten, wie in Eingangspuffer bereits liegen, was auch Null sein könnte.

Mehrere Verbindungen parallel können damit leicht behandelt werden, das Programm muss aber in einer Endlosschleife reihum alle Verbindungen ständig immer wieder abfragen.

Der Schreib- oder Lesebefehl wird sofort, aber möglicherweise nicht vollständig ausgeführt, sondern nur, soweit Daten bereits auf Vorrat sind bzw. noch Pufferplatz besteht.

asynchronous I/O Auch diese Methode ist ähnlich wie blocking I/O, blockiert den Prozess aber nach einem Aufruf nicht, sondern führt den Aufruf – etwa eine bestimmte Menge von Daten zu lesen – im Hintergrund aus und informiert den Prozess, der inzwischen andere Dinge tun konnte, sobald der Auftrag ausgeführt ist.

Der Schreib- und Lesebefehl wird vollständig, aber nicht sofort ausgeführt.

I/O multiplexing Der Prozess wartet (über select oder das neuere poll), bis es auf einer der Leitungen etwas zu tun gibt, und wird dann vom Betriebssystem geweckt und informiert, auf welcher Verbindung es etwas zu tun gibt, etwa weil Daten eingegangen sind, die zu lesen und zu verarbeiten wären.

Man wartet, bis einen das Betriebssystem darüber informiert, wo man einen Schreib- oder Lesebefehl ausführen soll, weil Daten eingegangen oder Platz für Ausgangsdaten ist.

signal driven I/O Hierbei handelt es sich um eine Art „Interrupt-gesteuerter“ Programmierung: Das Programm kann sich anderen Dingen und Aufgaben widmen, etwa intensiven Rechenaufgaben, ohne sich um I/O zu kümmern. Immer dann, wenn es etwas zu tun gibt, erhält das Programm vom Betriebssystem ein Signal, *wird unterbrochen*, um dann – z. B. non-blocking – die eingegangenen Daten usw. zu lesen, also zu reagieren.

Man macht etwas anderes, und das Betriebssystem unterbricht einen dabei, wenn wieder was zu tun wäre.

Für Interessierte am besten nachzulesen im Standardwerk Richard Stevens, UNIX Network Programming, **Volume 1, Third Edition**, insbesondere Kapitel 6.2.

Jede dieser fünf Methoden verhält sich unterschiedlich, was das Zeitverhalten, die Reaktionszeit zwischen Eingang eines IP-Paketes und abschließender Bearbeitung des Auftrags – und damit meist des Log-Zeitpunktes – betrifft.

Bei schwacher Auslastung des Servers dürften diese Unterschiede keine merkliche Rolle spielen, weil mit allen fünf Methoden „gefühlte sofort“ reagiert werden kann.

Ist die Maschine aber stark ausgelastet, die Netzwerklast hoch, die Zahl der Anfragen hoch, oder muss ein Prozess erst geweckt werden, der wegen Speicherknappheit in den Swap-Space ausgelagert wurde, **können sich ganz erhebliche Zeitunterschiede im Bereich vieler Sekunden oder noch mehr ergeben.**

6.8.3 Socket Activation

Weitere Zeitverzögerungen sind zumindest denkbar, wenn Prozesse erst über „socket activation“ gestartet werden, um zu reagieren. Früher machte man dies per inetd, heute meist über systemd.socket oder CGI.

Je nach konkreter Ausgestaltung und in Abhängigkeit davon, ob der Applikation der Listen Socket oder der Accepted Socket übergeben wird, können sich weitere, erhebliche Zeitunterschiede ergeben, wenn der Datenpuffer beim Start des Programms bereits gefüllt wurde und alle nötigen Daten schon übertragen wurden.

6.8.4 Cloud Computing

Ähnliche Effekte gibt es im Cloud Computing, wenn virtuelle Maschinen erst „on demand“ gestartet werden müssen, etwa vom Lastverteiler angestoßen.

Bei Amazon Web Services (AWS) gibt es neben virtuellen Maschinen auch den „serverless service“ („Lambda“), bei dem bei Eingang eines HTTP-Aufrufs (REST API) erst ein Docker-Container geladen und gestartet werden muss.

6.8.5 Apache und Nginx

Die zwei mit Abstand meistverwendeten Webserver im Internet sind Apache und Nginx.

Nginx basiert auf einem radikal vereinfachten Modell, das – quasi in einer Endlosschleife – ausschließlich non-blocking I/O verwendet und dadurch in der Lage ist, eine besonders hohe Zahl an Verbindungen gleichzeitig und sehr effizient zu bedienen.

Die Kehrseite ist, dass Nginx wegen dieses Modells keinerlei Aufgaben erfüllen kann, die den Programmablauf verzögern könnten, also keine Zusatzaufgaben wie PHP usw. erfüllen. Die Funktionalität von Nginx beschränkt sich deshalb auf

- das Ausliefern von Dateien
- die Funktion als Reverse-Proxy für alle anderen Aufgaben.

Apache hat verschiedene Modelle („Worker“) zur Auswahl, und kann asynchron oder mit Multi-Thread oder Multi-Prozess-Verteilung arbeiten.

Dadurch ist Apache deutlich „schwerfälliger“ und langsamer, kann dafür aber weitaus komplexere Aufgaben erfüllen, etwa PHP ausführen.

Wegen der Kürze der zur Verfügung stehenden Zeit **nicht mehr nachprüfen**, nur aus der Erinnerung entnehmen kann ich wesentliche Unterschiede beim Logging-Verhalten, die aus den unterschiedlichen I/O-Modellen resultieren (wäre auf Aktualität zu überprüfen):

- Apache verwendet für das Logging die Uhrzeit nach Eingang des Requests und vor dessen Bearbeitung
- Nginx nimmt keine Uhrzeit, und loggt den Request nach Abschluss der Bearbeitung mit der Uhrzeit zum Zeitpunkt des Loggens

6.9 Angriff

Ich skizziere in der Zusammenfassung einen Angriff, der

- bezüglich DHCP in DOCSIS-Netzen auf tatsächlich erfolgten Angriffen und einem durchgeführten Experiment im Jahr 2009 beruht,
- gedanklich auf TCP/HTTP ausgeweitet wurde,
- wegen der Kürze der Zeit aber nicht durch aktuelles Experiment verifiziert wurde.

Ich weiß deshalb nicht, ob sich DOCSIS-Router heute noch so verhalten wie 2009.

Für einige der Schritte sind Eingriffe in den Kunden-Router erforderlich.

Ziel: Herunterladen einer hinreichend großen Datei strafbaren Inhalts (z. B. Kinderpornovideo) von einem Server unter Austricksen der IP-Adressspeicherung.

Annahme 1: Wir nehmen an, dass unser Internet-Anschluss ein DOCSIS-Anschluss mit DHCP ist (Kabelnetz), wie etwa 25% der Haushaltsanschlüsse in Deutschland. (Alternativ: Glasfasernetz mit DHCP)

Annahme 2: Wir nehmen an, dass der Webserver ein Nginx ist (vgl. 6.8.5), wie 32% der Webserver im Internet.

Vorbereitung: Wir benötigen die Größe der Datei entweder in Byte oder als Video in Sekunden bekannt ist. In der Regel erfahren wir die Größe aber schon während Schritt 3 mit dem `content-length`-Header der Server-Antwort, was hier völlig genügt.

Schritt 1: Wir fordern per DHCP eine IP-Adresse beim Provider an und notieren die mitgeteilte Lease-Time. Der Provider loggt unsere Router-ID, die IP-Adresse, den Zeitpunkt der Zuweisung und die Lease-Time mit.

Schritt 2: Wir warten, bis die Lease-Time abgelaufen ist. Wir fordern keine Verlängerung an, geben die IP-Adresse auch nicht zurück, sondern bleiben einfach still.

Nach den Logs des Providers sind wir damit nicht mehr im Besitz der zugewiesenen IP-Adresse – können Sie technisch aber weiter verwenden, bis sie einem anderen Benutzer zugewiesen wird, weil erst dann die Zuordnung zum Router geändert wird. In der Praxis bedeutet das einige Sekunden bis Minuten.

Schritt 3: Wir senden einen HTTP-Get Request an den Webserver.

Der Webserver sendet uns die Datei, die per TCP in einzelne IP-Pakete aufgeteilt wird.

Kurz vor Ende der Übertragung, wenn noch so viele Bytes fehlen, wie in den Buffer passen, also ungefähr noch 11 oder 12 TCP-Pakete¹⁰, oder bei einem Video noch ein oder zwei Sekunden, **stellen wir unseren Ausgang auf stumm**.

Das heißt, dass wir zwar noch die letzten TCP-Pakete erhalten, sie aber nicht mehr quittieren.

Der Server geht deshalb von verlorenen Paketen aus und geht in den in 6.6.2.3 beschriebenen retransmission mode, um die verlorenen Pakete wiederholt zu senden.

Variante 1: Wird die IP-Adresse nicht innerhalb von 15,6 Minuten (vgl. 6.6.2.3) an einen anderen Kunden vergeben, bleiben wir „auf Empfang“, aber stumm, und erhalten alle Paket-Wiederholungen, bis der Server schließlich die Verbindung per Timeout abbricht und loggt.

Die auf dem Server geloggte Uhrzeit liegt mindestens 15 Minuten nach dem Ende der Leasetime und der gelogten IP-Adresszuweisung.

Der Provider würde auf eine polizeiliche Anfrage eine Negativauskunft erstellen, weil die Adresse nicht zugewiesen war.

Variante 2: Die IP-Adresse wird innerhalb dieser 15,6 Minuten Retransmission an einen anderen Kunden vergeben.

Je nachdem, wie Router und Firewall dieses Kundens als neuem Inhaber konfiguriert sind, kommen zwei Untervarianten vor.

Entweder antworten seine Systeme mit ICMP Destination Unreachable, ICMP Port Unreachable, oder TCP Reset, womit die Verbindung abgebrochen wird.

¹⁰Die Werte – minimum, default, maximum – finden sich unter Linux in `/proc/sys/net/ipv4/tcp_wmem`, die normalerweise auf 4096 16384 4194304 stehen, der default-Wert also bei 16384

Die Verbindung kann damit bis zu 120 Sekunden (bei Paketverlust auch länger, z. B. 240 Sekunden) nach Zuweisung an den neuen Kunden bestehend und erst dann geloggt werden.

Antworten dessen Systeme gar nicht (Firewallregel „Drop“), kann es sogar bis zu 15,6 Minuten dauern.

In beiden Fällen würde der Provider auf Anfrage Name und Anschrift des neuen Inhabers beaskunften, obwohl der nichts gemacht hat.

Zu entdecken und nachzuweisen wäre dies nur, wenn – präzise Uhrzeiten vorausgesetzt – der Provider neben Name und Anschrift auch die Uhrzeit der ersten Adresszuweisung mitteilt, der Webserver auch die Dauer der gesamten Bearbeitung mitloggt und die Polizei auch diesen Wert hat. Dann lässt sich aus Dauer und Endzeitpunkt rückrechnen, dass der HTTP-Request gestellt worden sein muss, bevor die IP-Adresse dem neuen Nutzer zugewiesen worden war.

In der Vorratsdatenspeicherung von 2009 wurde weder das eine, noch das andere mitgeteilt.

7 Ergänzende Beispiele für Angriffe gegen die Authentizität von IP-Adressen

7.1 Angriffe gegen Autonome Systeme/BGP

Das Bundesministerium des Inneren betreibt das **Autonome System AS49234**, zu dem auch der IP-Adressbereich 193.17.232.0 - 193.17.247.255 des Deutschen Bundestags gehört. Diese Routen können z. B. mit

```
whois -h whois.radb.net -- '-i origin AS49234'
```

abgefragt werden. Darin findet sich

```
route:          193.17.240.0/21
descr:          Deutscher Bundestag
origin:         AS49234
mnt-by:         BSI-IVBB
mnt-routes:     DFN-MNT {193.17.240.0/23^+}
created:        2009-07-31T13:41:37Z
last-modified:  2015-05-04T08:36:48Z
source:         RIPE
remarks:        *****
remarks:        * THIS OBJECT IS MODIFIED
remarks:        * Please note that all data that is generally regarded as personal
remarks:        * data has been removed from this object.
remarks:        * To view the original object, please query the RIPE Database at:
remarks:        * http://www.ripe.net/whois
remarks:        *****
rpki-ov-state:  valid
```

Die Abfrage etwa des MX-Records bestätigt dies.

Ergänzend können wir per leichtem Phishing etwa einen Abgeordneten oder dessen Büro – etwa über ein eingebettetes Bild o.ä. – dazu bringen, auf einen harmlosen

Webserver zuzugreifen, dessen Logs wir lesen können, um an dessen konkrete (NAT-) IP-Adresse zu kommen.

Wir suchen uns nun

- irgendeinen Social Media-Server, ein Forum oder ähnliches, oder
- eine vom FBI hochgenommene und zur Fahndung weiterbetriebene Kinderpornoseite

bei der wir einen Router auf der Route zum Bundestagsnetz per BGP angreifen oder anderweitig hacken können (oder dessen Personal bestechlich ist), und jubeln diesem Router für einige Minuten oder Stunden eine falsche BGP-Route unter, die 193.17.240.0/21 umroutet oder durch einen Tunnel lenkt.

Wir können damit gegenüber dem Server mit einer IP-Adresse des Deutschen Bundestags auftreten, und

- schlimme Dinge posten oder
- Kinderpornos herunterladen und sicher sein, dass das FBI die Logs prüft und die Zugriffe findet und an die deutschen Behörden weitermeldet.

Währenddessen wäre aus dem Netz des Bundestags eine Störung nicht zu bemerken, dessen Internet läuft normal weiter. Es bestünde kein Ansatzpunkt für das Erkennen einer Fälschung.

7.2 Angriffe gegen den Internetprovider

7.2.1 Von innen

7.2.1.1 Innentäter

Auch Internetprovider haben politische Aktivisten, Terroristen, Geheimdienstmitarbeiter, Korruption, Hass unter ihren Mitarbeitern, und es ist naheliegend und kommt auch tatsächlich vor, dass diese ihre Stellung missbrauchen, um Dritten, politischen Gegnern, zu schaden.

Ich selbst habe in meiner beruflichen Tätigkeit als Security und Compliance Officer solche Angriffe in der IT-Industrie beobachtet und aufgedeckt. In Abschnitt [22.2.4](#) werde ich aufzeigen, wie ein Girokonto bei der Deutschen Bank durch einen unbefugten Innentäter eigenmächtig als gekündigt eingetragen und damit sabotiert wurde.

7.2.1.2 Fälschung der RADIUS-Nachrichten

DSL- und manche andere Router¹ kommunizieren zur Prüfung der Benutzeranmeldung per RADIUS-Protokoll („Remote Authentication Dial-In User Service“, RFC 2865 und RFC 2866) mit einem RADIUS-Server (Zweck AAA = Authentication, Authorization, Accounting).

In diesem Fall sind die RADIUS-Logs die Daten, die zur IP-Adressspeicherung herangezogen werden können und müssen.

Obwohl RADIUS verschlüsselt verwendet wird, ist es ein altes, sehr einfaches und nicht sehr sicheres Protokoll, und wird oft noch weniger sicher verwendet, als es von seiner Konstruktion her ist. Die Sicherheit beruht normalerweise darauf, dass beim PAP- (oder seltener CHAP-)Verfahren das übertragene Benutzerpasswort symmetrisch verschlüsselt oder gehasht wird, aber viele Internetprovider benutzen gar keine Passworte mehr, sondern verwenden direkt die Anschlussnummer des Anschlusses, an den der Telefondraht zur Kundenwohnung angelötet ist. Man erkennt dies daran, dass Benutzername und Passwort egal sind und man stattdessen beliebige Eingaben, wie etwa nur einen Punkt, machen kann.

Die Sicherheitsmechanismen im RADIUS-Protokoll und dessen Bedrohungsmodell

- sind darauf ausgelegt, den Router vor falschen Antworten des Servers (Replay-Attacke u.ä.) zu schützen, also unerlaubte Logins zu verhindern.
- Sie wirken aber deutlich schwächer oder nicht gegen das Gegenteil, dem Logging des Radius-Servers einen Anmeldevorgang vorzutäuschen, den es gar nicht gab.

Im Normalfall würde man darin keinen Zweck und Vorteil, und deshalb keinen Angriff sehen.

Haben wir aber eine IP-Adressspeicherung zum Zweck der Strafverfolgung, dann wird es plötzlich zum Angriffsziel und Zweck, die Nutzung von IP-Adressen durch Kriminelle, Hacker und Agenten Dritten anzuhängen und dazu falsche Log-Einträge zu erzeugen.

So schützt der Authentifikationsmechanismus von RADIUS gegen Replay-Attacken gegen die Antworten des Servers an den Router, aber nicht oder nur eingeschränkt gegen die Meldungen des Routers an den Server.

Es wäre, je nach Konfiguration, Implementierung und Gerät, durchaus denkbar, dass ein Administrator oder Hacker, der Kenntnis des Shared Secrets hat, womöglich sogar ohne Kenntnis in Verbindung mit Replay-Attacken, die Nachrichten des Routers an den RADIUS-Server fälscht, um bei einer bestehenden Verbindung dem Server vorzugaukeln, dass die Verbindung mit dem Kunden A beendet und die Adresse einem

¹insbesondere beim Einsatz von PPP

anderen Kunden B zugewiesen worden sei, obwohl weiterhin A die Verbindung nutzt, also Log-Einträge über Adresszuweisungen fälscht.

Mit anderen Worten:

Die Log-Einträge der Provider über die Vergabe von IP-Adressen sind forensisch kaum nutzbar, weil sie nicht authentisch sind.

Es ist ein typischer Fall von stillschweigend angenommenen, implizit unterstellten Sicherheitseigenschaften, die aber nicht spezifiziert sind und nicht Teil des zugrundeliegenden Bedrohungsmodells waren.

So kann man nicht an die Sache heran gehen.

7.2.1.3 Fälschung der RADIUS-Logs

Weitaus schlichter und einfacher wäre es aber für einen Administrator oder Hacker mit Zugang zum RADIUS-Server falsche Log-Einträge zu erzeugen oder echte Einträge zu ändern, und eine Adresszuweisung vorzugaukeln, die nicht stattgefunden hat, etwa

- um Straftaten – Download Kinderpornos – zu begehen und anderen anzuhängen,
- Leuten vorsätzlich zu schaden, indem er durch sie begangene Straftaten vor-täuscht.

denn zu den – bisher kaum beachtlichen, aber hier gefährlichen – Schwächen des RADIUS-Protokolls zählt, dass die Daten nach Ankunft am RADIUS-Server über keinerlei Authentifikationsdaten mehr verfügen.

RADIUS-Logs tragen keinerlei Informationssicherheit und beruhen allein auf der Systemsicherheit der beteiligten Geräte. Und die ist in der Praxis schlecht – man braucht es bisher auch nicht besser.

Für eine forensische Verwendung ist das nicht ausreichend.

7.2.1.4 Manipulation der Routen/Destination NAT

Wer – Insider oder Hacker – Zugriff auf das Routing eines Providers nehmen kann, kann ohne weiteres eine Source-abhängige Route eintragen.

Er könnte damit dafür sorgen, dass eine IPv4-Adresse w.x.y.z, die gerade dem Kunden A zugeordnet ist und von diesem auch nachweislich benutzt wird, etwa in social media, zum Mail-Zugriff, Videokonferenzen und so weiter, **dann, wenn die IP-Pakete von einem bestimmten Kinderpornoserver kommen, stattdessen an den Kunden B umgeleitet werden.**

Ein analoger Angriff wäre mit der Umleitung einer IPv6-/128-Adresse möglich.

Der Kunde A würde davon nichts merken, weil sein Internet-Zugang ganz normal weiterfunktionieren würde².

Kommt es aber zu einem Strafverfahren, würde die IP-Adressspeicherung auf den Kunden A zeigen.

Alle Gegenwehr wäre aussichtslos, weil es genug Beweise aus Social Media, vom Mailserver und so weiter gibt, dass der Kunde A tatsächlich in diesem Zeitraum die IP-Adresse w.x.y.z genutzt hat.

Gericht und Staatsanwaltschaft würden es durch die nachweisliche tatsächliche Nutzung der IP-Adresse als erwiesen ansehen, dass Kunde A zu diesem Zeitpunkt Nutzer der IP-Adresse und folglich der Täter war.

7.2.2 Von außen

7.2.2.1 Angriffe gegen die Router

Dies wurde bereits oben in Abschnitt 5.3 beschrieben.

7.2.2.2 Angriffe gegen BGP

Dies wurde bereits oben in Abschnitt 5.2 beschrieben.

7.2.2.3 Angriff auf Kundenleitungen

Stromdiebstahl ist ein verbreitetes Phänomen. Nachbarn, Anwohner klemmen sich auf fremde Stromleitungen mit auf.

Verwendet ein DSL-Provider, wie es viele tun, keine Passworte zur Benutzerauthentifikation, sondern die Leitungsnummer, mit der die Telefonleitung am DSLAM angebunden ist, kann etwa ein Nachbar im Keller, oder, wenn die Telefonleitungen außen verlegt sind, auch ein Fremder die Leitung unterbrechen und sich selbst auf die Verbindung aufklemmen. Wenn dann keine Authentifikation erforderlich ist, hält ihn der Provider für den Kunden, an den der Anschluss vergeben ist, und protokolliert dies entsprechend.

In Fachmedien wurde damals ein Fall beschrieben, in dem jemand, der „zum Blumen gießen“ einen Schlüssel für die Wohnung seiner oft verreisten Nachbarin hatte, sich in

²Außer wenn er im IPv4-Fall selbst auf denselben Kinderpornoserver zugreifen würde, wir gehen hier aber von einem ehrlichen, rechtstreuen Kunden aus.

deren Abwesenheit immer deren Internet-Router „ausborgte“ und in seiner Wohnung anschloss, und ihn dann immer unbemerkt und rechtzeitig wieder zurückbrachte, und damit diese Nachbarin in den Verdacht seiner Taten geriet. Ihr Glück war, dass sie ein Alibi hatte.

7.2.2.4 Fake-Anschlüsse

Ich kann mich aus meiner Tätigkeit in der Vorratsdatenspeicherung 2009 und der Konzernsicherheit erinnern, dass es einige Fälle gab, in denen es Rückmeldungen der Polizei gab, dass die zu einer IP-Adress-Anfrage beauskunfteten Anschriften nicht stimmen könnten, weil die Anschriften gar nicht existierten oder da nur jemand anderes wohne.

In einem Fall hatte die Stadt Häuser schon vor Jahren den Straßen neu zugeordnet und die Hausnummern neu vergeben, nachdem man bei Renovierungsarbeiten der Häuser *die Hauseingänge auf die gegenüberliegende Hausseite verlegt hatte*, ohne dies den Providern zu melden. Die Verträge liefen mit den alten Kunden und alten Anschriften einfach weiter, die Bestandsdaten waren damit aber veraltet und falsch, und gaben dadurch falsche Anschlussinhaberadressen an, in einem Fall sogar mit einem sehr ähnlichen Namen, den man für lediglich einen Schreibfehler gehalten hatte.

In anderen Fällen hatten sich Leute illegal mit oder ohne Wissen der Vorbesitzer der Kabelrouter und Zugangsdaten bei deren Wegzug oder Abwesenheit vorübergehend oder dauerhaft bemächtigt und teils die monatlichen Kosten weiter bezahlt, einen Weiterbestand des Vertrags vorgegaukelt, ohne dass den Vorbesitzern bewusst war, dass ihr Anschluss weiter angemeldet und in Gebrauch war.

Auch seltsame Fälle von – freiwilligen und unfreiwilligen – Überlassungen kamen vor.

Die Frage, wie die Bestandsdaten aktuell und richtig zu halten wäre, kommen im Entwurf nicht vor.

7.3 Angriffe gegen den Home-Router

7.3.1 Bedrohungslage

Golem: Chinesische Hacker kapern massenhaft Router und IoT-Geräte

Die kompromittierten Netzwerkgeräte werden laut Behördenwarnung missbraucht, um darüber Cyberangriffe auszuführen und Traffic zu verschleiern.

Heise: Warnung aus UK: Russische Cyberkriminelle kapern Router zum Passwort-Klau

Das britische Cybersicherheitszentrum NCSC meldet Cyberangriffe auf Internetrouter. Die Bande aus Russland ist auch mehrerer Attacken in Deutschland verdächtig.

Cyberkriminelle mit Verbindungen zur russischen Regierung kapern gängige Internetrouter, um Passwörter für E-Mail-Konten und andere Online-Dienste zu stehlen. Davor warnt Großbritanniens Nationales Zentrum für Cybersicherheit (NCSC) in einer am Dienstag veröffentlichten Studie.

Die britischen Cybersicherheitsexperten gaben bekannt, dass mutmaßliche russische Angreifer sich Zugang zu Routern von Herstellern wie MikroTik und TP-Link verschaffen, um den ausgehenden Internetverkehr über von ihnen kontrollierte Server umzuleiten. Die Betroffenen seien durch den Diebstahl von Zugangsdaten, Datenmanipulation und umfassendere Sicherheitslücken gefährdet.

Heise: Microsoft warnt vor chinesischer Cyberspionage gegen kritische US-Infrastruktur

Eine Gruppe chinesischer Cyberspione hat kritische Infrastrukturen der USA infiltriert, meldet Microsoft. Dabei handelt es sich um die staatlich gestützte Hackergruppe "Volt Typhoon", die sich auf die Sammlung von Daten und Zugangsinformationen spezialisiert.

[...]

Volt Typhoon ist nach Angaben Microsofts seit Mitte 2021 aktiv. Für ihre Spionageaktivitäten nutzt die Gruppe vor allem bereits im System vorhandene Tools für ihre Zwecke – diese Vorgehensweise ist als Living off the Land (LotL) bekannt. Dabei werden Standard-Router etwa in kleinen Büros oder an Heimarbeitsplätzen angegriffen, um in das Netzwerk zu gelangen.

DIE WELT: Verfassungsschutz warnt vor russischen Hackerangriffen auf beliebte Router

Das Bundesamt für Verfassungsschutz (BfV) warnt gemeinsam mit Partnerdiensten vor russischen Hackerangriffen auf Internetrouter. Die Gruppe APT28 – auch unter den Namen Fancy Bear oder Forest Blizzard bekannt – habe weltweit anfällige Internetrouter des Herstellers TP-Link infiltriert, um militärische Informationen, Regierungsinformationen oder Informationen über kritische Infrastruktur (KRITIS) zu erhalten.

Der Verfassungsschutz rechnet die Gruppe dem russischen Militärgesamtdienst GRU zu. Insgesamt seien mehrere tausend öffentlich auffindbare TP-Link-Geräte angegriffen worden. In Deutschland seien circa 30 verwundbare Geräte festgestellt worden. „Dabei konnte bereits in einzelnen Fällen die Kompromittierung durch APT28 bestätigt werden.“ Die Betreiber hätten Empfehlungen bekommen, um sich vor weiteren Angriffen zu schützen, viele der Router seien ausgetauscht worden.

BILD: 14.000 Router gekapert – ist Ihrer auch dabei?

Alarm im Homeoffice! Internet-Gangster haben weltweit Tausende Router angegriffen und zu einem gefährlichen „Botnetz“ zusammengeschaltet. Die fiese Software namens „KadNap“ schleicht sich unbemerkt auf Ihr Gerät – und macht es zur Waffe für Kriminelle!

Das Tückische an der neuen Hacker-Welle: Man merkt absolut nichts! „KadNap“

schleicht sich über Sicherheitslücken auf den Router. Die Malware ist so programmiert, dass sie die Verbindung zu den Gangster-Servern perfekt tarnt. Herkömmliche Sicherheits-Checks versagen meist kläglich. Laut „Ars Technica“ sind bereits über 14.000 Geräte weltweit infiziert. Bisher hat es vor allem Asus-Geräte getroffen, andere Router sind aber ebenfalls in Gefahr. Gute Nachricht: Fritz! teilte BILD mit, dass Fritz!Boxen sicher sind.

7.3.2 Malware und Fehlkonfiguration

Der naheliegendste Angriff auf Heimrouter ist, darauf Malware zu installieren oder sie in entscheidenden Details umzukonfigurieren, beispielsweise die Konfigurationsseite oder ssh-Zugänge aus dem Internet zugänglich zu machen, Firewallregeln zu ändern und dergleichen.

7.3.3 Andere Nameserver, DNS-Einträge

Man kann in gewissen Grenzen³ Angriffe unternehmen, indem man auf dem Router einen anderen DNS-Resolver einträgt oder zusätzliche DNS-Einträge vornimmt, um Passworte abzugreifen oder – auch aus dem LAN über manipulierte SRV-Records – Verkehr über Server der Angreifer umzuleiten, und von dort aus beispielsweise weitere Malware in das Netz einzubringen.

7.3.4 VPN-Tunnel

Fast jeder moderne Heim-Router oberhalb der einfachsten Grundausstattungsgeräte unterstützt eine oder mehrere Varianten von VPN-Tunneln, in der Regel in zwei Grundkonfigurationen:

- Als Client gegenüber einem Unternehmens-LAN, um möglichst transparent und komfortabel aus dem „Home-Office“ zu arbeiten (seit der Corona-Krise Standard-Ausstattung von Heimroutern)
- Als Server, damit Bewohner der Wohnung auch von unterwegs mit Notebooks, Tablets, Handys
 - auf das Wohnungs-LAN und damit auf Geräte wie NAS-Server, „Smart-Home“-Geräte, Telefonanschlüsse zugreifen zu können,
 - aus dem Ausland Internet-Zugriffe über den Heimrouter leiten können, um beispielsweise auf ARD und ZDF mit deutschen IP-Adressen zugreifen zu

³Bei der heute üblichen weiten Verbreitung von HTTPS/TLS nicht mehr so einfach, aber immer noch üblich

können oder um sich nicht aus unsicheren Hotelnetzen ausspionieren zu lassen.

Trägt sich nun ein Angreifer einfach einen VPN-Zugang auf dem Router ein, kann er damit – das ist ja ein Hauptzweck solcher Zugänge – von außen mit der IP-Adresse des Anschlusses im Internet kommunizieren.

Nur die wenigstens Internet-Kunden sind befähigt und in der Lage, einen fremden VPN-Zugang in der Konfiguration zu erkennen, **und** schauen dort regelmäßig nach.

Hand aufs Herz: Wie oft prüfen Sie zuhause, ob auf Ihrem Internet-Router VPN-Einträge existieren, die dort nicht hingehören?

Das zu erkennen wird aber noch schwerer, oder, je nach Routersoftware und VPN-Technik sogar unmöglich, wenn kein falscher VPN-Eintrag erstellt wird, sondern der Anschlussinhaber selbst einen VPN-Eintrag – etwa auf Reisen – nutzt und eingetragen hat, und der Angreifer die VPN-Zugangsdaten von dessen Notebook stehlen konnte, und damit einen normalen, gewollten VPN-Zugang benutzt.

Das ist im Normalgebrauch praktisch kaum, nicht oder nur durch Zufall⁴ zu bemerken und erlaubt unbefugten Dritten, dauerhaft mit der IP-Adresse des Anschlusses zu surfen.

7.3.5 Manipulation des Routings

Ein Angreifer kann durch quellenabhängiges Routing dafür sorgen, dass Teile des Internets unterschiedlich behandelt werden.

Beispiel:

Der Angreifer möchte Kinderpornos verteilen und muss dazu *aus dem Internet erreichbar sein*. Mit einem gewöhnlichen VPN-Zugang ist das noch nicht möglich.

Er greift dazu den Home-Router von Tante Erna an und kann das mit weiteren Maßnahmen erreichen:

7.3.5.1 Port per Static NAT routen

Er kann einen Port oder Port-Bereich per Destination NAT auf seine VPN- oder andere öffentliche Adresse routen.

⁴ Etwa wenn Angreifer und befugter Benutzer gleichzeitig denselben VPN-Tunnel verwenden wollen, die verwendete Methode aber nur einen Nutzer gleichzeitig zulässt. Bei Nutzung von Wireguard würde eine solche Kollisionen auffallen, während bei OpenVPN Konfigurationen möglich sind, in denen Angreifer und befugter Nutzer störungsfrei nebeneinander agieren können.

7.3.5.2 Quellenabhängiges Routing

Er kann Routen eintragen, wonach nur Verkehr, der von einem bestimmten Server, oder aus einem bestimmten Netz kommt (Pornoserver, Darknet, usw.) durch den VPN-Tunnel an ihn weitergeleitet wird, während Tante Erna ungestört weiter im Internet surfen und die ZDF Mediathek schauen kann.

7.3.5.3 IPv6-Adresse

Der Angreifer kann eine IPv6-/128-Adresse in den VPN-Tunnel oder per Destination NAT an eine andere offizielle IP-Adresse routen, und bekommt damit eine eigene, ganz offizielle, auch servertaugliche und nameservereintragsfähige Internet-Adresse verwenden.

7.3.5.4 Tante Erna ist dran

Ermittelt die Polizei deswegen, ist Tante Erna dran. Und neben den Logs des Providers gibt es noch reichlich Logs von anderen Diensten, bei denen sie eingeloggt war, die „beweisen“, dass sie zu diesem Zeitraum

- ihr Internet tatsächlich benutzt hat,
- diesen Adressebereich hatte.

Leugnen zwecklos, auch ihr beschlagnahmter Computer beweist, dass sie im fraglichen Zeitraum zuhause war, den Computer benutzt hat und diese IP-Adressen verwendet hat.

Tante Erna geht in den Knast.

7.4 Angriffe gegen das Heimnetz

Das typische private Heimnetz ist in der Regel durchseucht von Malware und Backdoors. Die Software ist veraltet und löchrig, weil Updates nicht regelmäßig und zeitnah eingespielt werden, die Rechner von Laien gewartet werden, und sie regelmäßig weit über ihre vertretbare Nutzungsdauer hinaus verwendet werden, auch wenn es Updates und Patches schon längst nicht mehr gibt.

Die Geräte werden von Menschen benutzt, die keine Ausbildung, keine Sachkunde haben – Alte, Kinder, bildungsferne Schichten, Leute, die für so etwas schlicht keine Zeit haben.

Dazu kommen Geräte der Kategorie „Smart Home“, die nicht wartbar sind, die nicht unterstützt werden, oder deren Hersteller nicht mehr existiert oder anonym im Ausland sitzt.

Und trotzdem unterstellt dieser Staat, der nicht einmal seine eigenen Schulen, Universitäten, Gerichte, Stadtverwaltungen sauber und frei von Malware halten kann, dem ständig die Systeme zusammenfallen, dessen Sicherheitskonzept in Berlin seit rund 10 Jahren nicht mehr gepflegt wurde, **dass bei Privatnetzen der Anschlussinhaber immer für alles verantwortlich wäre, was mit der ihm gerade zugewiesenen IP-Adresse passiert.**

Das ist ein Witz.

7.5 Angriffe gegen das Betriebssystem

Privatanwender, insbesondere von Windows-Rechnern und Android- und iOS-Geräten, haben längst die Hoheit und Kontrolle über ihre eigenen Geräte verloren.

Nicht nur sind die Systeme oft von Malware und Backdoors durchseucht, und damit Spielball und Verfügungsmasse von Angreifern und Dritten, sondern die Hersteller selbst, allen voran Microsoft, Google, Apple, haben längst die Hoheit, die volle Kontrolle über die Rechner.

Microsoft etwa nimmt sich heraus, auch die Privatdateien, die auf dem Rechner gespeichert sind, zu untersuchen. Dateien, Passwörter und so weiter landen schneller in der Cloud, als man sehen kann, wenn Anwendungen nicht ohnehin schon direkt in der Cloud landen.

Die Hersteller können beliebige Änderungen am Rechner vornehmen, den Nutzern beliebige Software oktroyieren.

Wie kommen Sie auf die Idee, dass die Nutzer eines Computers noch eine ihnen zurechenbare wesentliche Verantwortung für das hätten, was von ihrem Computer aus geschieht?

7.6 Angriffe gegen die Applikation

7.6.1 Web-Browser

Die heute längst führende Applikation ist der Web-Browser. Nichts geht mehr ohne, alles geht mit Web-Browser. Web-Browser sind mit Javascript und anderen Techniken längst zu einer eigenen Softwareplattform geworden, und Betriebssysteme wie ChromeOS haben als zentrale Funktion, den Browser zu betreiben.

Heise: 271 Firefox-Lücken dank Mythos-KI geschlossen: Durchbruch für IT-Sicherheit?

Allein im April 2026 wurden in einem einzigen Update 271 – teils schwerste – Sicherheitslücken im Browser Firefox geschlossen, einem der meistgenutzten. Diese Fülle an Sicherheitslücken waren nur mit Hilfe des KI-Modells Claude Mythos Preview von Anthropic gefunden worden.

Wieviele gibt es noch?

Wieviele neue kommen hinzu?

Wann immer ich an meinem Blog etwas an Datenformaten ändere – beispielsweise webp statt JPEG als Bilddateiformat, oder avif statt webp, bekomme ich Zuschriften von Lesern, dass sie mein Blog nicht mehr vollständig anzeigen können. Frage ich nach, stellt sich oft heraus, dass betroffene Leser noch 8 oder 10 Jahre alte Browserversionen einsetzen, weil sie uralte Computer verwenden, auf denen sich neuere Versionen nicht mehr installieren lassen – oder sie das gar nicht wollen.

Dazu kommen die normalen Funktionen des Browsers, die per se schon „unsicher“ sind.

Jederzeit kann Ihnen jemand eine harmlos wirkende Webseite unterjubeln, die

- geschrumpft auf die Größe eines Pixels,
- versteckt hinter anderen Seitenelementen wie Bildern oder Layern,
- außerhalb des sichtbaren Bereichs,
- versteckt in Javascript-Code

Tausende von Kinderpornodateien herunterladen – *ohne dass Sie etwas davon bemerken.*

Verfolgt die Polizei das zurück und beschlagnahmt sie den Rechner, wird sie „zu Beweis“ die Bilder sogar auf dem Rechner im Browsercache finden.

Das reicht, um Sie des Besitzes von Kinderpornographie in großem Umfang zu verurteilen, obwohl Sie nichts gemacht haben und nicht wissen, wie es dazu kommen konnte.

Ein Strafverteidiger würde wohl sogar dazu raten, ein (falsches) Geständnis abzulegen, um die Strafe in aussichtsloser Lage zu mildern.

Solche Angriffe werden mit Sicherheit als moderne Fortsetzung der „Honigfalle“ politisch und geheimdienstlich eingesetzt, um unerwünschte Leute abzuschießen und kaltzustellen (Stichworte: Tauss, Edathy). Solche Angriffe sind gar kein Problem für moderne KI-Systeme und werden mit Sicherheit auch als „Crime as a Service“ angeboten.

Im Prinzip kann man damit jede x-beliebige Person erledigen.

Bedenkt man, dass auch wüstestes Verleumdung und üble Nachrede zu den Methoden der aktuellen Berliner Politik gehören, kann man sich auch vorstellen, wer solche Angriffe in Auftrag geben würde.

7.6.2 Beispiel: Signal

Es wäre zum heulen, wenn man nicht so lachen müsste: Die Russen haben sich in Signal-Konten der Regierung gehackt.

BILD: Hacker-Angriff auf Abgeordnete, Beamte, Journalisten

In den vergangenen Tagen waren im Deutschen Bundestag mehrere Fälle von Abgeordneten bestätigt worden, deren Signal-Konten kompromittiert sind. Im Zentrum der Attacken: hochrangige Politiker, sogar Bundestagspräsidentin Julia Klöckner (53, CDU) ist betroffen. Nach der SPD meldete auch die Linke mehrere gehackte Accounts.

Wie weit der Schaden reicht, ist unklar. Laut „Spiegel“ war Klöckner Teil einer sensiblen Signal-Gruppe des CDU-Präsidiums – gemeinsam mit Kanzler Friedrich Merz (70, CDU).

DIE ZEIT: Warum Politiker derzeit so viel Angst vor Spionage haben wie noch nie

»Es ist davon auszugehen, dass zahlreiche Signal-Gruppen im parlamentarischen Raum derzeit von den Angreifern nahezu unbemerkt ausgelesen werden.« Der Satz braucht einen Moment, bis er in seiner Tragweite einsickert: Unbekannte lesen offenbar mit, was im politischen Berlin zwischen Abgeordneten ausgetauscht wird.

Der Satz steht in einem 20-seitigen Sicherheitshinweis an die Fraktionsvorsitzenden und Bundesgeschäftsstellen der Parteien, den das Bundesamt für Sicherheit in der Informationstechnik (BSI) und das Bundesamt für Verfassungsschutz (BfV) vergangenen Dienstag verschickt haben.

DIE ZEIT: Bundesanwaltschaft übernimmt Ermittlungen zu Signal-Phishingangriffen

In den vergangenen Tagen waren im Bundestag mehrere Fälle von Phishing gegen Abgeordnete bekannt geworden. Den Betroffenen wurde dabei vorgespielt, sie würden vom Signal-Support kontaktiert. War die Masche erfolgreich, hatten die Angreifer Zugriff auf die Signal-Chats und Gruppen sowie dort geteilte Fotos und Dateien. Sie können sich bei Signal auch als die Person ausgeben, deren Konto gehackt wurde.

Machen Sie sich klar, was hier abläuft:

Ein und dieselbe Bundesregierung, die es selbst nicht einmal in Geheimangelegenheiten, mit Millionenbudget, mit BSI, BfV, BND, Polizei, Geheimschutz, SINA-Boxen, beliebig vielen Experten und Beratern, jeder Abgeordnete mit eigenem Mitarbeiterrudel, schafft, ihren Hosen oben zu behalten, legt einen Gesetzentwurf vor, in dem jedem Haushalt, der Oma, dem Analphabeten, der Mutter mit

10 Kindern, dem Sozialhilfeempfänger unterstellt wird, für die ihm zugewiesenen IP-Adressen in vollem Umfang verantwortlich zu sein und selbst für deren Sicherheit sorgen zu müssen.

Wie erklären Sie das?

7.7 Angriffe gegen den Server

7.7.1 Logs fälschen

Der einfachste Angriff ist, ganz schlicht und einfach die Log-Dateien des Servers zu fälschen. Entweder direkt mit einem Texteditor oder Anhängen von Textzeilen (Shell: echo » ...) oder Verwenden von syslog o.ä.

Mir ist kein Webserver bekannt, bei dem die Logdateien forensische Sicherheit böten. Wer Root-Rechte hat oder sich aneignet, kann da reinschreiben, was immer er will.

7.7.2 Routing

Auch die Server sind durch die bereits beschriebenen Angriffe gegen Routing/BGP angreifbar, indem man ihnen falsche IP-Adressen vorgaukelt und dadurch unwahre Log-Einträge provoziert.

7.7.3 Zeitfälschung

Wenn ein Angreifer es schafft, per NTP oder Root-Zugang eine falsche Uhrzeit auf dem Server einzustellen, oder die Uhrzeit oder Zeitzone versehentlich falsch eingestellt werden, stimmen alle Log-Dateien nicht.

7.7.4 Timing-Angriffe

Diese werden in Kapitel [6](#) beschrieben.

7.7.5 Reverse DNS

Ein Angriff, der eigentlich längst nicht mehr möglich sein sollte, manchmal aber immer noch gut ankommt und bei Erfolg immer für gute Stimmung sorgt, den ich vor 25 Jahren in Workshops vorgeführt habe:

Ist bei einem Server beim Logging die DNS-Auflösung eingeschaltet, kann man z. B. vom der IP-Adresse 1.2.3.4 zugreifen und in der DNS-Rückwärtsauflösung als DNS-Namen „5.6.7.8“ eintragen. Dann steht im Log, der Zugriff sei von 5.6.7.8 erfolgt.

8 Tatsächliche Vorfälle

8.1 Negativauskünfte

Während meiner Tätigkeit in der Vorratsdatenspeicherung 2009 kam es wiederholt zu **Negativauskünften**, weil angefragte IP-Adressen

- im angefragten Zeitpunkt gerade nicht vergeben worden waren (also etwa die Uhrzeit falsch sein musste) oder
- sie auf Vorrat beschafften Adresskontingenten angehörten, die seit ihrer – länger zurückliegenden – Beschaffung *noch nie* eingesetzt worden waren und deshalb noch nie vergeben worden sein konnten (also die angefragte IP-Adresse entweder nicht stimmen konnte oder im Internet gefälscht worden war).

Teilweise stellte sich danach heraus, dass den Anfragen Schreib- und Übermittlungsfehler zugrundelagen oder Polizisten die Zeitzonen nicht verstanden, nicht richtig umgerechnet oder auch gar nicht beachtet hatten – oder die Daten schlicht und einfach falsch waren **und es den Zugriff nie gegeben hatte**.

8.2 Kundenbeschwerden

Es kam auch zu Kundenbeschwerden, weil Kunden nach Einleitung von Strafvermittlungen oder zivilen Klagen *glaubwürdig und nachvollziehbar* beteuerten, dass sie das nicht gewesen seien oder sogar im fraglichen Zeitraum mehrwöchig verreist waren und alle Computer abgeschaltet, nur den Router wegen des Telefons und Anrufbeantworters angeschaltet gelassen hatten.

8.3 Malware

Es gab auch einen Fall, in dem sich ein Kunde beklagte hatte, dass ein Strafvermittlungsverfahren gegen ihn laufe, obwohl er die vorgeworfene Tat nicht begangen habe.

Ein auf Malwareanalyse spezialisiertes Sicherheitsunternehmen fand auf seinem Rechner mehr Malwareprogramme als Tasten auf der Tastatur.

Teil II

Praktische Mängel

9 Anknüpfung an EuGH C-793/19

Die Anforderung des EuGH an eine Vorratsdatenspeicherung lautet (C-793/19 und C-794/19):

„Diese Rechtsvorschriften müssen durch klare und präzise Regeln sicherstellen, dass bei der Speicherung der fraglichen Daten die für sie geltenden materiellen und prozeduralen Voraussetzungen eingehalten werden und dass die Betroffenen über wirksame Garantien zum Schutz vor Missbrauchsrisiken verfügen.“

Ich werde in diesem Teil aufzeigen, dass der Gesetzentwurf schon sprachlich keine „klaren und präzisen Regeln“ enthält, und die materiellen und prozeduralen Voraussetzungen nicht normiert.

10 Unklarheiten des Gesetzestextes

10.1 Schlechte, ungeeignete Passivsprache

Die Texte wimmeln vor Passivsprachkonstruktionen, um sich um wesentliche Aussagen und Klarstellungen herumzudrücken. Sätze wie

§ 100g StPO: „Verkehrsdaten dürfen erhoben werden.“

§ 100g StPO: „Standortdaten dürfen erhoben werden.“

§ 100k StPO: „Nutzungsdaten dürfen erhoben werden.“

§ 175 TKG: „Die Auskunft darf erteilt werden.“

§ 176 TKG: „Verkehrsdaten dürfen beauskunftet werden.“

§ 177 TKG: „Daten dürfen verwendet werden.“

sind nur gebellte Satzstümpfe. Das sind keine grammatikalisch korrekten und vollständigen Sätze. *Sprechen Sie in klaren, ganzen, verständlichen Sätzen.*

„Dürfen“ bezeichnet ein aktives Handeln und kann nicht als Passivsatz verwendet werden, weil ein Passivkonstruktion kein Handeln ist, sondern das Handeln eines anderen beschreibt. „Dürfen“ kann nur der, der es tut, und nicht der, dem es getan wird.

Man kann schreiben, dass die Staatsanwaltschaft Daten erheben darf. Oder die Polizei. Aber man kann nicht schreiben, dass Daten erhoben werden dürfen, weil Daten gar nichts dürfen können. Daten sind tot, deshalb können sie nichts tun, und somit auch nichts dürfen, weder aktiv noch passiv.

Im Latein- und Griechisch-Unterricht lernt man (oder lernte zumindest früher), dass nur der in einer Passivkonstruktion stehen kann, der auch aktivhandlungsfähig ist, und nur der das Passiv bewusst, subjektiv erleben, erfahren kann. *Ich* kann gewaschen werden, den Vorgang erfahren – aber mein Auto kann es nicht, solange nicht wenigstens der Kontext das Handlungssubjekt mitteilt. Das Auto muss einer aktiv waschen, der mindestens aus dem Kontext hervorgeht, denn die Struktur Subjekt-Prädikat-Objekt nicht völlig starr, sondern erlaubt, das Handlungssubjekt im Kontext unterzubringen. Daran fehlt es hier.

In der Folge sind diese Sätze schon sprachlich unklar: *Wer* darf hier was? *Wem* soll hier etwas erlaubt werden? Der Text erreicht schon auf sprachlicher Ebene nicht die

nötige Normenklarheit und Normierungsdichte.

Wir erleben hier einen katastrophalen Sprachverfall:

- Satzverstümmelungen, die die Benennung eines Subjekts vermeiden, um sich um gedanklich vollständige und sinnvolle Sätze herumzudrücken,
- miserable Passivkonstruktionen,
- penetrante Substantivierung,
- Partizipiendurchfall als woke Gendersprache,

sind übelstes Politiker- und Juristensprech, und nicht nur einer Sprache mit intakter Grammatik, sondern auch des Abiturs unwürdig.

Im Kontext dieses Gesetzesentwurfs entsteht sogar der Eindruck, dass man das bewusst gar nicht so genau festlegen und lieber offen lassen und der Rechtsprechung überlassen wollte, wer tatsächlich Zugriff auf die Daten hat und damit **in das Brief- und Fernmeldegeheimnis, die Meinungs- und Pressefreiheit eingreifen darf**. Als Bürger, Wähler und Grundrechtsträger darf man deshalb wohl erwarten, dass Sie sich mehr Mühe geben und wenigstens ein gewisses Sprach- und Inhaltsniveau und eine inhaltliche Mindestsubstanz erreichen.

10.2 Unklare Berechtigte

10.2.1 Berechtigte des § 174 TKG

Ich kann hier nur vermuten, dass man sich bezüglich der Berechtigung, wer Anfragen stellen darf, an der Formulierung aus § 174 Abs. 3 TKG orientiert hat, wo sich Formulierungen wie

an die für die Verfolgung von Straftaten und Ordnungswidrigkeiten zuständigen Behörden,

[...]

an die für die Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung zuständigen Behörden

finden.

Doch wer soll das sein? Woher und mit welchem Wissen soll ein Anbieter von Telekommunikationsdienstleistungen wissen sollen, können, müssen, welche Behörde wofür zuständig ist? Ich hatte Ihnen in der Stellungnahme von 2023 schon dargelegt, dass das in der Praxis völlig unklar und für Provider nicht erkennbar und nicht nachzuprüfen ist.

In der Praxis wissen es sogar viele Behörden selbst nicht, ob und was sie dürfen, und warum vielleicht.

Soll es Aufgabe der Telekommunikationsdienstleister sein, zu prüfen und entscheiden, ob eine Behörde wirklich Behörde ist, und ob sie auch noch befugt und zuständig ist?

10.2.2 Berechtigte des § 175 TKG

§ 175 Abs. 3 TKG *soll* regeln, an wen aus der „IP-Adressspeicherung“ zu beaskunften ist.

Wer genau sind aber etwa

- „die für die Verfolgung von Straftaten zuständigen Behörden“?
- die Gefahrenabwehrbehörden der Länder?
- die Verfassungsschutzbehörden der Länder?

Wer soll das sein? Soll man da raten? Bei wem liegt die Beweislast? Wer ist verantwortlich und wer haftet für Verstöße, straf-, zivil- und datenschutzrechtlich? **Das ist kein hypothetisches Problem. Ich belege einen konkreten juristischen Fall dieser Unklarheit in Abschnitt 28.**

Ich hatte in meiner Stellungnahme vom 9. Oktober 2023 aus meiner Praxis der Vorratsdatenspeicherung 2009 berichtet, dass in vielen Fällen unklar war, ob eine Anfrage berechtigt, oder überhaupt „echt“ war, ob es die angebliche Polizeistation überhaupt gibt, und ob die Adressangaben dazu wie die Faxnummer überhaupt stimmen.

Wie soll ein Verpflichteter, insbesondere, wenn er kein Jurist ist, erkennen und beurteilen können, wer zur Abfrage berechtigt ist und wer nicht? Zumal unter Juristen die Auffassung herrscht, dass nur Juristen Gesetze verstehen und auslegen können? Wie also soll ein Provider erkennen können, wem gegenüber er zur Auskunft verpflichtet ist, und wem nicht?

10.2.3 Behörden welcher Staaten?

Während in § 175 Abs. 2 und 3 TKG Bezüge auf Deutschland enthalten sind („Bundes...“, „Der Länder“), ist bei Nr. 1 keine Einschränkung gegeben, *welche* für die Verfolgung von Straftaten zuständigen Behörden berechtigt sein sollen. Auch der Verweis auf § 100g StPO hilft da nicht weiter.

Sind also Strafverfolgungsbehörden anderer Staaten oder der EU zuständig?

Nach juristischer Auslegungsweise zwingend ja, denn Gesetze sind stets so auszulegen, dass kein Wort überflüssig ist. Wenn aber die Absätze 2 und 3 auf den Bund und die Länder eingeschränkt sind, kann es Absatz 1 nicht sein, weil sonst die Einschränkung überflüssig wäre, wenn sich der ganze § 175 nur auf deutsche Behörden bezöge.

Anders gesagt: Nach diesem § 175 TKG Abs. 1 TKG dürfte auch an Strafverfolgungsbehörden, Geheimdienste oder sogar die Botschaften *der USA, Russlands, des Irans* Auskunft erteilt werden, sofern § 100g StPO erfüllt ist.

Gemeint und gewollt ist das sicherlich nicht. Der Text ist aber so formuliert, dass das der Fall wäre.

Die Frage ist nicht hypothetisch. In meiner Tätigkeit in der Vorratsdatenspeicherung 2009 hatte ich auch je eine Anfrage von Polizeibehörden aus Österreich und der Schweiz. Beide sagten, dass sie auf direkte Anfragen angewiesen seien, weil der offizielle Weg über ein internationales Amtshilfeverfahren wegen deutscher Bürokratie ein halbes Jahr dauere und damit immer scheitere, weil die Daten bis dahin gelöscht sind.

Wie also soll dieser § 175 Abs. 1 TKG auszulegen sein?

10.2.4 Internationale Amtshilfeersuchen

In gleicher Weise stellt sich die Frage, ob internationale Amtshilfeersuchen beauftragt werden dürfen – und wer dann als anfragende Stelle gilt.

10.2.5 Warum Zoll, Verfassungsschutz, MAD und BND?

10.2.5.1 Ziel Kinderpornographie?

War nicht das offiziell angegebene Ziel der IP-Adressspeicherung, *Kinderpornographie* zu verfolgen?

Was haben Zoll, Verfassungsschutz, MAD und BND mit Kinderpornographie zu tun?

Beim Zoll könnte man sich noch vorstellen, dass im Post- und Paketverkehr Kinderpornographie gefunden wird, aber das sind dann physische Sendungen, für die eine IP-Adressabfrage keinen erkennbaren Sinn ergibt. Für elektronische Sendungen ist der Zoll meines Wissens nicht zuständig.

10.2.5.2 Zuständigkeiten der Verfassungsschutzbehörden der Länder

Nach den Landesverfassungsschutzgesetzen dürfen die Landesverfassungsschutzbehörden immer nur innerhalb ihrer Bundesländer tätig werden und nicht „in fremden Wäldern jagen“. Bei grenzüberschreitenden Ermittlungen sind die jeweiligen Behörden der betroffenen Bundesländer hinzuzuziehen bzw. um Amtshilfe zu bitten.

Wie verhält sich das bei TKG-Abfragen, wenn

- der Verpflichtete (Anbieter) außerhalb der Landeszuständigkeit der anfragenden Behörde sitzt?
- der Anschlussinhaber außerhalb der Landeszuständigkeit sitzt?

Ist die Anfrage dann berechtigt oder als unberechtigt abzuweisen?

10.3 Unklare Verpflichtete

10.3.1 Unklare Abgrenzung durch technischen K.O.

Wie oben in Abschnitt 3.1.6 beschrieben, halluziniert der – zweifellos juristische – Verfasser der Begründung anhand vermeintlicher technischer Unterschiede eine Differenzierung zwischen **verpflichteten** „Internetzugangsdiensten“ und **nicht verpflichteten** „Bereitstellern von lokalen drahtlosen Netzwerken“, anhand der Frage, ob man offizielle oder nicht offizielle IP-Adressen erhalte.

Die Auffassung ist technisch falsch und laienhaft, der Verfasser hat schlicht nicht verstanden, wie das Internet funktioniert, wie IPv6 funktioniert und dass auch bei CGNat die Anschlussinhaber keine offizielle IPv4-Adresse erhalten.

Daraus resultiert aber, dass es keine klare Abgrenzung zwischen Verpflichteten und nicht verpflichteten Anbietern gibt:

- Ein großer Provider, der lediglich IPv4 mit CGNAT anbietet, wäre – entgegen der Absicht des Verfassers – **nicht verpflichtet**,
- Ein Hotel, Restaurant, Supermarkt, die IPv6 anbieten, wären dann aber – wieder entgegen der Absicht des Verfassers – **verpflichtet**.

10.3.2 „Wer öffentlich zugängliche Telekommunikationsdienste erbringt“

§§ 175, 176 verwenden Formulierungen wie „Wer öffentlich zugängliche Telekommunikationsdienste erbringt“, § 177 „Wer Internetzugangsdienste erbringt“

Nach § 3 TKG ist

„**Anbieter von Telekommunikationsdiensten**“ jeder, der Telekommunikationsdienste erbringt;

„**öffentliches Telekommunikationsnetz**“ ein Telekommunikationsnetz, das ganz oder überwiegend der Erbringung öffentlich zugänglicher Telekommunikationsdienste dient, die die Übertragung von Informationen zwischen Netzabschlusspunkten ermöglichen;

„**Netzabschlusspunkt**“ der physische Punkt, an dem einem Endnutzer der Zugang zu einem öffentlichen Telekommunikationsnetz bereitgestellt wird; in Netzen, in denen eine Vermittlung oder Leitwegebestimmung erfolgt, wird der Netzabschlusspunkt anhand einer bestimmten Netzadresse bezeichnet, die mit der Nummer oder dem Namen eines Endnutzers verknüpft sein kann;

„**Internetzugangsdienst**“ ein Internetzugangsdienst im Sinne der Begriffsbestimmung des Artikels 2 Absatz 2 Nummer 2 der Verordnung (EU) 2015/2120 des Europäischen Parlaments und des Rates vom 25. November 2015 über Maßnahmen zum Zugang zum offenen Internet und zu Endkundenentgelten für regulierte intra-EU-Kommunikation sowie zur Änderung der Richtlinie 2002/22/EG und der Verordnung (EU) Nr. 531/2012 (ABl. L 310 vom 26.11.2015, S. 1), die zuletzt durch die Verordnung (EU) 2018/1971 (ABl. L 321 vom 17.12.2018, S. 1) geändert worden ist;

Und liest man **in dieser EU-Verordnung nach**, dann findet man dort

„**Internetzugangsdienst**“ ein öffentlich zugänglicher elektronischer Kommunikationsdienst, der unabhängig von der verwendeten Netztechnologie und den verwendeten Endgeräten Zugang zum Internet und somit Verbindungen zu praktisch allen Abschlusspunkten des Internets bietet.

Demnach würde jedes Hotel, Restaurant, jeder Flughafen und jeder Bahnhof, jede Bahn verpflichtet – **obwohl in der Begründung steht, dass gerade das nicht der Fall sei**.

Ein virtueller SIP-Telefonanbieter oder ein VPN-Anbieter ohne physischen Zugangspunkt würden dagegen wohl nicht verpflichtet – **obwohl das beabsichtigt ist**.

Da passen Gesetzestext und -begründung nicht zusammen.

10.3.3 Unklare räumliche Abgrenzung

Auf den ersten Blick steht außer Frage, dass diese Gesetze als Bundesgesetze als Geltungsbereich die Bundesrepublik Deutschland haben.

Was aber ist maßgeblich dafür, ob ein Anbieter verpflichtet ist?

- Der rechtliche Firmensitz?
- Der technische Ort der Dienstleistungen? Das Rechenzentrum? Der Router? Die Mobilfunkantenne?
- Der Ort des Anschlusses?
- Der Wohnort des Nutzers/Anschlussinhabers?
- Der Aufenthaltsort des Nutzers/Anschlussinhabers?

Beispiele:

- Wenn man im Ausland Kunde der Telekom ist, fällt man dann darunter?
- Fallen Mobilfunkkunden deutscher Anbieter darunter, wenn sie per Roaming im Ausland sind?
- Fallen ausländische Mobilfunkanbieter darunter, wenn deren Netze in Deutschland zu empfangen sind?
- Wenn ein Nutzer in einem Nachbarland – Österreich, Schweiz, Frankreich,... – aus seinem Land einen 5G-Router eines deutschen Anbieters mietet und im Ausland grenznah betreibt, fällt er dann darunter?
- Fallen Satelliten-Internet- und -Telefonanbieter wie Starlink darunter?
- Fallen VPN-Anbieter darunter?

10.4 Unklarer Umfang der Verpflichtung

10.4.1 Nur mögliche Speicherung oder auch Ermöglichung der Speicherung?

Wie in der Stellungnahme vom 9. Oktober 2023 und oben in Abschnitt [2.2](#) beschrieben, kann die Pflicht der Speicherung von IP-Adressen und Portnummern im Fall von CGNAT *im Allgemeinen* wegen der enormen Datenmengen nicht erfüllt werden. Dies ist erst dann möglich, wenn man *herstellerspezifische Verfahren* wie Deterministic NAT oder Block-Allocation erforderlich.

Die Formulierungen lassen immer wieder erkennen, dass der Verfasser nicht richtig verstanden haben, was NAT bedeutet und wie das mit den Portnummern funktioniert.

Deshalb bleibt *aus dem Gesetzestext* unklar, ob Anbieter nur speichern müssen, soweit es ihnen in ihrer bestehenden Konfiguration möglich ist, oder es ermöglichen müssen, indem sie die Konfiguration ändern oder neue Geräte beschaffen.

Auf Seite 31 *der Begründung* heißt es dagegen

Bei Unternehmen, die die öffentlichen IP-Adressen mehreren Anschlussinhabern gleichzeitig mittels Verfahren der Network Address Translation (NAT) zuweisen und daher auch Portnummern und gegebenenfalls andere Daten speichern müssen, um einen Anschlussinhaber zu identifizieren, ist zu beachten, dass diese Daten regelmäßig nicht außerhalb der eingesetzten NAT-Systeme zur Verfügung stehen. **In diesen Fällen müssen diese NAT-Systeme zunächst ausgetauscht werden, was einen erheblichen Eingriff in die Wirknetze der Unternehmen darstellt und entsprechend zusätzliche Kosten verursacht.**

Zudem müssen alle Anbieter von Telekommunikationsdiensten technische und organisatorische Vorkehrungen für die Sicherung und Herausgabe von Verkehrsdaten treffen. Dies betrifft insbesondere die Einrichtung einer Speicherinfrastruktur, die es ermöglicht, Identifizierungsdaten für bis zu drei Monate oder länger zu speichern und wieder zu löschen, einschließlich der Integration in die bestehenden Prozesse. Von den Vorkehrungen sind circa 3 000 Unternehmen betroffen.

Das Verfahren der Sicherung und Herausgabe unterscheidet sich durch die Schutz- und Löschvorgaben von den bereits heute stattfindenden Auskunftersuchen zur Strafverfolgung, die von den Unternehmen auf der Grundlage des geltenden Rechts beantwortet werden müssen. Insoweit besteht ein nennenswerter zusätzlicher Aufwand für die Sicherung und Herausgabe von Verkehrsdaten, die alle Anbieter von Telekommunikationsdiensten unterschiedslos betrifft.

Einige Verbände und Unternehmen geben an, dass für die Umsetzung der Speicherpflicht je nachdem, ob NAT-Verfahren eingesetzt werden oder nicht, und in Abhängigkeit der noch festzulegenden Details der Schutz- und Löschmaßnahmen **einmalige Investitionskosten von 1 bis 2 Millionen Euro für große Anbieter, 150 000 bis 200 000 Euro für mittlere und 80 000 Euro für kleine Anbieter anfallen könnten.** Die laufenden Kosten betragen nach diesen Angaben durchschnittlich 10 Prozent der Investitionskosten. Personalkosten könnten nach der Einschätzung einiger großer Unternehmen zwischen 200 000 und 550 000 Euro liegen; für mittlere und kleinere Unternehmen liegen hierzu keine konkreten Angaben vor.

Für die Umsetzung der Sicherung und Herausgabe von Verkehrsdaten geben einige Unternehmen an, dass in Abhängigkeit der noch festzulegenden Schutzmaßnahmen von einmaligen Investitionskosten von 60 000 bis 300 000 Euro für große Anbieter und von 30 000 Euro für kleine Anbieter notwendig seien. Die laufenden Kosten wurden hierzu von bis zu 40 Prozent der Erstinvestition angegeben. Personalkosten könnten zudem zwischen 100 000 und 250 000 Euro für große Anbieter betragen und rund 10 000 Euro für kleinere Anbieter.

Was gilt? Das Gesetz oder der Begründungstext?

10.5 Unklare sonstige Angaben

10.5.1 Kosten?

Warum steht auf Seite 3

E. Erfüllungsaufwand

E.1 Erfüllungsaufwand für Bürgerinnen und Bürger

Keiner.

E.2 Erfüllungsaufwand für die Wirtschaft

Keiner.

Davon Bürokratiekosten aus Informationspflichten

Keine.

wenn doch (siehe vorangegangener Abschnitt) auf Seite 31 **Kosten bis Millionenhöhe und Umbauten beschrieben werden und diese Kosten auf die Kunden umgelegt werden müssen?**

Ist das ein Täuschungsmanöver gegenüber Abgeordneten, die nur die ersten 3 Seiten lesen und nicht merken, dass in der Begründung etwas anderes steht?

10.6 Unklare Feststellung der Anschlussinhaber

Woher will man eigentlich wissen, ob die Bestandsdaten beim Provider zutreffend sind?

Ich habe mich bei der Anmeldung von Mobilfunkkarten stets mit Personalausweis ausweisen müssen – **aber noch nie bei der Anmeldung eines Festnetzanschlusses.**

Was hindert einen daran, einen Anschluss auf den Namen einer anderen Person anzumelden? Die etwa im selben Haus wohnt?

Es ist kein Problem, während der Abwesenheit von Nachbarn – Arbeit, Urlaub – die Adressschilder der Briefkästen vorübergehend auszutauschen und einen Anschluss zu bestellen, der per Post geliefert wird. Auf diese Weise können Schattenanschlüsse auf den Namen anderer Bewohner desselben Hauses erfolgen.

Wenn der vermeintliche Inhaber des Anschlusses dann nicht – etwa als Beschuldigter – befragt wird, sondern Daten bei den Geheimdiensten bleiben, kommt es zu falschen Daten.

10.7 Standortfeststellung

Warum wird im Gesetzentwurf immer wieder behauptet, die gespeicherten Daten taugen nicht zur Feststellung des Standorts, wenn es in § 100j heißen sollte

§ 100j Erhebung von Bestandsdaten

(1) Soweit dies für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes eines Beschuldigten erforderlich ist, darf Auskunft verlangt werden

1. über Bestandsdaten gemäß § 3 Nummer 6 des Telekommunikationsgesetzes und über die nach § 172 Absatz 1 des Telekommunikationsgesetzes erhobenen Daten bei demjenigen, der öffentlich zugängliche Telekommunikationsdienste anbietet oder daran mitwirkt, und

2. über Bestandsdaten gemäß § 2 Absatz 2 Nummer 2 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes bei demjenigen, der digitale Dienste anbietet.

(2) Die Auskunft nach Absatz 1 darf auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse verlangt werden.

[...]

Wie passt das zusammen?

10.8 Keine erkennbare Fehlerkontrolle

10.8.1 Sorgfaltspflichten und Nachprüfbarkeit?

Es geht aus dem Gesetztext nicht hervor, wie

- die sachliche Richtigkeit der Auskünfte sichergestellt wird,
- Richtigkeit, Fehlerfreiheit, Authentizität und Integrität innerhalb der Provider sichergestellt werden,
- ein Strafgericht oder ein Strafverteidiger diese überprüfen können.

10.8.2 Haftung, Schadensersatz, Richtigstellung

Es ist nicht ersichtlich, wer für Schäden aus unrichtigen oder unberechtigten Auskunftersuchen haftet.

10.8.3 Beispiele

10.8.3.1 Fake-Anschlüsse

Das Phänomen, das mir in meiner Tätigkeit in der Vorratsdatenspeicherung und Konzernsicherheit 2009 einige Male begegnete, wurde oben unter [7.2.2.3](#) beschrieben. In einigen Fällen ließen sich die tatsächlichen Nutzer der Anschlüsse nur über die Inhaber der Bankkonten ermitteln, von denen die monatlichen Kosten bezahlt wurden.

Wie ist mit unrichtigen Daten umzugehen?

10.8.3.2 Kinderpornographie auf Nachbars Leitung

Wie etwa soll Fehlererkennung laufen, wenn bei einem DSL-Provider oder im Keller eines Hauses Leitungen versehentlich oder absichtlich vertauscht werden?

Viele DSL-Provider identifizieren ihre Kunden nicht mehr über Benutzernamen/Passwort, sondern über die Router-Port, an dem die Kupferleitung aus der Wohnung angelötet ist.

Was, wenn

- ein Techniker die Anschlüsse zweier Wohnungen in der Datenbank verwechselt oder böswillig vertauscht?
- ein böser Nachbar die Leitungen in der Verteilerdose im Keller gelegentlich vertauscht?

Im Zeitalter der Flatrates und der Handytelefonie würde das überhaupt nicht auffallen, aber der Provider würde bei TKG-Auskünften die Inhaber der Anschlüsse vertauschen.

Man könnte so Straftaten begehen und sie dem Nachbarn anhängen – beispielsweise um ihn loszuwerden oder zu diffamieren, oder selbst straflos auszugehen.

Geht man davon aus, dass Pädophile bezüglich Kinderpornographie geradezu ein Suchtverhalten entwickeln, ist davon auszugehen, dass sie – ähnlich wie Drogensüchtige – jede Methode nutzen werden, um an Kinderpornographie zu gelangen.

Ein Bestreiten durch den Anschlussinhaber ist nicht vorgesehen.

10.8.3.3 Inkompetenz des Verfassungsschutzes

Das vorliegende Gesetz soll auch BND, MAD und Verfassungsschutz Zugriff auf die Daten verschaffen.

Im März 2026 wurde ein Fall bekannt, in dem der Verfassungsschutz durch Inkompetenz großen Schaden anrichtete. DIE WELT: **Berlin – Hochschulmitarbeiterin verliert Job, weil Verfassungsschutz sie mit Rechtsextremistin verwechselt**

Eine Frau wurde ruiniert, weil ihr Name gleichlautend mit dem Pseudonym einer Rechtsextremistin war, mit der sie außer dieser Namensgleichheit gar nichts zu tun hatte.

Wer haftet, wenn Provider-Auskünfte in solchen Fällen eine Rolle spielen?

11 ETSI-Standard TS 102 657

11.1 Version V2.7.1 vom November 2025

Der ETSI-Standard TS 102 657 „Lawful Interception (LI); Retained data handling; Handover interface for the request and delivery of retained data“ ist in der Version V2.7.1 vom November 2025 **frei verfügbar**.

Die Anlagen zum Standard (ASN.1 Modul und XML Schema) sind entgegen der Formulierungen im Foreword der Norm und auf den Webseiten der ETSI nicht als PDF-Attachment, sondern **als separates ZIP-Archiv zugänglich**.

Hinweis: Da die Norm selbst sehr lückenhaft und inkonsistent und das XML-Schema unübersichtlich, zudem anscheinend automatisch aus dem ASN.1 Modul erzeugt ist, und XML-typisch wenig zu den Datentypen enthält, empfiehlt es sich, zum Verständnis des Protokolls und der ausgetauschten Daten, das gut lesbare ASN.1-Schema zu lesen.

Zum Umfeld gehören weitere Normen wie

ETSI TR 102 503 Lawful Interception (LI); ASN.1 Object Identifiers in Lawful Interception and Retained data handling Specifications

ETSI TS 103 120 Lawful Interception; Interface for warrant information

ETSI TR 103 727 Lawful Interception (LI); Library and mapping for Lawful Interception (LI) and Lawful Disclosure (LD)

11.2 Verfahrensvorschrift

11.2.1 Gesetzentwurf und ETSI TS 102 657

Soweit bisher ersichtlich, gibt die Bundesnetzagentur ein automatisiertes und ein manuelles Verfahren per E-Mail vor, und verwendet beim automatisierten Verfahren die Spezifikationen des ETSI-ESB-Komitees.

(ETSI = European Telecommunications Standards Institute, ESB = Elektronische Schnittstelle Behörde)

Der Gesetzentwurf beschreibt in der Begründung auf Seite 60 zu § 177 Abs. 4:

Satz 1 bestimmt weiter, dass ein leistungsfähiges technisches Verfahren einzusetzen ist, das die getrennte Speicherung nach Absatz 2 Nummer 2 nicht beeinträchtigt. Für Auskünfte nach § 174 Absatz 1 Satz 3 wird mit Satz 3 auf das Verfahren nach § 174 Absatz 7 zur Beauskunftung von Anschlussinhabern verwiesen. Es verwendet eine gesicherte elektronische Schnittstelle für 100 000 und mehr Vertragspartnern sowie das E-Mail-basierte Übermittlungsverfahren, das auch von allen anderen Verpflichteten zu verwenden ist. Die gesicherte elektronische Schnittstelle nutzt ein seit Jahren etabliertes Verfahren und von allen Seiten angesehenes Mittel zur Beauskunftung. Die Schnittstelle basiert auf einem ETSI-Standard (TS 102 657), der eine einheitliche Beauskunftung auf beiden Seiten der am Verfahren Beteiligten garantiert. Die standardisierten Prozesse für die Auskunftersuchen sowie für die Antworten garantieren eine schnelle Bearbeitung und eine gleichbleibend hohe Qualität auf beiden Seiten. Sie reduziert die Fehlerhäufigkeit auf ein Minimum, ist durch den einheitlichen Standard zukunftssicher und auf dem freien Markt verfügbar. Durch den einheitlichen Standard und das verwendete maschinenlesbare Format ist bei den verpflichteten Unternehmen eine Teilautomatisierung möglich, die die Zusammenstellung der angefragten Daten erleichtert und eine Beauskunftung beschleunigen kann. Auf Seiten der berechtigten Stellen können umfangreiche Anfragen mittels aufbereiteter Dateien schnell und unkompliziert in die Ersuchen importiert werden und die beauskunfteten Ersuchen mit individuellen Filtern problemlos aufbereitet und ausgewertet werden.

11.2.2 Verordnungs-Ermächtigung an Frankreich

Formal wird die Bundesnetzagentur ermächtigt, im Verordnungswege technische Details festzulegen, für Mobilfunk in § 170 Absatz 6 TKG. Darin heißt es auch

... sowie zu den Mitwirkungspflichten bei technischen Ermittlungsmaßnahmen bei Mobilfunkendgeräten nach § 171 erforderlich sind, in einer im Benehmen mit den berechtigten Stellen und unter Beteiligung der Verbände und der Hersteller zu erstellenden Technischen Richtlinie fest. Dabei sind internationale technische Standards zu berücksichtigen; Abweichungen von den Standards sind zu begründen.

Für allgemeine Telekommunikationsdienste wird in § 174 Absatz 7 und dem geplanten § 176 Absatz 4 und § 177 Absatz 5 darauf verwiesen.

Damit wird indirekt die ETSI, *eine privatrechtliche Organisation mit Sitz in Frankreich*, ermächtigt, Rechtsverordnungen in Deutschland durchzuführen, indem sie mittels der Norm Einfluss darauf nimmt, welche Daten übertragen werden.

11.3 Fehlende Beteiligung von Datenschutz, Technik und Verbrauchern

Dazu schreibt das GKDZ (Gemeinsames Kompetenz- und Dienstleistungszentrum der Polizeien der Länder Berlin, Brandenburg, Sachsen, Sachsen-Anhalt und Thüringen auf dem Gebiet der polizeilichen Telekommunikationsüberwachung als rechtsfähige Anstalt öffentlichen Rechts, AöR)

Nach einer durch die Corona-Pandemie bedingten mehrjährigen Pause, konnte in diesem Jahr die ETSI-ESB (Elektronische Schnittstelle Behörde) Bundestagung in Kiel vom 28.11 zum 29.11.2023 wieder durchgeführt werden. Ausrichter war diesmal das LKA Schleswig-Holstein, welches mit Auswahl des Tagungsortes und der besprochenen Themen, sowie der Organisation des Rahmenprogramms, die Erwartungen der Teilnehmer übertroffen hat.

Teilnehmer waren neben Sicherheitsbehörden aus dem gesamten Bundesgebiet auch die Bundesnetzagentur und Telekommunikationsnetzbetreiber, sowie Vertreter aus Wirtschaft und Industrie. In Vorträgen und Diskussionen wurden aktuelle Herausforderungen Rund um Themen wie bspw. Automotive, dem 5G-Kommunikationsstandard und OTT-Diensten besprochen, sowie Lösungen aufgezeigt, um auch künftig dem gesetzlichen Auftrag gerecht zu werden.

Von Seiten des GKDZ wurde die Information der Bundesnetzagentur positiv aufgenommen, die TKÜV (Telekommunikations-Überwachungsverordnung) so anzupassen, dass die spezifischen Belange von zentralen Empfangsstellen für berechnigte Stellen zukünftig berücksichtigt werden.

Das deutet darauf hin, dass die Norm zwischen Polizei und Anbietern ausgekugelt wurden und Daten- und Persönlichkeitsschutzbelange hier nicht vertreten waren.

11.4 Genereller Eindruck der Laienhaftigkeit

11.4.1 Naive Darstellungen

Schon bei der ersten Sichtung – etwa Figure 2 auf Seite 18 – entsteht der Eindruck, dass diese Norm schnell, schlampig und laienhaft erzeugt wurde.

Seite 37:

Two data exchange techniques are presented: "HTTP" and "direct TCP". The choice of technique is a national option.

The data exchange techniques for HI-A and HI-B may be different. For instance XML encoding may be used for HI-A, while ASN.1 BER encoding may be used for HI-B. This is a matter for agreement between CSP and Authorized Organization on case-by-case basis.

Wofür schreibt man eine Norm, wenn die Einzelheiten dann doch zwischen Behörde und CSP vereinbart werden müssen?

The direct TCP mechanism uses XML, or BER encoding derived from the ASN.1 in annex A. The direct TCP option uses data exchange details on top of the standard TCP/IP stack.

Keine Verschlüsselung, keine Verbindungssicherheit bei „direct TCP“?

XML über HTTP: Was darf's denn heute sein? POX? Atom? SOAP? REST?

11.4.2 Schiefe Pfeile

Nur so ein Detail am Rande:

Die Graphiken sind so schlampig gemacht, dass sogar die Pfeile schief und nicht aneinander ausgerichtet sind. Ebenso Boxen (Figure 4) oder Farbfehler (Figure 5), unterschiedliche Pfeilspitzen und Strichdicken (Figure 7),

11.4.3 Status Diagram Figure 5

Nicht wesentlich besser wird der Eindruck auf Seite 24 mit Status Diagram Figure 5.

Absesehen davon, dass ein Zustandsdiagramm wie „Wir fragen, dann warten wir auf Antwort und haben dafür drei Zustände »(waiting for response)«, und wenn die Antwort kommt, dann freuen wir uns und sind fertig“, nicht ernstlich Substanz haben, ist ungeklärt, woher »Cancel« kommt und welche Rolle die Zeit spielt.

Timeouts?

Wiederholungen?

Wer cancelt?

Warum wird der Provider über ein Cancel nicht informiert?

Was passiert bei einem Timeout?

Wie wird das protokolliert?

Wie ist bei einer Übertragung per HTTP überhaupt eine Anfrage ohne Ack möglich?

Die Status-Diagramme passen auch nicht zu den Kommunikationsdiagrammen.

11.4.4 Message Flow Figure 7, 9

Es ist Konvention, dass Kommunikationsdiagramme immer von links anfangen und der Initiator der Kommunikation auf der linken Seite steht, um das Diagramm in Leserichtung zu lesen.

Unklar ist, warum in Figure 7 und 9 der CSP jeweils zwei Pakete hintereinander sendet. Das ist in solchen Diagrammen normalerweise nicht möglich, weil es immer um das Hin- und Her geht.

Offenbar soll hier eine Wartezeit dargestellt werden, es bleibt aber unklar, wie der Verbindungswiederaufbau oder der Verbindungsbestand funktionieren sollen.

Seltsam auch: Es soll auch HTTP als Basisprotokoll eingesetzt werden. HTTP kennt aber nur eine Antwort auf einen Request. HTTP kann nicht (ohne dubiose Klimmzüge) sofort mit einem ACK quittieren und dann später noch eine inhaltliche Antwort schicken. Dazu wäre eine neue HTTP-Verbindung (oder ein neuer Request bei HTTP/2 oder HTTP/3, Websocket o.ä.) erforderlich.

Es bleibt aber unklar, ob der CSP die zweite Antwort per HTTP (push) liefern soll, oder ob die Behörde die Antwort per Pull in einem neuen HTTP-Request holt.

11.4.5 HTTP-Versionen

Es ist auch nicht ersichtlich, ob für jeden Austausch eine neue HTTP/1.0 Verbindung aufgebaut werden soll, oder ob eine stehende HTTP/2 oder HTTP/3-Verbindung aufgebaut werden kann, über die der Server einen HTTP/2 Server Push treiben kann.

11.4.6 Time Stamps

6.1.4 Timestamp (timeStamp)

The time the message was created shall be included in the message.

All timestamps shall contain the time and date, and an indication of the time zone.

Dass eine Timestamp Zeit, Datum und Zeitzone enthält, ist eine Selbstverständlichkeit. Warum wird kein konkretes, präzises Format wie GeneralizedTime oder ISO 8601/RFC 3339 spezifiziert?

Schaut man jedoch in das ASN.1-Modul, dann wird *darin* die Zeitangabe als im Format GeneralizedTime definiert.

11.4.7 Prioritäten

Eine Aufgabe wie diese drängt es förmlich auf, dass Abfragen priorisiert werden können.

Tatsächlich findet sich in der Norm und im ASN.1-Modul auch ein Prioritätenfeld:

```
RequestPriority ::= OCTET STRING
-- Priority considerations are a matter for national implementation
-- This standard makes no statement regarding how such priorities are
represented or used
```

Welchen Zweck hat es, ein Prioritätenfeld vorzugeben, wenn weder dessen Ordnungsrelation ersichtlich ist, noch überhaupt definiert ist, welche Prioritäten es gibt und wie

sie zu benutzen sind, und das *der landesspezifischen Implementierung* überlassen, also nicht genormt wird?

11.4.8 Fehlende Differenzierung zwischen synchroner und asynchroner Kommunikation

11.4.8.1 Unklare Struktur

Das ganze System beruht auf einer Doppelstrategie zwischen HTTP und E-Mail, obwohl HTTP zumindest auf Anwendungsebene ein synchrone Kommunikationsform ist, weil auf jede Anfrage unmittelbar und – auch wenn mit Wartezeit verbunden – innerhalb derselben, vom Client aufgebauten Kommunikationsverbindung genau eine Antwort erfolgt, während E-Mail ein strukturell asynchrones Nachrichten-Protokoll ist, bei dem die Antwort über einen eigenen Kommunikationsaufbau erfolgt.

Die Beauskunftung von solchen Abfragen ist aber ihrem Wesen nach grundsätzlich eine asynchrone Angelegenheit.

Zwar kann im Rahmen einer synchronen Anfrage eine Eingangsbestätigung erstellt werden, grundsätzlich aber wäre zu klären, wie die Rückantworten asynchron und ohne Bestand der Kommunikationsverbindung erfolgt. Bei E-Mail ist das noch per se klar, bei HTTP aber nicht.

Die Diagramme geben hierüber auch keine Auskunft.

11.4.8.2 Message und Request verwechselt

Die technisch richtige Vorgehensweise wäre gewesen, einen zentralen, redundanten, gesicherten, **fehlertoleranten und fehlererkennenden** Message Broker aufzusetzen und für jeden CSP eine entsprechende Message Queue mit Priorisierung aufzusetzen und das gesamte System asynchron mit maximalen Response-Zeiten zu betreiben.

Das ist State of the Art und Industriestandard für derartig strukturierte Aufgaben und AMQP ein etabliertes Protokoll dafür.

Nachrichten per E-Mail oder HTTP zu verschicken mag für eine Test- und Aufbauphase eine vorrübergehende Ersatzlösung sein, und die Implementierung und das Verständnis deutlich vereinfachen.

11.4.9 Ungenügende Trennung zwischen Transport und Applikation

11.4.9.1 Kein Schichtenmodell

Ein wesentlicher Grund für die unaufgeräumte und ambivalente (TCP/HTTP/EMail, XML/ASN.1/XDR) Struktur ist, dass man hier keine klare Trennung zwischen Transport und Applikation eingezogen hat. Anders gesprochen: Nicht in Schichtenmodellen (vgl. 4.2) denkt. Ein Ausbildungsmangel.

Bei sauberer Vorgehensweise hätte man die ausgetauschten Nachrichten auf Applikationsebene definiert und – getrennt davon, in einer separaten Norm – eine Reihe von Transportprotokollen.

Damit hätte man sauber und leicht zunächst für die Test- und Einführungsphase einfache und später dann besser geeignete Protokolle wie Message Queues einsetzen können.

11.4.9.2 Keine Message Queue – Kein Deutschland-Stack

Die vorliegende Problemstellung des Transportprotokolls schreit geradezu nach einer „Message Queue“, einer Standardanwendung und -lösung in der IT, weil solche Aufgabenstellungen häufig vorkommen.

Deshalb bietet jede Softwaredistribution für Server, und jeder Anbieter von Cloud-Diensten schon seit vielen Jahren Anwendungen für Message Queues¹.

Der Bundesminister für Digitales und den aussichtsarmen Versuch der Staatsmodernisierung hat geäußert, dass er die IT-Infrastruktur für die öffentliche Verwaltung vereinheitlichen wolle. *Der Deutschland-Stack ziele darauf ab, digitale Dienste, Cloud-Infrastrukturen und digitale Identitäten (wie die Wallet für Ausweis und Führerschein) bundesweit zu vereinen und zu modernisieren.*

Das ist eine sehr gute Absicht und die richtige Vorgehensweise.

Und wie bei jedem vollsortierten Cloudanbieter müsste auch der Deutschland-Stack redundante, ausfallsichere, fehlertolerante MessageQueues anbieten, weil dies eine ständig und immer wiederkehrende Aufgabe in sehr vielen Bereichen ist. Sogar viele große Unternehmen haben ihre Unternehmenslogik auf asynchrone MessageQueues umgestellt.

Es wäre eine zentrale Aufgabe, robuste und auf Sicherheit geprüfte Message Queues bereitzustellen.

Es ist mir völlig unverständlich, wie man mit einer solchen Aufgabe derartig an einem dafür zuständigen Ministerium vorbeifrickeln kann.

¹z. B. RabbitMQ, Kafka, ActiveMQ neben vielen anderen

11.4.10 Keine Fehlerbehandlung

Eine nennenswerte Fehlerbehandlung habe ich nicht gefunden.

Was passiert zum Beispiel, wenn es beim CSP zu einem Ausfall kommt und Nachrichten verloren gehen?

Kann er sie noch einmal anfordern? „Bitte senden Sie mir noch einmal alle Anfragen, die seit heute morgen 10:25 an uns gesandt wurden“?

Können CSPs mehrere, redundante Empfangspunkte haben?

Was passiert, wenn ein CSP keine Antwort schickt? Und wann passiert es?

11.4.11 ASN.1

11.4.11.1 BER/DER

Im Text (z. B.) heißt es

When using ASN.1 the messages are BER encoded.

Daten, die zu signieren sind, werden aber per Konvention und aus technischen Gründen DER-encoded. DER ist eine Untermenge von BER, im Gegensatz zu BER aber eindeutig.

11.4.11.2 XDR

Warum werden als Darstellungsformate XML und ASN.1 definiert, zur Übertragung von XML über TCP (7.3.1) aber XML in XDR codiert, statt in das ohnehin eingesetzte ASN.1 oder gleich eine ASN.1-Nachricht zu verwenden, ohne aber wiederum XDR explizit zu erwähnen?

11.4.11.3 Definitionsfehler

Im ASN.1-Modul steht

```
NationalRequestParameters ::= SEQUENCE
{
  countryCode      [1] UTF8String (SIZE (2)),
  -- Country Code according to ISO 3166-1 [4],
  -- the country to which the parameters inserted after the extension marker apply.
  ...
  -- In case a given country wants to use additional national parameters according to its law,
```

```
-- these national parameters should be defined using the ASN.1 syntax and added after the
-- extension marker (...).
-- It is recommended that an version indicator is included in the national parameters
-- definition.
}
```

Das ist Pfusch und keine zulässige oder eindeutige Norm, wenn da jedes Land noch drin herummurksen soll, wie es passt.

Die richtige Vorgehensweise wäre, wie beispielsweise bei Extensions in X.509-Zertifikaten, beschrieben in **RFC 5280, Abschnitt 4.1** eine Sequenz aus opaken Datentypen mit OID und critical-Flag zu setzen, in die dann länderspezifische Parameter mit jeweiliger OID eingesetzt werden können:

```
Extension ::= SEQUENCE {
    extnID      OBJECT IDENTIFIER,
    critical    BOOLEAN DEFAULT FALSE,
    extnValue   OCTET STRING
                -- contains the DER encoding of an ASN.1 value
                -- corresponding to the extension type identified
                -- by extnID
}
```

Wer diese Norm und dieses ASN.1-Modul geschrieben hat, hat die Methodik von ASN.1 und auch den Zweck einer Norm und den Sinn eines Protokolls nicht verstanden, denn diese Vorgehensweise bricht das Protokoll.

11.5 Unzureichende Sicherheit

11.5.1 Keine Verschlüsselung auf Anwendungsebene

Soweit ersichtlich, ist eine Verschlüsselung nur auf HTTPS-, aber nicht auf Applikationsebene vorgesehen.

11.5.2 Definition auf Laienniveau

Es wird erklärt, was eine Signatur überhaupt ist (8.3):

Digital signature on RDHI requests for HI-A, by an Authorized Organization entity: Such an entity might be a person authorizing RDHI requests on HI-A (e.g. an Authorized Organization officer or some other person authorized by law or regulation to authorize RDHI requests), or some other entity defined by national law or regulation.

The process involves the Authorized Organization computing a hash over the entire set of fields in the request (including the time stamp). Then the hash is digitally signed with the entity's private key. The signed hash and the entity's certificate (validating its public key) are sent in the request to the CSP. In effect, the request may be viewed as comprising two

parts - one part is composed of the request fields without the signature and certificate, and the other is the signature (of the hash of the first part) and the certificate.

The CSP may choose to validate the request by computing the request's hash and verifying that it matches the one signed by the Authorized Organization. The CSP may choose to validate the certificate as well. The generation of certificates and the nature of the assigning authority are out of scope of the present document. The CSP may choose just to keep the requests with their associated signatures and certificates for audit trail and any other validation or official procedure.

Das ist eine einfache Erklärung für jemanden, der gar nicht weiß, was eine Signatur ist, aber keine technisch greifbare oder gar hinreichende Spezifikation.

Das liest sich wie „viele Laien und einer hat mal gegoogelt, was das ist“.

11.5.2.1 Verfahren nicht hinreichend definiert

Es wird auch nur in Grundzügen beschrieben, was eine digitale Signature überhaupt ist, aber nicht definiert, wie und nach welchen Verfahren zu signieren ist.

11.5.2.2 Nur „recommended“ und „may validate“

Im ETSI-Standard TS 102 657 werden Sicherheitsmaßnahmen in Kapitel 8 „Security Measures“ zwar beschrieben, **aber unzureichend**. Denn auf dem Application Level sind Security Measures lediglich „recommended“. Wie oben zitiert:

The CSP may choose to validate the request by computing the request's hash and verifying that it matches the one signed by the Authorized Organization.

„May choose“ – was soll das sein?

Sollte eine Echtheitsprüfung nicht verbindlich sein?

11.5.2.3 „For Example“

Unter 8.4.2 heißt es

The level and implementation of for example the TLS, IPSec and HTTPS security mechanisms are a matter of national regulations.

Und welche national regulations wären das dann?

Und wenn es um national regulations gehen soll, welche gelten dann bei Anfragen aus dem Ausland?

11.5.2.4 Schlüsselhandling nicht definiert

11.5.2.4.1 Private Keys In 8.3 heißt es

Such an entity might be a person authorizing RDHI requests on HI-A (e.g. an Authorized Organization officer or some other person authorized by law or regulation to authorize RDHI requests), or some other entity defined by national law or regulation.

The process involves the Authorized Organization computing a hash over the entire set of fields in the request (including the time stamp). Then the hash is digitally signed with the entity's private key.

„Might be a person authorizing RDHI requests“ – was soll das sein?

„Might“ – und wer sonst noch, wenn nicht eine „person“?

Wer ist denn eine „person authorizing RDHI“?

Wer hat Zugang zu diesem Schlüssel?

Wird der in Software oder Hardware gespeichert?

Wie sehen Key Recovery und Key Revocation aus?

11.5.2.4.2 Key Revocation Was ist, wenn es zu einer Schlüsselkomprimierung und Key Revocation kommt?

Verlieren die Anfragen dann ihre Gültigkeit?

11.5.2.4.3 Public Keys Woher kommen die Public Keys zur Überprüfung?

Wie sieht die PKI (Public Key Infrastructure) aus?

11.5.3 Mangelnde Identifikation der anfragenden Behörde

11.5.3.1 Inkonsistenz

Erstaunlicherweise besteht eine RequestID laut Anhang A.2.1.2, Table A.2 mit Verweis auf 6.1.2 aus **vier Feldern**, nämlich

- countryCode
- authorisedOrganisationID
- requestNumber

- externalIdentifier

wobei die Felder in 6.1.2 definiert würden.

Unter 6.1.2 besteht die RequestID aber nur aus **drei Feldern** (mit anderen Bezeichnungen und Schreibweisen):

- a country code
- an Authorized Organization code
- a unique reference Number

assignable within the given country to distinguish between different Authorized Organizations

Ein Datentyp, eine Syntax – String, Zahl, OID, UUID ist nicht angegeben.

11.5.3.2 Granularität und Definition der Organisationscodes

Wie genau die Zuordnung – und Rückwärtsauflösung – von Behörden und IDs (Codes) erfolgen soll, und mit welcher Granularität, ist nicht erkennbar.

Soll beispielsweise die ganze Polizei Bayern eine ID erhalten? Oder München? Jedes Präsidium? Jede Abteilung? Jeder Sachbearbeiter?

Und wie erfolgt die Rückauflösung, wenn man wissen will, wer die Anfrage gestellt hat, wer dafür verantwortlich ist?

11.5.3.3 Aktenzeichen?

Auch ein Aktenzeichen ist nicht erkennbar. Es gibt eine requestNumber, die aber pro Anfrage neu sein muss. Was der externalIdentifier ist, ist nicht ersichtlich.

11.6 Keine Protokollierung

Eine Protokollierung ist nicht erwähnt.

Auch ist nicht ersichtlich, wie die Eingangszeiten von Anfrage und Antwort vermerkt werden.

11.7 Unhaltbare Beweisfiktionen

Unter 8.3 (Seite 41) heißt es

Hashing and digital signatures on HI-B:

For the purpose of the Authorized Organization providing court evidence that the retained data is truly CSP originated, the HI-B information is hashed, and these hashes are digitally signed. The HI-B information sent with the hashes and the CSP certificate (validating its public key). The Authorized Organization should keep the digitally signed hashes and certificates together with the data.

Man baut ein löchriges Ding, legt dazu eine Norm vor, die, wäre sie ein Schiff, Seenot funken müsste, und meint dann, das alles taue als „Beweis“ vor Gericht?

11.8 Seltsame Versionssprünge

Bei der Erstellung dieses Kapitels ist mir ein schwerer Fehler unterlaufen: Ich hatte versehentlich die **alte Version V1.29.1 (2022-12)** heruntergeladen und bearbeitet, während die neueste Version V2.7.1 (2025-11) drei Jahre Unterschied und eine neue Major-Version anzeigt, und diesen Fehler erst spät bemerkt. Ich hatte mich deshalb zunächst sehr geärgert, weil diese bedeuten müsste, dass ich die gesamte Arbeit dieses Kapitels neu anfangen müsste, weil die beobachteten Mängel inzwischen behoben sein müssten.

Zu meiner Verblüffung unterscheiden sich die beiden Versionen aber kaum. Ein diff² zeigt, dass es um formale Änderungen geht, Schreibfehlerkorrekturen, Versionsaktualisierungen, Begriffsanpassungen, Abkürzungsverzeichnisse, Formatierungen.

Kein greifbarer inhaltlicher Unterschied Ein inhaltlicher Fortschritt ist nicht zu sehen. Alle Mängel der Version 1.29.1 liegen in der 2.6.1 immer noch vor.

Warum aber wird ein großer Versionssprung von 1.29.1 auf 2.6.1 vorgenommen, wenn es keine greifbaren inhaltlichen Änderungen gibt?

Gaukelt da jemand Arbeit und Fortschritt vor?

Denkbar wäre, dass die Versionsänderungen mit wesentlichen Änderungen im ASN.1 module oder XML schema einhergehen, die aber nicht zu finden waren.

²Beide Dateien jeweils nach Text wandeln mit pdftotext -layout und anschließend diff -b -B *.txt |less

11.9 Einschätzung: Luftnummer und Blendwerk

Diese „Norm“ ist in ihrer Oberflächlichkeit, Lückenhaftigkeit, ihrem Niveau, stellenweise sogar Naivität, ihrer Oberflächlichkeit und ersichtlich hastigen Erstellung weit entfernt von den Qualitäts- und Inhaltsanforderungen an eine IT-Norm.

Sie ist ungeeignet, und – basierend allein auf der Norm, ohne die Anlagen – in der vorgefundenen Form auch nicht implementierbar, weil die Normungsdichte nicht erreicht wird.

Dazu kommt, dass mehrmals darauf verwiesen wird, dass Einzelheiten in ASN.1-Definitionen nachzuschauen oder zwischen CSP und Behörde einzeln auszuhandeln seien – was eine Norm ja gerade verhindern soll.

Auffällig auch die vielen kleinen, aber augenfälligen Fehlerchen, die normalerweise Leuten, die die Norm befolgen oder implementieren, auffallen und branchenüblich sofort an den Autor gemeldet werden (Usus unter Informatikern). *Wieso können sich solche Fehler dann über Jahre halten?*

Es ist nachvollziehbar, dass man in ersten Draft-Versionen Graphiken noch nicht perfekt und als ersten Entwurf einbaut. Aber spätestens ab einer Version „1.0“ sollte man Graphiken überarbeitet und sauber und gerade haben, wenn man den eigenen Text ernst nimmt und erwartet, dass den irgendwer liest. Zumal es neben einfachen Graphikprogrammen auch spezielle Diagramm-Software gibt.

Diese Norm wirkt „tot“ – obwohl unfertig und trotz erheblicher Aktivitäten bei den Versionsnummern. Es entsteht der Eindruck, dass die nur pro forma existiert und niemand sie liest, und nur das ASN.1-Modul und das XML-Schema beachtung finden – und auch das nur elektronisch. Es waren auch keine öffentlichen Kommentare dazu zu finden.

An dieser Norm hat nach meinem Eindruck auch niemand mit Sachkunde mitgearbeitet. Es wirkt alles, als hätten Laien versucht, andere Normen und deren Arbeitsschritte einfach nachzuahmen.

Es ist ein Gerippe, dem nicht nur Sicherheitsfunktionen, sondern elementare Funktionen selbst fehlen.

Ich halte diese „Norm“ und die Normungsarbeit dazu daher nur für vorgetäuscht: Man versucht, eine in ASN.1 formulierte, schlechte Bastelei als „internationale Norm“ mit Normungsarbeit hinzustellen.

12 Überkomplexität

12.1 Unverständliche Gesetzestexte

Dieser Gesetzestext ist ein verworrenes Gestrüpp aus Kunstbegriffen, Querverweisen, Referenzen, Rückgriffen auf verunglückte Definitionen, gemacht von realitätsfremden Behördenjuristen, die nicht verstanden haben, wie das Internet funktioniert.

Man merkt diesem Text an jeder Stelle an, dass die Verfasser nicht nur nicht verstanden haben, was sie tun, sondern auch, dass es sie nicht stört – und dass es vielleicht auch bewusst gewollt ist, dass der Text schwer verständlich ist.

Es ist aufgrund der vielen Querverweise, der widersprüchlichen Aussagen, der auf technischen Falschvorstellungen beruhenden fehlerhaften Definitionen, der überaus schlechten Sprache enorm schwer herauszufinden, was genau dieser Gesetzestexte eigentlich erlaubt – und was nicht. Und wem, und wem nicht. Und wann, und wann nicht.

Und gleichzeitig erwartet man, dass *andere* irgendwie versuchen, durch dieses Gefpriel und Geflicke hindurchzusteigen, darin irgendeinen Sinn zu finden oder ihm zuzuschreiben.

Wer soll dieses Machwerk lesen, verstehen, befolgen, dessen Einhaltung überprüfen, über Berechtigungen entscheiden können?

Ich bin mir sicher, dass die meisten normalen Richter und Rechtsanwälte den Text nicht verstehen und die Gerichte – wie so oft, und wie von Gender Studis und „Rechtssoziologen“ sogar gewünscht – das schriftliche Recht übergehen und durch ihre moralische „Hausauslegung“ und gegenseitiges Zitieren ersetzen werden.

Ich beobachte seit langem, und werde darin immer wieder von Lesern bestätigt, dass die Leute solche Gesetzestexte nicht mehr ernst nehmen und in einer gewissen Gesetzeslethargie und Staatsverdrossenheit „abschalten“.

Wenn man solche Texte liest – wobei man das eigentlich nicht „lesen“ nennen kann, das ist dann näher an der archäologischen Grabung nach dem Sinn, muss man bei der Qualität dieses Textes die Frage aufwerfen, ob die Bundesregierung überhaupt in der Lage – und willens – ist, verständliche, konsistente, fehlerfreie Gesetzestexte zu erstellen.

Schlimm schon, dass Sie niemanden gefunden haben, der versteht, wie das Internet

funktioniert – aber dass es nicht einmal jemanden gibt, der Gesetze geradeziehen und lesetauglich machen kann ...

Ich habe die schlechte Angewohnheit, gelegentlich Leute, die große Autos fahren, aber nicht einparken können, zu fragen, warum sie sich keinen Kleinwagen kaufen, mit dem sie umgehen könnten.

Ich bin versucht zu fragen, warum man sich keine einfacheren Gesetze macht, die man beherrschen kann.

12.2 Schreckliches Flickwerk

Ich bin weder Politiker noch Jurist.

Ich bin Informatiker. Und Informatiker haben in weit größerem Umfang mit der Erstellung von Normen, Standards, Definitionen, Handbüchern zu tun.

Die übliche Praxis von Gesetzgebern und Juristen, an einem bestehenden Gesetzeswerk durch Änderungsgesetze herumzuflicken, indem man mit Änderungsgesetzen an bestehenden Gesetzen herumschustert, **und sogar noch die Änderungen der Inhaltsverzeichnisse beschließt** (was eigentlich automatisch passieren und keiner Erwähnung wert sein sollte), ist aus Sicht eines Informatikers **katastrophaler, unvertretbarer Murks**.

Dazu kommt noch der strukturelle Fehler, Gesetze linear in Paragraphen durchnummerieren zu wollen und für bestimmte Vorschriften feste „Plätze“ einnehmen zu wollen, um dann unterschiedliche Dinge in einzelne, mehrfach geänderte Paragraphen zu stopfen und sich in der Not Stauraum durch Anhängen von Paragraphen mit Buchstaben zu verschaffen.

Das alles sind Arbeitstechniken des 18. und 19. Jahrhunderts, als man noch in Papierdarstellungen herumflicken und kleben musste.

Es erinnert stark an die damaligen Land- und Seekarten, bei denen man die Lithographiesteinplatten für Korrekturen abschmirgelte und beim Drucken dann das Papier unterlegen musste, damit es die korrigierte Stelle noch erreicht. Oder als Seekarten noch so teuer waren, dass man für Korrekturen nur kleine Papierstückchen kaufte, die man über die geänderte Stelle pappte.

Wir sind im Zeitalter der Digitalisierung.

Auch der Gesetzgeber muss lernen, Gesetze modern zu organisieren, wie das in vielen Ländern üblich ist, und

- statt linearer Nummerierung eine hierarchische zu verwenden, die das An- und Einfügen und das Ersetzen ganzer Kapitel einfacher macht,

- bei der Änderung grundlegender Dinge, statt Änderungen einzelner Paragraphen kapitelweise vorzugehen und statt verworrener kaskadierter Querbezüge den Kontext in ordentlicher, vernünftiger Sprache zu überarbeiten.

Hören Sie auf, Gesetze (nur) von Juristen schreiben zu lassen. *Die können das nicht.*

Lassen Sie die Gesetze von Leuten schreiben, die

- Ahnung von der Sache haben,
- Verständliches Deutsch können und zur Erstellung von strukturierten, lesbaren Texte in der Lage sind.

Es wäre auch schon viel geholfen, wenn man die geänderten oder neuen Paragraphen *jeweils auf eigene, neue Seiten* setzen würde, damit man nicht ständig suchen muss, wo sie anfangen, wenn man versucht, sie zu lesen und zwischen den Querverweisen hin- und herzuspringen. *Wie soll man diesen Salat eigentlich lesen können?*

Ich habe bei dieser Darstellungsweise nicht den Eindruck, als würden diese Gesetzestexte ernstlich durchgearbeitet und nachvollzogen.

Dankenswerterweise klärte die Abgeordnete Franziska Brantner uns einfache Bürger, Wähler und Steuerzahler darüber auf, dass auch dem, der des Lesens nicht mächtig sei, *alle* Möglichkeiten im Bundestag offen stünden, folglich auch des Erstellens und Beschließens von Gesetzestexten wie dem Vorliegenden ([Plenarprotokoll 20/130, Seite 16251 \(42 im PDF\)](#)).

Der Befund gibt Anlass, diese Praxis zu überdenken.

12.3 Zunehmende Richterkapitulation

Ich beobachte seit Jahrzehnten, und das steil zunehmend, dass selbst Richter vor Gesetzestexten kapitulieren und diese nicht mehr lesen oder beachten, sondern nach Lust, Laune und (politischer) Windrichtung urteilen oder bestenfalls einen Blick in eine juristischen Kommentar werfen und sich mit einem Halbsatz begnügen.

Erschwerend kommt die linke, feministische „Rechtssoziologie“, „Gender Studies“ hinzu, die empfehlen, dass sich Richter sowieso nicht mehr an *geschriebenes* Gesetz halten sollen, weil das von Männern gemacht und deshalb immer frauendiskriminierend sei, und deshalb empfehlen, dem persönlichen Gerechtigkeitsgefühl zu folgen und das Recht durch „subversiv veränderte Wiederholungen“ umzubiegen.

Je mehr solcher Gesetzestexte veröffentlicht werden, desto mehr kommt man Richtern entgegen, die sich für Gesetze ohnehin nicht mehr interessieren und machen, was sie wollen – oder das, so weit das mangelhafte Wissen eben reicht oder was im Kurzkomentar steht.

Praktische Beispiele dafür in den Teilen IV und V.

Warum wird die Strafprozessordnung, dieser Stapel aus unzähligen Änderungen und Flickern, nicht einfach mal komplett weggeworfen und frisch sortiert und geordnet neu aufgesetzt und etwa die Ermittlungsmethoden und -befugnisse geordnet und aufgeräumt?

Dieser Teil der StPO ist ein so elendes Durcheinander und Gewurschtel, dass niemand mehr durchblickt und das mit Normenklarheit gar nichts mehr zu tun hat.

Ich werde Ihnen unten in den Kapiteln 25 und 28 darlegen, **dass deutsche Staatsanwälte und Richter eine Beschlagnahme nicht von einer Zeugenvernehmung unterscheiden können und nicht einmal wissen, was ein „Zeuge“ ist** – obwohl das eines der ältesten und elementaren Beweis- und Ermittlungsmittel ist. Die Rechtskunde von den Zwangsmitteln ist nahe bei Null.

Warum also schreibt man die StPO nicht so auf, dass auch Richter, Staatsanwälte und – notfalls in der bei der Regierung so beliebten „einfachen Sprache“ – vielleicht sogar das Landeskriminalamt Berlin (22) und der Landesdatenschutzbeauftragte von Hessen (Professor des Rechts) (28) sie verstehen und befolgen können?

Und wenn schon Richter, Staatsanwälte und Rechtsprofessoren am Verstehen und Befolgen der StPO scheitern – wie soll es dann ein Internetprovider können? Insbesondere, weil Juristen doch so gerne die Auffassung vertreten, dass nur Juristen Gesetze verstehen und auslegen könnten und kommentieren dürften?

12.4 Bürokratieabbau?

War es nicht ein Versprechen, Bürokratie abzubauen?

Stattdessen werden immer mehr Pflichten, Aufgaben, Ausgaben, Ansprüche, Datenspeicherungen und, und, und aufgetürmt und immer mehr Kosten verursacht.

Ähnlich wie bei Strom werden hier Grundversorgungselemente der Infrastruktur immer mehr verkompliziert und verteuert.

12.5 Kontraproduktiv für die Netzabdeckung

Deutschland ist längst internationales Spottobjekt, weil das ehemalige Industrieland es nicht einmal mehr schafft, flächendeckend moderne Mobilfunkabdeckung und schnelle Internetzugänge anzubieten.

Glauben Sie, das werde besser, wenn man die Anbieter noch mit zusätzlichen Aufga-

ben und Kosten belastet?

13 Polizeiliche Probleme

13.1 Mangelnde Ausbildung

Zur mangelnden Ausbildung der Polizei bei der Vorratsdatenspeicherung 2009 verweise ich auf meine Darstellung und die Beispiele in meiner Stellungnahme vom 9. Oktober 2023.

14 Umgehung der Adressspeicherung

14.1 Zweckverfehlende Unwirksamkeit

Dieser Gesetzentwurf wird teuer, aber unwirksam in Bezug auf den angegebenen Zweck, weil jeder Kriminelle, jeder halbwegs ordentlich ausgebildete Berufsverbrecher, der etwas auf sich hält, natürlich weiß, dass er Straftaten begeht, und dazu keine IP-Adressen verwendet, die dieser Überwachung unterliegen.

Für wie doof halten Sie eigentlich Kriminelle?

Gerade im Bereich organisierter Kriminalität, auch in Bereichen wie der Kinderpornoszene oder dem linksextremistischen Bereich wimmelt es mit Sicherheit längst von Anleitungen, wie man solche Überwachungen umgeht. Das ist längst Allgemeinwissen.

Es wird also nicht funktionieren, weil es in diesen Kreisen selbstverständlich zu genug Warnungen und Belehrungen kommen wird.

14.2 Frei verfügbare Internetzugänge im Inland

Es gibt mehr als genug frei verfügbare Internetzugänge, die man so nicht rückverfolgen kann. Flughäfen und Verkehrsmittel, Idealisten und Ideologen bieten weithin frei zugängliche Netze an.

Wer einmal in einem Hotel übernachtet hat, kennt das Passwort, das erfahrungsgemäß nur selten oder nie gewechselt wird, und auch aktiv weitergegeben oder von Hackern ausspioniert werden kann. Damit kann man sich jederzeit vor das Hotel setzen und das WLAN benutzen, ohne als Übernachtungsgast angemeldet und namentlich bekannt zu sein.

Ich wohne in Berlin in Nachbarschaft zu einem Supermarkt. Mit einem Wifi6-Router im Wert von **50 Euro**, ausgestattet mit freier Firmware, konnte ich mich im Experiment **von meinem Schreibtisch aus, durch die geschlossene Außenwand** im kostenlosen Kundennetz des Supermarktes einloggen und dieses benutzen. Ich war damit für niemanden sichtbar, auf keiner Überwachungskamera. Selbst wenn man IP-Zugriffe auf diesen Supermarkt zurückführte und den Supermarkt observierte, die Kameras auswertete, käme man nicht darauf, wer der Nutzer ist, weil man es von außen nicht



Abbildung 14.1: Kostenloses WLAN als Strandbeigabe in Paphos

sehen kann. Man bräuchte sehr fortgeschrittene und teure Methoden, wie die Peilung und Triangulation, um das Signal einzugrenzen.

Zusätzlich habe ich im Experiment einen anonymisierenden Proxy auf dem Router installiert und die **MAC-Randomisierung eingeschaltet**. Selbst wenn man es schaffte, den Router anzupeilen und zu beschlagnahmen, hätte man keinen Beweis, dass es dieser Router war, von dem die strafbaren Zugriffe erfolgten.

Und das ist kein Geheimwissen. Das ist verbreitetes und allgemein zugängliches Standardwissen, das in kriminellen Kreisen mit Sicherheit aufgenommen und weitergegeben wird.

14.3 Frei verfügbare Internetzugänge im Ausland

In vielen Ländern werden Internet-Zugänge recht freizügig gehandhabt und als Kundenservice und Gastfreundschaft angeboten – selbstverständlich ohne Registrierung.

So gibt es in den Touristengegenden auf Zypern viele Restaurants, die kostenloses WLAN anbieten, und an den Stränden gibt es kostenloses WLAN als Zugabe zur Strandliege (Abbildung 14.1).

Man kann nicht nur den ganzen Tag im Internet surfen, ohne rückverfolgbar zu sein – die Passworte werden auch nicht gewechselt.

Eine Rückverfolgung ist praktisch unmöglich.

14.4 VPN-Tunnel

Es gibt reichlich gewerbliche VPN-Anbieter im Ausland. Einen VPN-Zugang auf Privat-Router in Privatwohnungen zu legen ist kein Problem.

Das ist beherrschte Technik. Das kann heute jeder.

14.5 Tor-/Onion-Router

Es gibt eine ganze Infrastruktur zum Verbergen der eigenen IP-Adresse, das nach dem Zwiebschalenmodell arbeitet, um in einer Kaskade zu verdecken, woher ein Zugriff kommt („onion routing“). Es heißt „Tor“ (=The Onion Router).

Tor-Clients sind als Browser-Plugins, als eigene Betriebssysteme wie

Whonix Kompaktes virtuelles Betriebssystem mit Tor-Browser

Tails Betriebssystem zur Installation auf USB-Sticks, das nach Gebrauch alle Sitzungsdaten löscht (non-persistent, Tails = The Amnesic Incognito Live System)

Diese sind weithin bekannt und leicht zu finden.

14.6 „Tipps und Tricks für ANTIFAs und ANTIRAs“

14.6.1 Die Terror-Fibel des Unrast-Verlags

Im Unrast-Verlag ist von der Antifaschistischen Aktion und dem „Kollektiv Schulschluss“ die kleine Terror-Fibel „Tipps und Tricks für ANTIFAs und ANTIRAs“ erschienen.

In dieser Terror-Fibel heißt es (3. Auflage, Januar 2026)

[Seite 26]

Tails und Tor

Bei allem, was ihr im Internet tut, hinterlasst ihr Spuren, sowohl auf eurem Computer als auch auf den Servern, die ihr besucht. Daher solltet ihr von zu Hause keine Seiten besuchen, die mit euren Aktionen in einem engen Zusammenhang stehen. Wenn ihr am Tag, nachdem ihr das Auto von einem Nazi abgebrannt habt, bei Google »Brandanschlag, Stuckenborstel, 13.12.2019« eingibt, bekommt ihr möglicherweise bald Besuch von den Bullen. Wenn ihr davon ausgeht, dass es von der Seite des Staates ein hohes Interesse an eurer Gruppe gibt, solltet ihr euch für die politische Arbeit mit dem Livebetriebssystem Tails und dem Onionrouter Tor vertraut machen.

[...]

Chaos Computer Club

Der Chaos Computer Club hat Ortsgruppen in jeder größeren Stadt. Hier findet ihr in der Regel Menschen, die sich gut mit Technik auskennen und denen Sicherheit und Anonymität im Internet ein Anliegen ist.

[Seite 70]

Bekenner*innenschreiben

Falls die gelaufene Aktion es notwendig macht, dazu ein »Bekenner*innenschreiben« anzufertigen, sollte dies zwar schon vorher diskutiert sein, aber möglichst nicht schon irgendwo fertig herumliegen, weil dies, falls eine Aktion schiefgeht und die Bullen eine Hausdurchsuchung machen, der beste Beweis für eure Beteiligung daran wäre. Besser ist es in fast jedem Fall, sich erst danach hinzusetzen und so ein Teil zu verfassen. Dabei muss darauf geachtet werden, keine Spuren zu hinterlassen. Falls ihr das Schreiben auf Papier anfertigt, sollten auf Blatt und Umschlag keinerlei Fingerabdrücke oder DNA Spuren zu finden sein.

Wahrscheinlich entscheidet ihr euch dafür, das Schreiben auf *radikal.news* zu veröffentlichen oder auf *indymedia.de* hochzuladen. In dem Fall solltet ihr darauf achten, keine Spuren auf eurem Computer zu hinterlassen. **Daher ist es sinnvoll das Live-Betriebssystem Tails zu verwenden.** Mehr dazu findet ihr im Ersten Teil unter Tails&Tor.

Im Januar 2026 kam der Verlag in das Licht der Aufmerksamkeit, weil

- ein Autor des Verlags bei einem Treffen in Basel (Schweiz) **mutmaßlich zu Anschlügen auf die technische Infrastruktur aufgerufen haben soll**
- der Verdacht entstand, dass dieser Autor im Zusammenhang mit dem Anschlag auf die Stromversorgung in Berlin Lichtenfelde am 3. Januar 2026 und die berüchtigte „Vulkangruppe“ steht, deren Werdegang der frühen RAF gleicht,
-
- der Verlag im Oktober 2025 im Rahmen des Deutschen Verlagspreises einen mit 50.000 Euro dotierten Spitzenpreis erhielt.

Der Preis wurde vom Beauftragten der Bundesregierung für Kultur und Medien (BKM) verliehen

14.6.2 Die Rote Hilfe

In der Terrorfibel heißt es weiter

[Seite 79]

Rote Hilfe

Die *Rote Hilfe* ist eine Solidaritätsorganisation, die politisch Verfolgte aus dem linken Spektrum unterstützt. Von der Roten Hilfe könnt ihr Geld bekommen, um Repressionskosten zu zahlen. Wenn es in eurer Stadt eine Ortsgruppe gibt, könnt ihr euch dort vielleicht auch

zu Repressionfragen beraten lassen. Die Rote Hilfe kann auch Kontakt zu Anwält*innen herstellen.

Auf der Internetseite rote-hilfe.de findet ihr im Downloadbereich gutes Informationsmaterial zu vielen Repressionsthemen (etwa zu Hausdurchsuchung, DNA-Entnahme, Anquatschversuchen, Beugehaft oder zum Umgang mit Strafbefehlen).

Nach der Wahl zum Berliner Abgeordnetenhaus im September 2026, aus der die LINKE als Wahlsieger hervorging und voraussichtlich die Regierung in Berlin übernimmt, stellte sich heraus, dass

- die LINKE, insbesondere Ferat Koçak, Verbindungen ins kriminelle Berliner Clan-Milieu hat,
- deren Bürgermeisterkandidatin Elif Eralp mehrere Jahre **Mitglied im linksextremen Verein „Rote Hilfe“** war.

14.6.3 Die Capulcu-Gruppe

Die Capulcu-Gruppe beschreibt sich als Autorenkollektiv auf der **Webseite des Unrast-Verlags**:

çapulcu redaktionskollektiv

Çapulcus sind (türkisch) ›Wegelagerer‹ bzw. ›Nichtsnutze‹. Der damalige Ministerpräsident Erdogan versuchte mit dieser Bezeichnung, die Regierungsgegner*innen der breiten Revolte 2013 zu diffamieren. Statt über die Gezi-Proteste in Istanbul zu Beginn des Aufstands zu berichten, ließ Erdogan eine Pinguin-Dokumentation im Staats-Fernsehen zeigen. Der Widerstand machte daraufhin den Pinguin zu seinem Symbol. Die Revoltierenden nannten sich fortan Çapulcus.

Das çapulcu redaktionskollektiv ist eine Gruppe technologie-kritischer Aktivist*innen und Haktivist*innen, die seitdem ihre Arbeit solidarisch in diesen Kontext stellt. Sie veröffentlicht Texte in verschiedenen linken Medien, bringt regelmäßig Broschüren heraus und bietet Diskussionen, Seminare und Schulungen für linke Aktivist*innen, Journalist*innen und Anwält*innen an.

Dieses readaktionskollektiv çapulcu gibt bei digitalcourage eine **60-seitige Anleitung zur Nutzung des Tails-Betriebssystems** aus der Reihe „Hefte zur Förderung des Widerstands gegen den technologischen Angriff“ heraus. Zentrales Thema: „Nur über Tor ins Netz“.

Auch die **Antifa** arbeitet – natürlich – mit der Capulcu-Gruppe zusammen. Und netzpolitik.org war schon 2015 **von denen begeistert**:

Das linke Internet- und Technik-Kollektiv „Capulcu“ veröffentlichte kürzlich zwei Broschüren, die sich zum einen mit dem Schutz eigener Daten vor dem Zugriff Dritter und zum anderen mit der politischen Dimension des Angriffs auf unsere Privatsphären auseinandersetzen.

Dabei soll der erste Band „Anleitung zur Nutzung des Tails Live-Betriebssystems für sichere Kommunikation, Recherche, Bearbeitung und Veröffentlichung sensibler Dokumente“,

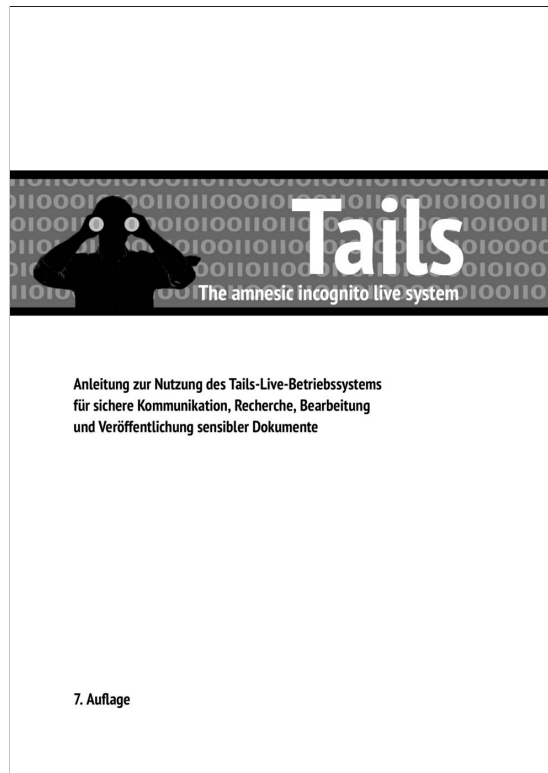


Abbildung 14.2: Broschüre zur Umgehung der IP-Adressspeicherung

wie der Titel schon verrät, einen Leitfaden dazu liefern, um sich vor Angriffen der Geheimdienste zu schützen, etwa dann, wenn man sensible Dokumente bearbeitet oder sich mit vertraulichen Quellen austauschen möchte. Um nicht in die Fänge des automatisierten Spionageprogramms Turbine zu geraten, empfiehlt das Kollektiv das Live-Betriebssystem Tails. Die Anleitung erhebt den Anspruch, auch für Computer-Laien verständlich und hilfreich zu sein.

Soll keiner sagen, es wäre nicht bekannt, was die machen.

14.6.4 Kulturstaatsminister Weimer

Am 22.12.2025 legte die Bundesregierung ihren ersten Referentenentwurf für die IP-Adressspeicherung vor.

Kurz vorher, am 15.10.2025, zeichnete die Bundesregierung in Person ihres Kulturstaatsministers Weimer eben jenen Unrast-Verlag mit dem mit 50.000 Euro dotierten „Deutscher Verlagspreis 26“ aus.

Die Bundesregierung hat also kurz vor dem Referententwurf, **in dem sie behauptet, die Adressspeicherung sei zur Bekämpfung der Kriminalität erforderlich**, man wolle damit „alle Formen der Gewalt“ und „alle Formen organisierter Kriminalität“ be-

kämpfen, einem Verlag 50.000 frisch gewaschene Euro zugespielt, der die gewaltbereite linksextreme Szene, die Gewalt „gegen rechts“ übt, mit Anleitungen versorgt, wie man eben diese Adressspeicherung aushebelt.

Aus der Begründung des Kulturbeauftragten:

Unrast Verlag

In dieser Zeit, in der kritisches Denken, das Infragestellen traditioneller Normen, von allen Richtungen her bedroht wird, tun wir gut daran, uns Texten zu versichern, die zum intellektuellen und politischen Ungehorsam, zum tieferen und weiteren Verständnis unserer Welt ermutigen. Seit 36 Jahren schon hat sich der Unrast Verlag aus Münster genau diesem Ansinnen, diesem einen Interesse verschrieben. Die Ungeduld im Namen müssen wir programmatisch verstehen: undogmatisch, und thematisch breit aufgestellt, ist der Unrast Verlag dem Traum einer anderen Wirklichkeit verpflichtet. Die über 528 Titel – von antifaschistischer und feministischer Gesellschaftstheorie bis hin zu internationaler Belletristik und Graphic Novels -, die der Verlag bisher veröffentlicht hat, beweisen die Treue, die der Verlag seiner Gründungsidee hält.

Ein Betriebsunfall war das nicht.

Teil III

Rechtliche Mängel

15 Meinungsfreiheit

15.1 Der Bundesgerichtshof

Eine Beschränkung der Meinungsäußerungsfreiheit auf Äußerungen, die einem bestimmten Individuum zugeordnet werden können, ist mit Art. 5 Abs. 1 Satz 1 GG nicht vereinbar. Die Verpflichtung, sich namentlich zu einer bestimmten Meinung zu bekennen, würde nicht nur im schulischen Bereich, um den es im Streitfall geht, die Gefahr begründen, dass der Einzelne aus Furcht vor Repressalien oder sonstigen negativen Auswirkungen sich dahingehend entscheidet, seine Meinung nicht zu äußern. Dieser Gefahr der Selbstzensur soll durch das Grundrecht auf freie Meinungsäußerung entgegen gewirkt werden (vgl. Ballhausen/Roggenkamp K&R 2008, 403, 406). (VI ZR 196/08)

15.2 Der Bundeskanzler

 tagesschau Live  

[Startseite](#) ▶ [Inland](#) ▶ [Gesellschaft](#) ▶ Kanzler Merz für Klarnamenpflicht im Internet



Soziale Medien

Merz will Klarnamen im Internet lesen

Stand: 19.02.2026 • 08:32 Uhr

Internet-Nutzer sollen sich nach dem Willen von Kanzler Merz künftig nicht mehr anonym äußern dürfen. Merz setzt sich für eine Klarnamenpflicht ein, um die freiheitliche Gesellschaft zu schützen.

Abbildung 15.1: Tagesschau vom 19.02.2026

16 Rechtliches Gehör, Rechtswegsgarantie, Unschuldsvermutung

16.1 Das Pferd von hinten aufgezäumt

In den USA war und ist es seit dem Wilden Westen gute Tradition, für einen Mord nicht den Hinzurichten, der nachweislich der Täter war, sondern einfach immer den, der sich gegen die Anklage am wenigsten wehren kann.

Das hat sich bewährt. Es ist billiger, führt zu deutlich höheren Verurteilungsquoten und kürzt langwierige, zeitraubende Gerichtsprozesse und Nachweispflichten ungemein ab. Und es führt auch immer zum Erfolg. Einer wird immer gehängt.

Nicht wesentlich anders, nur formalrechtlich ausgefeilter, arbeitet die deutsche Justiz.

Man fragt nicht, ob jemand der Täter war.

Man fragt, welche Beweis- oder Verantwortungsfiktion man braucht, um am leichtesten jemanden zu verurteilen.

Deutsche Gerichte betreiben keine Rechtsfindung. Sondern sie entscheiden willkürlich, politisch, sofort und mit dem geringsten Aufwand, und betreiben dann *hinterher* Begründungsfindung. Und wenn erforderlich, auch noch Voraussetzungs- und Verantwortlichenfindung. Das ist nicht rechtsstaatlich. Das ist das Gegenteil, das ist justizstaatlich.

Befördert wird dies durch die Geisteswissenschaften, deren marxistische Denkweisen und Leithammel wie Michel Foucault und Jürgen Habermas, die nicht mehr die Wirklichkeit und Realität betrachten, sondern mittels willkürlicher „Diskurse“ unter Utopien subsumieren, die so gebaut sind, dass sie das gewünschte Ergebnis liefern. Dann wird moralisch, politisch, nach Konformität und politischer Position entschieden.

Das glauben Sie mir nicht? Die Pressekommission des Verwaltungsgerichts Berlin hat mir schon die Ansichten von Habermas statt geltenden Rechts vorgehalten.

Bei uns nennt man das dann „freie Beweiswürdigung“, „Störerhaftung“ und so, um eine Urteilung da zu erreichen, wo die Sach- und Beweislage das nicht hergibt.

Diese Herangehensweise wird fortgeführt und weiterentwickelt, indem man nun mit

der IP-Adressspeicherung eine Maschine baut, die auf die Fließbandstrafanzeigen der Staats-, Regierungs- und Partei-NGOs wie „Meldestelle REspect!“, „HateAid“, „so-done“ im Massenverfahren einfach und am laufenden Band nicht nachprüfbare Beschuldigungen ausspuckt, die dann automatisch zur Verurteilung samt Kostentragungspflicht führen.

Im Namen des Volkes. Zugunsten der Partei. Nicht selten in die Taschen von Abgeordneten.

16.2 Versagen des Richterbundes

Der Deutsche Richterbund **begrüßt den Gesetzentwurf:**

Der Deutsche Richterbund begrüßt den Referentenentwurf eines Gesetzes zur Einführung einer IP-Adressspeicherung und Weiterentwicklung der Befugnisse zur Datenerhebung in seiner Gesamtheit ausdrücklich.

Der Referentenentwurf führt die von Seiten des Deutschen Richterbundes seit langem nachhaltig geforderte vorsorgliche Speicherung von IP-Adressen ein und leistet damit einen besonders werthaltigen Beitrag zur Verbesserung der Strafverfolgung unter anderem in den Deliktsbereichen Cybercrime, sexueller Kindesmissbrauch sowie Kinder- und Jugendpornographie. Damit wird den Ermittlern ein dringend notwendiges Werkzeug an die Hand gegeben. Die vorgesehene Speicherpflicht von drei Monaten wird den Bedürfnissen der Praxis gerecht. Sie ist maßvoll ausgestaltet. Die Aussagekraft der zu speichernden Daten ist auf das für die Strafverfolgung zwingend Notwendige begrenzt. Die Speicherpflicht stellt daher keinen unverhältnismäßigen Eingriff in Bürgerrechte dar. Sie bringt das Interesse des Staates an einer effektiven Aufklärung von Straftaten in einen angemessenen Ausgleich mit den Grundrechten derjenigen Bürgerinnen und Bürger, die von der Speicherung betroffen sind.

Das geht an der Sache vorbei, denn es betrachtet nur die Eingriffstiefe in die *Bürgerrechte* durch die *Speicherpflicht*.

Die Rechte von Betroffenen missbräuchlicher Zugriffe auf die Speicherung werden erst gar nicht betrachtet.

Unmittelbar nach der Veröffentlichung des Referentenentwurfs war in der rechtspolitischen Debatte vereinzelt von einer „anlasslosen Massenüberwachung“ die Rede, mit der ein „heftiger Eingriff in die Bürgerrechte“ verbunden sei.

Diese Kritik ist verfehlt. Sie wird dem Inhalt des Referentenentwurfs nicht gerecht und suggeriert unzutreffend, dass es sich bei der vorgesehenen Speicherpflicht um eine besonders grundrechtsintensive Maßnahme handeln würde.

Die Anbieter für Internetzugangsdienste werden durch § 176 TKG-E lediglich dazu verpflichtet, für die Dauer von drei Monaten die Information darüber zu speichern, welchem Internetanschluss eine IP-Adresse zu einem bestimmten Zeitpunkt zugeordnet war. Darüber hinaus sind weitere Daten wie die Portnummern und weitere Verkehrsdaten zu speichern, sofern dies für die eindeutige Zuordnung der IP-Adresse zu einem Anschlussinhaber erforderlich ist.

Informationen über besuchte Internetseiten oder genutzte Online-Dienste sind demgegenüber gerade nicht zu speichern.

Anders als teilweise in der öffentlichen Debatte unterstellt, werden die Anbieter auch nicht zur vorsorglichen Speicherung von Informationen über den geographischen Standort eines internetfähigen Geräts zu einem bestimmten Zeitpunkt (sogenannte Standortdaten) oder sonstiger Verkehrsdaten verpflichtet.

Das ist falsch, wie oben unter 3.1.5 ausgeführt.

Dass die Standorte nicht gespeichert würden, bezieht sich nur auf Mobilfunkzellen.

Überwacht man aber die Verkehrsdaten beim Zugriff auf Mailboxen, Social Media usw., bekommt man die IP-Adressen, von denen aus zugegriffen wurde. Wenn das persönliche Handy dann in einem WLAN eingebucht war, etwa dem der eigenen Wohnung, dem Gastnetz einer anderen Privatwohnung, ein Flughafen, Restaurant, Bahnhof, dann weiß man spätestens mit einer TKG-Abfrage, oft aber schon nach einer einfachen Whois- oder RDAP-Abfrage, wo derjenige sich aufhält.

16.3 Beweisfiktion, Unschuldsvermutung, Beweislastumkehr

16.3.1 Beweis durch Ignoranz

Sowohl aus der Diktion des Gesetzesentwurfs, als auch aus dem Text der ETSI TS 102 657 geht hervor, dass das Ziel ist, Provider-Auskünfte als „Beweise“ anzusehen und zu verwenden.

Auch die Erfahrung mit straf- und zivilrechtlichen Gerichten zeigt, dass Richter hemmungslos und willkürlich

- per „freier Beweiswürdigung“ alles als Beweis nehmen, was nicht bei drei auf dem Baum ist,
- und was auf dem Baum ist, beschlagnahmen oder von der Polizei vorführen lassen.

In Deutschland ist inzwischen gar nichts mehr zu falsch, zu willkürlich oder zu blöd, um nicht von Leuten in albernen Kitteln im Namen des Volkes, der Wissenschaft oder irgendeines Gottes für richtig, zwingend und bewiesen erklärt zu werden.

Wie schon oben im Abschnitt 3.1.2 erläutert, **ist das Internet nicht „sicher“, es ist nicht als sicher spezifiziert und nicht konstruiert, und es hat keine Sicherheitseigenschaften.** Nur so funktioniert es. Sicherheit ist immer eine Angelegenheit der höheren (End-zu-End) oder – seltener – der darunterliegenden (Node-zu-Node) Schichten.

Man kann keine sicheren, beweisfähigen Daten gewinnen, indem man an ein per se unsicheres System eine Protokollierung anflanscht. Und die Sicherheit und Zuverlässigkeit der Protokollierung selbst kommt im Gesetzentwurf und den technischen Richtlinien erst gar nicht vor.

Man kann ein sicheres System leicht durch Ignoranz unsicher machen. Aber man kann ein unsicheres System nicht zu einem sicheren hochignorieren – nicht einmal durch die besondere staatsexaminierte Ignoranz der Juristen.

Vor einiger Zeit schrieb mich ein Jura-Student an, der eine Hausarbeit über IP-Vorratsdatenspeicherung zu schreiben und deshalb Fragen zu meiner Stellungnahme vom 9. Oktober 2023 hatte.

Es war sehr deutlich zu merken, dass derjenige nicht verstanden hatte, wie das Internet funktioniert, was NAT ist und macht, und dass es bei CGNAT sogar zwei NAT-Stufen gibt. Und dass sein technisches Verständnis sehr, sehr gering war und er sich nur mit sprachlichen Analogien behelf. Das hielt ihn nicht im Geringsten davon ab, zu glauben, die Sache rechtlich beurteilen zu können und dazu berufen zu sein.

Ich habe es oft erlebt, dass Richter völlig willkürlich Dinge als bewiesen annehmen, einfach schon um sich die Arbeit zu erleichtern.

16.3.2 Bruch der Unschuldsvermutung durch Beweislastumkehr

Hier passiert nichts anderes als die Unschuldsvermutung zu brechen und durch eine Beweislastumkehr, die zudem unerfüllbar ist, **jeden Beschuldigten und Angeklagten vollautomatisiert und ohne Sachverhaltsprüfung zum Verurteilten zu machen**. Schuldig durch Logeintrag.

Normalerweise müsste die Anklage dem Beschuldigten/Angeklagten nachweisen, dass er die Tat begangen hat.

Wenn die IP-Adressspeicherung aber zu einem Vorgang mit einer IP-Adresse und Uhrzeit einen angeblichen oder vermeintlichen Anschlussinhaber identifiziert, wird das einfach als „bewiesen“ hingestellt – obwohl es nichts anderes ist, als dass eine Maschine einfach irgendeinen Namen aus der Kundendatenbank ausgespuckt hat – ohne dass noch eine Möglichkeit der Nachprüfung oder Fehlerprüfung bestünde.

Man wird von einem fehleranfälligen Automaten beschuldigt, das wird zum Beweis erhoben, und man hat in der Regel keine Möglichkeit mehr, den „Beweis“ zu widerlegen.

16.4 Verantwortungsfiktion

16.4.1 Das Verantwortungsparadoxon

Es ist erstaunlich: Immer wieder legen „Hacker“ – meist Erpresser mit „Ransomware“, die Daten verschlüsselt und dann Lösegeld fordert – ganze Gerichte, Stadtverwaltungen, Landkreisverwaltungen, Behörden, Universitäten für Monate lahm. **2019 war sogar das Berliner Kammergericht für lange Zeit lahmgelegt.**

Die Politik jammert ständig, wir bräuchten ein „Cyberabwehrzentrum“, weil alle Welt, Chinesen, Russen, Amerikaner uns permanent angreifen würden.

Geht es aber um einen *privaten* Internetanschluss, dann unterstellen dieselben Politiker und Richter, dass selbstverständlich der Anschlussinhaber selbst für den Anschluss verantwortlich ist und dass die Straftat von dieser IP-Adresse kam, oder zivilrechtlich der Anschlussinhaber als „Störer“ verantwortlich sei – ohne Möglichkeit der Gegenrede.

Wie es ist zu erklären, dass man dem Staat zugesteht, dass er nicht Herr über seine Netzwerke ist, aber Tante Erna, dem gestressten Familienvater mit Hauptschulabschluss, dem Analphabeten unterstellt, sie hätten ihren Internetanschluss und ihre Geräte voll unter Kontrolle?

Warum können dieselben Richter, die die Dienstcomputer in ihrem Gericht nicht sauber halten können, Privatleute als verantwortlich verurteilen, wenn etwas von deren IP-Adresse gekommen sein soll?

16.4.2 „Die Russen waren’s.“

Ein ähnlicher Effekt ist zu beobachten, wenn es zu einem Datenabfluss kam, enorme Datenmengen gestohlen wurden.

Dann steht für Politik und Medien sofort fest: „*Die Russen waren’s.*“

Normalerweise steht sonst immer fest, dass es die Chinesen waren, aber weil gerade Ukraine-Krieg ist, waren es jetzt immer die Russen.

Die Amerikaner können es natürlich nicht gewesen sein, denn wie Kanzlerin Merkel einst verkündete, „Abhören unter Freunden geht gar nicht“.

Dass die Amerikaner die volle Kontrolle über jeden Windows- und jeden Apple-Rechner haben, und selbst die Browser vor Sicherheitslücken strotzen, interessiert niemanden. Richter, Staatsanwälte, das BKA sind überzeugt: Haben sie die IP-Adresse, wissen sie, „von welchem Gerät die Straftat begangen worden ist“ (3.2.3).

Unmittelbar daran schließt sich dann die schöne alte Berliner Polizeitradition an, dem

Anschlussinhaber morgens um 6 Uhr die Wohnungstür einzutreten, ihn mit vorgehaltener Waffe aus dem Bett zu holen und alle Geräte mitzunehmen.

Das ist so lächerlich, dass uns die Amerikaner dafür verspotten und drei deutsche Staatsanwälte als Witzfiguren vorführen ([CBS 60 Minutes](#)), die mit ihrem realitätsverschobenen und rechtsstaatsfernen Auftreten jede Absicht überflüssig machen, Deutschland noch lächerlich machen zu wollen, weil sie in voller Überzeugung lachend zugeben, dass die Beschlagnahme nicht der Ermittlung oder Sicherstellung, sondern der Bestrafung unterhalb einer Strafbarkeitsschwelle diene.

16.4.3 Der Bundestag und die Russen

Es gab mehrere Vorfälle, in denen „die Russen“ Rechner und Abgeordnete des Bundestags angegriffen haben sollen, etwa 2015 ([Wikipedia](#)), 2020 ([Hackerangriff auf den Deutschen Bundestag durch den russischen Militärgeheimdienst GRU](#)) oder 2021 ([Russische Gruppe »Ghostwriter« attackiert offenbar Parlamentarier](#)).

Wenn es aber so viele Angriffe ausländischer Geheimdienste auf deutsche Parlamentarier gibt - warum unterstellen dann dieselben Parlamentarier¹, dass jeder selbst für die Angriffe verantwortlich sei, die von seiner IP-Adresse ausgingen?

Warum gelten für Tante Erna so ganz andere Maßstäbe als für den Deutschen Bundestag?

16.4.4 Webbrowser

16.4.4.1 Sicherheitslücken

Nahezu alles – legal wie illegal – läuft heute über Webbrowser.

Webbrowser sind aber notorisch unsicher (Abbildung [16.1](#) und [16.2](#)).

Webbrowser strotzen vor Sicherheitslücken, die man ausnutzen könnte, um den eigenen Konsum von Kinderpornographie oder das Begehen anderer Straftaten auf die IP-Adressen anderer zu begehen – oder als Rufmord, Verfolgung, berufliche und zivile Erledigung.

16.4.4.2 Böswilliger Web-Content

Dabei bedarf es nicht einmal einer Sicherheitslücke:

¹ Hinweis: Damit meine ich Sie.

271 Firefox-Lücken dank Mythos-KI geschlossen: Durchbruch für IT-Sicherheit?

Anthropics „gefährliche“ KI könnte Verteidigern der IT-Sicherheit den entscheidenden Vorteil liefern. Das meint zumindest das Firefox-Team, das Zugriff hat.

heise.de bei Google bevorzugen

🇬🇧 🔊 🖨️ 💬 200



(Bild: Firefox)

22.04.2026, 11:35 Uhr | Lesezeit: 4 Min. | Security

Von Martin Holland

Abbildung 16.1: Meldung auf **Heise.de**



Abbildung 16.2: Meldung auf **Cyberunit.com**

Man muss einfach nur auf einer Webseite Kinderpornos von einem polizeilich überwachten Kinderpornoserver *unsichtbar* einbinden. Etwa auf die Größe eines Pixels schrumpfen. Hinter einem anderen Seitenelement verstecken. Absolut außerhalb des sichtbaren Fensters platzieren. Mit Offset anzeigen. Und so weiter und so fort.

Es gibt unzählige Möglichkeit, einem arglosen Benutzer Webseiten mit eingebetteten **unsichtbaren** Kinderpornos unterzujubeln, ohne dass er es merkt. Er glaubt, ganz andere, harmlose Webseiten vor sich zu haben.

Trotzdem tauchte die IP-Adresse des arglosen Anwenders nicht nur im Log des Pornoservers auf und könnte zu polizeilichen Ermittlungen führen – bei der Beschlagnahme des Rechners würde man sogar die „Beweise“ finden: Der Zugriff auf die Bilder steht im Browser-Log, und die Bilder selbst finden sich im Browser-Cache.

Für die deutsche Justiz gälte der Benutzer als überführter Straftäter, Gegenbeweis nicht mehr möglich – obwohl er gar nichts gemacht hat und nicht weiß, wie ihm geschieht.

16.4.5 „Crime as a Service“

Die Bundesregierung selbst beantwortet eine Anfrage zu „Crime-as-a-Service“. (Anfrage [BT-Ds 21/4365](#), Antwort [BT-Ds 21/5166](#), [Pressemeldung](#))

Wenn die Bundesregierung aber schon selbst über „Crime as a Service“ als professionalisiertes und aufgabenverteiltes Kriminalitätssystem berichtet – warum fehlt es dann am gedanklichen Schritt dazu, dass

- diese Netzwerke Zugriff auf Millionen von Privatrechnern mit Backdoors, Forwardern, Proxies haben, um auf fremder Leute IP-Adressen zu agieren, sich hinter fremder Verantwortung zu verstecken?
- es gerade Gegenstand der Straftat sein kann, jemand anderen zu belasten, indem man ihm Straftaten im Internet unterjubelt?

Wenn Sie schon die fehlerhafte Analogie von IP-Adressen zu KFZ-Kennzeichen verwenden ([3.2.1](#)), warum ziehen sie dann nicht wenigstens auch die Analogie zu geklauten KFZ-Kennzeichen und geklauten Autos? Zu in das Betriebssystem implantierten Forwardern, Proxies, Browserlücken?

16.4.6 Ransomware 2.0

Es ist eine Frage der Zeit, bis man erpresst wird, Schutzgeld zu zahlen, damit Angreifer nicht über die IP-Adresse des Nutzers Kinderpornos auf Rechner herunterladen, Mordaufrufe starten oder deutsche Politiker kritisieren.

16.5 Kein Rechtsweg

Es gibt keinen effektiven Rechtsweg gegen unrechtmäßige Abfragen.

Gerichte können höchstens innerhalb eines Gerichtsverfahrens ein Beweisverbot aussprechen, aber nicht der Staatsanwaltschaft die Nutzung und Weitergabe untersagen und auch nicht die Löschung anordnen.

Artikel 19 Absatz 4 GG

Wird jemand durch die öffentliche Gewalt in seinen Rechten verletzt, so

steht ihm der Rechtsweg offen. Soweit eine andere Zuständigkeit nicht begründet ist, ist der ordentliche Rechtsweg gegeben. Artikel 10 Abs. 2 Satz 2 bleibt unberührt.

Wie also sieht der Rechtsweg gegen unrechtmäßige Abfragen aus?

Wie erfährt man überhaupt davon?

16.6 Kein rechtliches Gehör

16.6.1 Keine Informationspflicht

Es ist keine Pflicht vorgesehen, den Betroffenen von Abfragen seiner Bestands-, Verkehrs- und anderer Daten zu informieren.

Damit sind rechtliches Gehör und Rechtsweg nicht möglich, wenn man von der Abfrage gar nichts oder erst dann erfährt, wenn es zu spät ist.

Kurioserweise sorgen sich Regierung und Gesetzgeber um „Quick Freezes“, manchmal sogar die Rechte „Unbeteiligter“, aber niemals um die Rechte Betroffener, „Beteiligter“.

Warum werden Unbeteiligte besser geschützt als Beteiligte?

16.6.2 Erforderliche Sachkunde

Das Bundesministerium der Justiz hat rund 30 Stellungnahmen von Verbänden und Fachleuten eingeholt (ZIP-Datei auf [Übersichtsseite](#))

- Vergleichen Sie deren Stellungnahmen – alles Profis ihres Faches – mit meiner als Informatiker mit entsprechender Berufserfahrung und Vorwissen.
- Vergleichen Sie den Arbeitsaufwand, den selbst ich mit einschlägiger Berufserfahrung für die Erstellung dieser Stellungnahme treiben musste, und das Fachwissen, das ich dazu brauchte, mit dem, was einem Richter in einem Straf- oder Zivilprozess zur Verfügung steht, der über *keinerlei* IT-bezogene Ausbildung oder Berufserfahrung verfügt und allein aus einer Laiensphäre heraus agiert.

Sie wagen sich hier in Themenbereiche vor, die selbst unter Informatikern – dezent formuliert – etwas „für Fortgeschrittene“ sind.

16.6.3 Richter?

Es gibt in Deutschland etwa 22.000 Berufsrichter, von denen etwa 4.500 Berufsrichter im Bereich der Straf- und Bußgeldsachen tätig sind.

Wieviele allein dieser 4.500 Strafrichter sollen denn in der Lage sein, das Thema zu durchdringen oder auch nur zu verstehen, wovon ich hier schreibe?

Wieviele dieser Richter können IPv4 von IPv6 unterscheiden?

Wieviele dieser Richter bemerken die Fehler im Gesetzentwurf, wenn schon der Deutsche Richterbund es nicht kann?

Bei welchem dieser Richter wollen Sie *rechtliches Gehör* finden können?

16.6.4 Rechtsanwälte/Strafverteidiger?

Woher sollen Rechtsanwälte als Juristen das Fachwissen haben, solche „Pseudo-Beweise“ auf technischer oder rechtliche Ebene angreifen zu können und ihre Mandanten im – hier sogar gefährlich erhöht – erforderlichen Maß zu verteidigen?

Wie soll eine Verteidigung gegen die vielen möglichen Fehler und Angriffsmöglichkeiten der IP Adressspeicherung möglich sein?

16.6.5 Gerichtsgutachter?

Wo wollen Sie denn die nötige Zahl an sachkundigen und kompetenten Gerichtsgutachtern herbekommen?

Und wer soll die alle bezahlen?

16.6.6 Beschuldigte?

Wie sollen „normale Sterbliche“ in der Lage sein, auch nur das Problem zu verstehen? Zu erkennen, wie ihnen geschieht?

Tante Erna?

Die 90-jährige Oma?

Die Mutter mit 6 Kindern?

Eine 14-Jährige?

Der Sozialhilfeempfänger ohne Ausbildung?

Jemand, der kaum lesen kann?

Jemand, der kein Deutsch kann und gar nicht weiß, wie man sich in Deutschland verteidigt?

16.6.7 Kein Gehör vor der Weitergabe an Privatklässer

Wie schon bei der Vorratsdatenspeicherung 2009 zu sehen war, aber auch in Teil IV ausgeführt wird, gelangen Daten aus der Vorratsdatenspeicherung und polizeilichen Ermittlungen oft über Akteneinsichten und Auskunftsgestattungen an privatrechtliche Klässer weiter.

Ein rechtliches Gehör **vor** der Weitergabe oder überhaupt ein Verbot der Weitergabe und Verwertung außerhalb von Strafverfahren ist nicht ersichtlich.

16.6.8 Beweisverbote des EuGH

16.6.8.1 EuGH C-670/22 (EncroChat)

Der EuGH hat im Fall C-670/22 entschieden:

104 Zum anderen verpflichtet Art. 14 Abs. 7 der Richtlinie 2014/41 die Mitgliedstaaten dazu, sicherzustellen, dass in einem Strafverfahren im Anordnungsstaat bei der Bewertung der mittels einer Europäischen Ermittlungsanordnung erlangten Beweismittel die Verteidigungsrechte gewahrt und ein faires Verfahren gewährleistet werden.

105 Was konkret das Recht auf ein faires Verfahren betrifft, ist insbesondere darauf hinzuweisen, dass ein Gericht, wenn es zu dem Ergebnis kommt, dass eine Partei nicht in der Lage ist, sachgerecht zu einem Beweismittel Stellung zu nehmen, das geeignet ist, die Würdigung der Tatsachen maßgeblich zu beeinflussen, eine Verletzung des Rechts auf ein faires Verfahren feststellen und dieses Beweismittel ausschließen muss, um eine solche Rechtsverletzung zu verhindern (vgl. in diesem Sinne Urteil vom 2. März 2021, Prokuratuur [Voraussetzungen für den Zugang zu Daten über die elektronische Kommunikation], C-746/18, EU:C:2021:152, Rn. 44).

16.6.8.2 EuGH C-746/18 (Vorratsdatenspeicherung)

Und im Fall C-746/18

43 Zum Effektivitätsgrundsatz ist festzustellen, dass die nationalen Vorschriften über die Zulässigkeit und die Verwertung von Informationen und Beweisen darauf abzielen, nach Maßgabe der im nationalen Recht getroffenen Entscheidungen zu verhindern, dass einer Person, die im Verdacht steht, Straftaten begangen zu haben, durch rechtswidrig erlangte Informationen und Beweise unangemessene Nachteile entstehen. Dieses Ziel kann aber im nationalen Recht nicht nur durch ein Verbot der Verwertung solcher Informationen und

Beweise erreicht werden, sondern auch durch nationale Vorschriften und Praktiken für die Würdigung und Gewichtung der Informationen und Beweise oder durch eine Berücksichtigung ihrer Rechtswidrigkeit im Rahmen der Strafzumessung (Urteil vom 6. Oktober 2020, *La Quadrature du Net* u. a., C-511/18, C-512/18 und C-520/18, EU:C:2020:791, Rn. 225).

44 Ob es erforderlich ist, Informationen und Beweise auszuschließen, die unter Verstoß gegen unionsrechtliche Vorschriften erlangt wurden, ist insbesondere anhand der Gefahr zu beurteilen, die mit der Zulässigkeit solcher Informationen und Beweise für die Wahrung des Grundsatzes des kontradiktorischen Verfahrens und damit für das Recht auf ein faires Verfahren verbunden ist. Kommt ein Gericht zu dem Ergebnis, dass eine Partei nicht in der Lage ist, sachgerecht zu einem Beweismittel Stellung zu nehmen, das einem Bereich entstammt, in dem das Gericht nicht über Sachkenntnis verfügt, und das geeignet ist, die Würdigung der Tatsachen maßgeblich zu beeinflussen, muss es eine Verletzung des Rechts auf ein faires Verfahren feststellen und dieses Beweismittel ausschließen, um eine solche Rechtsverletzung zu verhindern. Der Effektivitätsgrundsatz verpflichtet ein nationales Strafgericht somit dazu, im Rahmen eines Strafverfahrens gegen Personen, die im Verdacht stehen, Straftaten begangen zu haben, Informationen und Beweise, die durch eine mit dem Unionsrecht unvereinbare allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten oder durch einen unionsrechtswidrigen Zugang der zuständigen Behörde zu den fraglichen Daten erlangt wurden, auszuschließen, sofern diese Personen nicht in der Lage sind, sachgerecht zu den Informationen und Beweisen Stellung zu nehmen, die einem Bereich entstammen, in dem das Gericht nicht über Sachkenntnis verfügt, und geeignet sind, die Würdigung der Tatsachen maßgeblich zu beeinflussen (vgl. in diesem Sinne Urteil vom 6. Oktober 2020, *La Quadrature du Net* u. a., C-511/18, C-512/18 und C-520/18, EU:C:2020:791, Rn. 226 und 227).

45 Nach alledem ist auf die erste und die zweite Frage zu antworten, dass Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 sowie von Art. 52 Abs. 1 der Charta dahin auszulegen ist, dass er einer nationalen Regelung entgegensteht, die es Behörden zur Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten ermöglicht, Zugang zu einem Satz von Verkehrs- oder Standortdaten zu erlangen, die geeignet sind, Informationen über die von einem Nutzer eines elektronischen Kommunikationsmittels getätigten Kommunikationen oder über den Standort der von ihm verwendeten Endgeräte zu liefern und genaue Schlüsse auf sein Privatleben zuzulassen, ohne dass sich dieser Zugang auf Verfahren zur Bekämpfung schwerer Kriminalität oder zur Verhütung ernster Bedrohungen der öffentlichen Sicherheit beschränken würde; dies gilt unabhängig davon, für welchen Zeitraum der Zugang zu den betreffenden Daten begehrt wird und welche Menge oder Art von Daten für einen solchen Zeitraum verfügbar ist.

16.6.8.3 Anwendung auf nationales Recht

Zwar bezieht sich der EuGH in diesen Entscheidungen nur auf Unions- und nicht auf nationales Recht.

Aber auf welcher Grundlage sollte man auf nationaler Ebene schwächere Anforderungen und Maßstäbe für ein „faires Verfahren“ und rechtliches Gehör anstellen wollen?

Sollte Deutschland beim „fairen Verfahren“ deutlich hinter die EU zurücktreten wollen?

Insofern kann für deutsches nationales Recht kein geringeres Schutzniveau gelten.

Folglich unterliegen Auskünfte der Vorratsdatenspeicherung einem Beweisverbot, weil weder die Gerichte über die nötige Sachkunde verfügen, noch die Beschuldigten und ihre Anwälte in der Lage sind, sachgerecht zur Informationen und Beweisen Stellung zu nehmen.

16.7 Verfassungswidrigkeit des Gesetzentwurfs

Der Gesetzentwurf ist verfassungswidrig.

Er verletzt in mehrfacher und eklatanter Weise das rechtliche Gehör und die Rechtswegsgarantie.

Er belastet Verdächtige, Beschuldigte und Angeklagte mit fehlerbehafteten und nicht nachprüfaren Pseudobeweisen am Fließband und verletzt die Unschuldsvermutung, weil er zu einer nicht erfüllbaren Umkehrung der Beweislast führt.

In Verbindung mit den in Teil I beschriebenen technischen Fehlern und forensischen Mängeln besteht die Gefahr, dass in signifikanter Zahl Unschuldige ohne Möglichkeit der Verteidigung verurteilt werden, und dabei – typisch für deutsche Justiz – deren Bestreiten noch als strafverschärfend gewertet wird.

17 Berufsgeheimnis, Pressefreiheit, Datenschutz

17.1 Das Berufsgeheimnis und seine Schändung

17.1.1 Die Rechtslage

Wesentliche zu beachtende Normen sind

Artikel 5 Absatz 1 GG: Die Meinungs- und Pressefreiheit, aus der auch das Redaktionsgeheimnis und der Schutz der Presse hervorgehen.

§ 53 StPO: Das Zeugnisverweigerungsrecht der Berufsgeheimnisträger, namentlich der Geistlichen, Verteidiger, Rechtsanwälte, Ärzte, Apotheker, Mitglieder des Bundestages und der Landtage und Personen, die bei der Vorbereitung, Herstellung oder Verbreitung von Druckwerken, Rundfunksendungen, Filmberichten oder der Unterrichtung oder Meinungsbildung dienenden Informations- und Kommunikationsdiensten berufsmäßig mitwirken oder mitgewirkt haben.

§ 97 StPO: Beschlagnahmeverbot

§ 500 StPO: Da die DSGVO nicht für die Strafverfolgung gilt, rückt an deren Stelle Teil 3 des BDSG.

§ 46 BDSG Nr 14: „besondere Kategorien personenbezogener Daten“

- a) Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen,
- b) genetische Daten,
- c) biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person,
- d) Gesundheitsdaten und
- e) Daten zum Sexualleben oder zur sexuellen Orientierung;

§ 48 BDSG: Grundsätze für die Verarbeitung besonderer Kategorien personenbezogener Daten wie die Verschlüsselung

Die Verarbeitung besonderer Kategorien personenbezogener Daten ist nur zulässig, wenn sie zur Aufgabenerfüllung unbedingt erforderlich ist.

17.1.2 Die Schändung durch die Justiz

Die Praxis zeigt, dass sich Polizei, Staatsanwaltschaft und Gerichte nicht nur nicht darum scheren und dies völlig übergehen, sondern dass sie diese Vorschriften auch nicht kennen und nicht verstehen. Sie wollen sie nicht einhalten, aber sie könnten es nicht einmal, wenn sie wollten.

Die Rechte scheinen völlig unbekannt zu sein.

Ich lege dies ausführlich mit Belegen in den Teilen IV und V dar.

17.1.3 Kein Schutz im vorliegenden Gesetzentwurf

Berufsgeheimnisse, Pressegeheimnis, Datenschutz kommen im vorliegenden Entwurf nicht oder nur ganz am Rande bezüglich der Übertragungssicherheit beim Provider vor.

Man könnte dagegen einwenden, dass dies auch nicht erforderlich sei, weil die oben genannten Vorschriften schon entsprechend binden.

Das stimmt aber nicht. Die Justiz hält sich nicht nur tatsächlich nicht daran, es ist auch systematisch nicht möglich, den Schutz einzuhalten.

Woher sollte die Polizei vor der Abfrage des Inhabers eines Anschlusses und seiner Kommunikationspartner wissen, dass der Anschlussinhaber ein Arzt ist, der Videotelefonate für Patienten anbietet?

Oder dass der Anschlussinhaber ein Pfarrer, ein Bundestagsabgeordneter oder ein Journalist ist, dem sich jemand anvertraut hat?

Folglich müssten alle Anschlussinhaber die Möglichkeit haben, bei ihrem Provider anzugeben, dass sie Berufsgeheimnisträger sind. Und in jeder Anfrage müsste angegeben sein, ob die Voraussetzungen gegeben sind, trotz Berufsgeheimnisses anzufragen.

17.1.4 Befürchtungen der Bundesrechtsanwaltskammer

Die Bundesrechtsanwaltskammer **äußert schwere Bedenken** bezüglich des Berufsgeheimnisses:

Ein zentraler Kritikpunkt betrifft den Schutz des anwaltlichen Berufsgeheimnisses. Durch die Speicherung und Zuordnung von IP-Adressen könne nachvollzogen werden, wann Mandant:innen mit einer Rechtsanwaltskanzlei in Kontakt getreten sind. Bereits diese Metadaten erlaubten Rückschlüsse auf Mandatsverhältnisse und berührten damit den Kernbereich der anwaltlichen Berufsausübung gemäß § 53 StPO.

Der Entwurf enthalte keine ausreichenden prozeduralen Sicherungen, um zu verhindern, dass Kommunikationsdaten von Berufsgeheimnisträgern gesichert oder in Ermittlungsmaßnahmen einbezogen werden.

Ich stimme dem nicht nur zu. Ich gehe darüber hinaus.

Denn nicht nur kann damit (siehe 3.1.5) etwa der Aufenthaltsort eines rechtlichen Beistand suchenden Gesuchten bestimmt werden, sondern **allein schon die Gefahr, dass das passieren könnte, führt, ebenso wie bei der Meinungsfreiheit (Kapitel 15) zu einem „chilling effect“**, weil sich der Hilfesuchende nicht mehr traut, einen Anwalt zu kontaktieren.

17.2 Der Presseausweis als untauglicher Anknüpfungspunkt

17.2.1 Umgang der Justiz mit dem Presseausweis

Seit vielen Jahren passiert es mir immer wieder, dass insbesondere die Pressesprecher von Staatsanwaltschaften und Gerichten sehr oft, manchmal auch Behörden und Anstalten öffentlichen Rechts (z. B. Berliner Verkehrsbetriebe) für Presseauskünfte **die Vorlage des Presseausweises** verlangen.

Dem kann ich nicht nachkommen, weil ich als Blogger zwar Presse bin, aber aus nicht ersichtlichen Gründen keinen Presseausweis erhalte.

Inzwischen haben das Bundesverwaltungsgericht (10 A 5.23), der Bundesgerichtshof (VI ZR 426/24) und das Obergerverwaltungsgericht Berlin-Brandenburg in mehreren Entscheidungen endlich klargestellt, dass auch elektronische redaktionelle Medien dem Schutz der Pressefreiheit unterliegen, was die Presserechtskammer des Verwaltungsgerichts Berlin jahrelang so eigenmächtig wie willkürlich und ohne Begründung verweigert und als Privileg von Druckmedien angesehen hatte. In den Köpfen von Richtern (vor allem der unteren Instanzen), Staatsanwälten, Politikern und Journalisten ist das aber nicht angekommen und wird es wohl auf lange Zeit auch nicht.

Viele Gerichte und Staatsanwaltschaften halten noch immer stur daran fest, dass einen presserechtlichen Auskunftsanspruch ihnen gegenüber nur der hat, der einen *Presseausweis* vorlegt – und nicht selten konsterniert sind, wenn ich dagegen förmlich Widerspruch einlege und ihn damit begründe, dass die anzuwendende Norm das jeweilige Landespressegesetz sei und darin von einem Presseausweis kein Wort stehe.

Erstaunlich viele Pressesprecher – stets selbst Richter oder Staatsanwälte – scheitern *als Pressesprecher* am Verständnis des eigenen Landespressgesetzes und der Anwendung der Frage, wer Presse ist und wer nicht, und verlagern die Entscheidung auf andere, indem sie stur an der Vorlage eines Presseausweises festhalten.

Man wird dies bei der Frage der Anwendung der §§ 53, 97 StPO und damit der Kommunikationsüberwachung kaum anders handhaben wollen und können.

17.2.2 Die Rechtslage

Der sogenannte (und einzig von Regierung, Gerichten und Behörden anerkannte) „Bundeseinheitliche Presseausweis“ existiert *rechtlich* eigentlich gar nicht. Er ist rechtlich nicht geschützt und unterscheidet sich in seinem Gehalt überhaupt nicht von jedem anderen beliebig ausgedruckten Phantasieausweis. *Lediglich das Design ist gegen Nachahmung geschützt (Quelle: presseausweis.de):*

Der Presseausweis ist zum Schutz vor Nachahmern als Geschmacksmuster beim Deutschen Patent- und Markenamt hinterlegt. Jeder Nachahmer wird auf Unterlassung und Schadenersatz in Anspruch genommen.

Die Anerkennung des – und nur des – „bundeseinheitlichen Presseausweises“ ist völlig willkürlich und entbehrt jeglicher Rechtsgrundlage.

Es ist eine Korruptionsverbindung zwischen Politik und staatskonformen Medien.

17.2.3 Die Innenministerkonferenz

In Deutschland beruht der Presseausweis auf einer „**Vereinbarung zwischen der Innenministerkonferenz und dem Presserat**“ von 2016. Welche Rechtsform und Rechtswirkung das habe soll, und woher die Innenminister befugt sein sollten, die Länder, oder der Presserat die Presse zu vertreten, bleibt offen.

Auf Anfragen und Beschwerden bekommt man von der Innenministerkonferenz nur inhaltslose, inkompetente und oft unsinnige oder blöde Abwimmelantworten – aber jährlich wechselnd, weil der Vorsitz der IMK jährlich wechselt.

Auf eine **Ausarbeitung des Wissenschaftlichen Dienstes** des Deutschen Bundestags dazu wird verwiesen.

17.2.4 Abwimmeln, Täuschen, Hinhalten

17.2.4.1 Zuständigkeits-Ping-Pong

- Richtet man Fragen oder Beschwerden an die Innenministerkonferenz, wird man mit dem Argument abgewimmelt, der Staat habe sich da nicht einzumischen, das sei allein Sache des Presserats.

An den müsse man sich wenden.

- Richtet man Fragen oder Beschwerden an den Presserat, wird man mit dem Argument abgewimmelt, der Presseausweis konstituiere gar nichts, und wie Staat und Behörden damit umgingen, sei allein Sache der Innenminister.

An die müsse man sich wenden.

17.2.4.2 Bedeutungswechsel

- Beschwert man sich darüber, keinen Ausweis zu erhalten, bekommt man als Antwort, der Ausweis sei gar nicht erforderlich und konstituiere gar nichts, er sei lediglich eine *Beweiserleichterung* für hauptberufliche Journalisten.
- Bittet man aber bei Staatsanwaltschaften oder Gerichten um Presseauskünfte, erhält man als Antwort, dass ohne den Presseausweis gar keine Auskünfte erteilt werden können, der sei zwingende formale Voraussetzung.

17.2.4.3 Das Beweisparadoxon

- Fragt man die Innenministerkonferenz, für *welchen Beweis* der Presseausweis nur eine *Beweiserleichterung* sei, und wie man den Beweis ohne Ausweis, also unter erschwerten Bedingungen antreten könne, dann verweist einen die Innenministerkonferenz mit Hinweis auf die Uabhängigkeit der Presse an den Presserat.
- Fragt man aber den Presserat, dann verweist der an die Innenministerkonferenz, weil die doch wissen und entscheiden müssten, welche Nachweise sie für Auskünfte fordern.

17.2.4.4 Beschwerde-Ping-Pong

- Beschwert man sich bei der Innenministerkonferenz über die Nichteinhaltung der Vereinbarung, bekommt man als Antwort, es sei eine Selbstverpflichtung und damit Sache des Presserats.
- Beschwert man sich beim Presserat, heißt es, es sei Sache der Innenministerkonferenz als Vereinbarungspartner, Verletzungen zu rügen.

17.2.5 Ein verfassungswidriges Schatten-Pressecorps

17.2.5.1 Willkür in das Privatrecht verlagert

Bei gehöriger Betrachtung wird hier ein verfassungswidriges und politisch gesteuertes Schatten-Pressecorps mit faktischen Kooptationsrecht errichtet, das man perfiderweise gerade mit dem Argument der Unabhängigkeit der Presse und der verfassungsrechtlichen Schutz derart in das Privatrecht verschiebt, dass ein Rechtsweg nach Artikel 19 IV GG oder die Privatklage unmöglich sind.

17.2.5.2 Der doppelgesichtige Deutsche Journalistenverband

17.2.5.2.1 Das öffentliche Gesicht des DJV Der DJV fällt in diesem Zusammenhang zunächst damit auf, dass er den vorliegenden Gesetzentwurf kritisiert und sich um die Rechte von Journalisten sorgt: **IP-Adressen – Berufsgeheimnis weiter schützen**

Das Medienbündnis, dem auch der Deutsche Journalisten-Verband angehört, fordert das Bundesjustizministerium auf, den vorhandenen Schutz von journalistischen Berufsgeheimnisträgern zu erhalten.

Anlass ist der Referentenentwurf des BMJV für das Gesetz zur Einführung einer IP-Adressspeicherung und Weiterentwicklung der Befugnisse zur Datenerhebung im Strafverfahren. Demnach könnten Ermittlungsbehörden einfacher als bisher auf digitale Verkehrs- und Nutzungsdaten von Journalistinnen und Journalisten zugreifen, was den Zugriff auf journalistische Quellen und Rechercheinhalten erleichtert. Darüber hinaus ermöglicht der Entwurf die Erstellung von Bewegungsprofilen. Für Journalistinnen und Journalisten wäre es fatal, wenn Polizeibehörden den Rechercheschwerpunkt nach geografischen Daten orten könnten, da sie so gezielt Recherchen vorab beeinflussen können. Schließlich fehlt eine effektive gerichtliche Kontrolle dieser Maßnahmen, was aus Sicht des Medienbündnisses mit EU-Recht nicht vereinbar ist.

„Die Presse- und Rundfunkfreiheit gebietet es, dass gerade im digitalen Raum der journalistische Berufsgeheimnisschutz gewahrt bleibt“, erklärt DJV-Bundesvorsitzender Mika Beuster. Er erwarte vom Gesetzgeber, dass er die Bedenken des Medienbündnisses ernst nimmt.

17.2.5.2.2 Das andere Gesicht des DJV Das andere Gesicht des DJV ist, dass er über die oben beschriebene Auslagerung der Vergabe von Presseausweisen und der Entscheidung darüber zum rechtlich nicht angreifbaren Willkürdienstleister, der politisch erwünschten, mainstreamkonformen, zuverlässig linken Journalisten den Ausweis ohne Prüfung automatisch zuschiebt, während er ihn Leuten wie mir, die sich kritisch äußern, **nicht nur willkürlich und ohne jegliche Begründung verweigert, sondern auch den Einspruch nach § 10 Absatz 4 der Vereinbarung über den Bundeseinheitlichen Presseausweis komplett ignorieren und darauf überhaupt nicht reagieren.**

Diese Vereinbarung wird also nicht „gelebt“, sondern dient nur zum Schein und zur Täuschung der Öffentlichkeit.

Vergabekriterien existieren ebenfalls nicht.

Presseausweise werden völlig willkürlich und allein nach politischer Gesinnung vergeben. Ein Rechtsweg oder erkennbare Kriterien, die zu erfüllen wären, existieren nicht. Die von der Innenministerkonferenz behauptete „Beweiserleichterung“ ist reiner Schwindel.

17.2.5.3 Genießen auch Heini Pressefreiheit?

Wie sehr die Parteipolitik und die Parteiinteressen in die Vergabe des Presseausweises vertrackt sind, zeigt eine Äußerung des Ex-MdB und Ex-Generalsekretärs der CDU, Ruprecht Polenz (Abbildung 17.1):

„Politiker haben nicht zu bestimmen, was Journalismus ist. Aber wer wie Nius den Pressekodex nicht unterschreibt, den sich die Medien selbst gegeben haben, ist eben kein journalistisches Medium. Es bekommt auch nicht jeder Heini einen Presseausweis.“



Abbildung 17.1: **Tweet** von Ruprecht Polenz, Ex-MdB, Ex-Generalsekretär der CDU

Für solchen Blödsinn in Folge hat man Ruprecht Polenz gerade das Bundesverdienstkreuz verliehen. Ein juristisches Staatsexamen¹ hat er auch. Es fällt schwer zu entscheiden, was von beidem absurder, lächerlicher, unglaublicher ist.

Damit ist aber erwiesen, **dass aus Sicht der CDU nur solche Journalisten als Presse gelten und Pressefreiheit haben sollen, die sich dem linken Kollektiv unterwerfen (und dafür zahlen) – und die CDU darüber bestimmt, wer „Journalist“ sein soll.**

Man fragt sich unwillkürlich, wofür sich dieser Mann – oder die CDU im Ganzen sich – eigentlich hält, dass er sich derartige Entscheidung darüber anmaßt, wer und was

¹ Von Konrad-Adenauer-Stiftungs-Gnaden, das Bundesverdienstkreuz dürfte er inhaltlich und in Bezug auf die Wahlergebnisse der CDU eher von der SPD bekommen haben.

journalistisches Medium ist.

Mit seiner notorisch linksextremen und hoch aggressiven, gegenüber Andersdenkenden extrem intoleranten Ausrichtung und nach solchen Äußerungen darf man Ruprecht Polenz wohl gewisslich als einen der politischen Drahtzieher der Bekämpfung unerwünschter Presse ansehen. Das ist ein Geständnis.

Die CDU und die Bundesregierung müssen sich die Frage gefallen lassen, wo genau die Trennlinie zwischen Heini und Presseausweisberechtigtem verläuft, und wieso die CDU darüber zu befinden habe, dass die Eigenschaft als Presse davon abhängig sei, sich einem politisch gesteuerten Codex und – was er geflissentlich nicht erwähnt – einer, zudem kostenpflichtigen Medienaufsicht unterwirft.

Und davon hängt dann auch die Frage nach dem Berufsgeheimnis ab – und damit, ob die CDU eigenmächtig und verfassungswidrig entscheidet, wer ein Berufsgeheimnis hat und wer nicht.

17.2.6 Korruption

Ich habe mich auf Journalistenkonferenzen auch mit Kameralen und Toningenieuren über die Frage unterhalten, wer einen Presseausweis erhält und warum.

Dabei wurde mir aus Insiderwissen von verschiedenen Leuten erklärt, dass die Vergabe oft korrupt verlaufe.

So erhielten auch Leute, die keinen Anspruch darauf hätten, weil sie keinerlei journalistische Tätigkeit hätten und keine Auskunftsrechte in Anspruch nähmen, wie Fernsehköche oder Kameralen bei Sportveranstaltungen, ohne weiteres Presseausweise.

Ein wesentlicher Grund dafür sei, dass sich die Gewerkschaften auf diese Weise künstlich ihre Mitgliederzahl erhöhten, weil der Presseausweis für Mitglieder kostenlos sei, **ohne Berechtigungsprüfung, allein aufgrund Mitgliedschaft ausgestellt würden** und die Mitgliedsbeiträge in der Gewerkschaft auf gleicher Höhe oder sogar unter den Gebühren für Presseausweise für Nichtmitglieder lägen.

Davon abgesehen werde der Presseausweis aber aus wirtschaftlichen Gründen knapp gehalten: Die meisten Inhaber verwendeten ihn nämlich nicht für Auskünfte, sondern allein, um sich wirtschaftliche Zuwendungen wie

- kostenlose Eintritte
- kostenloses Essen
- teure Sitzplätze Gratis
- Geschenke
- Allerlei Einladungen

und dergleichen zu verschaffen. Und diese Quelle würde versiegen, wenn es zu viele Ausweisinhaber gebe.

17.3 Das Fernmeldegeheimnis und die informationelle Selbstbestimmung

Was mir in diesem gesamten Konglomerat überall, ausnahmslos und immer wieder auffällt: *Grundrechte, Verfahrensrechte von Verdächtigen, Beschuldigten, Angeklagten kommen darin überhaupt nicht vor, finden keinerlei Beachtung.*

Das Wort „Fernmeldegeheimnis“ kommt im Gesetzentwurf zweimal vor: Auf Seite 17 und Seite 20. *Beidesmal nur, um pro forma das Zitiergebot zu erfüllen und „Das Fernmeldegeheimnis wird eingeschränkt“ zu sagen.*

Eine Begründung, eine Abwägung, eine Rechtfertigung erfolgt nicht. Vom Schutz des Fernmeldegeheimnisses ist nirgends die Rede.

Wir haben hier eine völlige, noch weit unter der Geringschätzung liegende Missachtung von Grundrechten. Sie kommen im Gesetzentwurf überhaupt nicht vor.

Man greift, wie selbstverständlich, in Grundrechte ein, in das Grundrecht auf informationelle Selbstbestimmung – und es stört niemanden. So wenig, dass man es nicht einmal für nötig hält, es zu erwähnen oder Gefahren abzuwägen.

17.4 Der Medienstaatsvertrag

Nicht besser sieht es beim Medienstaatsvertrag aus. Der Medienstaatsvertrag ist ein Produkt der Bundesländer – aber der vorliegende Gesetzentwurf ist es über die Initiative des Bundesrates ebenfalls.

Der Medienstaatsvertrag ist verfassungswidrig und willkürlich, weil er

- elektronischen Medien nur die Nachteile einer Presse-eigenschaft wie Sorgfaltspflichten und Behördenaufsicht aufzwingt,
- ihnen die Vorteile wie Auskunftsrechte, Schutz, Unabhängigkeit aber vorenthält.

Wie man als elektronisches Medium die vom Medienstaatsvertrag auferlegten und von Aufsichtsbehörden erzwungenen Sorgfaltspflichten überhaupt erfüllen können sollte, wenn einem gleichzeitig die dafür erforderlichen Auskunftsrechte vorenthalten werden, bleibt unklar.

Ein tauglicher Anknüpfungspunkt ist das nicht.

17.5 Verfassungswidrigkeit des Gesetzentwurfs

17.5.1 Missachtung im Gesetzentwurf

Wie in Teil [IV](#) dargelegt wird, werden Pressefreiheit und Pressegeheimnis in der Realität von Polizei, Staatsanwaltschaft und Gerichten völlig hemmungslos und ohne jede Beachtung der Vorschriften oder der Presseeigenschaft übergangen und verletzt.

Das interessiert die gar nicht.

Im Gesetzentwurf findet sich aber weder ein Schutz der Pressefreiheit, noch ein gangbarer Rechtsweg gegen diese Verletzung oder ein Schutz gegen Gebrauch oder gar Missbrauch der erlangten Daten.

17.5.2 Gesamtsicht

In der Gesamtsicht ist der Gesetzentwurf deshalb verfassungswidrig, weil er die Berufsgeheimnisse und die Pressefreiheit verletzt.

- Der Gesetzentwurf enthält keinerlei Elemente zum Schutz der Berufsgeheimnisse und Pressefreiheit.
- Die dafür vorgesehenen §§ 53 und 97 StPO sowie Teil 3 BDSG sind in der Praxis völlig wirkungslos, werden von Polizei Staatsanwaltschaft und Gerichten völlig ignoriert, sind unbekannt (dazu Teil [IV](#) und Teil [V](#)).
- Der Besitz des Presseausweises ist kein tauglicher Anknüpfungspunkt für den Schutz der Pressefreiheit. Die Vergabe verläuft willkürlich, politisch und wirtschaftlich korrupt und auch auf dem Rechtsweg nicht verfolgbar.
- Andere Anknüpfungspunkte für einen sind nicht ersichtlich.

18 Verhältnismäßigkeit

18.1 Verfassungsrechtliche Anforderungen

Maßnahmen müssen nach Artikel 20 Abs. 3 GG dem Grundsatz der Verhältnismäßigkeit entsprechen und dazu vier Anforderungen erfüllen:

Legitimer Zweck: Die Maßnahme muss ein verfassungsrechtlich zulässiges Ziel verfolgen.

Geeignetheit: Das gewählte Mittel muss taugen, das Ziel zumindest in einem wesentlichen Teil der Fälle zu erreichen.

Erforderlichkeit: Es darf kein milderes, gleich wirksames Mittel geben, das den Zweck erfüllt.

Angemessenheit: Die Schwere des Eingriffs darf nicht außer Verhältnis zum angestrebten Erfolg stehen (innere Angemessenheit).

Das Bundesverfassungsgericht lässt es zur Eignung genügen, wenn die Maßnahme dem Zweck förderlich ist, auch wenn sie ihn nicht ganz erreicht, und nur in einem Teil der Fälle wirkt („teilgeeignet“). Sie ist nur dann ungeeignet, wenn das gewählte Mittel untauglich oder das Ziel unerreichbar ist. Dem Gesetzgeber steht bei der Frage der Geeignetheit ein weiter Einschätzungs- und Prognosespielraum zu.

18.2 Fehlende Zweckangabe

Es fehlt bereits an einer greifbaren, verbindlichen Zweckangabe.

In der Öffentlichkeit, gegenüber den Medien reden die Regierung und das Bundeskriminalamt ach so gerne und oft vom Kampf gegen Kinderpornographie – aber warum dafür auch die Geheimdienste und der Zoll Zugriff bekommen sollen, erschließt sich mir nicht.

Ein Gesetz, eine Maßnahme können nicht verhältnismäßig sein, wenn der konkrete Zweck nicht hinreichend substantiiert ist.

18.3 Fehlende innere Verhältnismäßigkeit (Angemessenheit)

18.3.1 Schwere Straftaten

Ich halte die „Vorratsdatenspeicherung“ – wie schon in der Stellungnahme vom 9. Oktober 2023 ausgeführt, durchaus für angemessen, wenn es um schwere Straftaten geht, wie Mord, Waffen-, Drogen-, Menschenhandel, Vergewaltigung, Raub und dergleichen.

Auch bei dem gegenüber der Öffentlichkeit vorgeschobenen Zweck, der Verfolgung von Kinderpornographie, kann ich eine Verhältnismäßigkeit je nach Fall zumindest für vertretbar halten.

18.3.2 Äußerungsdelikte

Die neuen Vorschriften der StPO sollen lauten (Auszug):

§ 100g Absatz 2

(2) Besteht kein Verdacht hinsichtlich einer Straftat von auch im Einzelfall erheblicher Bedeutung, ist die Erhebung von Verkehrsdaten unter den übrigen Voraussetzungen von Absatz 1 mit folgenden Maßgaben zulässig:

1. bestimmte Tatsachen begründen den Verdacht, dass jemand als Täter oder Teilnehmer eine Straftat mittels Telekommunikation begangen hat, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht hat oder durch eine Straftat vorbereitet hat, und

2. abweichend von Absatz 1 Satz 1 Nummer 2 wäre die Erforschung des Sachverhalts auf andere Weise aussichtslos oder wesentlich erschwert; eine Erhebung zur Ermittlung des Aufenthaltsorts des Beschuldigten ist unzulässig.

§ 100k Absatz 2

(2) § 100g Absatz 2 gilt für die Erhebung von Nutzungsdaten bei dem Verpflichteten nach Absatz 1 mit der Maßgabe entsprechend, dass eine Erhebung zulässig ist, wenn der Verdacht hinsichtlich einer mittels eines digitalen Dienstes begangenen Straftat besteht.

Damit werden *alle* Straftaten erfasst, die mittels Telekommunikation begangen werden können, und damit eben auch die Äußerungsstraftaten.

Hier kann ich überhaupt keine Verhältnismäßigkeit zwischen Grundrechtseingriff und Schwere der Tat erkennen.

18.3.3 Täuschung der Öffentlichkeit

Der Öffentlichkeit wird suggeriert, es gehe hier um schwerste Straftaten (Abbildung 18.1), und sich an Schwerverbrechen mit Empörungswert anzuhängen. Nach dem

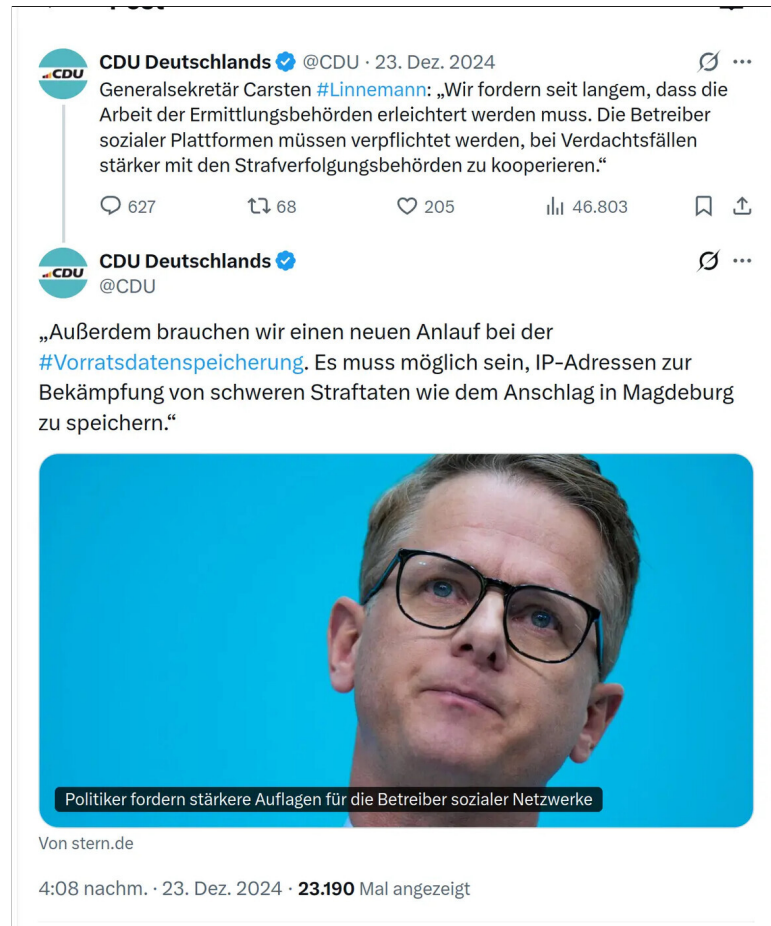


Abbildung 18.1: CDU-Generalsekretär Linnemann beim politischen Verbrechensmelden – tatsächlich erfasst der Gesetzentwurf auch Äußerungsdelikte.

Gesetzestext aber werden auch einfache Äußerungstaten erfasst.

Was der Anschlag in Magdeburg mit IP-Adressen zu tun hatte, und was eine Vorratsdatenspeicherung dabei geholfen hätte, war der Berichterstattung nicht zu entnehmen.

18.3.4 Gummiparagraphen §§ 130, 185, 188 StGB

Die Straftaten des StGB sind nahezu alle an konkret definierte Kriterien gebunden, wie etwa Mordmerkmale, Diebstahl, Betrug, Verleumdung.

§ 185 StGB (Beleidigung) ist dagegen die einzige mir spontan bekannte Strafvorschrift des StGB, die **gar keine Legaldefinition** enthält und allein die Beleidigung als – undefinierten – Begriff, der kein Rechtsbegriff ist, unter Strafe stellt.

Das ist eigentlich verfassungswidrig, weil es an der Normenklarheit fehlt und die Tat

damit nicht unter Strafe gestellt war.

Das Bundesverfassungsgericht hat zwar in verschiedenen Entscheidungen (z. B. **1 BvR 1476, 1980/91 und 102, 221/92**) entschieden,

§ 185 StGB ist auch nicht zu unbestimmt und verstößt damit nicht gegen Art. 103 Abs. 2 GG. Zwar unterscheidet er sich von den übrigen Vorschriften des Strafgesetzbuchs dadurch, daß er den BVerfGE 93, 266 (291) BVerfGE 93, 266 (292) Straftatbestand lediglich mit dem Begriff der Beleidigung benennt, aber nicht näher definiert. Auch wenn das für eine unter der Geltung des Grundgesetzes erlassene Strafvorschrift als unzureichend anzusehen sein sollte, hat der Begriff der Beleidigung jedenfalls durch die über hundertjährige und im wesentlichen einhellige Rechtsprechung einen hinreichend klaren Inhalt erlangt, der den Gerichten ausreichende Vorgaben für die Anwendung an die Hand gibt und den Normadressaten deutlich macht, wann sie mit einer Bestrafung wegen Beleidigung zu rechnen haben (vgl. BVerfGE 71, 108 [114 ff.]).

Ich halte das aber für blanken Unfug.

Denn das Bundesverfassungsgericht stellt selbst die Anforderung auf, dass der Bürger das Strafrecht so weit verstehen müsse, dass er weiß, welche Handlungen und Unterlassungen von ihm erwartet werden. Es ist nutzlos, wenn man *den Gerichten* Vorgaben gibt.

Außerdem sind die Vorgaben nicht hinreichend klar, sonst müsste das Bundesverfassungsgericht ja nicht ständig Urteile selbst des BGH aufheben und die Richter wegen falscher Anwendung rügen. Also können die Vorgaben nicht klar sein.

Als ich in der in Kapitel **22** dargestellten Rechtssache nach einem Strafverteidiger suchte, ist mir aufgefallen, **dass viele Strafverteidiger keine Äußerungsdelikte mehr vertreten, weil die Rechtsprechung völlig willkürlich und unvorhersehbar geworden ist und sie sich nicht mehr in der Lage sehen, eine Verteidigung zu formulieren und vorzubringen.**

Da ich mich während des Ermittlungsverfahrens selbst vertreten habe, ist mir auch aufgefallen, dass die Staatsanwaltschaft gar keine Rechtskunde zu §§ 185, 188 hatte und nicht einmal wusste, dass es dazu Verfassungsgerichtsentscheidungen gibt und Art. 5 GG einschlägig ist, sondern sich mit ein paar Blicken in den Kurzkomentar zum StGB begnügte – das muss ihrer Meinung nach reichen.

Das führt aber dazu, dass heutzutage nahezu jede x-beliebige Aussage, die über die Uhrzeit und den Wochentag hinausgeht, als Verletzung von §§ 130 oder 185 ausgelegt werden und zumindest ein Ermittlungsverfahren in Gang setzen kann.

18.4 Mangelnde Eignung

Ich halte die IP-Adressspeicherung für nicht geeignet, den – nicht angegebenen – Zweck zu erfüllen, denn sie ist für Kundige zu leicht zu umgehen.

Wie oben in Abschnitt 14.6 gezeigt, hat die Bundesregierung kurz vor dem Referentenentwurf sogar einem Verlag eine Zuwendung von 50.000 Euro geleistet, der Links-extreme und Terroristen mit Anleitungen versorgt, die die IP-Adressspeicherung auszuhebeln ist.

Man kann verfassungsrechtlich keine Eignung behaupten, wenn man den Erfolg gleich selbst vereitelt.

19 Unklarheiten, Inkonsistenzen, Widersprüche

19.1 Inkonsistenz zwischen § 175 und § 176 TKG

In § 175 Abs. 1 TKG ist die Rede von der Erfüllung einer *Pflicht*:

§ 175 Befugnis zur Verarbeitung von Verkehrsdaten zur Auskunftserteilung an Strafverfolgungs- und Sicherheitsbehörden

(1) Wer öffentlich zugängliche Telekommunikationsdienste erbringt oder daran mitwirkt, darf Verkehrsdaten nach Maßgabe dieser Vorschrift zur Erfüllung von Auskunftspflichten gegenüber den in Absatz 3 genannten Stellen verarbeiten. [...]

In den folgenden Absätzen wird nicht die Verarbeitung, sondern nur die Auskunft beschränkt.

Das heißt, dass „wer öffentlich zugängliche Telekommunikationsdienste erbringt“, alle Verkehrsdaten speichern darf, die abgefragt werden *könnten*, ohne dass es auf das Vorliegen einer konkreten Anforderung im Einzelfall ankommt.

In § 176 Abs. 1 TKG dagegen ist die Rede von der Erfüllung einer *Anordnung*:

§ 176 Befugnis zur Verarbeitung von Verkehrsdaten zur Erfüllung von Sicherungsanordnungen

(1) Wer öffentlich zugängliche Telekommunikationsdienste erbringt oder daran mitwirkt, darf Verkehrsdaten verarbeiten, soweit dies erforderlich ist zur Erfüllung

1.einer Sicherungsanordnung nach § 100g Absatz 7 der Strafprozessordnung,

2.einer Sicherungsanordnung nach § 10b Absatz 1 oder § 52 Absatz 3 des Bundeskriminalamtgesetzes oder

3.einer Sicherungsanordnung nach § 25a Absatz 1 des Bundespolizeigesetzes. Verkehrsdaten, die allein aufgrund einer Sicherungsanordnung gemäß Satz 1 gesichert wurden, dürfen nur im Rahmen des jeweiligen Sicherungszwecks verwendet und unter den Voraussetzungen des § 175 beauskunftet werden.

Während § 175 Abs. 1 dem, der Telekommunikationsdienste erbringt, allgemein erlaubt, Daten „zur Erfüllung von Auskunftspflichten“ zu speichern, ohne dass es auf ein konkretes, vorliegendes Ersuchen ankäme, bindet § 176 Abs. 1 dieselben, nämlich wer Telekommunikationsdienste erbringt, bezüglich derselben Erlaubnis, nämlich

Verkehrsdaten zu speichern, an das Vorliegen einer Anordnung.

19.2 „Die Verantwortung trägt ...“

In § 175 Abs. 2 Satz 2 TKG heißt es:

Die Verantwortung für die Rechtmäßigkeit des Auskunftsverlangens tragen die um Auskunft ersuchenden Stellen.

Was soll das heißen?

Wie kann eine Stelle – Polizeipräsidium, Staatsanwaltschaft – eine „Verantwortung tragen“?

Strafrechtlich?

Zivilrechtlich?

Datenschutzrechtlich?

Wie soll sich eine Staatsanwaltschaft im Ganzen strafbar machen? Wie soll ein Datenschutzbeauftragter ihr ein Bußgeld auferlegen?

Soll das heißen, dass sich der Provider und der anfragende Beamte nicht um die Rechtmäßigkeit zu kümmern haben? So wie es in Abschnitt [28](#) beschrieben, in Hessen passiert?

Teil IV

Missbrauch

20 Anknüpfung an EuGH C-793/19

Die Anforderung des EuGH an eine Vorratsdatenspeicherung lautet (C-793/19 und C-794/19):

„Diese Rechtsvorschriften müssen durch klare und präzise Regeln sicherstellen, dass bei der Speicherung der fraglichen Daten die für sie geltenden materiellen und prozeduralen Voraussetzungen eingehalten werden und dass die Betroffenen über wirksame Garantien zum Schutz vor Missbrauchsrisiken verfügen.“

Ich werde in diesem Teil aufzeigen, dass in der Bundesrepublik Deutschland hoheitliche Macht und Befugnisse in erheblichem Umfang und nicht nur in seltenen Einzelfällen systematisch missbraucht werden.

Der vorliegende Gesetzentwurf entbehrt jeglicher Betrachtung von Missbrauchsrisiken.

- Keinerlei vorbeugende oder missbrauchsverhindernde Maßnahmen
- Keinerlei nachlaufenden Rechtsweg gegen erfolgten Missbrauch
- Keinerlei Diskussion von Missbrauchsrisiken in der Begründung

Ich habe das Wort „Missbrauch“ nur einmal im Absatz auf Seite 54/55 gefunden, wonach ein Missbrauch gar nicht vorkommen könne:

Dennoch bleiben die nun geregelten Anforderungen an den Schutz der zu sichernden Daten bewusst hinter den Vorgaben zum Schutz und zur Sicherheit der Daten aus der – dauerhaft für unanwendbar erklärten – allgemeinen und unterschiedslosen Vorratsdatenspeicherung zurück. Die strengen Datenschutz- und Datensicherheitsvorschriften der §§ 176 bis 181 sind in direkter Umsetzung des Urteils des Bundesverfassungsgerichts entstanden, das die erste deutsche Regelung zur Vorratsdatenspeicherung für verfassungswidrig erklärt hatte (Urteil vom 2. März 2010 – 1 BvR 256/08, BVerfGE 125, 260–385). Sie müssen für die Sicherungsanordnung – abgesehen von den zuvor genannten Vorschriften – nicht nachgebildet werden, da insoweit kein dauerhaft vorhandener Datenpool mit entsprechenden Gefahren missbräuchlicher Nutzung vorgesehen ist. Die Datenspeicherung bei der Sicherungsanordnung erfolgt nämlich im Gegensatz zur Vorratsdatenspeicherung anlassbezogen, im Einzelfall, für einen begrenzten Zeitraum und nur hinsichtlich eines beschränkten Datenumfangs. Ferner ist nicht öffentlich bekannt, ob, in welchem Umfang und wen betreffend Daten gespeichert werden. Damit sind die aufgrund einer Sicherungsanordnung gespeicherten Verkehrsdaten ein deutlich weniger reizvolles Ziel für potentielle Angriffe von außen. Für die zu betrieblichen Zwecken gespeicherten Verkehrsdaten sind

im bisher geltenden Recht, insbesondere im TKG und im TDDDG, Regelungen zu Datenschutz und Datensicherheit vorgesehen, die – neben den Vorgaben des Absatzes 2 – auch für die aufgrund der Sicherungsanordnung gespeicherten Daten gelten werden.

Mit anderen Worten: Missbrauch gibt es nach Auffassung der Regierung eigentlich gar nicht, und den Rest deckt man ab, indem man oft genug das Wort „Datenschutz“ sagt. Bei einfacher Zählung (ohne Zeilentrennungen) kommt das Wort „Datenschutz“ in diesem Gesetzentwurf 23 Mal vor, aber eine inhaltliche Befassung gibt es nicht, und alles wird auf die Provider abgewälzt – die kurioserweise dabei gar nicht prüfen sollen, ob eine Anfrage rechtmäßig ist, weil die anfragende Stelle die Verantwortung tragen soll.

Das kann nicht funktionieren. Das ist ein Schein-Datenschutz.

Ein Missbrauch der Abfragebefugnis wird erst gar nicht betrachtet.

Der Gesetzentwurf hält keinerlei Schutz oder Sicherung gegen Missbrauch.

21 Formen von Missbrauch

21.1 Fälschung durch Dritte

Bereits in meiner Stellungnahme vom 9. Oktober 2023 hatte ich ausführlich und anhand von Beispielen dargelegt, dass es für Provider unmöglich ist, mit pflichtgemäßem und zumutbarem Aufwand, oder in manchen Fällen überhaupt zu prüfen, ob eine anfragende Stelle befugt ist – oder ob sie überhaupt existiert.

Im Jahr 2009 lief nahezu die gesamte Vorratsdatenspeicherung per Fax ab, sowohl bei den Anfragen und Anordnungen, als auch bei der Beauskunftung. Authentifikation und Autorisation fanden praktisch gar nicht statt, weil es jedem trivial möglich war, den Briefkopf einer Polizeidienststelle zu kopieren, einzuscannen und lediglich die Faxnummer auszutauschen – oder eine Dienststelle gleich ganz zu erfinden, die es nicht gibt.

- Das wäre nicht aufgefallen, weil sie meisten Polizeidienststellen zwar oft liebevoll gestaltete Briefköpfe, mitunter mit historischem Stadtbild verzierte, aber eben doch völlig willkürliche Phantasiebriefköpfe verwendeten.
- Es wäre mitunter nicht einmal strafbare Amtsanmaßung, weil viele Dienststellen nicht einmal das Wort „Polizei“ verwendeten, sondern nur „PI“ für Polizeinspektion¹
- Und es bestand keine Gefahr der Aufdeckung, weil alle Anfragen nach kurzer Zeit aus Datenschutzgründen gelöscht werden mussten.

Damit konnte *jeder* Anfragen stellen, der genug Chuzpe und ein Faxgerät hatte.

Hier nun soll die Übermittlung durch den ETSI-Standard TS 102 657 ersetzt werden, der eine international anerkannte, etablierte und einheitliche Methode zu sein suggeriert wird. Tatsächlich aber habe ich ernsthafte Zweifel (ausführlich Kapitel 11), ob es sich bei dieser Norm um eine reale, technisch angewandte Norm handelte, oder eine Luftnummer, die diese nur vorgaukeln soll. Es ist zu befürchten, dass diese Norm als Fassade gilt und dann in der Realität

- bis zu deren Umsetzung zwischen „Berechtigten“ und Providern doch wieder gefaxt wird,

¹Was genauso gut Paul Irgendwas, Private Investigator oder Pistazienimporteure bedeuten könnte.

- zwischen der Dienststelle, die etwas abfragen will, und der, die ETSI-Nachrichten schicken kann, gefaxt wird.

Der Gesetzentwurf reagiert nicht auf meine Warnungen aus dem Jahr 2023.

21.2 Missbrauch durch mangelnde Schulung/Inkompetenz

Ich hatte in der Stellungnahme vom 9. Oktober 2023 beschrieben, dass es zu ernsthaften Datenschutzverstößen kam, die nicht einmal auf böser Absicht, sondern auf Unkenntnis des Verfahrens beruhten, und man aus der Not der Polizei heraus, keine Möglichkeit zu haben, „jemanden zu fragen“ oder sich zu informieren, überhaupt zu wissen, was man wie abfragen kann, einfach irgendetwas anfragte. Da herrschte weite Hilflosigkeit.

Eine Reaktion darauf sehe ich hier nicht.

Wenn nicht einmal der Gesetzgeber versteht, was er hier treibt, wie soll es dann die Polizei können und ihre Anfragen sachgerecht stellen?

21.3 Missbrauch für private Zwecke

Wie in meiner Stellungnahme vom 9. Oktober 2023 erwähnt, habe ich zweimal Polizisten dabei erwischt, für private, nichtpolizeiliche Zwecke anzufragen. Die Erkennung war hier nur deshalb möglich, weil in beiden Fällen die Polizisten unzulässig telefonisch anfragten und sich dabei verdächtig unsicher und vortastend benahmen.

Grundsätzlich aber ist oder war eine solche Zweckentfremdung nicht zu erkennen und die Echtheit der Anfragen, Aktenzeichen, Angaben usw. nicht zu prüfen.

Ein aktuelles Beispiel für zweckfremde Anfragen lege ich in Abschnitt [22](#) dar.

21.4 Politischer Missbrauch

21.4.1 Politische Weisungen

Der EuGH hat 2019, [C-508/18](#), entschieden, dass deutsche Staatsanwälte mangels Unabhängigkeit und wegen ihrer Weisungsgebundenheit keinen europäischen Haftbefehl ausstellen dürfen.

Der Tagesspiegel: [SPD blockiert Richter, weil ihr Urteile nicht passen: Berliner Justiz droht schwere Krise](#)

Es bestehe die Gefahr politischen Missbrauchs.

21.4.2 Politische Korruption

Um den politischen Druck auf die Strafverfolgung zu entdecken, muss man nicht einmal suchen. Das steht schon in der Zeitung (Abbildung 21.1 und 21.2).

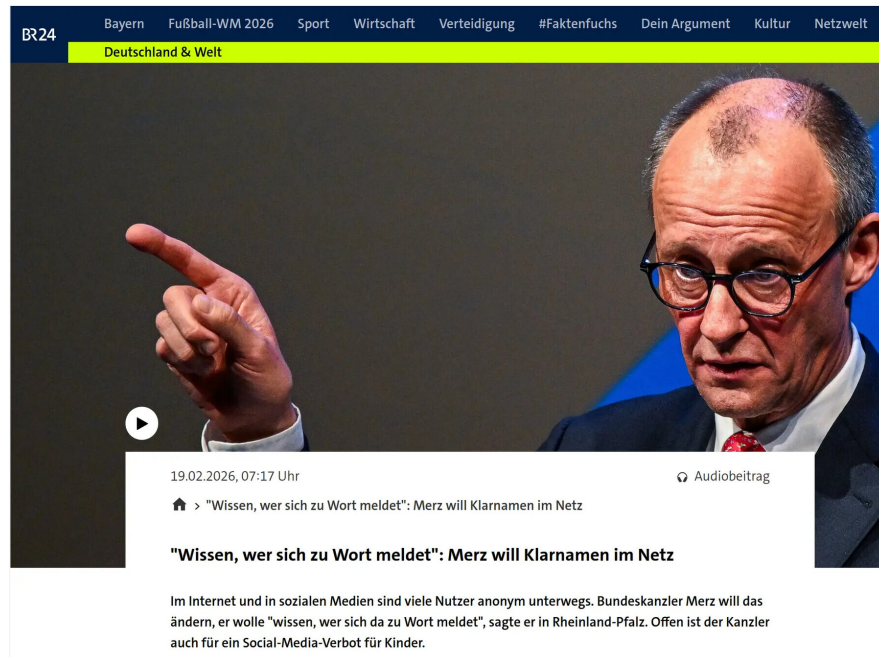


Abbildung 21.1: Wofür die CDU die IP-Adressspeicherung braucht.

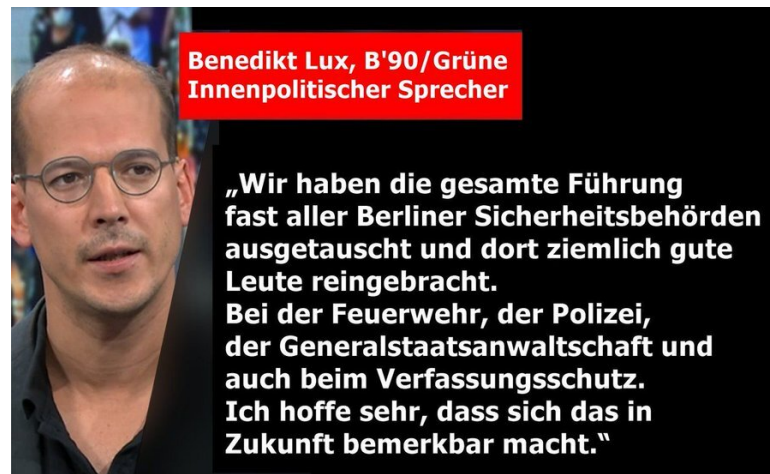


Abbildung 21.2: Internet-Meme zu Benedikt Lux in **Neues Deutschland**, 14.8.2020, Urheber unbekannt

Einschlägig hierzu bekannt ist die Causa „Lügenfritz“, die – zusammen mit der reichhaltigen Kommentierung – deutlich zeigt, wohin die Absichten der Regierung und Gesetzgebung verlaufen.

21.4.3 Ideologische Woke-Verflechtung von Polizei und Justiz

Die Berliner Polizei und die Berliner Staatsanwaltschaft sind derartig stark mit Woke- und Genderideologie verflochten, verwoben, von ihr unterwandert und durchsetzt, dass sie praktisch nicht mehr von linken Aktivisten, der Antifa, LGBT, und inzwischen auch von linkem Terrorismus zu unterscheiden ist.

Ein Element der Gender Studies und des links-soziologischen Kanons ist, sich an *schriftliche* Gesetze nicht mehr zu halten, weil sie von weißen Männern für weiße Männer gemacht und deshalb sexistisch, frauenausgrenzend und rassistisch seien. Stattdessen solle man durch subversiv veränderte Wiederholungen die Rechtslage seinem persönlichen Gerechtigkeitsgefühl anpassen. Das Ergebnis zeigt Abbildung [21.3](#).

Ganze Teile der Berliner Justiz scheinen inzwischen nur ein linker, marxistischer Apparat zu sein, der hoheitliche Staatsgewalt unter dem Anschein einer Strafverfolgung zu politischen Zwecken missbraucht.

21.5 Verbindungen zwischen Polizei und organisierter Kriminalität

21.5.1 Bisherige Fälle

Bisher schon häuften sich Fälle, in denen sich die Polizei mit der organisierten Kriminalität vermischt. Schon bei der Festnahme der Terroristin Daniela Klette (Linksextremismus) und der Sicherstellung von Teilen des Beuteguts aus dem Dresdener Grünen Gewölbe (Clankriminalität) war den Medien zu entnehmen, dass die dabei aktiven Polizeien anderer Bundesländer die Berliner Polizei nicht informiert hatten, weil die Gefahr bestanden habe, dass die Informationen sofort an die Clans oder Linksextreme durchgestochen würden.

Auch sonst ist immer wieder von Kontakten die Rede, von **Arbeitsverhältnissen** (vgl. Abbildung [21.4](#)), bis hin zu **Liebesbeziehungen**

Es gab in den Berliner Medien Berichte, wonach kriminelle Clans einzelne Mitglieder schon als Kinder auswählen, um sie aus allem „heraus und die Weste sauber“ zu halten, damit sie als Erwachsene in die Polizei eintreten und den Clan mit Insiderinformationen und Dienstleistungen versorgen können.



Abbildung 21.3: Verflechtung von Polizei und Staatsanwaltschaft mit Woke-/Queer-/LGBT-Ideologie – sogar mit eigenen Abteilungen

In der ZDF-Dokumentation „**Kriminelle Clans in Deutschland**“ vom 1.7.2025 wird angedeutet, dass **korrupte Berliner Polizisten gegen Geld für kriminelle Clans polizeiliche und Ermittlungsmaßnahmen gegen deren Gegner durchführen.**

Es ist also davon auszugehen, dass es dann bald einen Schwarzmarkt für IP-Adressabfragen geben wird. **Der SPIEGEL: Berliner Staatsanwaltschaft klagt Polizeibeamten an:**

Die Berliner Staatsanwaltschaft hat Anklage gegen einen 33 Jahre alten, mutmaßlich korrupten Polizisten erhoben. Sie wirft dem Beamten unter anderem vor, zwischen Februar 2020 und Februar 2023 **in 17 Fällen polizeiliche Erkenntnisse an Mitglieder der kriminellen**



Abbildung 21.4: Über die Berliner Polizei

Szene weitergegeben zu haben, wie die Behörde mitteilte .

Dem Neuköllner Streifenbeamten werden demnach Geheimnisverrat, Bestechlichkeit und Rechtsbeugung zur Last gelegt.

Dazu auch **der Tagesspiegel**:

In sechs Fällen soll der Angeklagte offenbar in Rücksprache mit seinen Bekannten im Milieu gezielt Ermittlungen eingeleitet haben, die er mit „anonymen Hinweisen“ begründete. So sollten womöglich Kontrahenten im kriminellen Milieu unter Druck gesetzt werden. Dabei beantragte der Beamte bei der Staatsanwaltschaft sogar Durchsuchungsbeschlüsse, die das Amtsgericht Tiergarten tatsächlich erließ.

Bedenkt man, dass es in Berlin inzwischen nahezu täglich Schießereien gibt, ist es nur eine Frage der Zeit, bis der erste Widersacher, Zeuge oder V-Mann mit Hilfe polizeilicher Ermittlungen wie dann der IP-Vorratsdatenspeicherung umgelegt wird.

21.5.2 Berliner Wahl zum Abgeordnetenhaus 2026

Nach der Wahl zum Berliner Abgeordnetenhaus 2026, die DIE LINKE gewann, wurden Kontakte von Linken-Politiker

- ins linksextreme, gewalttätige Milieu bekannt: Elif Eralp war Mitglied der Roten Hilfe (vgl. Unterkapitel 14.6),

- ins Clanmilieu bekannt: Ferat Koçak hat Verbindungen zum Remmo-Clan

Beides entwickelt sich gerade erst noch.

Prinzipiell sind damit künftige Vorgesetzte von Polizei, Staatsanwaltschaft und Verfassungsschutz stark mit Linksextremisten und Clans verbandelt und verschaffen denen – spätestens, wenn sie erpresst werden – Zugang zu polizeilichen Ermittlungsmethoden.

21.6 Das Abmahnunwesen

Wir haben eine Juristenschwemme, die ernährt werden will, weshalb die Zahl der Streitfälle mit der Zahl der Juristen steigt.

Sie steigt aber nicht proportional, weil die Kapazität der Gerichte nicht mitsteigt, was zu einem ausufernden vor- und außergerichtlichen Abmahnunwesen führte, die inzwischen zu einer Zwangsabgabe für überflüssige und arbeitslose Juristen wurde. Was erstaunlich ist, wenn man bedenkt, dass es die Abmahnung gesetzlich im Wettbewerbs-, Marken- und Urheberrecht gibt, aber nicht im Zivilrecht, wo sie gerade blüht.

Dazu kommt, dass gerade Fraktionen des Bundestages, voran die Grünen, aber auch SPD und – wer sich noch an sie erinnert – die dankenswerterweise verblichene FDP mit HateAid, So Done und ähnlichem versuchte, sich die Taschen noch weiter zu füllen, ohne einer Übergewinnsteuer zu unterliegen.

In der Vorratsdatenspeicherung 2009 kam es zu einer auffälligen Häufung immer gleicher Fälle, zu der ich auch Telefonate mit zwei von diesen Fällen extrem genervten und belasteten Staatsanwälten führte.

Ein Unternehmen vertrieb digital urheberrechtlich geschützte Werke mit brachial auffälliger Namensgebung, aber nach Einschätzung der Staatsanwälte unterirdisch schlechter inhaltlicher Qualität, weshalb Zweifel daran aufkamen, ob das Geschäftsmodell überhaupt in Produktion und Vertrieb oder in Abmahnungen lag. Die (Mach-)Werke wurden digital verbreitet, und wenn jemandes IP-Adresse bei der Verbreitung (z. B. unbemerkt per Torrent) erwischt wurde, setzte es eine Strafanzeige.

Die Strafanzeigen wurden sämtlichst von den Staatsanwaltschaften eingestellt, aber immer erst, nachdem per VDS-Abfrage der Beschuldigte mit Namen und Anschrift ermittelt wurde.

Sodann nahm das Unternehmen Akteneinsicht, um Name und Anschrift zu erfahren, und denjenigen kostenpflichtig abzumahnern. Die Staatsanwaltschaften wurden im großen Stil mit einer großen Zahl von Abfragen als Strohmann eingespannt, um für das Unternehmen die VDS-Abfragen vorzunehmen, die das Unternehmen selbst nicht stellen durfte.

Soll dies nach dem Gesetzentwurf nun gestattet und legal sein, oder als Missbrauch angesehen werden?

Soll die IP-Adressspeicherung auch für zivilrechtliche Streitigkeiten zur Verfügung stehen?

21.7 Die Methoden des Bundeskriminalamts

Der Präsident des Bundeskriminalamtes, Holger Münch, „wartet sehnsüchtig auf die Vorratsdatenspeicherung“.

Mir fallen dazu eher sehr negative berufliche Erfahrungen mit dem Bundeskriminalamt im Jahr 2009 ein.

Während meiner Tätigkeit in der Vorratsdatenspeicherung bekam ich nach der Ablehnung fehlerhafter, unverständlicher, formal unzulässiger oder inhaltlich unrechtmäßiger Auskunftersuchen rabiate Telefonanrufe vom BKA, oft in ungehaltenem bis aggressiv ausfälligem Tonfall, in denen Drohungen gegen mich erhoben wurden, wie mir sofort einen Streifenwagen mit Blaulicht zu schicken und mich vom Schreibtisch weg wegen Strafvereitelung verhaften zu lassen, wenn ich nicht sofort Auskunft erteile.

Meine Antwort darauf war stets dieselbe, nämlich dass ich gerade in einer Rechtsabteilung, inmitten eines Rudels zähnefletschender Juristen, die meisten mit Anwaltszulassung, sitze, und ich so gerne sehen würde, wie sie das machen wollen. Beim Poker würde man es „Hosen runter, will sehen!“ nennen. Danach kam entweder gar nichts mehr oder ein korrigiertes Auskunftersuchen. Ich halte das für Nötigung und für missbräuchlich.

Bei Ursula von der Leyens Kinderpornosperrre versuchte das BKA, die Sperre durch persönliche Einschüchterung und „Manndeckung“ durchzusetzen, bis es letztlich einsehen musste, dass das Unterfangen aus technischen Gründen nicht möglich und zudem unsicher ist, sie die Liste der Kinderpornoserver damit effektiv selbst veröffentlichen würden, was damals zur Aufgabe der Sperre führte.

Erschreckend war immer wieder die Mischung aus Halbwissen bis Inkompetenz und die Aggressivität der Durchsetzung politischer Ziele.

So verlangte das BKA in der Sitzung Anfang 2009 im Familienministerium, dass die Provider Kinderpornoserver „im DNS“ sperren, dem BKA aber *ein ungesperrrtes DNS* zur Verfügung stellen müssten, damit das BKA weiter ermitteln könne.

Ich hatte ausgeführt, dass das auf einem erheblichen technischen Fehlverständnis beruhe, weil das BKA – wie jedes Unternehmen oberhalb einer gewissen Größe – mit an Sicherheit grenzender Wahrscheinlichkeit über eigene DNS-Recursor verfügt und gar nicht am DNS der Provider hängt, und weil für das BKA das BSI zuständig sei und das BSI das mit Sicherheit weiß und so eingerichtet hat. Und sollte das nicht der Fall sein,

man dies dringendst einrichten müsse. Deshalb hätten die Provider-DNS-Sperren auf das BKA – wie auf jedes Unternehmensnetzwerk – *gar keine Sperrwirkung*, und die Forderung sei weder technisch erfüllbar, noch erforderlich.

Das wurde mir als Polemik und Desinformation ausgelegt, obwohl die Vertreter des BKA erkennbar keinerlei Ahnung von der Funktionsweise und dem Aufbau des DNS hatten. Erst einige Tage später bei einem zweiten Termin im BKA war zusätzlich eine andere Abteilung anwesend, die zumindest über so viel Sachkunde verfügte, dass man ihnen technische Sachverhalte erklären konnte.

Nun ist zwar anzunehmen, dass sich die technische Sachkunde seit 2009 verbessert hat. Ich bezweifle aber, dass sich Benehmen und Rechtskunde verbessert haben. Hier gehe ich eher noch von einer deutlichen Verschlechterung aus.

Insbesondere ist dabei zu sehen, dass das BKA in letzter Zeit eher durch Angriffe gegen die Meinungsfreiheit als durch die Verfolgung von Kinderpornographie aufgefallen ist.

Wie sich bei den damaligen Vorgängen – insbesondere der Kinderpornosperrung von der Leyens – zeigte, ist das BKA politischer Befehlsempfänger und Scherge des Bundesinnenministeriums. Die damalige Kinderpornosperrung war weder wirksam, noch technisch umsetzbar. Gleichwohl wurde sie mit hohem *politischem* Druck durchzusetzen versucht.

Und wie diese Vorgänge ebenfalls zeigten, wird das BKA auch zur Umsetzung von Parteiinteressen und einzelner Politiker – damals von der Leyen – eingesetzt – rabiät, aggressiv und auch entgegen Technik und Recht. Denn die Kinderpornosperrung **war offenkundig Ursula von der Leyens persönliches Profilierungsprojekt und diente ihrer persönlichen politischen Karriere – aber nie den Kindern**. Persönliche Racheaktionen von der Leyens inbegriffen.

Dass eine Besserung eingetreten ist, glaube ich nicht, denn ähnliche Vorgänge habe ich in jüngster Zeit bei LKA und Staatsanwaltschaft Berlin beobachtet (Kapitel 22).

Die politische Abhängigkeit, Hörigkeit, Weisungsgebundenheit des BKA stehen einem ordentlichen Gerichtsverfahren entgegen.

Normalerweise verbietet es sich, sich in einer Stellungnahme zu einem Gesetzentwurf ad personam zu äußern. Wenn aber wie hier jemand wie Holger Münch als treibende Kraft hinter dem Gesetzentwurf und seiner Umsetzung steht, muss auch hier Kritik möglich sein – insbesondere wenn der Lebenslauf SPD-näher als bildungsnäher wirkt, und nicht erkennbar ist, wo in seiner **auf den BKA-Seiten selbst** veröffentlichten Lebenslaufdarstellung

RedaktionsNetzwerk Deutschland: Herr Münch, Sie sind 1978 Polizist geworden. Warum?

Holger Münch: Ich war in der Pubertät kein sehr fleißiger Schüler. Nach einem Schulwechsel musste ich richtig kämpfen. Da habe ich mich entschieden, doch nicht Abitur zu machen, sondern abzugehen. Außerdem wollte ich nicht zur Bundeswehr, und das konnte man da-

mals mit drei Jahren bei der Polizei vermeiden. Aber schon ganz schnell, nach meinem ersten Praktikum auf einem Revier, habe ich gewusst: „Hier bleibst Du. Das willst Du tun.“ Das Eintreten für die Gesellschaft, das Schlichten von Konflikten, dafür zu sorgen, dass die Menschen nachts ruhig schlafen können: Das hat mich sehr stark motiviert – und motiviert mich bis heute.

Sachkunde über Demokratie vorkommt. Wenn man aber, wie er, daneben sitzt, **wie Nancy Faeser am 13.02.2024 groben Unfug über Demokratie erzählt**, nämlich

„Diejenigen, die den Staat verhöhnen, müssen es mit einem starken Staat zu tun bekommen.“

und dazu nickt, der gehört nicht nur demokratiefernen Schichten an und ist für sein Amt ungeeignet, sondern der führt – als Verlängerung von Nancy Faeser – Böses im Schilde.

Wie dieses Böse aussieht, belege ich im folgenden Kapitel **22**. Denn nach **von der Bundesregierung geförderter Auffassung** sind bereits „Alternativmedien“ (wozu auch mein Blog gehört) per se „rechtsextrem“ und „verfassungsfeindlich“ und damit legitimes Ziel von Faesers Angriffen.

22 Die Affäre Baerbock/Özdemir/Lang

22.1 Der Auslöser

22.1.1 Annalena Baerbock

Im Frühjahr 2021 betrieben ARD, ZDF und Printmedien massive Wahlkampfunterstützung für die Kanzlerkandidatin der Grünen, Annalena Baerbock.

Die Art und Weise, insbesondere Talkshowszenen, in denen sie trotz überheblich-naiven Auftretens als „internationale Spitzenjuristin“ u.ä. vorgestellt wurde, erregte Unmut in den Social Media, und der ÖRR focht Kämpfe auf Seiten der Grünen aus (Abb. 22.1).



Abbildung 22.1: Die ARD macht Wahlkampf für Baerbock

Als Blogger kam ich der Aufforderung nach, suchte – zunächst vergeblich – nach der Ausbildung Baerbocks, und fand dann einen Propagandaartikel der Süddeutschen Zeitung, der sie als künftige Kanzlerin bejubelte, und stellte der Redaktion die Frage, wie sie an den dort und bei den Grünen behaupteten Bachelor gekommen sein solle, wenn es den an dieser Universität zu diesem Zeitpunkt noch gar nicht gab.

Die Süddeutsche reagierte umgehend mit der Streichung der Angabe aus dem Artikel, **worüber ich im Blog berichtete**.

Dadurch kam eine Lawine aus Nachprüfungen in Gang, in deren Verlauf Baerbock über Wochen fast täglich ihren Lebenslauf korrigieren und reduzieren musste. Nicht wenige Politologen und Journalisten sind der Auffassung, dass das Baerbock die sichere Kanzlerschaft gekostet und Olaf Scholz zum Kanzler gemacht hat.

22.1.2 Cem Özdemir

Im Versuch, den Wahlkampf zu retten, vielleicht auch aus persönlicher ideologisch-überheblicher Überzeugung, setzte Cem Özdemir im Juni 2021 **die Behauptung in Umlauf**, hinter der Kritik an Baerbock könnten nur Türken und die Russen stecken (Abbildung 22.2), weil

- man die zauberhafte Annalena Baerbock nur kritisieren könne, wenn man mit den Russen unter einer Decke stecke und ein russischer Agent sei, einen anderen Grund gebe es nicht,
- denn Baerbock sei gegen Nordstream 2, weshalb die Russen alles daran setzten, ihre Kanzlerschaft zu verhindern, um Nordstream 2 in Betrieb nehmen zu können.
- die Türken verhindern wollten, dass er ... *tut mir leid, das habe ich nicht verstanden*. Anscheinend ist Cem Özdemir da ähnlich aufgehängt wie die Capulcu-Gruppe (türkischstämmig, linksextrem und gegen Erdogan, vgl. Kapitel 14.6). Die brauchen auch keine Gründe, um jeden zum Gegner zu erklären.

In allen Berichten stand

Inzwischen befinde man sich im Austausch mit deutschen Sicherheitsbehörden.

Die Grünen, insbesondere Özdemir, haben im Juni 2021 dem Verfassungsschutz eingeredet, die Kritik an Baerbocks Lebenslauf sei ein Angriff der Türken und der Russen.

Maischberger @maischberger · 28. Apr. ...

Warum die #Kanzlerkandidatin von Bündnis 90/Die Grünen, Annalena #Baerbock (@ABaerbock), ihr Angst macht, erklärt die Wirtschaftsreporterin Nena Schink (@Nenacase; @Bild) bei #maischberger @DasErste

#KFrage #Habeck #Söder #Laschet



361 880 2.470

Joachim Morgenstern @leineimmo · 1. Mai ...

Dass Politiker traditionell keine Fachkenntnisse besitzen, ist hinlänglich bekannt.
Die Grünen haben es allerdings salonfähig gemacht, politische Ämter auch ohne Allgemeinbildung zu besetzen.

7 23 492

Das Erste @DasErste ...

Antwort an @leineimmo @maischberger und 2 weitere Personen

Wie kommen Sie dazu, dass Frau Baerbock nicht gebildet ist? Schauen Sie sich die Ausbildung der Frau an. Wenn das keine Bildung ist...

5:24 nachm. · 1. Mai 2021 · Swat.io

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

analysieren, um konsequent gegen Finanzgeflechte im Rechtsextremismus vorgehen zu können.

(Als „rechtsextrem“ gilt bekanntlich schon jeder, der anderer Meinung als die Regierung ist. Holger Münch ist als der einzige der drei, der noch im Amt ist, ein Protagonist der Vorratsdatenspeicherung.)

Das ist freilich leichter gesagt als getan, denn dafür gibt es **keine Rechtsgrundlage. Der Verfassungsschutz ist schlicht nicht befugt, „Finanzaktivitäten aufzuklären“ oder gar „auszutrocknen“.**

2022/2023 hat man das dann an mir ausprobiert, indem man – wie nachfolgend beschrieben – ein fingiertes Strafermittlungsverfahren gegen mich inzeniert hat, um unter dem Vorwand strafrechtlicher Ermittlungen auf das Spendenkonto meines Blogs zuzugreifen.

Es lief aber nicht so, wie man sich das vorgestellt hatte. Ich haben den – heimlich durchgeführten – Zugriff nicht nur bemerkt, sondern mich auch dagegen zur Wehr gesetzt.

Danach, im Februar 2024, stellte Nancy Faeser – wieder mit Haldenwang und Münch – das 13-Punkte-Paket **„Rechtsextremismus entschlossen bekämpfen – Instrumente der wehrhaften Demokratie nutzen“**, wo es wiederum heißt

Finanzquellen rechtsextremistischer Netzwerke austrocknen: Operativ wurden die Finanzermittlungen beim Bundesamt für Verfassungsschutz bereits deutlich verstärkt. Banken werden sensibilisiert, Finanzstrukturen werden detailliert aufgearbeitet. Aber gesetzlich gibt es derzeit Grenzen, da die Befugnis für Finanzermittlungen auf volksverhetzende und gewaltorientierte Bestrebungen beschränkt ist. Das Bundesverfassungsschutzgesetz soll daher so geändert werden, dass es auf das Gefährdungspotenzial ankommt, für das Faktoren wie Aktionspotenzial und gesellschaftliche Einflussnahme relevant sein können. Außerdem sollen Verfahren schneller und unbürokratischer werden.

Man wollte also, nachdem der Zugriff auf mein Konto¹ nicht lief, wie gewünscht, eine gesetzliche Grundlage haben, damit der Verfassungsschutz direkt zugreifen kann. Man bekam sie aber nicht, weil die „Ampelkoalition“ vorzeitig zusammenbrach.

22.2 Ein fingiertes Strafermittlungsverfahren als Vorwand

22.2.1 Ricarda Lang

Nach der Bundestagswahl wurden die Grünen-Vorsitzenden Baerbock und Habeck Minister, die Posten mussten neu besetzt werden. Ricarda Lang und Omid Nouripour kandidierten.

¹ Mir ist nicht bekannt, ob noch weitere Konten von dieser Vorgehensweise betroffen waren.

Lang betrieb einen bizarren Wahlkampf. Während die Grünen seit Jahren und auch im Programm zur Bundestagswahl 2021 fetten und zuckerhaltigen Speisen den Kampf ansagten (vgl. Abb. 22.3), betrieb Lang das genaue Gegenteil, zeigte sich in den Social Media provokativ mit großen Portionen Eis, fettiger Kuchen u.ä., und betritt ihren Wahlkampf und Fernsehauftritte fast ausschließlich damit, sich als Opfer von Body Shaming aufzuspielen und mit Slogans wie „My body, my choice“ zu arbeiten.



Abbildung 22.3: Buch von Renate Künast

Im November und Dezember 2021 kam es sowohl in den Öffentlich-Rechtlichen Sendern, als auch in großen Printmedien zu konzertierten Kampagnen, die sie als armes Opfer zeichneten und forderten, sie nicht mehr nach ihrem Körper zu beurteilen.

Ich schrieb eine – ausgedruckt je nach Schriftart etwa 8 bis 10-seitige – Replik auf einen solchen Artikel in der WELT, und hielt dem entgegen, dass sie das

- selbst seit Jahren zum Gegenstand ihres Social Media Accounts und ihres aktuellen Wahlkampfes mache,
- dass das rechtlich zulässig ist,
- und dass man, wenn man sie nicht danach beurteilen solle, erst einmal etwas anderes als Urteilsgrundlage haben müsse.

Doch Lebenslauf, Ausbildung, Tätigkeiten, Schriften, Leistungen waren von ihr nicht zu finden. Ich habe schlicht nichts gefunden, was man sonst beurteilen könnte. Die Forderung liefe also einfach nur darauf hinaus, sie gar nicht zu beur-

teilen und leistungslos, allein aufgrund Opferstatus, durchzuwinken.

Am Wochenende des 29./30. Januar 2022 wurden Ricarda Lang und Omid Nouripour zu Vorsitzenden der Grünen gewählt.

22.2.2 Fingierte Strafanzeige § 188 StGB

In der Nacht von Montag auf Dienstag, den 1.2.2022, um 0:38 Uhr, also gerade 48 Stunden nach der Wahl, ging per E-Mail eine Strafanzeige nach § 188 StGB wegen des Artikels vom Dezember 2021 über Ricarda Lang beim Landeskriminalamt Berlin ein, die vorgeblich von der Meldestelle REspect! kam, obwohl dies weit außerhalb deren Bürozeiten lag.

Die Anzeige enthielt keinerlei Begründung, keiner Darlegung einer Straftat, sondern nur pro forma einen Screenshot, der *einen einzelnen Satz aus dem 10-seitigen Artikel ausgeschnitten* hatte und den Eindruck erweckte, dieser Satz wäre isoliert und ohne Kontext veröffentlicht worden. Auch das ist dubios, denn der angeblich dafür verantwortliche Leiter der Meldestelle hatte zuvor in zwei Interviews selbst erklärt, dass man Äußerungen immer nur im Kontext beurteilen könne und nicht herauschneiden dürfe.

LKA und Staatsanwaltschaft eröffneten ein Strafermittlungsverfahren gegen mich, **interessierten sich aber überhaupt nicht für die „Straftat“. Es gab keinerlei Versuch, die angezeigte Äußerung im Internet zu sichten, oder als Beweis zu sichern. Erst viel später und auf meine Schriftsätze hin, in denen ich darauf und auf den Kontext hinwies, merkte die Staatsanwaltschaft, dass das ein Blogartikel ist und nicht nur aus einem Satz besteht.**

Wieviele Strafermittlungsverfahren kennen Sie, in denen sich die Staatsanwaltschaft überhaupt nicht für die Straftat interessiert?

Der zentrale Zweck dieser „Meldestellen“ (die anscheinend vom Verfassungsschutz betrieben werden) ist,

- möglichst viele Daten über Kritiker zu sammeln,
- mit denen man bei Bedarf jederzeit ein Strafverfahren fingieren kann,
- und deren Kenntnis dem „Geschädigten“ nicht anzurechnen ist, somit die 3-Monatsfrist für Strafanträge nicht in Gang gesetzt wird.

Diese Meldestellen – Polizeidienststellen kritisierten sie schon, weil sie überflüssig seien und man Anzeigen bei der Polizei direkt zu stellen habe – sind dafür gebaut, Gründe für Anzeigen auf Vorrat zu sammeln, ohne dass die Frist für Strafanträge zu laufen beginnt, weil der „Geschädigte“ immer dabei bleiben kann, davon noch nichts gewusst zu haben. Braucht man einen Ermittlungsvorwand, holt man einen aus dem Magazin.

Kaum war Lang Vorsitzende und damit unter dem Schutz des § 188, und die Gefahr nicht mehr gegeben, dass ein Bekanntwerden der Anzeige ihre Wahl beeinträchtigen könnte, stieß man die Anzeige an.

22.2.3 Die heimliche rechtswidrige Kontenabfrage – 20 Rechtswidrigkeiten

Statt sich für die „Straftat“ zu interessieren, nahm die Staatsanwaltschaft eine Kontenabfrage zum Spendenkonto meines Blogs vor, und zwar **über mehr als zwei Jahre, vom 1.1.2021 bis 28.3.2023** (Belege [22.1](#) und [22.2](#)).

Schon der Zeitraum ab 1.1.2021 zeigt eindeutig, dass es nicht um den Artikel über Ricarda Lang, die angebliche Straftat ging, sondern um Annalena Baerbock.

Die Anfrage ist in vielfacher Hinsicht rechtswidrig:

1. Es besteht kein Zusammenhang zur vorgeworfenen Tat.
2. Sie ist schon menschenrechtswidrig.

Der **Europäische Gerichtshof für Menschenrechte** hat im Fall **Sommer v. Germany, Individualbeschwerde 73607/13** mit Urteil vom 27.4.2017 entschieden, dass eine Kontenabfrage

- in Bezug auf einen Zeitraum von 2 Jahren,
- ohne einschränkende Suchkriterien,
- unter Aufforderung an die Bank, den Kunden nicht zu informieren

Artikel 8 der Europäischen Menschenrechtskonvention verletzt. Und das, obwohl es – im Gegensatz zum hiesigen Fall – im dort entschiedenen Fall sogar verdächtige Zahlungen und einen Verdacht auf Straftaten im Zusammenhang mit dem Konto gab.

Der EGMR führt dazu aus, dass es **im deutschen Strafprozessrecht keine einzige Vorschrift gibt, die einen derartigen Eingriff tragen könnte**, Artikel 8 EMRK aber eine gesetzliche Vorschrift für einen Eingriff voraussetzt.

In meinem Fall gab es aber weder verdächtige Zahlungen, noch einen Verdacht auf Straftaten im Zusammenhang mit dem Konto.

3. Sie ist noch einmal menschenrechtswidrig:

Der Europäische Gerichtshof für Menschenrechte hat in der Affaire **Jecker c. Suisse, Individualbeschwerde 35449/14** mit Urteil vom 6.10.2020 entschieden, dass Publizisten – wie ich – Berufsgeheimnisträger sind und die Ausforschung

Polizei Berlin
LKA 535
Bayernring 44
12101 Berlin

Berlin, den 28.03.23

Tel.: (030) - 4664 - 953537
Fax: (030) - 4664 - 953599

18

BITTE SOFORT VORLEGEN / WEITERLEITEN

An
Deutsche Bank AG
DB Service/Auskunftersuchen
Per Fax: 0201-24648867

Seitenzahl: 2

Auskunftersuchen

Betreff: Einholung von Bankauskünften
Aktenzeichen: 237 Js 1124/22
Vorgang: 220201-1131-535000

Sehr geehrte Damen und Herren,

im Ermittlungsverfahren der Staatsanwaltschaft Berlin, Az 237 Js 1124/22 ist die Einholung von Bankauskünften, gem. einem Auftrag nach § 163 Abs. 3 StPO, staatsanwaltschaftlich angeordnet. Es ist notwendig, einen Überblick über den Geldverkehr der folgenden Person zu gewinnen:

Hadmut Werner Danisch
10179 Berlin, Dresdener Str. 96

Nach hier vorliegenden Erkenntnissen soll die o.g. Person folgendes Konto bei Ihnen geführt haben/führen:

IBAN: DE45 1007 0848 0305 1935 00

Es wird um Übersendung der Kontoumsatzlisten für den Zeitraum ab 01.01.2021 bis tagesaktuell in digitaler Form (möglichst als Excel-Tabelle) gebeten.

Seite 1 von 2

Beleg 22.1: „Auskunftersuchen“ Seite 1

182

Die angeforderten Umsatzübersichten sollten folgende Mindestvoraussetzungen enthalten:

- Buchungs- und Valutadatum
- Vollständige Bankverbindung des Auftraggebers/Empfängers (IBAN/BIC, Name des Kreditinstitutes)
- Name des Auftraggebers/Empfängers der Zahlung
- Verwendungszweck
- Art der Transaktion
- Umsatz bzw. Betrag
- Tages- bzw. Kapitalsaldo

Bitte senden Sie Ihre Antwort an:

Polizei Berlin
LKA 535
Bayernring 44
12101 Berlin
Fax.: 030-4664-953599.

Bitte behandeln Sie dieses Schreiben und den gesamten Vorgang vertraulich. Informieren Sie insbesondere weder die genannten Personen noch sonst dritte Personen darüber, damit Sie sich nicht der Gefahr der Strafvereitelung gem. § 258 StGB aussetzen. Diese Anfrage darf nicht als Grundlage einer Kündigung der Geschäftsbeziehung verwendet werden.

Mit freundlichen Grüßen


Wied, KK

Beleg 22.2: „Auskunftsersuchen“ Seite 2

der Informantenbeziehungen Artikel 10 EMRK verletzt.

4. Sie ist verfassungswidrig:

Das Bundesverfassungsgericht hat (2 BvR 1372/07, 2 BvR 1745/07) im Fall einer Kreditkartenzahlungssuche nach kinderpornographischen Schriften eine Grundrechtsverletzung **verneint, weil**

- nicht alle Zahlungen an die Polizei übermittelt wurden, sondern die Strafverfolgung **Suchkriterien angegeben hatten**, wonach man suchte, **und**
- im Ergebnis gar keine Daten von der Bank an die Strafverfolgung übermittelt wurden, weil keine Zahlung den Suchkriterien entsprach.

Im **Umkehrschluss** muss dann gelten, dass wenn diese Voraussetzungen nicht gegeben sind, weil wahllos alle Zahlungen durchsucht wurden, eine Grundrechtsverletzung vorliegt.

5. Sie ist datenschutzrechtswidrig:

Für Strafermittlungsverfahren gilt nicht die DSGVO, sondern über § 500 StPO Teil 3 des BDSG.

Mein Blog ist politisch (die Regierung wirft mir ja selbst vor, ich sei „rechts“), und damit sind

- Spendernamen
- Kontonummern
- Verwendungszwecke

besondere Kategorien personenbezogener Daten, weil sie Aufschluss über die politische Meinung geben, und die Polizei und Staatsanwaltschaft so gar nicht erheben und verwenden dürfen.

Auch danach liegen hier

6. Es gibt kein „Auskunftersuchen“ gegenüber Privatbanken, weil diese keine Auskunftspflicht haben.

Auskunftersuchen gibt es nur gegenüber Kommunikationsdienstleistern, sowie öffentlich-rechtlichen Banken, weil diese wie Behörden gestellt sind (Sparkassen).

7. Es ist strafprozessordnungswidrig: Auch in der Akte ist kein Ermittlungszweck genannt. Es ist überhaupt nicht ersichtlich, wozu man das wollte (siehe dazu aber die Auswertung weiter unten).

8. Als Rechtsgrundlage wird § 163 Abs. 3 StPO genannt:

Zeugen sind verpflichtet, auf Ladung vor Ermittlungspersonen der Staatsanwaltschaft zu erscheinen und zur Sache auszusagen, wenn der Ladung ein Auftrag der Staatsanwaltschaft zugrunde liegt. Soweit nichts anderes bestimmt ist, gelten die Vorschriften des Sechsten Abschnitts des Ersten Buches entsprechend. Die eidliche Vernehmung bleibt dem Gericht vorbehalten.

Ein Auskunftersuchen und eine Zeugenbefragung sind völlig unterschiedliche Dinge.

9. Man kann eine Bank nicht als Zeugen befragen, weil man nur natürliche, aber nicht juristische Personen als Zeugen vernehmen kann, also die Bankmitarbeiter.
10. Man kann Personen (Bankmitarbeiter) nur nach tatsächlich gemachten Wahrnehmungen befragen (Kunde bringt Geldkoffer und zahlt am Schalter ein, Kunde ruft an und fragt um Kredit usw.)

Man kann aber niemanden als Zeugen elektronischer Banküberweisungen befragen, weil die niemand mit seinen fünf Sinnesorganen wahrgenommen hat.

11. Man kann niemanden anonym als Zeugen befragen. Ein Zeuge muss immer konkret benannt werden.
12. Es fehlt die Zeugenbelehrung.
13. Die Übermittlung einer Datei ist keine „Zeugenaussage“. Zeugenaussagen sind nur das, was man erlebt hat und aus dem Gedächtnis mündlich vortragen kann.
14. Zeugen sind keine Hilfssheriffs. Man kann Zeugen nicht beauftragen, Informationen erst zu beschaffen.
15. Zeugen müssen namentlich benannt sein, weil sie in der Hauptverhandlung vom Gericht vorgeladen werden müssen.
16. Es ist kein Beschuldigter genannt. Dieser muss aber genannt sein, damit Zeugen ihr Zeugnisverweigerungsrecht prüfen können.
17. Es ist kein Strafvorwurf genannt. Dieser muss aber genannt sein, um die Verhältnismäßigkeit und Zeugnisverweigerungsrechte zu prüfen.

Das ganze Ding erweckt den Eindruck, als ginge es um Schwerstkriminalität wie Drogen-, Waffen-, Menschenhandel, als würde ich Kinderpornographie im großen Stil verkaufen.

Es ist nicht erkennbar, dass es um den Vorwurf ging, ich hätte mit *einem Satz* in einem Blockartikel eine Politikerin beleidigt.

18. Es ist kein Beweiszweck genannt.
19. „Es ist notwendig, einen Überblick über den Geldverkehr der folgenden Person zu gewinnen“ gibt es im Strafrecht nicht.

Das ist eine Geheimdienstformulierung.

20. Man kann Zeugen nicht auffordern, die Sache „vertraulich“ zu behandeln, und insbesondere von einer Bank nicht zu verlangen, gegen ihre Treuepflicht zu verstoßen und den Kunden nicht zu informieren.

Kein „Zeuge“ muss über die Zeugenvernehmung schweigen.

Es ist sogar im Bankrecht beschrieben, dass die Staatsanwaltschaft dann, wenn sie nicht will, dass der Kontoinhaber davon erfährt, die Kontenabfrage eben bleiben lassen muss. **Es gibt rechtlich keine geheime Kontenabfrage der Staatsanwaltschaft oder der Polizei.**

21. Es ist nicht nur rechtswidrig, **sondern offen kriminell und strafbare Nötigung**, der Bank als „Zeugen“ damit zu drohen, wegen Strafvereitelung § 258 StGB verfolgt zu werden, wenn sie mich informieren.

22. Es fehlt die richterliche Anordnung (dazu unten mehr).

Was soll der ganze Unfug?

LKA und Staatsanwaltschaft müssen gewusst haben, **dass diese Abfrage komplett rechtswidrig ist, sonst hätten sie sie nicht als Zeugenvernehmung getarnt und der Bank gedroht, darüber zu schweigen. Man hat hier gezielt die richterliche Anordnung umschifft.**

Warum braucht es eine richterliche Anordnung?

Es gibt kein Sonderrecht für Bankdaten bei Privatbanken. Sie werden rechtlich behandelt wie alles andere auch, im Prinzip nicht anders als ein Messer oder ein Brief. Sie gelten als Sache, und die Herausgabe von Sachen ist keine Zeugenvernehmung. Kein Zeuge muss etwas übergeben. Er muss nur aussagen, was er weiß.

Die Staatsanwaltschaft muss daher der Bank eine Herausgabeforderung schicken. Dazu ist die Bank formalrechtlich dann verpflichtet, muss sie aber trotzdem ablehnen, weil sie dem Kunden gegenüber zum Bankgeheimnis verpflichtet ist, sie deshalb nicht „freiwillig“ herausgeben kann, und das Verweigern gegenüber der Staatsanwaltschaft keine Folgen hat, die Staatsanwaltschaft kann kein Bußgelder verhängen.

Die Bank kann an dieser Stelle Daten nur mit Einverständnis des Kunden herausgeben, was nach Literatur typisch in zwei Fällen vorkommt:

- Der Kunde ist geständig und stimmt zu.
- Der Kunde legt die Daten selbst vor, um sich zu entlasten.

Anfrage und Ablehnung können sogar übersprungen werden, wenn Banken die Ablehnung allgemein erklären.

Dann muss die Staatsanwaltschaft beim Gericht einen Beschlagnahmebeschluss be-

antragen, **in dem konkrete Zwangsmittel – Beugehaft usw. – gegen Vertretungsberechtigte (Vorstand) der Bank unmittelbar angedroht werden.**

Erst wenn die Staatsanwaltschaft diesen Beschluss der Bank vorlegt, darf die Bank *zur Abwendung der Zwangsmittel* die Daten herausgeben.

Einen solchen Beschluss hätte die Staatsanwaltschaft aber nicht bekommen, weil die Richterin, die das Verfahren dann einstellte, auf die Frage, was die Kontenabfrage sollte, erklärte, dass sie davon nichts wisse, das nicht angeordnet habe und auch nicht erkennen kann, was das überhaupt mit dem Vorwurf zu tun haben könnte.

In den Antrag auf Beschlagnahme hätte man außerdem reinschreiben müssen, wofür man die Daten braucht.

Deshalb hat man hier mit kriminellen Mitteln die nötige richterliche Anordnung umgangen.

Der hier handelnde KK Thomas Wied ist *namensgleich* mit einem früheren Politiker der linksextrem gewordenen Piratenpartei. Ob es sich auch um dieselbe Person handelt, war bisher nicht belastbar und zitierfähig zu klären.

Die von ihm verwendeten Formulierungen im „Auskunftersuchen“, das Schweigeverlangen an die Deutsche Bank und die Nötigung mit Verfolgungsdrohungen lassen keinen anderen Schluss zu, als dass er sich dabei voll bewusst war, verboten und strafbar zu handeln und das zu verdunkeln suchte.

Der Verdacht steht im Raum, dass Organisationen wie REspect! und HateAid als Datenbunker dazu dienen, um jederzeit gegen jeden Kritiker Strafermittlungen zu fingieren und hoheitliche Gewalt einsetzen zu können.

Berlin ist, wenn die Strafverfolger krimineller sind als die Verfolgten.

22.2.4 Die Auskunft und Kontenkündigung der Deutschen Bank

Die Deutsche Bank hat die Anfrage – trotz offensichtlicher Rechtswidrigkeit – beauskunftet (Belege [22.3](#) und [22.4](#)) und ein Kündigungsschreiben geschickt, das Konto dann als gekündigt behandelt.

Auffällig: Die Deutsche Bank hat normalerweise eine strikte Unterschriftenordnung mit der verbindlichen Vorgabe **zweier Unterschriften** (Vier-Augen-Prinzip). Selbst die kleinste Belanglosigkeit und rechtlich unbedeutende Mitteilung wird von zwei namentlich genannten Mitarbeitern unterschrieben.

Aber beide, die Beauskunftung und die Kündigung **sind weder unterschrieben, noch nennen sie den Absender.**

Es gibt keinen Kündigungsvorgang.

Deutsche Bank



Polizei Berlin
LKA 535
Bayernring 44
12101 Berlin

Deutsche Bank AG
Auskunftsersuchen
04024 Leipzig
Fax-Hotline für Rückfragen: 0201 2464 8867
Vorgang: 3417839848

21.04.2023

Auskunftsersuchen
Aktenzeichen: 220201-1131-535000
Schreiben vom: 28.03.2023

Sehr geehrte Damen und Herren,

die beigefügten Informationen haben wir in Beantwortung Ihres Auskunftsersuchens zusammengestellt.

Der Anhang Kontoaufstellung spiegelt die

- aktuell bzw. im Anfragezeitraum ermittelten Geschäftsverbindungen (Konten/Depots) mit der/den jeweiligen Filial/Kontonummern incl. Unterkonto, Eröffnungs-/Schließungsdatum sowie Währungen, Kontoarten und Kontobezeichnungen
- ggf. angefragte Limite
- ggf. angefragte Postversandart
- ggf. angefragte Bevollmächtigte bzw. Verfügungsberechtigte
- ggf. angefragte Vertretungsberechtigte
- ggf. angefragte wirtschaftl. Berechtigte

wieder.

Sollten darüber hinaus Informationen erforderlich sein, die sich aus den Unterlagen nicht ergeben oder muss aus anderen Gründen ein Zeuge gehört werden, werden wir gerne einen geeigneten Mitarbeiter für Sie ermitteln. Dafür sind konkrete Angaben erforderlich, welche Fragen durch diesen beantwortet werden sollen.

Die hier erteilte Auskunft betrifft Geschäftsbeziehungen zur Marke Deutsche Bank AG unter der Marke Deutsche Bank. Sofern wir festgestellt haben, dass Ihr Auskunftsersuchen auch Geschäftsbeziehungen der Marken Postbank oder DSL-Bank umfasst, erhalten Sie von diesen Marken separat Auskunft. Sie müssen Ihr Auskunftsersuchen nicht erneut an diese Marken richten.

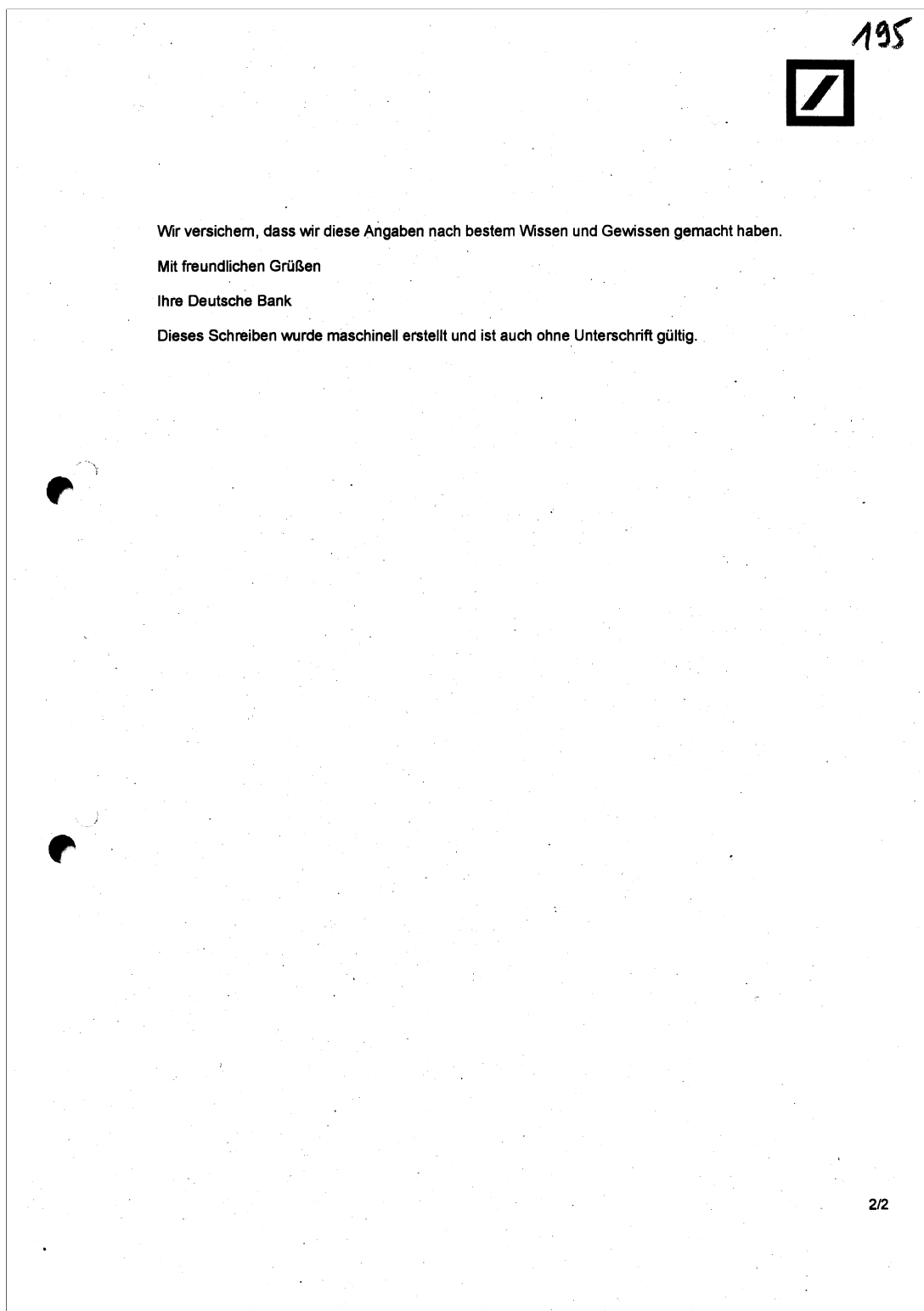
Sofern Sie Informationen von einer unserer selbständigen Tochtergesellschaften benötigen, richten Sie dahin bitte eine gesonderte Anfrage.

ORINCC001 20230421

Vorsitzender des Aufsichtsrats: Alexander R. Wynaendts
Vorstand: Christian Sewing (Vorsitzender), James von Moltke, Karl von Rohr, Fabrizio Campelli, Bernd Leukert, Alexander von zur Mühlen, Christiana Riley, Rebecca Short, Stefan Simon, Olivier Vigneron
Deutsche Bank Aktiengesellschaft mit Sitz in Frankfurt am Main, Amtsgericht Frankfurt am Main, HRB Nr. 30 000; Umsatzsteuer-Id.-Nr. DE114103379;
www.db.com/de, www.deutsche-bank.de

1/2

Beleg 22.3: Auskunft der Deutschen Bank Seite 1



Beleg 22.4: Auskunft der Deutschen Bank Seite 2

Nicht einmal die Datenschutzabteilung konnte gegenüber dem Landesdatenschutzbeauftragten klären,

- wer
- wie
- und warum

das Konto gekündigt haben soll.

Offenkundig hat hier ein Unbefugter – ein Aktivist der Antifa, ein linker Saboteur, ein Agent des Verfassungsschutzes, Grüne, wer auch immer – mit Zugang zu den Datenbanken der Deutschen Bank das Konto eigenmächtig und spurlos als gekündigt eingetragen.

22.2.5 Die Auswertung der Bankauskunft

Die Deutsche Bank hat dem Landeskriminalamt Berlin 1475 Kontenbewegungen mit Namen, Kontonummern und Verwendungszwecken, und Angaben zu 465 Personen übermittelt.

Das Landeskriminalamt hat diese laut Akte systematisch ausgewertet und

- nach Herkunftsländern
- und Verwendungszwecken

untersucht und sich dabei enttäuscht gezeigt, dass da nur Texte wie „Geburtstagsgeschenk“ oder „Allgemeine Unterstützung für das Blog“ zu finden waren, dass es sich wirklich nur um ein Unterstützterkonto handelt und sich darin *keine spezifischen Zahlungen für einzelne Blogartikel finden*.

In Verbindung mit dem Zeitraum wird dadurch klar, dass man hier allen Ernstes nach Zahlungen Russlands der Art

Agent XXX, hier haben Sie 100.000 Euro, erledigen Sie dafür die Kanzlerkandidatin Baerbock!

suchte und dafür ein Strafverfahren vorgetäuscht hat.

22.2.6 Verfahrenseinstellung

Die Staatsanwaltschaft beantragte einen Strafbefehl gegen mich, den das Amtsgericht aber ablehnte und das Verfahren einstellte, weil eine Straftat weder ersichtlich noch dargetan war.

Das ganze Verfahren war eine reine Luftnummer zur Ausspähung des Kontos.

§ 344 StGB Verfolgung Unschuldiger

(1) Wer als Amtsträger, der zur Mitwirkung an einem Strafverfahren, abgesehen von dem Verfahren zur Anordnung einer nicht freiheitsentziehenden Maßnahme (§ 11 Abs. 1 Nr. 8), berufen ist, absichtlich oder wissentlich einen Unschuldigen oder jemanden, der sonst nach dem Gesetz nicht strafrechtlich verfolgt werden darf, strafrechtlich verfolgt oder auf eine solche Verfolgung hinwirkt, wird mit Freiheitsstrafe von einem Jahr bis zu zehn Jahren, in minder schweren Fällen mit Freiheitsstrafe von drei Monaten bis zu fünf Jahren bestraft. Satz 1 gilt sinngemäß für einen Amtsträger, der zur Mitwirkung an einem Verfahren zur Anordnung einer behördlichen Verwahrung berufen ist.

22.3 Missbrauch der Finanzbehörden

22.3.1 Der Zoll

Obwohl es sich um unrechtmäßig erhobene und zudem als besondere Kategorien personenbezogener Daten besonders geschützte Daten handelt, hat man die Daten aus Frustration darüber, den sicher geglaubten Russenauftrag nicht entdeckt zu haben, den gesamten Datenbestand einfach mal an den Zoll weitergeschickt, ob die etwas finden.

Ohne jeden Grund. Ohne jeden Anlass. Ohne jede Rechtsgrundlage. Einfach so zur rechtswidrigen „Umschau“.

22.3.2 Das Finanzamt: Schein-Außenprüfung

Nachdem man noch immer keinen Russenauftrag gefunden hatte, und offenbar der Meinung war, das falsche Konto durchsucht zu haben, hat das Finanzamt 24.2.2025 die Außenprüfung für die Steuerjahre 2020, 2021 und 2022 angeordnet.

Ich bin als Blogger zwar Freiberufler und damit kann formal auch eine Außenprüfung bei mir angeordnet werden. Aber: *Es gibt bei mir nichts außenzuprüfen.* Im Gegensatz zu etwa einem Arzt oder einem Anwalt habe ich weder Praxis noch Kanzlei, keine Angestellten, keine Kasse. Ich zahle keine Gehälter, keine Sozialabgaben für Angestellte, ich verkaufe nichts. Ich habe keine Warenlager, und auch keine nichtabnutzbaren Anlagen.

Und wieder gibt es Anhaltspunkte für eine vorgetäuschte Ermittlung:

1. Die Prüfungsanordnung war nicht unterschrieben, obwohl sie aus einem Sekretariat kam und nicht „maschinell erstellt“ war.
2. Der, der sie laut Anordnung erlassen habe, **wusste davon gar nichts.**

Polizei Berlin
LKA 535 - 220201-1131-535000
KK Wied, Tel: +49 30 4664 953537



W. A. W.
(Name, Amtsbezeichnung)



Verm

Es wird um Prüfung
einer evtl. Steuerhelfer
ersucht. Abgabe an den Zoll.

Spayler 3/5

Schlussvermerk - 220201-1131-535000
Dokument erstellt: 03.05.2023

Seite 2 von 2

Beleg 22.5: Weitergabe an den Zoll

3. Aus den Akten ergab sich, dass die Anordnung von jemand ganz anderem erlassen wurde, dessen Stellung, Dienstgrad, Befugnis nicht ersichtlich ist.
4. Als Grund für die Anordnung wurde angegeben, dass **die Absetzung der Kosten für mein häusliches Arbeitszimmer meiner Zweitwohnung geprüft werden müsse.**

Doch weder hatte ich diese Kosten in der Steuererklärung angegeben, noch hatte ich die Wohnung in diesem Zeitraum schon. Die habe ich erst seit Ende 2022.

5. Später behauptete das Finanzamt, die Außenprüfung sei erforderlich gewesen, weil man die Zusammensetzung von Beträgen der Steuererklärung nicht habe nachvollziehen können.

Ich lege der Steuererklärung aber immer Anlagen bei, in denen das aufgeschlüsselt ist.

Nach über einem Jahr und etlichen Beschwerden gab der Betriebsprüfer schließlich zu, dass man von Anfang an im Besitz dieser Anlagen war, und sie den Anforderungen genügen, also ausreichend sind.

6. Der Betriebsprüfer hat keinen Dienstgrad.
7. Der Betriebsprüfer **kannte meine Steuererklärung gar nicht – der wusste schlicht nicht, was er überhaupt prüfen sollte.**
8. Der Betriebsprüfer hatte Tag, Zeit und Raum im Finanzamt angegeben, war aber nicht dort.
9. Der Betriebsprüfer kannte ELSTER nur dem Namen nach, wusste aber nicht, was man damit machen kann.

Er hatte auch keinen Zugriff auf ELSTER und deshalb auch keinen Zugriff auf die Steuererklärung und die Anlagen.

10. Der Betriebsprüfer **wusste nicht, was eine Einnahmenüberschussrechnung (EÜR) ist und was darin steht.**

Wie kann man Betriebsprüfer eines Finanzamtes sein und nicht wissen, was eine Einnahmenüberschussrechnung ist?

Wie kann man eine Betriebsprüfung durchführen wollen und die zu prüfende Steuererklärung nicht kennen und nicht wissen, was man überhaupt prüfen soll?

Wie kann man Betriebsprüfer eines Finanzamtes sein und nicht wissen, was ELSTER ist? Keinen Zugang zur Steuererklärung und den Anlagen darin haben?

Auch diese Außenprüfung war – ebenso wie das Strafverfahren – ein fingiertes, vorgetäushtes Verfahren zur Spionage.

Worum ging es?

Dem Prüfer ging es nur um eines: Er forderte gleich zu Anfang der Prüfung aggressiv, dass ich ihm meine gesamte elektronische Buchhaltung zu übersenden hätte. Wieder die Suche nach russischen Aufträgen.

Das aber ist unzulässig und war ein weiterer Spionageversuch des Verfassungsschutzes. Denn nach ständiger Rechtsprechung des Bundesfinanzhofs sind Selbständige, die nach EÜR abrechnen, nicht verpflichtet, eine elektronische Buchführung über die EÜR hinaus zu führen, weil in der EÜR bereits alles steht, was man zu führen hat.

Tut man es trotzdem als Hilfsmittel, ist es *freiwillig*. Und auf Daten, die nur freiwillig geführt werden, hat das Finanzamt nach BFH keinen Anspruch.

Der Verfassungsschutz versucht mit allen Täuschungsmitteln, Publizisten auszuspionieren.

Wie ist das möglich?

§ 8 Absatz 2 Verfassungsschutzgesetz Berlin lautet:

Die Verfassungsschutzbehörde darf zur heimlichen Informationsbeschaffung, insbesondere zur Erhebung personenbezogener Daten, nur in begründeten Fällen folgende nachrichtendienstliche Mittel anwenden:

[...]

8. Verwendung fingierter biografischer, beruflicher oder gewerblicher Angaben (Legenden),

[...]

Die Behörden des Landes Berlin sind verpflichtet, der Verfassungsschutzbehörde technische Hilfe für Tarnungsmaßnahmen zu geben.

Der Verfassungsschutz darf sich also auch als Steuerprüfer ausgeben, und sogar das Finanzamt ist verpflichtet, im Tarnung und Unterstützung zu gewähren, eine Außenprüfung vorzutäuschen.

Ganz dumm halt, wenn der dann nicht weiß, was EÜR und ELSTER sind, und sofort auffliegt, dass der nicht im Finanzamt sitzt.

22.4 Alles nur ...

Und das alles nur, weil ich bei der Süddeutschen Zeitung nach deren Wahlwerbejubiläum über Annalena Baerbock angefragt hatte, wie sie zu einem Bachelor gekommen sein soll, den es zu diesem Zeitpunkt an dieser Universität noch nicht gab.

Und deshalb Olaf Scholz statt Annalena Baerbock Kanzler wurde.

Hier wird nicht nur Recht gebrochen.

Hier ist jede Verhältnismäßigkeit verloren gegangen. Verfassungsschutz, Justiz, Finanzbehörden von Berlin sind völlig außer Kontrolle geraten und drehen völlig durch, missbrauchen jegliche staatliche Gewalt, die sie greifen können. Achten keinen Datenschutz und kein Berufsgeheimnis, wenn sie glauben, jemand sei ein Agent der Russen – weil er nach dem Bachelor von Annalena Baerbock fragte.

Und diesen durchgeknallten Leuten wollen Sie einen Zugriff auf eine Vorratsdatenspeicherung ohne jegliche Missbrauchskontrolle geben?

Ist das Ihr Ernst?

23 Die Verstrickung des Deutschen Bundestags

23.1 Die „Meldestelle REspect!“

Zentrales Werkzeug zur Inszenierung des in Kapitel 22 beschriebenen Missbrauchs, polizeiliche Macht (von Befugnissen kann man nicht sprechen, denn befugt war die Polizei dazu nicht, und dem Verfassungsschutz ist gesetzlich verboten, sich polizeiliche Befugnisse anzueignen) für Zwecke der damaligen rot-grünen Regierung und insbesondere der beiden Regierungsparteien SPD und Grüne einzusetzen, war die „Meldestelle REspect!“ (Sitz in Stuttgart bei den Grünen).

Es bestehen deutliche Anhaltspunkte für die Annahme, dass REspect! eine Tarnorganisation des Verfassungsschutzes ist und nur nach außen hin vorgaukelt, privatrechtlich organisiert zu sein. Verbindungen zum Sozialministerium Baden-Württemberg als führender Behörde sind evident, und die Gelder fließen reichlich von der Bundes- und der Landesregierung.

Rechtlich dürfte es diese Meldestelle gar nicht geben. Sie existiert nicht einmal als Rechtsperson, sondern ist ein Projekt der „Jugendstiftung“ – obwohl sie außerhalb des Stiftungszwecks liegt. Sie verstößt zudem mit ihrer Tätigkeit direkt gegen

Artikel 9 DSGVO, der die Verarbeitung „besonderer Kategorien“ personenbezogener Daten wie politische Meinungen oder sexuelle Vorlieben einschränkt und verbietet.

Zwar gelten die Einschränkungen und Verbote nicht, wenn (Absatz 2 f) sich „die Verarbeitung sich auf personenbezogene Daten bezieht, die die betroffene Person offensichtlich öffentlich gemacht hat“, was für social media sicherlich gilt.

Ob dies aber eine flächendeckende, systematische, datenbankmäßige Erfassung und Zusammenführung von verteilten Social Media Posts zu Profilen und Dossiers erlaubt, ist mindestens zweifelhaft.

Artikel 10 DSGVO schränkt die Verarbeitung von Daten über Straftaten massiv ein.

Gerade darum geht es aber bei „REspect!“, nämlich (aus deren Sicht) strafbare Posts zu sammeln und Anzeigen zu erstatten.

Das ist nach DSGVO verboten.

Artikel 6 DSGVO bindet die Rechtmäßigkeit der Verarbeitung an einen Katalog von Voraussetzungen, **doch keine einzige ist hier erfüllt**. Es fehlt schon an der Rechtsgrundlage für die Verarbeitung personenbezogener Daten schlechthin.

„REspect!“ verletzt aber auch unmittelbar den Anspruch auf Datenschutzauskunft aus Artikel 15 DSGVO. Ich selbst bekam die in Beleg [23.1](#) gezeigte Datenschutzauskunft, aber auch andere bekamen dieselbe oder ähnliche Auskünfte.

Darin:

Bei einem Verstoß gegen deutsches Recht beantragt REspect! beim Netzwerkbetreiber die Löschung des Beitrags. Verfasserinnen und Verfasser von strafbaren hetzerischen Inhalten werden konsequent angezeigt.“

Der Zweck der Datenverarbeitung liegt somit in der Strafverfolgung.

Gemäß Art. 23 DSGVO in Verbindung mit § 34 Abs. 1 Nr. 1 BDSG und § 33 Abs. 2 Nr. 2 lit. b Hs. 2 BDSG besteht keine Pflicht zur Information der betroffenen Person und zur Auskunft gegenüber der betroffenen Person über die Datenverarbeitung.

Die Meldestelle REspect! erteilt deshalb grundsätzlich keine Informationen darüber, ob und gegebenenfalls welche Daten sie zum Zwecke der Strafverfolgung von dritten Personen erhält und verarbeitet.

Das ist blanker Unfug. Denn Artikel 23 DSGVO gilt **nur für Strafverfolgungsbehörden wie die Staatsanwaltschaft und die Polizei**, aber nicht für privatrechtliche selbsternannte Hobbysheriffs.

Auch dies deutet darauf hin, dass REspect! eine Tarnorganisation von BKA und Verfassungsschutz sein könnte, wenn sie sich selbst für eine Strafverfolgungsbehörde halten.

Effektiv ist das eine Form der strafbaren Amtsanmaßung.

Die Landesdatenschutzbehörde von Baden-Württemberg bleibt völlig untätig.

Man hat hier einen völlig außerhalb des Datenschutzes stehenden Datenbunker gebaut.

„REspect!“ ist stark mit den Grünen verwoben.

23.2 „HateAid“

Die zur Verfügung stehende Zeit für die vorliegende Stellungnahme genügt nicht, um die zivil- und strafrechtliche Verwicklung von HateAid in den in Kapitel [22](#) beschriebenen Missbrauchsfall auszuführen. Es gab aber Anhaltspunkte, dass die Straftakte, Kontodaten und Schriftsätze eines Zivilrechtsstreits datenschutzwidrig an HateAid weitergeleitet wurden und sich eine Anwaltskanzlei, die in Wirklichkeit für HateAid tätig war, sich als Vertreterin Ricarda Langs ausgab.

AW: AW: Antrag auf/Verlangen nach Datenschutzauskunft nach DSGVO

Subject: AW: AW: Antrag auf/Verlangen nach Datenschutzauskunft nach DSGVO
From: Salome Ebinger <ebinger@jugendstiftung.de>
Date: 24.11.22, 13:34
To: Hadmut Danisch <hadmut@danisch.de>

Sehr geehrter Herr Danisch,

hiermit lasse ich Ihnen die Antwort der Meldestelle bezüglich Ihrer Anfrage auf Auskunft Ihrer Daten zukommen.

Mit freundlichen Grüßen,

Salome Ebinger

Sehr geehrter Herr Danisch,

Ihre Anfrage vom 28.10.2022 haben wir erhalten.

Die Meldestelle REspect! nimmt Meldungen potentiell strafbarer Inhalte im Internet entgegen. Dazu erklären wir auf der Homepage:

„Das Internet ist kein rechtsfreier Raum. Volksverhetzung und politisch motivierte Drohungen sind auch in den sozialen Netzwerken strafbar. Wir wenden uns an alle, die im Netz auf Hasskommentare stoßen und etwas dagegen unternehmen möchten.“

Das geht ganz einfach: Meldemaske ausfüllen und abschicken.

Bei einem Verstoß gegen deutsches Recht beantragt REspect! beim Netzwerkbetreiber die Löschung des Beitrags. Verfasserinnen und Verfasser von strafbaren hetzerischen Inhalten werden konsequent angezeigt.“

Der Zweck der Datenverarbeitung liegt somit in der Strafverfolgung.

Gemäß Art. 23 DSGVO in Verbindung mit § 34 Abs. 1 Nr. 1 BDSG und § 33 Abs. 2 Nr. 2 lit. b Hs. 2 BDSG besteht keine Pflicht zur Information der betroffenen Person und zur Auskunft gegenüber der betroffenen Person über die Datenverarbeitung.

Die Meldestelle REspect! erteilt deshalb grundsätzlich keine Informationen darüber, ob und gegebenenfalls welche Daten sie zum Zwecke der Strafverfolgung von dritten Personen erhält und verarbeitet.

Gemäß § 33 Abs. 2 S. 1 BDSG sind die in Artikel 14 Absatz 1 und 2 der Verordnung (EU) 2016/679 genannten Informationen für die Öffentlichkeit in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache. Diese Informationen finden Sie auf unserer Website unter <https://meldestelle-respect.de/datenschutzerklaerung/>.

Verarbeitet die Meldestelle Daten auf Grundlage des Art. 6 Abs. 1 Buchstabe f DSGVO, liegt das berechnete Interesse der Meldestelle ausschließlich in der Strafverfolgung.

Automatisierte Entscheidungsfindung oder Profiling gem. Art. 14 Abs. 2 Buchstabe g DSGVO findet nicht statt.

Gemäß Art. 12 Abs. 4 DSGVO sind wir verpflichtet, Sie auf die Möglichkeit hinzuweisen, bei einer Aufsichtsbehörde Beschwerde einzulegen oder einen gerichtlichen Rechtsbehelf einzulegen. Gegen die Verweigerung der Auskunftserteilung ist die Beschwerde gem. Art. 77 DSGVO bei der Aufsichtsbehörde i.S.v. Art. 51 DSGVO zulässig. Die zuständige Aufsichtsbehörde für die Jugendstiftung ist das Regierungspräsidium Stuttgart, Postfach 80 07 09, 70507 Stuttgart. Zudem haben Sie gemäß Art. 79 DSGVO unbeschadet eines verfügbaren verwaltungsrechtlichen oder außergerichtlichen Rechtsbehelfs einschließlich des Rechts auf Beschwerde bei einer Aufsichtsbehörde gemäß Artikel 77 das Recht auf einen wirksamen gerichtlichen Rechtsbehelf, wenn Sie der Ansicht sind, dass die Ihnen aufgrund der DSGVO zustehenden Rechte infolge einer nicht im Einklang mit der DSGVO stehenden Verarbeitung Ihrer personenbezogenen Daten verletzt wurden.

Mit freundlichen Grüßen

Meldestelle REspect!

Von: Hadmut Danisch <hadmut@danisch.de>

Gesendet: Mittwoch, 16. November 2022 20:20

An: Salome Ebinger <ebinger@jugendstiftung.de>

Beleg 23.1: „Datenschutzauskunft“ der „Meldestelle REspect!“

In einer ersten Datenschutzauskunft vom 19.7.2024 wurden Daten aufgelistet, die man von meinem Blog erfasst hat. Dazu hieß es außerdem

Diese Angaben haben wir Großteils nicht erhoben, Sie sind durch die Website, Blog oder Screenshots ersichtlich geworden.

Ferner haben wir ein Urteil sowie Ihre Schriftsätze, Schriftsätze Ihres Anwalts und der Gegenseite vorliegen. Diese sind Ihnen im Rahmen des gerichtlichen Verfahrens, das noch nicht rechtskräftig abgeschlossen ist, auch zugegangen. Im Zusammenhang mit diesem Verfahren, haben wir auch die im Verfahren als Beweismittel aufgeführten Screenshots vorliegen.

[...]

Karina Filusch, LL.M.

Rechtsanwältin, Fachanwältin für IT-Recht und externe Datenschutzbeauftragte

Und auf weitere Nachfrage, wie HateAid an die Schriftsätze aus einem Zivilrechtsverfahren zwischen Ricarda Lang und mir kam, die nach Artikel 9 und 10 DSGVO geschützt sind, antwortete HateAid am 9.8.2024

Sehr geehrter Herr Danisch,

vielen Dank für Ihre Geduld. Aufgrund von Abwesenheiten erhalten Sie leider erst jetzt eine Antwort, wofür wir uns entschuldigen möchten.

Bedauerlich weise können wir auf Ihre Anfrage hin keine weiteren Auskünfte geben und berufen uns auf Art.15 Absatz 4 DSGVO. Dieser Absatz schützt die Interessen unserer Klientin. Bei einer Auskunft sähen wir die Rechte unserer Klientin verletzt.

Mit freundlichen Grüßen Karina Filusch Datenschutzbeauftragte bei HateAid

Auch das ist Unfug, denn Artikel 15 Absatz 4 DSGVO sagt nur

Das Recht auf Erhalt einer Kopie gemäß Absatz 3 darf die Rechte und Freiheiten anderer Personen nicht beeinträchtigen.

Kopien wurden aber nicht angefordert, zumal ich Kopien meiner eigenen Schriftsätze nicht brauche. Artikel 15 Absatz 4 DSGVO ist insbesondere keine Grundlage dafür, die Auskunft zu verweigern, von wo personenbezogene Daten erhoben wurden, schon gar nicht für Verstöße gegen die Mitteilungspflicht aus Artikel 14 DSGVO.

Auch hier liegen massive Datenschutzverstöße vor.

Auch „HateAid“ ist stark mit den Grünen, außerdem mit dem linksextremistischen Compact e.V. verwoben.

23.3 Die Bundesnetzagentur und der Bundestag

Eine zentrale Rolle bei der Zensur im Netz und beim vorliegenden Gesetzentwurf für die IP-Adressspeicherung spielt die Bundesnetzagentur, geführt vom **Grünen-Politiker Klaus Müller**.

Im Zusammenhang mit dem DSA und dem dazu erlassenen Digitale Dienste Gesetz musste der Bundestag 2024 einen Beirat bei der „Koordinierungsstelle für digitale Dienste“ einzurichten, also der Bundesnetzagentur.

Dazu sagt § 21 Digitale Dienste Gesetz:

§ 21 Beirat

(1) Bei der Koordinierungsstelle für digitale Dienste wird ein Beirat eingerichtet.

(2) Der Beirat besteht aus den folgenden 16 Mitgliedern:

1. vier Vertreterinnen und Vertreter der Wissenschaft,
2. acht Vertreterinnen und Vertreter der Zivilgesellschaft, einschließlich Verbraucherverbänden, und
3. vier Vertreterinnen und Vertreter von Wirtschaftsverbänden.

Unternehmen können nicht Mitglieder des Beirats sein. Die Vertreterinnen und Vertreter sollen hinsichtlich der Art und Weise der Tätigkeit digitaler Dienste über besondere rechtliche, wirtschaftswissenschaftliche, sozialpolitische oder technologische Erfahrungen oder über ausgewiesene einschlägige wissenschaftliche Kenntnisse verfügen.

(3) Der Beirat hat die Aufgabe,

1. die Koordinierungsstelle für digitale Dienste und die weiteren zuständigen Behörden nach § 12 Absatz 2 und 3 in grundsätzlichen Fragen der Anwendung und Durchsetzung der Verordnung (EU) 2022/2065 zu beraten,
2. der Koordinierungsstelle für digitale Dienste und den weiteren zuständigen Behörden nach § 12 Absatz 2 und 3 allgemeine Empfehlungen zur wirkungsvollen und einheitlichen Durchführung der Verordnung (EU) 2022/2065 vorzuschlagen und
3. wissenschaftliche Fragestellungen, insbesondere auch zum Umgang mit Daten, an die Koordinierungsstelle für digitale Dienste und die weiteren zuständigen Behörden nach § 12 Absatz 2 und 3 heranzutragen.

(4) Die Mitglieder des Beirats werden vom Deutschen Bundestag vorgeschlagen und für die Dauer der Wahlperiode des Deutschen Bundestages vom Bundesministerium für Wirtschaft und Klimaschutz im Einvernehmen mit dem Bundesministerium für Digitales und Verkehr berufen. Sie bleiben nach Beendigung der Wahlperiode des Deutschen Bundestages noch so lange im Amt, bis die neuen Mitglieder berufen worden sind. Die Mitglieder des Beirats können auf ihre Mitgliedschaft verzichten. Der Verzicht ist gegenüber dem Bundesministerium für Wirtschaft und Klimaschutz schriftlich oder elektronisch zu erklären. Hierüber ist das Bundesministerium für Digitales und Verkehr vom Bundesministerium für Wirtschaft und Klimaschutz zu unterrichten. Scheidet ein Mitglied vorzeitig aus, so ist unverzüglich an seiner Stelle ein neues Mitglied zu berufen.

(5) Die Mitglieder des Beirats sind in der Ausübung ihrer Tätigkeit im Beirat unabhängig, un-

terliegen keinen Weisungen und sind ausschließlich dem öffentlichen Interesse verpflichtet.

[... Abs. 6 bis 14 hier nicht relevant ...]

Aufgrund meiner Ausbildung, meiner Berufserfahrung und meiner Erfahrung mit den Datenschutzmängeln bei REspect! und HateAid hat die Bundestagsfraktion der AfD im Juli 2024 *mich* für diesen Beirat vorgeschlagen (**BT Drucksache 20/12123**).

In den Drucksachen und insbesondere in der Plenarsitzung vom 4.7.2024, **Plenarprotokoll 20/181** Seite 23490 (82 im PDF),

- werden die Vorschläge als „Wahlvorschläge“ bezeichnet,
- dann wurde eine „Wahl“ abgehalten,
- in der *alle Vorschlagenen außer mir* „gewählt“ wurden.

Wie ist das möglich?

Im Gesetz steht kein Wort von einer „Wahl“. Die Formulierung lässt sich auch nicht so auslegen, denn dieselbe Formulierung wird in Artikel 64 Absatz 1 GG verwendet:

Die Bundesminister werden auf Vorschlag des Bundeskanzlers vom Bundespräsidenten ernannt und entlassen.

Minister werden aber auch nicht vom Bundestag gewählt. Man wird dem Bundestag bei allem Wissensverfall immer noch unterstellen müssen, *dass er weiß, dass er selbst Minister nicht wählt*.

Wie also kommt der Bundestag auf die Idee, dass er die Mitglieder des Beirats wählen könne?

Das Bundesverfassungsgericht hat kurz darauf, am 18. September 2024, in zwei Organklagen, **2 BvE 1/20 und 2 BvE 10/21**, entschieden:

Grundsätzlich muss jeder Ausschuss, soweit er Aufgaben des Plenums übernimmt beziehungsweise dessen Entscheidungen vorbereitet, ein verkleinertes Abbild des Plenums sein und in seiner Zusammensetzung dessen Zusammensetzung widerspiegeln. Dies erfordert eine möglichst getreue Abbildung der Stärke der im Plenum vertretenen Fraktionen.

Der Grundsatz der Spiegelbildlichkeit gilt hingegen nicht für Gremien und Funktionen, die lediglich organisatorischer Art sind und daher nicht dem Einfluss des Prinzips gleichberechtigter Teilnahme an den dem Bundestag nach dem Grundgesetz übertragenen Aufgaben unterliegen. Art. 38 Abs. 1 Satz 2 GG begründet folglich für sich genommen keinen Anspruch auf Zugang zu Leitungsfunktionen, bei denen es nicht zur inhaltlichen Vorformung der parlamentarischen politischen Willensbildung kommt. Daraus folgt, dass sich gerade die Beschränkung der Vergabe von Vorsitzen in Ausschüssen durch die Geschäftsordnung des Deutschen Bundestages im Rahmen der dem Bundestag zustehenden Geschäftsordnungsautonomie hält. Bei dem Zugang zum Amt des Ausschussvorsitzes handelt es sich nicht um ein spezifisch mitgliedschaftliches Recht.

Deshalb darf sich der Bundestag zwar Ausschussvorsitzende wählen, muss aber bei

Aufgaben, die vertrauensbasiert sind und inhaltliche Arbeit machen, fraktionsproportional vertreten sein.

Eine Wahl ist also nicht nur gesetzlich nicht vorgesehen, sondern auch verfassungswidrig. **Trotzdem hat der Bundestag – wider rechtsbindendes bessers, vom Verfassungsgericht zugestelltes Wissen – den DSC-Beirat 2025 wieder gewählt.**

Und kurz nach dieser „Wahl“ zum DSC-Beirat 2024 hat die Bundesnetzagentur in Form dessen *grünen* Präsidenten Klaus Müller die *grüne* „Meldestelle REspect!“ und die *grüne* Organisation „HateAid“ **trotz schwerster Datenschutzverstöße und teils fehlender juristischer Existenz** zu *Trusted Flaggern* ernannt. Was ich mit meinem Wissen über REspect!, HateAid und Datenschutz selbstverständlich verhindert hätte.

Wie so etwas möglich ist, und wer es da unternommen und geschafft hat, eine Wahl auf die Tagesordnung des Bundestags zu setzen und durchführen zu lassen, die es gesetzlich nicht gibt, war bisher nicht herauszufinden.

Umso dubioser und unseriöser ist es, wenn ein ganzer Bundestag dann ohne das zu bemerken an dieser „Wahl“ teilnimmt, ohne deren Rechtsgrundlage zu sehen oder zu suchen. *Einfach nur, weil man eben macht, was auf der Tagesordnung steht. Egal was. Wie eine Schafherde.*

An der Befähigung des Bundestages zur Gesetzgebung darf gezweifelt werden. Wie will er dann mit einem ungleich schwierigeren Gesetzentwurf wie dem vorliegenden klarkommen?

Die Vertrauenswürdigkeit des Deutschen Bundestags rund um Digitalfragen, Netzwerke, Meinungsfreiheit und die Bundesnetzagentur liegt bei Null.

Teil V

Gaga-Justiz statt Rechtswegsgarantie

24 Anknüpfung an EuGH C-793/19

Die Anforderung des EuGH an eine Vorratsdatenspeicherung lautet (C-793/19 und C-794/19):

„Diese Rechtsvorschriften müssen durch klare und präzise Regeln sicherstellen, dass bei der Speicherung der fraglichen Daten die für sie geltenden materiellen und prozeduralen Voraussetzungen eingehalten werden und dass die Betroffenen über **wirksame Garantien** zum Schutz vor Missbrauchsrisiken verfügen.“

Ich werde in diesem Teil aufzeigen, dass die Bundesrepublik Deutschland ein Justizwillkürstaat ist, in dem

- die Rechtswegsgarantie aus Art. 19 Abs. 4 GG
- der Anspruch auf Rechtliches Gehör aus Art. 103 Abs. 1 GG
- der vom EuGH geforderte effektive Rechtsweg gegen Missbrauch staatlicher Gewalt

faktisch nicht mehr existieren. *Bei Licht betrachtet haben wir gar kein Recht mehr, weil sich bei Staat und Justiz niemand mehr an irgendwas hält und jeder macht, was er gerade will. Unsere Gesetze sind nur noch eine Art Rhetorik-Fundus, der dazu dient, so zu tun, als sei das und man selbst im Recht, und Gesetzgebung die Aufgabe, den Fundus so oft zu ändern, dass niemand mehr den Überblick hat.*

Die Bundesrepublik Deutschland ist nicht in der Lage, die oben zitierte Anforderung des Europäischen Gerichtshofes zu erfüllen.

Und sie wird es auch auf absehbare Zeit nicht mehr sein.

25 Gaga-Strafrecht Berlin

25.1 Fehlender Rechtsweg

Wie sieht der von Art. 19 Abs. 4 GG „garantierte“ effektive Rechtsweg gegen polizeiliche Übergriffe wie den in Kapitel 22 beschriebene Kontenzugriff aus?

Ganz einfach: *Es gibt keinen.*

Im Gesetz ist nichts vorgesehen außer einem nicht durchsetzbaren Löschanspruch im Kleingedruckten des BDSG.

Die Rechtsprechung hat deshalb als Notlösung entwickelt, in solchen Fällen *in analoger Anwendung von § 98 Abs. 2 Satz 2 StPO* die „gerichtliche Entscheidung beantragen zu können.

§ 98 Abs. 2 Satz 2 StPO ist dazu gedacht, in Fällen einer eigenmächtigen Beschlagnahme von Gegenständen durch die Staatsanwaltschaft die Rechtmäßigkeit klären zu lassen. *Das hilft einem aber nur in einem laufenden Gerichtsverfahren, und entscheidet über die Frage, ob ein Gegenstand als Beweis verwendet werden darf, oder ob man ihn wieder haben kann.*

Bei Daten hilft einem das nichts.

Und wenn das Verfahren, wie hier, bereits abgeschlossen ist, hilft es einem auch nichts. Denn selbst wenn das Gericht entschiede, dass die Beschlagnahme unzulässig war – nach Abschluss des Verfahrens nutzt einem das nichts mehr.

Außerdem ist das Gericht nicht Vorgesetzter oder Dienstaufsicht der Staatsanwaltschaft, und kann letztlich nur entscheiden, ob ein Beweis unrechtmäßig erhoben wurde und deshalb im laufenden Strafverfahren nicht verwendet werden darf. Es ist nur ein Abwehrmittel gegen die Verwendung des Beweises im Strafverfahren, aber kein Abwehrmittel gegen die Staatsanwaltschaft selbst.

Und selbst wenn das Gericht feststellte, dass eine Beschlagnahme unzulässig war, es brächte einem einfach gar nichts. Es wäre der Staatsanwaltschaft völlig egal, weil sie sich danach nicht richten muss.

In der Regel braucht man solche nachträglichen Verfahren auch nicht, weil mit der Eröffnung des Hauptverfahrens das Gericht über die Beschlagnahmen entscheidet und am Ende des Verfahrens mit dem Urteil klar wird, was man wieder bekommt und

was eingezogen wird.

Es ist auch nicht vorgesehen, die Handlungen der Staatsanwaltschaft zu prüfen. Berufungs- und Revisionsgerichte prüfen nur, ob das vorangehende Gericht selbst richtig darüber entschieden hat.

Trotzdem habe ich der Vollständigkeit halber diesen Antrag gestellt.

25.2 Gaga Staatsanwaltschaft

Stellt man einen solchen Antrag, muss zunächst die Staatsanwaltschaft dazu Stellung nehmen – Beleg [25.1](#).

Die Staatsanwältin, die mit dem Fall bisher gar nichts zu tun hatte und ihn nicht kennt, äußert sich zur Kontenabfrage gar nicht. Auch zum Antrag mit keinem Wort.

Stattdessen erklärt sie, dass § 100j StPO die Auskunft über Bestandsdaten zur Verfolgung von Straftaten erlaube – **obwohl der in diesem Fall gar nicht vorkam**.

§ 100j StPO regelt die Bestandsdatenauskunft von Telekommunikationsanbietern, die nach dem TKG dazu verpflichtet sind. Mit Banken und meinem Fall hat das *überhaupt nichts zu tun*. Und es ging hier um Kontenbewegung und nicht um die „Bestandsdatenauskunft“, wer Kontoinhaber ist.

Das heißt: Sie kannte die Akten und den Fall nicht, hat meinen Antrag nie gelesen, und einfach – **copy-paste** – **eine Stellungnahme von irgendeinem anderen Fall kopiert**, indem es um eine Abfrage nach § 100j gegangen war.

25.3 Gaga Ermittlungsrichterin

Nachdem das Hauptsacheverfahren eingestellt bzw. gar nicht erst eröffnet worden war, war in der Sache eine Ermittlungsrichterin zuständig. Mein Hinweis, dass die Staatsanwaltschaft eine Copy-Paste-Plagiats-Gaga-Stellungnahme vorgelegt hat, war ihr egal.

Die Ermittlungsrichterin entschied, dass der Zugriff auf das Konto *rechtmäßig* gewesen sei (Beleg [25.2](#),[25.3](#),[25.4](#)) , weil

- **§ 160 Abs. 3 StPO** die Staatsanwaltschaft auch ermitteln soll und darf, was für die Bestimmung der Rechtsfolgen benötigt wird. Staatsanwaltschaften dürfen Kontenauskünfte einholen, um die Höhe der beantragten Geldstrafe zu berechnen.

Das ist hier aber frei erfundener Unfug. Denn nicht nur steht in der Akte kein Wort davon, dass das Konto zu diesem Zweck abgefragt wurde, noch wurden die Kontodaten in irgendeiner Weise zur Berechnung verwendet.

Staatsanwaltschaft Berlin

30. Juni 2025

237 Js 1124/22 (238) A - 61.017/18.2029



U.m.A.

Vfg.

03. Juli 2025

dem AG Tiergarten, Ermittlungsrichter

349 Gs 1547/2025

zu dem Antrag Bd. II Bl. 120 d.A. übersandt.

Nach hiesiger Sicht ist dem Antrag des Beschuldigten nicht stattzugeben:

Die Anwendbarkeit des § 23 EEGVG setzt voraus, dass es sich bei der angegriffenen Maßnahme um einen Verwaltungsakt im Sinne des § 35 VwVfG handelt. Aufgrund des Gesetzeswortlautes, der von „sonstigen Maßnahmen“ spricht, wird überwiegend vertreten, dass auch Realakte umfasst sind, sofern die in Rede stehende Maßnahme Außenwirkung entfaltet. Nicht umfasst sind daher Auskünfte oder Stellungnahmen (Meyer-Goßner/Schmitt, STPO, 67. Aufl., § 23 EEGVG, Rn. 5, 6). Grundsätzlich fallen auch Maßnahmen der Staatsanwaltschaft im Ermittlungsverfahren im Strafverfahren nicht unter den Rechtsweg nach § 23 EEGVG (Meyer-Goßner/Schmitt, STPO, 67. Aufl., § 23 EEGVG Rn. 9). Eine Ausnahme bestehe jedoch dann gem. Art. 19 IV GG, wenn es sich um in Grundrechte eingreifende Maßnahmen handelt. Die Maßnahme darf jedoch für die Anwendung von § 23 EEGVG noch nicht vollzogen sein (Meyer-Goßner/Schmitt, STPO, 67. Aufl., § 23 EEGVG, Rn. 10), in diesem Fall ist § 98 II 2 StPO analog anzuwenden.

§ 98 II 2 StPO ist entsprechend auf die nachträgliche gerichtliche Prüfung der Rechtmäßigkeit bereits durch Vollzug erledigter Eingriffsmaßnahmen der Staatsanwaltschaft anwendbar, falls ein tiefgreifender Grundrechtseingriff zu besorgen ist (Meyer-Goßner/Schmitt, STPO, 67. Aufl., § 98 StPO, Rn. 23). Bei der Abfrage von Bestandsdaten könnte der grundrechtlich geschützte Schutz personenbezogener Daten (Art. 1 I iVm Art. 2 I GG) betroffen sein. § 100j StPO erlaubt jedoch ausdrücklich Auskunft über Bestandsdaten zur Verfolgung von Straftaten. Die Ausgestaltung der Vorschrift ist aufgrund dieser Zielbeschränkung und ihrer Ausdifferenziertheit auch verhältnismäßig. Zudem erfolgt keine Abfrage des Inhalts der Kommunikation, sondern die Auskunft zielt lediglich auf eine Identitätsfeststellung ab, der Eingriff ist daher auch nicht als besonders schwerwiegend zu bewerten.

Mithin kann vorliegend nach hiesiger Sicht aufgrund des Vollzugs der Maßnahme eine gerichtliche Überprüfung gem. § 23 EEGVG nicht erfolgen. Da kein tiefgreifender Grundrechtseingriff anzunehmen ist, kann auch keine gerichtliche Überprüfung gem. § 98 II 2 StPO analog erfolgen.

Dem Antrag des Beschuldigten ist mithin nicht stattzugeben.

2. 1 Monat.

Richter
Staatsanwältin

02. Juli 2025

Beleg 25.1: Gaga-Stellungnahme der Staatsanwaltschaft: § 100j StPO kam hier gar nicht vor

Beglaubigte Abschrift

Amtsgericht Tiergarten

Geschäftsnummer: 349 Gs 1547/25

Staatsanwaltschaft Berlin, 237 Js 1124/22



Beschluss

In dem Ermittlungsverfahren gegen

Hadmut Danisch,

geboren am 22.06.1966 in Mannheim, Staatsangehörigkeit: deutsch, wohnhaft: Dresdener
Straße 96, 10179 Berlin

wegen Beleidigung

hat das Amtsgericht Tiergarten am 30. September 2025 beschlossen:

Der Antrag des Beschuldigten vom 02.05.2025 auf gerichtliche Entscheidung wird auf seine Kosten

zurückgewiesen.

Gründe:

1. Unter dem staatsanwaltschaftlichen Aktenzeichen 237 Js 1124/22 ermittelte die Staatsanwaltschaft Berlin gegen den Beschuldigten wegen Beleidigung nach §§ 185, 188 StGB. Noch im Ermittlungsverfahren erfolgte eine Kontoabfrage bei der Deutschen Bank zum Konto des Beschuldigten und die entsprechende Weitergabe der Daten. Hiergegen wendet sich der Beschuldigte und begehrt insbesondere die Feststellung, dass die Kontoabfrage rechtswidrig war. Hinsichtlich der Einzelheiten seiner Begründung wird auf die Antragsschrift vom 02.05.2025 Bezug genommen.

Beleg 25.2: Gaga-Beschluss des Amtsgerichts

2. Der Antrag ist gemäß § 98 Abs. 2 Satz 2 StPO analog zulässig, hat in der Sache jedoch keinen Erfolg.

Die seitens der Staatsanwaltschaft Berlin erfolgte Kontoabfrage bei der Deutschen Bank war rechtmäßig. Die insoweit erhobenen Daten wurden rechtmäßig erhoben.

Die Strafverfolgungsbehörden sind befugt zur Aufklärung der Vermögensverhältnisse, soweit sie für die Rechtsfolgen von Bedeutung sind, u. a. eine Bankauskunft einzuholen. Rechtsgrundlage für ein entsprechendes Auskunftersuchen ist § 161 Abs. 1 Satz 1 StPO i.V.m. § 160 Abs. 3 StPO.

Gemäß § 161 Abs. 1 Satz 1 StPO ist die Staatsanwaltschaft befugt, von allen Behörden Auskunft zu verlangen und Ermittlungen jeder Art entweder selbst vorzunehmen oder durch die Behörden und Beamten des Polizeidienstes vornehmen zu lassen, soweit nicht andere gesetzliche Vorschriften ihre Befugnisse besonders regeln. Erforderlich für Ermittlungsmaßnahmen nach § 161 Abs. 1 StPO ist zunächst der Anfangsverdacht einer Straftat. Hier bestand gegen den Beschuldigten der Anfangsverdacht einer Beleidigung. Dass es sich hierbei um eine Straftat im eher unteren Kriminalitätsbereich / im Geringfügigkeitsbereich handelt, ändert aufgrund des klaren Wortlauts der Vorschrift an der Bewertung nichts. Auch beim Verdacht geringfügiger Taten können die Strafverfolgungsbehörden zur Aufklärung der Vermögensverhältnisse, soweit sie für die Rechtsfolgen von Bedeutung sind, Auskunftersuchen an Banken stellen (vgl. auch OLG Stuttgart, Beschluss vom 13.02.2015 - 4 Ws 19/25).

Nach § 160 Abs. 3 StPO sollen sich die Ermittlungen der Staatsanwaltschaft ausdrücklich auch auf die Umstände erstrecken, die für die Bestimmung der *Rechtsfolgen der Tat* von Bedeutung sind. Aus Sicht der Staatsanwaltschaft stand als Rechtsfolge der Beleidigung zutreffend eine Geldstrafe im Raum. Eine Geldstrafe wird in Tagessätzen verhängt, wobei die Höhe eines Tagessatzes unter Berücksichtigung der persönlichen und wirtschaftlichen Verhältnisse des Täters bestimmt wird, § 40 Abs. 1 und Abs. 2 StGB. Die richtige Festsetzung der Tagessatzhöhe setzt voraus, dass die Bemessungsgrundlage zutreffend (von den Ermittlungsbehörden) ermittelt wird. Gemäß Nr. 14 RiStBV sind die Einkommens- und Vermögensverhältnisse des Beschuldigten durch die Staatsanwaltschaft aufzuklären.

Das Auskunftersuchen war auch verhältnismäßig. Insbesondere war das Auskunftersuchen auch unter Berücksichtigung des durch die Erhebung der personenbezogenen Daten begründeten Eingriffs in das Recht auf informationelle Selbstbestimmung des Beschuldigten (Art. 2 Abs. 1, Art. 1 Abs. 1 GG) verhältnismäßig; es standen keine mildereren Ermittlungsmaßnahmen zur Be-

Beleg 25.3: Gaga-Beschluss des Amtsgerichts

349 Gs 1547/25

- Seite 3 -

messung der Höhe eines Tagessatzes für eine mögliche Geldstrafe zur Verfügung. Auch durch das Bankgeheimnis ist die Ermittlung der Vermögensverhältnisse nicht beschränkt (vgl. Fischer StGB, 72. Auflage § 40 Rn. 18).

Der Antrag auf gerichtliche Entscheidung war daher als unbegründet zurückzuweisen.

Yacob
Richterin am Amtsgericht



Für die Richtigkeit der Abschrift
Berlin, 01.10.2025

Salewski, JBesch
Urkundsbeamtin der Geschäftsstelle
Durch maschinelle Bearbeitung beglaubigt
- ohne Unterschrift gültig

Beleg 25.4: Gaga-Beschluss des Amtsgerichts

Ein Spendenkonto kann dafür auch nicht verwendet werden, weil Spenden Schenkungen sind, und Schenkungen nicht zum für die Höhe einer Geldstrafe relevanten Einkommen zählen. Auf dem Konto gibt es nichts, was man für die Höhe einer Geldstrafe verwenden könnte, und das wussten LKA und Staatsanwaltschaft, denn sie haben es vorher als „Unterstützerkonto“ bezeichnet, wussten also nachweislich, dass das Konto dafür nicht taugt.

Und selbst wenn es so gewesen wäre: *Wofür braucht man bei der Berechnung der Geldstrafe die Namen, IBAN-Nummern und Verwendungszwecke der Spender? Wofür macht man sich die Mühe, die Zahlungen nach Herkunftsländern zusammenzufassen und aufzuschlüsseln? Warum untersucht man die Verwendungszwecke danach, ob sie allgemein, oder auf bestimmte Artikel bezogen waren?*

Warum und wozu gibt man die Kontodaten an den Zoll weiter?

- Sie schreibt, Rechtsgrundlage sei **§ 161 Abs. 1 Satz 1 StPO**, wonach die Staatsanwaltschaft „von allen Behörden Auskunft verlangen darf“.

Auch das ist Unfug. Denn die Deutsche Bank ist eine Privatbank und keine Behörde. § 161 Abs. 1 Satz 1 StPO kann nicht gegen privatrechtliche Unternehmen eingesetzt werden.

- Sie beruft sich auf OLG Stuttgart, Beschluss vom 13.02.2015 - 4 Ws 19/25.

Das ist der größte Unfug. Da hat man einfach aus irgendeinem Kommentar irgendein Aktenzeichen als Verzierung abgeschrieben.

In diesem Beschluss des OLG Stuttgart geht es um Ersuchen **an die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) um Auskunft über Kontostammdaten auf der Rechtsgrundlage § 24c KWG**. Da geht es ausschließlich um Auskunft darüber, wer über ein Konto Verfügungsberechtigt ist und nicht um die Kontobewegungen. **Das hat mit dem vorliegenden Fall überhaupt nichts zu tun.** Einfach nur irgendein willkürliches Aktenzeichen zur Verzierung.

25.4 Gaga Landgericht

25.4.1 Beschwerde

Also habe ich Beschwerde zum Landgericht erhoben, weil die Staatsanwältin und die Ermittlungsrichterin offenkundig beide frei erfundenen Unsinn aufgetischt und weder Antrag noch Akte gelesen hatten.

Das Landgericht hat die Beschwerde abgewiesen. Und sie gar nicht erst gelesen, so wenig, wie die Akte, denn darin hatte ich ihnen das, was sie falsch machen, sogar erläutert. Sie versuchen es mit einer neuen Begründung (Belege [25.5](#), [25.6](#) und [25.7](#)).

Beglaubigte Abschrift

Landgericht Berlin I

Az.: 510 Qs 1/26
349 Gs 1547/25 AG Tiergarten
237 Js 1124/22 StA Berlin



Beschluss

In dem Ermittlungsverfahren gegen

Hadmut Danisch,
geboren am 22. Juni 1966 in Mannheim,
wohnhaft: Dresdener Straße 96, 10179 Berlin,
Staatsangehörigkeit: deutsch

wegen Beleidigung

hat das Landgericht Berlin I - 10. Strafkammer als Beschwerdekammer - am 15. Januar 2026 beschlossen:

1. Die Beschwerde des Beschuldigten gegen den Beschluss des Amtsgerichts Tiergarten vom 30. September 2025 wird als unbegründet verworfen.
2. Der Beschuldigte hat die Kosten seines Rechtsmittels zu tragen.

Beleg 25.5: Gaga-Beschluss des Landgerichts

Gründe:**I.**

Gegen den Beschwerdeführer hat die Staatsanwaltschaft Berlin ein Ermittlungsverfahren wegen Beleidigung geführt, weil er im Internet frei zugänglich über die Politikerin Ricarda Land geschrieben haben soll [REDACTED]

[REDACTED] Im Rahmen dieses Ermittlungsverfahrens hat die Staatsanwaltschaft Berlin angeordnet, Bankauskünfte betreffend den Beschwerdeführer einzuholen. Ein entsprechendes Auskunftersuchen hat das LKA Berlin an die Deutsche Bank AG übermittelt, welche nachfolgend die begehrten Informationen erteilt hat. Danach hat die Staatsanwaltschaft einen Antrag auf Erlass eines Strafbefehls wegen Beleidigung nach §§ 185, 188 StGB gegen den Beschwerdeführer gestellt. Mit Beschluss vom 6. Juni 2023 hat das Amtsgericht Tiergarten den Antrag abgelehnt, weil es Bedenken hatte, ohne Hauptverhandlung zu entscheiden. Schließlich ist das Verfahren nach § 153 Abs. 2 StPO mit Beschluss vom 11. August 2023 eingestellt worden. Mit Schreiben vom 2. Mai 2025 hat der Beschwerdeführer einen Antrag auf gerichtliche Entscheidung bezogen auf das Auskunftersuchen an die Deutsche Bank AG gestellt. Diesen Antrag hat das Amtsgericht Tiergarten – Ermittlungsrichter – mit Beschluss vom 30. September 2025 zurückgewiesen. Hiergegen wendet sich der Beschwerdeführer mit seiner Beschwerde vom 3. November 2025 und führt im Wesentlichen aus, dass die Ermittlungsrichterin für den Erlass des vorgenannten Beschlusses nicht zuständig gewesen sei, es kein Auskunftsanspruch der Staatsanwaltschaft und der Polizei gegenüber einer Privatbank wie der Deutschen Bank AG gäbe und der Richtervorbehalt umgangen worden sei. Das Amtsgericht Tiergarten hat der Beschwerde nicht abgeholfen.

II.

Die zulässige Beschwerde gegen den Beschluss des Amtsgerichts Tiergarten vom 30. September 2025 hat in der Sache keinen Erfolg. Die Ausführungen in dem angefochtenen Beschluss sind zutreffend.

1. Das Amtsgericht Tiergarten – Ermittlungsrichter – war gemäß § 162 Abs. 1, 3 Satz 3 StPO für die Entscheidung über den Antrag auf gerichtliche Entscheidung zuständig. Denn nach rechtskräftigem Abschluss des Verfahrens – wie vorliegend – fällt die Zuständigkeit wieder auf den Ermittlungsrichter zurück.

Beleg 25.6: Gaga-Beschluss des Landgerichts

2. Ferner weist die Kammer darauf hin, dass es zwar zutreffend ist, dass eine Pflicht zur aktiven Auskunftserteilung auf ein Auskunftersuchen nur für öffentlich-rechtliche Bankinstitute besteht. Wird jedoch ein Auskunftersuchen an ein privatrechtliches Kreditinstitut gerichtet, handelt es sich um eine schriftliche staatsanwaltschaftliche Zeugenvernehmung auf der Grundlage von § 161 Abs. 1 Satz 1 2. Halbsatz („Ermittlungen jeder Art“), welche allerdings keine Rechtspflicht zur Auskunftserteilung begründet. Kommt eine Bank dem Auskunftsverlangen jedoch nicht nach, so ist dieses durch Zeugenvernehmung von Mitarbeitern oder durch *Durchsuchung* und *Beschlagnahme* zwangsweise durchsetzbar. Die Bank muss indes solche Zwangsmaßnahmen nicht abwarten, sondern darf zu deren Abwendung Auskünfte freiwillig erteilen (vgl. KK-StPO/Weingarten, 9. Auflage 2023, § 161 Rn. 8). Dass vorliegend das LKA das Auskunftersuchen auf Anordnung der Staatsanwaltschaft Berlin abgesandt hat, ist zudem von § 161 Abs. 1 Satz StPO gedeckt. Danach kann die Staatsanwaltschaft Ermittlungen jeder Art auch durch die Behörden und Beamten des Polizeidienstes vornehmen lassen.

3. Eine richterliche Anordnung bedurfte es insoweit nicht, weil eine solche bezogen auf das in Rede stehende Auskunftersuchen nicht gesetzlich vorgeschrieben ist.

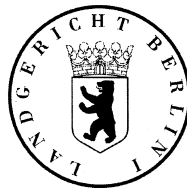
III.

Die Kostenentscheidung folgt aus § 473 Abs. 1 StPO.

Braunschweig

Mahlke

Kunkel



Für die Richtigkeit der Abschrift
Berlin, 19.01.2026

Rohrbach, JSekr
Urundsbeamter der Geschäftsstelle
Durch maschinelle Bearbeitung beglaubigt
- ohne Unterschrift gültig

Beleg 25.7: Gaga-Beschluss des Landgerichts

25.4.2 Gaga 1: Zeugen

Das Landgericht schreibt:

Ferner weist die Kammer darauf hin, dass es zwar zutreffend ist, dass eine Pflicht zur aktiven Auskunftserteilung auf ein Auskunftersuchen **nur für öffentlich-rechtliche Bankinstitute besteht**. Wird jedoch ein Auskunftersuchen an ein **privatrechtliches Kreditinstitut gerichtet**, handelt es sich um eine **schriftliche staatsanwaltschaftliche Zeugenvernehmung auf der Grundlage von § 161 Abs. 1 Satz 1 2. Halbsatz („Ermittlungen jeder Art“)**, welche **allerdings keine Rechtspflicht zur Auskunftserteilung begründet**.

Das ist juristischer Unfug, Phantasiegeschwafel. Da sitzen schon die Grundlagen der StPO nicht.

Man kann eine Bank, eine juristische Person nicht als Zeugen vernehmen, nur *natürliche Personen, die eindeutig bestimmt sind*. Man kann den Mitarbeiter Meier, aber nicht die Deutsche Bank als Zeugen vernehmen. Nur echte Menschen können Zeugen sein.

Insbesondere aber kann man Zeugen nur zu *gemachten Sinneswahrnehmungen über die fünf Sinnesorgane und inneren Vorgängen*¹ befragen.

- Kommt ein Kunde auf die Bank, und legt einen Geldkoffer zur Einzahlung vor, kann man den Kassierer befragen, weil er das gesehen hat.
- Ruft ein Kunde an und will keinen Kredit, kann man den Mitarbeiter befragen, der mit ihm telefoniert hat.
- Gab es einen Banküberfall, kann man die anwesenden Mitarbeiter als Zeugen befragen.

Aber man kann niemanden als Zeugen einer elektronisch ausgeführten Banküberweisung befragen, weil die niemand mit seinen Sinnesorganen wahrgenommen hat. Schon gar nicht alle aus mehr als zwei Jahren.

Man kann Zeugen auch nicht beauftragen, etwas für die Staatsanwaltschaft zu tun, Daten aus einem Computer zu holen. Man kann Zeugen nur nach dem befragen, was sie bereits *im Kopf* haben.

Und Zeugenaussagen sind auch nur das, was man als Zeuge persönlich – mündlich – mitteilen kann. Die Übermittlung einer Datei mit 1475 Einträgen ist keine „Zeugenaussage“.

Wie ist es möglich, dass gleich drei Richter eines Landgerichts, Juristen mit Staatsexamen und der „Befähigung zum Richteramt“, ausgestattet mit der Macht, Menschen für den Rest ihres Lebens ins Gefängnis zu sperren, nicht wissen, was ein „Zeuge“ ist?

¹ Ich hatte Angst, ich hatte Schmerzen, es tat weh, ich wollte das nicht, er gefiel mir nicht ...

Ausgehend von meinem eigenen Studienhintergrund in den MINT-Fächern und deren Systematik hatte ich darüber einen wütend-galligen Blogartikel geschrieben, und darin geschimpft, dass das doch Stoff des ersten Semesters Jura sein müsse.

Dazu schrieben mir mehrere Juristen, dass ich da falsch läge, denn **Zeugen kämen im gesamten Jura-Studium überhaupt nicht vor – man werde da ausschließlich mit nutzloser Rechtsdogmatik vollgepumpt und lerne praktisch gar nichts**. Erst im Referendariat zum zweiten Staatsexamen begegne man mit etwas Glück Zeugen im Gericht, könne mal welche sehen, lerne aber nichts über sie.

Juristen wissen tatsächlich nicht, was ein Zeuge ist.

Also habe ich – Bibliothek, Juris, Beck Online – nach juristischen Quellen dafür gesucht, was ein Zeuge ist. **Es gibt keine Legaldefinition**. Auch kein Lehrbuch.

Erst beim BGH bin ich fündig geworden:

BGH 6 StR 172/54:

Der BGH beschreibt, dass es *unmittelbare und mittelbare* Zeugen gibt.

Unmittelbare Zeugen sind die, die **Beweistatsachen aufgrund eigener, unmittelbarer Wahrnehmung** als Zeuge beschreiben können.

Mittelbare Zeugen sind die, die andere Personen berichten gehört haben, etwa „Hörensagen“ oder Polizeibeamte, die Zeugen vernommen haben.

BGH 2 StR 92/65:

Das Gesetz sieht die Möglichkeit, einen Zeugen wegen Besorgnis der Befangenheit abzulehnen und damit als Beweismittel auszuschalten, nicht vor; vielmehr kann und darf jede nicht am Verfahren als Beschuldigter oder Mitbeschuldigter beteiligte Person, die nicht von einem ihr etwa zustehenden Aussage- oder Auskunftsverweigerungsrecht Gebrauch macht, **als Zeuge über alle Tatsachen gehört werden, die Gegenstand ihrer sinnlichen Wahrnehmung waren**. Danach ist hier weder von Bedeutung, bei welcher Gelegenheit und auf welche Weise sie ihre Beobachtungen gemacht hat, noch kommt es darauf an, in welcher Beziehung sie zu dem Gegenstand des Verfahrens und zu den daran Beteiligten, insbesondere zu dem Angeklagten, gestanden hat und steht.

[...]

Deshalb kann auch die Besorgnis der Befangenheit, die Anlaß zur Ablehnung eines Sachverständigen gegeben hat, nicht dazu führen, diesen als Zeugen oder als sachverständigen Zeugen insoweit auszuschließen, als es sich um die Wiedergabe der ihm bei Durchführung des Auftrages bekannt gewordenen Tatsachen handelt. Sie können und dürfen mit zum Inhalt der Zeugenvernehmung gemacht werden, **weil sie Gegenstand seiner sinnlichen Wahrnehmung gewesen sind**.

BGH 4 StR 438/69:

Der Senat kann ferner der Ansicht des Beschwerdeführers nicht beitreten, daß von einer Aussage im Sinne des Verfahrensrechts nur gesprochen werden könne, wenn der Zeuge Tatsachen bekunde, die Gegenstand seiner (sinnlichen) Wahrnehmung gewesen seien. **Der Begriff der Zeugenaussage kann nicht in dieser Weise eingeschränkt werden. In der Regel werden freilich Zeugenaussagen Vorgänge in der Außenwelt betreffen, die der Zeuge sinnlich wahrgenommen hat. Jedoch können auch innere Vorgänge, Eindrücke, Gedanken, Überlegungen, Beweggründe, Affekte und andere geistig-seelische Vorgänge und Zustände des Innenlebens Gegenstand einer Zeugenaussage sein.** Bekundungen dieser Art sind vom Richter frei zu würdigen und dürfen von ihm bei der Bildung seiner Überzeugung verwertet werden.

Bankauskünfte, die erst als Datei aus einer Datenbank extrahiert werden müssen, sind keine „Zeugenvernehmungen“.

Machen Sie sich dieses Staatsversagen, für das Sie als Gesetzgeber verantwortlich sind, bewusst: Dieser Staat attestiert Leuten, die nach miserabelster Pseudoausbildung nicht einmal wissen, was ein Zeuge ist, per Staatsexamen die „Befähigung zum Richteramt“, und gibt ihnen die Macht, Menschen lebenslang einzusperren.

Das ist Ihr Werk als Gesetzgeber.

25.4.3 Gaga 2: Richtervorbehalt

Die Kammer schreibt weiter:

Kommt eine Bank dem Auskunftsverlangen jedoch nicht nach, so ist dieses durch Zeugenvernehmung von Mitarbeitern oder durch Durchsuchung und Beschlagnahme zwangsweise durchsetzbar. Die Bank muss indes solche Zwangsmaßnahmen nicht abwarten, sondern darf zu deren Abwendung Auskünfte freiwillig erteilen (vgl. KK-StPO/Weingarten, 9. Auflage 2023, § 161 Rn. 8).

[...]

Eine richterliche Anordnung bedurfte es insoweit nicht, weil eine solche bezogen auf das in Rede stehende Auskunftersuchen nicht gesetzlich vorgeschrieben ist.

Auch das ist grober Unfug.

Das ist schon deshalb Unfug, weil es das ganze Auskunftersuchen gesetzlich nicht gibt. Man kann nicht sagen, dass ein Auskunftersuchen, dass es nicht gibt, keiner richterlicher Anordnung bedarf, weil es in dem Gesetz dazu, das es nicht gibt, ja nichts davon steht.

Es ist zwar richtig, dass eine Bank Zwangsmaßnahmen nicht abwarten muss. **Deren konkrete Androhung gegen konkrete natürliche Personen muss sie aber schon abwarten.** Denn erst dann gibt es ja etwas abzuwenden. Erst wenn eine **konkrete**

Androhung konkreter Zwangsmaßnahmen gegen konkrete Menschen vorliegt, darf die Bank diese auch ohne Einverständnis des Kunden durch Herausgabe der Daten abwenden, weil es erst dann etwas abzuwenden gibt.

Und genau deshalb ist ein richterlicher Beschluss notwendig: Weil nur ein Gericht diese Zwangsmaßnahmen überhaupt anordnen kann.

Eine Staatsanwaltschaft hat keine Zwangsmaßnahmen. Deshalb kann eine Bank ohne Einverständnis des Kunden einer Staatsanwaltschaft niemals Auskunft erteilen, weil es nichts abzuwenden gibt.

Erst durch einen richterlichen Beschluss kann eine Bank erst in eine Abwendungssituation kommen. Doch das wissen *diese* Richter offenbar nicht.

Machen Sie sich bewusst: Diese drei Richter einer Strafkammer beherrschen noch nicht einmal Elementarwissen der Strafprozessordnung.

Und diesen Leuten wollen Sie ein IP-Adressspeicherungsgesetz geben, das schon juristisch nur Wirrwarr ist und das technisch nur für Internet-Profis verständlich ist?

25.5 Bundesverfassungsgericht als Regierungsvertretung

Gegen diese Kette von Unfug, Blödsinn und Unwissenheit habe ich Verfassungsbeschwerde erhoben und dazu die bisher ungeklärte Verfassungsrechtsfrage aufgeworfen, ob der Schutz der Pressefreiheit aus Artikel 5 GG und das daraus hervorgehende Berufsgeheimnis auch publikationsbezogene Spendenkonten mit personenbezogenen Angaben erfasst. Es gibt zwar einige Entscheidungen zum Schutz der *Redaktionsräume* und der *Telekommunikation*. Aber noch keine Entscheidung zu Bankkonten.

Außerdem habe ich die Frage nach dem Post- und Fernmeldegeheimnis aufgeworfen, weil auch die Übermittlung der Namen, Kontonummern und Verwendungszwecke Telekommunikation und damit geschützt ist.

Ergebnis: Die Beschwerde wird – ohne Begründung – nicht zur Entscheidung angenommen (Belege [25.8](#) und [25.9](#)).

Richter:

Stephan Harbarth Politiker der CDU

Ines Härtel Von der SPD installierte Richterin, Schwerpunkt Agrar- und Umweltrecht

Miriam Meßling Zuvor Richterin für Sozial- und Asylbewerberrecht, ebenfalls von der SPD „vorgeschlagen“.

Damit hat letztlich die Regierung selbst die Verfassungsbeschwerde verworfen.

Beglaubigte Abschrift

BUNDESVERFASSUNGSGERICHT

- 1 BvR 953/26 -



**In dem Verfahren
über
die Verfassungsbeschwerde**

des Herrn Hadmut D a n i s c h ,
Dresdener Straße 96, 10179 Berlin,

I. unmittelbar gegen

1. a) den Beschluss des Landgerichts Berlin I
vom 15. Januar 2026 - 510 Qs 1/26 -,
b) den Beschluss des Amtsgerichts Tiergarten
vom 30. September 2025 - 349 Gs 1547/25 -,
2. die Verweigerung der Datenlöschung in beiden Beschlüssen,
3. die Weitergabe der abgefragten Kontodaten durch Staatsanwaltschaft
und Landeskriminalamt an den Verfassungsschutz Berlin, den Zoll
und an die Kanzlei Preu Bohlig & Partner und damit die Organisation
„Hate Aid“,
4. die Auswertung der Kontobewegungen,
5. das „Auskunftersuchen“ der Staatsanwaltschaft und des
Landeskriminalamtes Berlin an die Deutsche Bank
vom 28. März 2023,

II. mittelbar gegen

§ 33a Strafprozessordnung (StPO)

hat die 1. Kammer des Ersten Senats des Bundesverfassungsgerichts durch
den Präsidenten Harbarth
und die Richterinnen Härtel,
Meßling

1/2

Beleg 25.8: Das Bundesverfassungsgericht schert sich nicht darum

gemäß § 93b in Verbindung mit § 93a BVerfGG in der Fassung der Bekanntmachung
vom 11. August 1993 (BGBl I S. 1473)
am 29. Juni 2026 einstimmig beschlossen:

Die Verfassungsbeschwerde wird nicht zur Entscheidung angenommen.

Von einer Begründung wird nach § 93d Abs. 1 Satz 3 BVerfGG abgesehen.

Diese Entscheidung ist unanfechtbar.

Harbarth

Härtel

Meßling

2/2

Beleg 25.9: Das Bundesverfassungsgericht schert sich nicht darum

Dies wird sie sich vor dem EuGH vorhalten lassen müssen.

26 Die Hilflosigkeit des Datenschutzes in Berlin

Die einzige Stelle überhaupt, der ich in dieser Stellungnahme zumindest den Anschein von Sachkompetenz bescheinigen kann, ist die der Berliner Beauftragten für Datenschutz und Informationssicherheit.

In Telefonaten und Schreiben ist zumindest aromatisch zu erkennen, dass sie die Datenschutzverletzungen richtig erkennen, richtig einordnen, missbilligen.

Aber: *Es passiert nichts.*

Obwohl der Zugriff auf das Bankkonto inzwischen **dreieinhalb Jahre** her ist, passiert außer seltenen Zwischennachrichten *einfach nichts*.

Aus Andeutungen lässt sich entnehmen, dass sich die Stelle der Datenschutzbeauftragten gegenüber Polizei, LKA, Staatsanwaltschaft einfach nicht durchsetzen kann, dass sie einfach nicht antworten und deren Anfragen einfach ignorieren.

Eine Datenschutzkontrolle der Justiz findet in Berlin im Ergebnis überhaupt nicht statt.

Der Datenschutzbeauftragten mag man zwar die Tapferkeit zugute halten, es wenigstens zu versuchen. Aber die Berliner Justiz ist offenbar nicht bereit und nicht willens, sich irgendwie an irgendwelche Gesetze zu halten.

27 Die Abwesenheit des Datenschutzes in Baden-Württemberg

Der Datenschutz in Baden-Württemberg ist einfach zu beschreiben: Es gibt ihn nicht.

Obwohl etwa die Meldestelle REspect! – wie beschrieben – massiv gegen Datenschutzrecht verstößt und so gar nicht existieren dürfte (ungeachtet des Umstandes, dass sie rechtlich gesehen tatsächlich nicht existiert), kümmert sich die Stelle des Landesdatenschutzbeauftragten von Baden-Württemberg einfach um gar nichts. Manchmal erhält man gar keine Antwort. Und wenn man eine erhält, ist das auch kein spürbarer Vorteil gegenüber keine Antwort erhalten zu haben.

Etwa auf meine Eingabe, ob die Meldestelle REspect! über die nötige Beaufsichtigung nach Artikel 10 DSGVO verfügt, habe ich nie eine Antwort erhalten.

28 Die Ruchlosigkeit des Datenschutzes in Hessen

28.1 Der Landesdatenschutzbeauftragte

Der Landesdatenschutzbeauftragte ist Prof. Dr. Alexander Roßnagel, grünennaher Professor für Technik- und Umweltschutzrecht, im Jahr 2020 von der Regierung aus CDU und Grünen vorgeschlagen.

28.2 Die Weigerung, sich mit der Sache zu befassen

Der Sitz der Deutschen Bank ist Frankfurt am Main. Als Verantwortliche Stelle im Sinne des Datenschutzes ist sie für die Übermittlung der Kontodaten an das LKA Berlin verantwortlich, und der Vorgang fällt in die Zuständigkeit des Landesdatenschutzbeauftragten von Hessen.

Dort will man sich damit nicht befassen. Man hat die Sache zunächst mit einer kurzen Mail abgewimmelt, und seit ich dagegen vor dem Verwaltungsgericht klage, ist man der Meinung, das sei alles allein ein Berliner Problem, Hessen habe damit nichts zu tun.

Man betont, ein gutes Verhältnis zur Datenschutzabteilung der Deutschen Bank zu haben.

28.3 Die Datenschutzabteilung der Deutschen Bank

Sie ist effektiv komatös und tritt in keiner für mich ersichtlichen Weise in Erscheinung oder Aktion, denn sämtliche Datenschutzbelange werden nach außen rein pro forma von der Kundendienstabteilung abgewickelt.

Der Datenschutz der Deutschen Bank hat großes Glück, dass er so liebe- und verständnisvolle Juristen wie den Landesdatenschutzbeauftragten Hessens gefunden hat, denn fiel er im selben Zustand unter Ärzte, wäre er längst zur Organspende freigegeben worden.

Die Deutsche Bank erklärte – **nach nach Aktenlage mindestens zwei nachweislichen Telefonaten mit dem Landesdatenschutzbeauftragten** – dass Datenschutzrecht für sie nicht gelte, weil sie vom Datenschutz „entbunden“ sei.

Dazu behauptet die Deutsche Bank gegenüber dem Bundesverband deutscher Banken e.V.:

Grundsätzlich gilt: Sofern wir Auskunftsanfragen von Behörden im Rahmen eines Ermittlungsverfahrens erhalten, **sind wir gesetzlich dazu verpflichtet, dieser Aufforderung nachzukommen.** In diesen Fällen sind wir von Datenschutz und Bankgeheimnis entbunden.

Ein solches Gesetz gibt es nicht. Eine solche Verpflichtung auch nicht. Was aber der Bundesverband deutscher Banken und der hessische Landesbeauftragte für Datenschutz nicht wissen. Woher auch? Man unterrichtet sie ja nicht über Gesetze, die es nicht gibt. Es gibt kein Fachjournal über Gesetze, die es nicht gibt.

28.4 Das Verwaltungsgericht Wiesbaden

Hiergegen habe ich vor dem zuständigen Verwaltungsgericht Wiesbaden Klage erhoben.

Es wird dauern, denn das Verwaltungsgericht ist auf Jahre hinaus überlastet. Es ist nicht möglich, die Entscheidung des Landesdatenschutzbeauftragten anzufechten, bevor die Sache verjährt ist.

Außerdem, so ließ das Verwaltungsgericht wissen, seien sie gehandicapt, weil der Vorsitzende auf unabsehbare Zeit krank zu Bette liege und nicht anzusprechen sei. Das ist großes Pech, denn das ist wohl ausgerechnet der, der am Verwaltungsgericht Wiesbaden weiß, was ein Zeuge ist.

28.5 Die Position des Landesdatenschutzbeauftragten

Vor Gericht trägt der Landesdatenschutzbeauftragte vor, dass ihn das alles eigentlich gar nichts angehe. Ich würde rein zivilrechtliche Ansprüche verfolgen – Datenschutz sei eine Zivilrechtssache.

Außerdem vertritt er die Auffassung, dass die Bank der Polizei einfach blind vertrauen könne und müsse, und deshalb verpflichtet und berechtigt sei, alle Daten ungeprüft herauszugeben.

So 9.4.2024:

Richtig ist, dass der Beklagte für das LKA Berlin nicht die zuständige Datenschutzaufsichtsbehörde ist, sodass sich die Prüfung des Beklagten nur auf die Übermittlung der

Deutsche Bank

04082 Leipzig
08 305E 62E1 A9 C000 01EB
DV 03.24 0,85 Deutsche Post 

*00369016*0703*20454794*00000031*
An
Bundesverband deutscher Banken e.V.
- Schlichtungsstelle -
Postfach 04 03 07
10062 Berlin



 043#3



Deutsche Bank AG
Beschwerdemanagement
60633 Frankfurt am Main

Manuela Hans
Tel. +49(69)910-36230

Unsere Vorgangsnummer: 23-141629
(Bitte stets angeben)

11.03.2024

06.03.2024

Schlichtungsverfahren AZ 23-008197
Danisch, Hadmut J. Deutsche Bank AG

Sehr geehrte Damen und Herren,

zu obigem Schlichtungsverfahren nehmen wir wie folgt Stellung:

Die Kontoverbindung des Beschwerdeführers haben wir gemäß unseren Allgemeine Geschäftsbedingungen (AGB) Punkt 19.1 ohne Angabe von Gründen fristgerecht und unter Einhaltung einer angemessenen Postlaufzeit zum 14.06.2023 gekündigt. Genau wie unsere Kunden haben auch wir die Möglichkeit, eine Kundenverbindung ohne Begründung zu beenden.

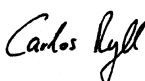
Ergänzend teilen wir mit, dass das betreffende Konto bereits seit 13. November 2023 geschlossen ist. Das Restguthaben wurde am 8. November 2023 gemäß Kundenauftrag vom 26. September 2023 an die dort genannte Kontoverbindung überwiesen.

Den vom Beschwerdeführer erhobenen Vorwurf, dass wir seine Kontodaten an unberechtigte Dritte offengelegt hätten, ist nicht zutreffend.

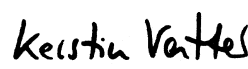
Grundsätzlich gilt: Sofern wir Auskunftsanfragen von Behörden im Rahmen eines Ermittlungsverfahrens erhalten, sind wir gesetzlich dazu verpflichtet, dieser Aufforderung nachzukommen. In diesen Fällen sind wir von Datenschutz und Bankgeheimnis entbunden.

Wir hoffen, dass wir mit unseren Ausführungen zur Klärung der Beschwerde beitragen können. Wir sehen weiterhin keine Möglichkeiten, weiterführende Auskünfte zu den in Rede stehenden Punkten zu erteilen und bitten Sie, die Beschwerde zurückzuweisen.

Mit freundlichen Grüßen



Carlos Ryll



Kerstin Vatter

Vorsitzender des Aufsichtsrats: Alexander R. Wynaendts; Vorstand: Christian Sewing (Vorsitzender), James von Moltke, Fabrizio Campelli, Bernd Leukert, Alexander von zur Mühlen, Claudio de Sarcia, Rebecca Short, Stefan Simon, Olivier Vigneron; Deutsche Bank Aktiengesellschaft mit Sitz in Frankfurt am Main; Amtsgericht Frankfurt am Main, HRB Nr. 30 000; Umsatzsteuer-Id.-Nr. DE114103378; www.db.com/de, www.deutsche-bank.de

1 / 2

Beleg 28.1: Auf der Entbindungsstation: Nach zwei Telefonaten mit dem hessischen Landesdatenschutzbeauftragten hält sich die Deutsche Bank für vom Datenschutz „entbunden“.

Kontodaten durch die Deutsche Bank erstreckte. Die in Rede stehende Übermittlung der personenbezogenen Daten durch die Deutsche Bank im Rahmen des Ermittlungsverfahren erwies sich aus datenschutzrechtlicher Sicht als rechtmäßig.

Die Pflicht der Deutschen Bank zur Beantwortung des Auskunftersuchens ergibt sich aus der staatsanwaltlichen Ermittlungsbefugnis in Verbindung mit § 163 Abs. 3 StPO. Die Rechtsgrundlage für die Übermittlung der angeforderten Kontodaten durch die Deutsche Bank stellt Art. 6 Abs. 1 UAbs. 1 Buchst. c DS-GVO i.V.m. § 163 Abs. 3 StPO dar.

Machen Sie sich klar, was hier abläuft: Der Hessische Landesdatenschutzbeauftragte redet – offenbar regelmäßig – den Banken ein, dass aus der Ermittlungsbefugnis und der Pflicht des Zeugen, zur Sache auszusagen, eine Verpflichtung zur Übermittlung von Kontodaten hervorgehe.

§ 163 Abs. 3 StPO:

Zeugen sind verpflichtet, auf Ladung vor Ermittlungspersonen der Staatsanwaltschaft zu erscheinen und zur Sache auszusagen, wenn der Ladung ein Auftrag der Staatsanwaltschaft zugrunde liegt. Soweit nichts anderes bestimmt ist, gelten die Vorschriften des Sechsten Abschnitts des Ersten Buches entsprechend. Die eidliche Vernehmung bleibt dem Gericht vorbehalten.

Machen Sie sich das unfassbare Ausmaß an Inkompetenz bewusst: Ein Landesbeauftragter für Datenschutz, der nicht weiß, dass die Übermittlung einer Datei mit personenbezogenen Daten besonderer Kategorien keine Zeugenaussage ist.

Ins Amt gesetzt von CDU und Grünen.

Und der soll in der Lage sein, als Aufsichtsbehörde über die IP-Adressspeicherung zu fungieren?

28.6 Wundersame Heilung: Asylbewerber

Es wäre allerdings voreilig, dem Landesdatenschutzbeauftragten von Hessen, Professor Roßnagel, Datenschutzdemenz zu unterstellen. Als Vorsitzendem der Datenschutzkonferenz fiel ihm nämlich, gleichzeitig, ebenfalls 2024, zur Frage, ob man Asylbewerbern Zahlkarten statt Geld geben könne, ganz plötzlich der Datenschutz wieder ein.

Als solcher hat er den Beschluss und die zugehörige Pressemitteilung der Datenschutzkonferenz *zum Einsatz von Bezahlkarten zur Leistungsgewährung nach dem Asylbewerberleistungsgesetz (AsylbLG)* mit Datum vom 19. und 23.8.2024 verantwortlich publiziert.

Darin betrachtet die Datenschutzkonferenz den Einsatz von Bezahlkarten für Asylbewerberleistungsempfängern als datenschutzrechtlich problematisch:

Durch diese Art der Leistungsgewährung sowie die avisierten weiteren Funktionsmöglichkeiten der Karte entstehen zwangsläufig datenschutzrechtlich relevante Verarbeitungsvorgänge der personenbezogenen Daten von Leistungsberechtigten. Damit wird in das Recht der Leistungsberechtigten auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 Grundgesetz (GG) in Verbindung mit Art. 1 Abs. 1 GG eingegriffen, welches im Lichte des Rechts auf den Schutz personenbezogener Daten nach Art. 8 Charta der Grundrechte der EU (GRCh) in Verbindung mit Art. 7 GRCh auszulegen ist. Dieses Recht gilt gleichermaßen für deutsche wie ausländische Staatsangehörige, die sich in der Bundesrepublik Deutschland aufhalten.

[...]

Eine eigenständige Einsichtnahme in den Guthabenstand von leistungsberechtigten Personen durch die Leistungsbehörden ist nach derzeitiger Rechtslage unzulässig. Ein solcher Abruf dieser Information ist eine Verarbeitung personenbezogener Daten, die eine Rechtsgrundlage benötigt. In Betracht käme hierfür einzig die o.g. datenschutzrechtliche Generalklausel nach dem jeweiligen Landesrecht. Deren Voraussetzung der Erforderlichkeit dieser Verarbeitung für die Gewährung der Leistungen nach dem AsylbLG ist jedoch nicht erfüllt.

Durch Einfügen des Wortes „Bezahlkarte“ in die §§ 2, 3 und 11 AsylbLG hat der Gesetzgeber zwar deutlich gemacht, dass die zuständigen Behörden Leistungen durch den Einsatz einer guthabenbasierenden Karte mit Debit-Funktion erbringen dürfen. Weder im Gesetzestext noch in der dazugehörigen Begründung findet sich jedoch ein Hinweis darauf, dass Leistungsbehörden Einsicht in den Guthabenstand nehmen dürfen.

[...]

Infolge der Nutzung der Bezahlkarte werden personenbezogene Daten der leistungsberechtigten Personen erhoben und gespeichert, die erheblichen Aufschluss über die private Lebensgestaltung geben können. Zugriffe durch Sicherheitsbehörden dürfen vor diesem Hintergrund nur nach den gesetzlichen Maßgaben der einschlägigen Sicherheitsgesetze, z.B. der Strafprozessordnung erfolgen, die auch für andere Personen und deren Bankaktivitäten gelten.

Geht es um Asylbewerber, tritt eine wundersame Heilung ein. Dann fällt ihm plötzlich ein, dass Zahlungsdaten personenbezogen sind und man da schon genau auf eine gesetzliche Grundlage achten müsse.

29 Die Verstrickung des Deutschen Bundesrats

Eine seltsame Koinzidenz fällt hier auf.

Ausgerechnet das Bundesland Hessen, das auf Länderebene und im Bundesrat der Treiber hinter der Neuauflage der Vorratsdatenspeicherung ist, ist dasselbe, das über seinen Datenschutzbeauftragten das Datenschutzrecht systematisch aushebelt und Banken einredet, dass sie auf Durchzug zu stellen, alles zu beantworten und gar nichts auf Rechtmäßigkeit zu prüfen hätten.

Nun ist der Landesdatenschutzbeauftragte Roßnagel sicherlich eine grüne Altlast, denn längst herrscht in Hessen eine Koalition aus CDU und SPD, ein Abbild der Bundesregierung.

Noch eine Koinzidenz: War nicht die SPD-Innenministerin Nancy Faeser, die alle Finanzströme ausspionieren und trocken legen wollte, die ihr nicht passten, auch aus Hessen? Zieht die ehemalige Bundesinnenministerin hier weiterhin ihre verfassungswidrigen Fäden, nunmehr aus Hessen, getarnt als Bundesrat?

Versucht man, Nancy Faesers mangels Rechtsgrundlage rechtswidriges Ansinnen, alle Kontendaten abfragen zu können, durch die Hintertür neu aufzubauen, indem man über die „Zeugenvernehmung“ ein Ersatzrecht bastelt und den Banken einredet, sie müssten darauf antworten ohne zu prüfen?

Passend zum Konstrukt, über die Meldestellen Strafermittlungsverfahren als Vorwand zu fingieren? Und betreibt nicht Hessen selbst eine solche Meldestelle?

Wer ist da bei Hessen und der Bundesregierung eigentlich Koch und wer ist Kellner?

Teil VI

Ergebnis

30 Ergebnis und Zusammenfassung

30.1 Tenor

Der betrachtete Gesetzentwurf ist **nicht zustimmungsfähig**.

Die Bundesrepublik Deutschland und ihre Legislative, Exekutive und Judikative sind derzeit und auf absehbare Zeit weder tatsächlich in der Lage, noch politisch willens, die vom EuGH in seiner Entscheidung vom 20.9.2022 aufgestellte Anforderung

„Diese Rechtsvorschriften müssen durch klare und präzise Regeln sicherstellen, dass bei der Speicherung der fraglichen Daten die für sie geltenden materiellen und prozeduralen Voraussetzungen eingehalten werden und dass die Betroffenen über wirksame Garantien zum Schutz vor Missbrauchsrisiken verfügen.“

zu erfüllen.

Der vorliegende Gesetzentwurf, seine Begründung und die Kontextäußerungen der Bundesregierung strotzen vor technischen Fehlern. Der Verfasser des Gesetzentwurfs ist erkennbar weit überfordert und entbehrt der nötigen Sachkunde. Die Herangehensweise ist ungeeignet, die Qualität unzureichend.

Der Gesetzentwurf und seine Begründung enthalten Bestandteile, die ich als Täuschungsversuch gegenüber Gerichten und der Öffentlichkeit, um bereits Verbotenes unter anderer Bezeichnung oder unter der Suggestion, etwas anderes als früher zu tun, an Rechtsprechung und Meinung vorbeizuschmuggeln, werte.

Dieses Gesetz kann und wird zur Verurteilung Unschuldiger führen und in großem Umfang missbräuchlich verwendet werden.

30.2 Einzelbegründungen

30.2.1 Inhaltlicher Schwindel

30.2.1.1 Angriff auf Meinungs- und Pressefreiheit

Nach außen wird vorgetragen und als Begründung vorgeschoben, eine IP-Adressspeicherung sei erforderlich, um schwerste Kriminalität zu bekämpfen. Man nutzt die Empörung über Terroranschläge (Abb. 18.1).

Das ist nicht glaubwürdig. Denn Schwermriminalität handelt nicht mehr von Einzeltätern (und wenn, hätten sie ja keine zu überwachende Kommunikation), sondern findet vernetzt und professionalisiert statt („crime as a service“). In diesen Netzen ist längst bekannt, dass einfache IP-Adressen rückverfolgbar sind, und wie man das umgeht. Und damit das auch so ist, fördert die Bundesregierung selbst einen Verlag, der noch rechtzeitig Anleitungen für Kriminelle herausgibt, wie man die IP-Adressspeicherung umgeht (Kapitel 14.6). Sie werden mit diesem Gesetz nur die ganz Dummen unter den Schwermkriminellen fangen können.

Dieses Gesetz ist eindeutig zur Verfolgung derer gebaut, die sich zum Zeitpunkt ihrer Nutzung einer IP-Adresse nicht bewusst sind, eine Straftat zu begehen, und deshalb keine Schutzmaßnahmen ergreifen. Und damit ist dieses Gesetz eindeutig darauf ausgelegt, die Gummi- und Überraschungsparagraphen §§ 130, 188 StGB anzuwenden. Wie der antragstellende Kanzler ja bereits sagte: *Er will wissen, wer sich äußert.*

Damit liegt auf der Hand, dass dieses Gesetz gegen die Meinungsfreiheit gerichtet ist – oder jedenfalls einen „chilling effect“ ausübt und der Einschüchterung dient.

30.2.1.2 Täuschung der Gerichte

Ich halte den vorliegenden Gesetzentwurf für einen Täuschungsversuch gegenüber den Gerichten, die darüber entscheiden werden.

Wie sich an mehreren Formulierungen und Fehlern zeigt, hat sich der Verfasser nicht mit technischen Grundlagen und dem befasst, was er da eigentlich machen will, sondern sich an der Kette bestehender Verbote von EuGH, BVerfG und BVerwG orientiert und daran vorbeiformuliert, und alte Begriffe durch neue ersetzt, um bei Gerichten den Eindruck zu erwecken, dass man sich an deren Entscheidungen halte und jetzt etwas deutlich anderes mache als zuvor.

Man verkauft hier nicht nur alten Wein in neuen Schläuchen, sondern hat einen gepanschten Wein, den das Gesundheitsamt bereits verboten hat, neu etikettiert, um diese naheliegende Metapher zu gebrauchen.

30.2.1.3 ETSI-Standard TS 102 657

Der vorliegende Gesetzentwurf suggeriert, technisch fortgeschritten, sicher und nach international etablierten und akzeptierten Standards arbeiten zu wollen, und beruft sich auf ETSI-Standard TS 102 657.

Dieser Standard ist eine Luftnummer und hält einer Nachprüfung nicht stand (Kapitel 11). Es entsteht der Eindruck, dass hier Halb- oder Dreiviertellaien den Auftrag erhalten haben, eine Standardisierungsarbeit vorzugaukeln, indem sie einfach nachahmen, was andere machen.

30.2.2 Allgemein mangelhafte Qualität

30.2.2.1 Zeitknappheit

Bereits die Zeitknappheit, mit der dieser Gesetzentwurf durchgeprügelt wird – obwohl noch durch die Sommerpause abgemildert – steht in keinem Verhältnis zur Schwere, Bedeutung und Komplexität des Inhaltes. Es entsteht der Eindruck, dass der Bundestag die Komplexität, Tiefe und Folgeschwere dieses Entwurfs weit unterschätzt – oder eine genaue Betrachtung eher vermeiden will.

Eine Gesetzgebung oder auch nur eine Stellungnahme in der angemessenen Tiefe und Qualität sind so nicht möglich. Die vorliegende Stellungnahme wurde unter höchstem Zeitdruck geschrieben, um sie noch vor der Anhörung abgeben zu können.

So erzeugt man nicht die Qualität, die von einem Gesetzgeber zu erwarten und als Grundlage vertretbarer Rechtsprechung erforderlich ist.

30.2.2.2 Mangelnde Normierungsdichte

Dieser Gesetzentwurf ist weit von der nötigen Normierungsdichte entfernt.

Zu vieles bleibt offen, undefiniert, unentschieden, unverständlich. Damit verlagert man die Aufgaben des Gesetzgebers auf die – ohnehin schwer überlasteten – Gerichte, in denen dann IT-Laien mit Zeitnot sich irgendetwas dazu überlegen sollen, wie man das verstehen und wie man damit umgehen könne.

30.2.2.3 Schlampig, sprachlich schlecht, unklar, unverständlich

Dieser Gesetzentwurf ist schon in seiner Ausarbeitung schlampig, sprachlich miserabel, in den Formulierungen unklar, missverständlich oder widersprüchlich.

Dieser Text ist ein verwirrendes, unlesbares Gestrüpp aus Querverweisen und Bezügen, das den Eindruck erweckt, dass da viele Köche ihren Senf dazugegeben haben, bis der Brei verdorben war.

Das ist schon normierungsuntauglich. Wenn man sieht, welche Probleme Berufsrichter schon mit Verständnis und Anwendung weitaus einfacherer Vorschriften der StPO mit rein juristischen Inhalten haben – wie sollen die denn dieses Ding verstehen können, das wirkt, wie eine Aufgabe aus einem Rätselbuch?

Peter Struck wird der Ausspruch nachgesagt, dass „kein Gesetz den Bundestag so verlasse, wie es hereingekommen sei“. Angaben dazu, ob Gesetze dadurch besser oder schlechter werden, konnte ich nicht finden.

30.2.2.4 Politischer Notrufmissbrauch

Ich halte diesen Gesetzentwurf, genauer gesagt, dessen Begründung, für eine Art politischen Notrufmissbrauchs.

Man beruft sich auf Nöte um Kinderpornographie, Schwere Kriminalität, den Anschlag in Magdeburg, um die Sache erst groß aufzuhängen und die Empörung zu surfen, und damit dann hinterher Äußerungen in den Social Media zu verfolgen, weil der Kanzler nicht kommod ruht und an Morbus Faeser leidet (wie noch kein Kanzler vor ihm).

Es ist, als ob man die Feuerwehr ruft, weil jemand schlecht singt.

30.2.2.5 Stellungnahme von 2023 ignoriert

Ich frage mich beim Lesen dieses Gesetzentwurfs, wofür ich mir 2023 eigentlich die große (und unbezahlte) Mühe als Bürgerpflicht gemacht habe, um Ihnen aus der Sicht eines ehemaligen Leiters einer Vorratsdatenspeicherung die Probleme und Anforderungen darzulegen, wenn Sie das gar nicht verarbeiten und zur Kenntnis nehmen.

Wozu veranstalten Sie diese Anhörungen überhaupt, wenn die Äußerungen so unbeachtet bleiben?

30.2.2.6 Quantität, Kosten, ausufernder Zugriff

Dem Gesetzentwurf fehlt jedes quantitative Maß.

Die Dimension ist gewaltig: **Nach Schätzungen des europäischen Providerverbands Euro-ISPA werden rund 400.000 Serviceprovider in ganz Europa mit mehr als 10.000 Strafverfolgungsbehörden vernetzt.**

Allein in Deutschland sind laut IHK Nürnberg „hunderttausende Unternehmen“ betroffen – darunter nicht nur Telekommunikationsanbieter, sondern auch Cloud-Dienste, Online-Shops, Foren und Gaming-Plattformen.

Besonders problematisch: Bei grenzüberschreitenden Anfragen gilt das Recht des anfragenden Staates. Wenn spanische Ermittler bei einem deutschen Provider Daten anfordern, müssen diese nach spanischem Recht herausgegeben werden. Kritiker sehen darin eine Einschränkung des deutschen Datenschutzniveaus.

Unternehmen müssen auf Anfragen ausländischer Behörden innerhalb von zehn Tagen – in Notfällen sogar binnen acht Stunden – Nutzerdaten herausgeben. Kritiker sehen hier ein erhöhtes Missbrauchsrisiko: Bei Kompromittierung eines Behörden-Accounts könnten Unbefugte theoretisch auf sensible Nutzerdaten zugreifen.

Zwar existieren rechtliche und organisatorische Sicherheitsvorgaben, doch aus Sicht des eco-Verbands sind diese angesichts der Systemgröße unzureichend.

Das kommt im Gesetzentwurf überhaupt nicht vor. Im Gegenteil suggerieren die Kostenangaben, dass es hier nur um eine Kleinigkeit und nicht um ein Überwachungsmonstrum geht.

Multipliziert man die hohen Kosten für jeden Provider mit der Zahl der Provider, kommt man in Bereiche, die volkswirtschaftliche Auswirkungen haben könnten.

Haben Sie schon einmal darüber nachgedacht, dass diese Adressspeicherung schlicht und einfach viel zu teuer sein könnte?

Wenn ja: Warum steht davon nichts im Entwurf? Wenn nein: Warum nicht?

30.2.2.7 Methode „Wünsch Dir was“ / Case Law

Der vorliegende Gesetzentwurf ist nicht konstruktiv, sondern petitiv. Sie bauen keine IP-Adressspeicherung, sondern Sie wünschen sich ein Ergebnis von Providern und Rechtsprechung, die das dann irgendwie erfüllen sollen.

Im Prinzip haben wir hier eine Petition der Legislative an die Exekutive und Judikative.

In den USA gibt es diese Vorgehensweise, in der das Gesetz nur den Rahmen vorgibt und das Case Law ihn ausfüllt, weil Staatsanwälte und Richter in den USA gewählt werden und damit demokratisch legitimiert sind.

In Deutschland geht das nicht.

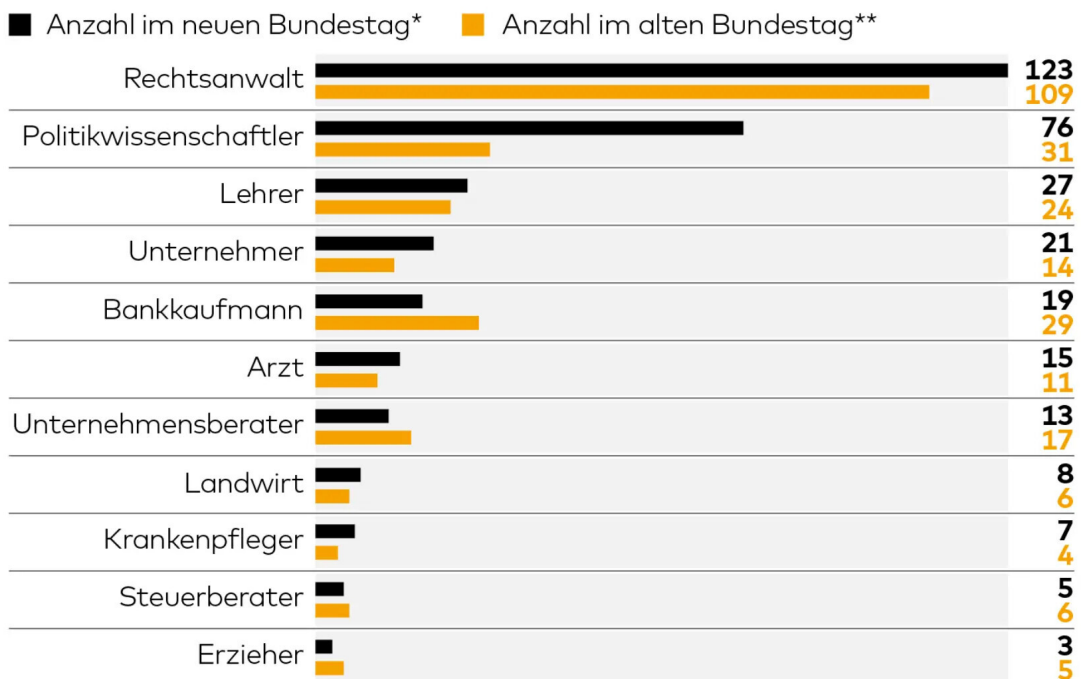
30.2.3 Grenzen von Laienregierung und Laienparlament überschritten

30.2.3.1 Zusammensetzung und Qualifikation

Man sieht hier deutlich, dass die Grenzen einer Laienregierung und eines Laienparlaments überschritten sind (Abbildung ??).

Beruflicher Hintergrund der neuen Abgeordneten

Berufe und Ausbildungen laut bundestag.de, Auswahl



*21. Legislaturperiode ab 2025 mit 630 Abgeordneten

**20. Legislaturperiode 2021-2025 mit 735 Abgeordneten

Quelle: bundestag.de

welt

Abbildung 30.1: Berufe der Abgeordneten (Quelle: Die WELT, **Mehr als doppelt so viele Politikwissenschaftler im neuen Bundestag**, 9.3.2025)

Was wollen Sie eigentlich mit so vielen Rechtsanwälten und Politikwissenschaftlern? Und wozu braucht man 123 Rechtsanwälte und 76 Politikwissenschaftler? Wenn das Ergebnis dann so aussieht wie dieser Gesetzentwurf?

Warum gibt es im Bundestag keine Informatiker, obwohl IT als eines der wichtigsten wirtschaftlichen und gesellschaftlichen Themen gilt?

Warum sind im Parlament geschätzte 87 Geschlechter repräsentiert, und alle Arten an einer Berufsausbildung zu scheitern vertreten, aber nicht die relevanten Berufe? Quality is a myth?

Wer von Ihnen versteht, was ich in Teil I beschrieben habe, wenn es dabei um Themen geht, das schon unter Informatikern nur für Fortgeschrittene ist?

Wie konnten die Grünen zu der Auffassung gelangen, dass auch Analphabeten im Bundestag arbeiten könnten, um dann solche Gesetzentwürfen zu schreiben?

Es genügt nicht, nur gewählt zu sein.

Ich möchte anregen, von Geschlechterquoten auf Sachkundequoten umzusteigen, damit die benötigten Fähigkeiten und nicht die 87 Geschlechter vertreten sind.

30.2.3.2 Kosten

Habe ich das richtig verstanden?

Dieser Bundestag kostet den Steuerzahler 1,25 Milliarden Euro *pro Jahr*, und was dabei herauskommt, ist derartig laienhaft und lausig wie dieser Gesetzentwurf?

Eine KI könnte das besser, schneller, billiger.

30.2.4 Das Problem evidenten Elends der Jurisprudenz

30.2.4.1 Massive Verwahrlosung der Justiz

Wir haben in Deutschland eine massive intellektuelle und charakterliche Verwahrlosung der Justiz zu beobachten und zu beklagen.

Schon die allgemeinen gesellschaftlichen Fehlentwicklungen wie mangelnde Lesefähigkeit, auf Twitter reduzierte Aufmerksamkeitsspannen, Bildungsverachtung, Dekadenz der Universitäten, Verclownung der Geisteswissenschaften, schlagen selbstverständlich auch auf die juristischen Berufswege voll durch.

Dazu kommt massiver marxistisch-feministisch-ideologischer Druck, Stichwort „Quality is a Myth“ und die Auffassung, dass geschriebenes Gesetz nicht mehr zu beachten sei, weil von weißen Männern für weiße Männer gemacht und deshalb sexistisch, rassistisch, frauenausgrenzend, und dass sich Richter stattdessen am persönlichen Gerechtigkeitsgefühl und ihrer Moral orientieren sollen.

Man merkt dies schon daran, dass das Gerede immer leerer wird, alles nur noch Meinungsjustiz ist. Alles Erwünschte ist Grundrecht, alles Unerwünschte gleich verfassungsfeindlich. Und alles wird auf „Menschenwürde“ reduziert, weil Artikel 1 noch in einen Tweet passt und man schon mit dem dritten Artikel des Grundgesetzes inhaltlich überfordert wäre, vorgeführt in Perfektion und Folge bei jedem Lanz-Besuch der selbstidentifizierenden Trans-Verfassungskoryphäe, gefangen im Körper eines Talkshowclochards, Frauke Brosius-Gersdorf, von derselben grundrechtsverachten-

den SPD für verfassungsgerichts befähigt gehalten, deren Justizministerin diesen Gesetzentwurf vorlegt, für den man dann Rechtsschutz von eben diesem Bundesverfassungsgericht bekommen solle, vor dem jeder sein Recht einklagen könne, wie uns das ZDF uns zu dessen 75-Jährigem Bestehen gerade öffentlich-rechtlich zusäuselte? Während der real existierende Parteienrat in den roten Kitteln des Bundesverfassungsgerichts kommentarlos ablehnt (25.5), was die Spionageambitionen von CDU und SPD gefährden könnte, wie den heimlichen Zugriff auf Journalistenkonten nach Art der Nancy Faeser?

Wo sind also diese vom EuGH geforderten „wirksamen Garantien“ gegen Missbrauch? In Karlsruhe sind sie jedenfalls nicht, und bei Lanz auch nicht.

Dazu kommt eine enorme Überlastung der Justiz, und die zusätzliche Belastung durch Sie, den Gesetzgeber, die die Gerichte mit verworrenen und verwirrenden Gesetzen wie diesem überschüttet, die ein Richter gar nicht verstehen und befolgen kann, dessen Löcher er aber ausspachteln soll.

Die Folge ist ein immer weiter in die Meinungs- und Willkürentscheidungen driftender dysfunktionaler Justizapparat, der nur noch danach entscheidet, was ihm am wenigsten Arbeit macht, am schnellsten zu „entscheiden“ ist, und zur Garnierung noch ein paar Paragraphen und Aktenzeichen aus dem Kommentar darüber streut, die er in 20 Sekunden finden konnte. Denn mehr, als im Handkommentar nach Zitierstücken zu suchen, können, machen *und wollen* die meisten Juristen nicht.

Der vorliegende Gesetzentwurf betrifft Themen und Problemstellung, die selbst unter Informatikern, dezent formuliert, „für Fortgeschrittene“ sind und einige Einarbeitung brauchen, weil das keine Alltagsthemen sind.

Wie sollen denn nach Ihrer Vorstellung Juristen als IT-Laien Frage- und Problemstellungen bearbeiten und lösen können, die schon für Informatiker was zu knabbern, al dente sind?

Es ist für mich auch unter Aufbietung selbst schmutziger Phantasien nicht ersichtlich, wie dieses Gesetz zu einer rechtsstaatlich akzeptablen Anwendung und Rechtsprechung führen können sollte.

Vergleichen Sie die Zeit, die ich als Informatiker mit Ausbildung, Berufserfahrung und Vorkenntnissen für diese Stellungnahme brauchte, mit der Zeit, die einem Richter als Laien zur Urteilsfindung bleibt. Dann wissen Sie, was dieses Gesetz wert ist.

Es wird deshalb nicht nur Willkür- und Verzweiflungsrechtsprechung geben – sie wird damit geradezu erzwungen.

30.2.4.2 Miserable Pseudoausbildung

Wie ein roter Faden zieht sich durch diese Stellungnahme, dass Staatsanwälte und Richter schon an Grundlagen der Strafprozessordnung versagen, sie überhaupt nicht

mehr anwenden, nur noch machen, was sie wollen, und bei Widerspruch einfach „irgendwas mit Paragraphen schwafeln“. Wird schon keiner so genau hinschauen.

Dieser Staat attestiert Leuten, drei Richtern einer Strafkammer, die nicht einmal die Grundlagen der StPO beherrschen, die – vgl. Kapitel 22 und 28 – **nicht einmal wissen, was ein Zeuge ist, eines der ältesten und einfachsten Ermittlungs- und Beweismittel, ein urjuristisches Ding** nicht kennen, die Befähigung zum Richteramt und gibt ihnen die Macht, Menschen ihr Geld wegzunehmen oder sie für den Rest des Lebens in ein Gefängnis einzusperren.

Die deutsche juristische Ausbildung, auf die man sich so viel einbildet, ist nicht nur nach meiner Ansicht wert- und inhaltslos, sondern auch nach Auffassung vieler Juristen.

Im Endeffekt dient die deutsche Juristenausbildung nicht der Ausbildung zum Juristen, sondern der Ausbildung einer elitären Kastenwesens, indem man Leute dazu bringt, sich für Juristen zu halten, Mitglied einer besonders privilegierten und befähigten Kaste zu sein, um sie in die mentale Konditionierung zu versetzen, ohne Sachkunde und im Handstreich bereitwillig Urteile am Fließband zu fällen.

Und dann verwundert es auch nicht, wenn Genderistinnen in der Rechtssoziologie zu dem Ergebnis kommen, dies sei alles nur „soziales Konstrukt“, alles nur Theater, „Quality is a Myth“. Weil die juristische Ausbildung genau das letztlich nur ist.

Wie anders könnte man es erklären, dass die Regierung hier einen Gesetzentwurf hinwerfen will, dessen Verständnis und Auslegung so viel technische Sachkunde erfordern, dass es völlig unmöglich ist, dass Richter als Juristen ihn verstehen und dies leisten können? Anders, als dass man sowieso der Auffassung ist, dass es bei Juristen nicht auf Sachkunden und Können ankommt, sondern irgendwie irgendwas zu entscheiden und dazu ein paar Paragraphen und Kommentarstellen zu werfen, und gut is’?

Wer einen solchen Gesetzentwurf vorlegt, der geht selbst erst gar nicht davon aus, der erwartet gar nicht, dass Richter ihn verstehen und befolgen können (oder wollen). Es geht nur noch darum, allen anderen vorzutäuschen, dass das etwas mit einem Recht zu tun habe, was eben leider nur Juristen verstehen.

30.2.4.3 Der „Freien Beweiswürdigung“ zum Fraß vorgeworfen

Perfektes Ansatzstück für die Laienanwendung unverständlicher Gesetze ist die „Freie Beweiswürdigung“.

Ein Gericht muss gar nicht nachprüfen, ob das so stimmen kann oder muss. Man wird eine Providerauskunft, in der irgendeine IP-Adresse mit irgendeiner Uhrzeit steht, von der keiner weiß, wie sie zustandekam oder was das bedeutet, zeitsparend, intellektuell bequem und zielführend „im Rahmen der freien Beweiswürdigung“ zum Beweis

erklären, mit der man schon immer jeglichen Mist zum „Beweis“ erhoben hat.

Nachprüfung, Gegenbeweis, Einrede nicht möglich.

Und welcher Staatsanwalt, welcher Polizist soll in der Lage sein, Fehlerquellen zu erkennen und auszuschließen? 2009 war ich umfangreich damit beschäftigt, Polizisten und teils auch Staatsanwälten telefonische Anfängereinführungen zu geben, worum es überhaupt geht und was man anfragen kann. Und die sollen Fehlerquellen im TCP-Timing eines Unix-Kernels bemerken können? Wenn nicht einmal die Bundesregierung mit beliebig viel Zeit, Geld und Personal versteht, was sie da macht, wie soll es dann das arme Polizistchen ohne Geld und Mittel können, dem man mancherorts nicht einmal ein Polizeiauto mit laufendem TÜV und vollem Tank hinstellen kann?

Dieser Gesetzentwurf wird unausweichlich zur Verurteilung Unschuldiger führen. Ermittlungs- und Polizeiarbeit werden an Provider und damit in das Privatrecht ausgelagert, und die Justiz wird diese als Beweise einfach übernehmen.

30.2.4.4 Kein rechtliches Gehör

Wo wollen Sie eigentlich Rechtsanwälte finden, die in der Lage sind, Beschuldigte gegen die Vielzahl von Fehlerquellen in der IT adäquat zu verteidigen?

30.2.5 Missbrauch

30.2.5.1 Faeser/Haldenwang

Deren Ansagen und Ankündigungen, was sie tun wollten, waren anders als durch Missbrauch gar nicht umzusetzen, weil ihnen die Rechtsgrundlagen fehlten (Kapitel [22](#)).

Es besteht kein Grund zur Annahme, dass das jetzt anders ist.

30.2.5.2 Grüne Missbrauchsstraße

Der Missbrauch polizeilicher Befugnisse zu politischen Zwecken ist nicht mehr zu befürchten, er ist längst da, wie auch in Kapitel [22](#) dargestellt.

1. Wenn man bemerkt, dass der Lebenslaufe einer **Grünen** nicht stimmt,
2. erstattet die **grüne** „Meldestelle RESpect!“ Strafanzeige nach § 188 StGB,
3. weil man eine andere **Grüne** beleidigt haben sollte, indem man deren eigene Wahlkampfthemen aufgriff,



**Benedikt Lux, B'90/Grüne
Innenpolitischer Sprecher**

**„Wir haben die gesamte Führung
fast aller Berliner Sicherheitsbehörden
ausgetauscht und dort ziemlich gute
Leute reingebracht.
Bei der Feuerwehr, der Polizei,
der Generalstaatsanwaltschaft und
auch beim Verfassungsschutz.
Ich hoffe sehr, dass sich das in
Zukunft bemerkbar macht.“**

müsse alles auf Durchzug schalten und Anfragen der Polizei zwingend und völlig ungeprüft beantworten.

Mir ist das entschieden zu grün, um da noch zusätzliche Befugnisse ohne jegliche Missbrauchskontrolle reinzuwerfen.

30.2.5.3 Korrupte Berliner Polizei

Wie in Teil IV ausführlich beschrieben, ist insbesondere die Berliner Polizei längst mit der organisierten Kriminalität – Clans, Linksextremismus – verwoben und missbraucht polizeiliche Ermittlungsmethoden in deren Auftrag und für deren Zwecke.

Eine Missbrauchskontrolle fehlt in diesem Gesetzentwurf völlig.

30.2.6 Technik

30.2.6.1 Der Fundamentalfehler

Das Internet hat

- nach seinem Zeitpunkt des Entstehens
- nach seiner Spezifikation
- nach seiner Konstruktion
- nach seiner technischen Umsetzung

keinerlei – insbesondere keine zugesicherten – Sicherheitseigenschaften, denn anders könnte man eine solche Maschine dieser Größe und dieser Geschwindigkeit nicht bauen und nicht betreiben.

Es gehört zu den schwersten Fehlern, die man in der IT und den anderen Ingenieurwissenschaften machen kann, eine Eigenschaft anzunehmen und darauf zu vertrauen, die nicht spezifiziert und konstruiert ist.

Man kann ein sicheres System durch Ignoranz unsicher machen, das ist möglich. Aber man kann nicht ein von vornherein unsicheres System zu einem sicheren hochignorieren.

30.2.6.2 Technisch bereits veraltet

Der Gesetzentwurf ist erkennbar an IPv4 und CGNAT ausgerichtet – freilich ebenso erkennbar, ohne diese verstanden zu haben.

Wie oben in Abschnitt 2.3 erläutert, wäre der Gesetzentwurf bald schon wieder technisch überholt, wenn nicht bereits jetzt.

Technisch bewegt sich der Gesetzentwurf ungefähr auf dem technischen Stand des Jahres 2010, wie in Kapitel 2 erläutert wurde.

Es macht den Eindruck, als wären die Verfasser nach der Untersagung der Vorratsdatenspeicherung durch das Bundesverfassungsgericht am 2.3.2010 inhaltlich stehen geblieben und hätten sich damit nicht mehr befasst, und wollten nun zur Fortführung einfach auf dem Stand vom März 2010 weitermachen.

16 Jahre entsprechen im Internet ungefähr 4 Ewigkeiten.

30.2.6.3 Volatilität zu hoch

Im Nachgang zu meiner Stellungnahme vom 9. Oktober 2023 hatte ich mir für Rückfragen Hersteller-Webseiten notiert, die CGNAT-Probleme erläutern und die ich aufgrund der kurzen Frist für die Stellungnahme nicht mehr hatte aufnehmen können.

Diese habe ich nun in in Kapitel 2 nachgereicht, dabei aber festgestellt, dass sich die Seiten und ihre Aussagen gegenüber dem Stand von 2024 schon erheblich verändert haben.

Provider-Technik, insbesondere CGNAT, ist in einem ständigen Fluss und in ständiger Veränderung, auch weil noch in der Entwicklung.

Dabei ist zu berücksichtigen, dass CGNAT generell nicht als akzeptierte Technik, sondern nur als Krücke, als vorübergehendes Hilfsmittel für die Transition von IPv4 mit Adressknappheit zu IPv6 betrachtet wird.

Wie volatil das Thema ist, zeigt sich schon allein daran, dass die Technik seit der Stellungnahme vom 9. Oktober 2023 die Bezeichnungen

- NAT44 (NAT 4->4)
- NAT444 (NAT 4->4->4 in Abgrenzung zu NAT44)
- CGNAT (Carrier Grade NAT)
- LSNAT (Large Scale NAT)

durchlaufen hat.

31 Verfahrensrügen

31.1 Ungenügende Bearbeitungszeit

Die für eine angemessene Bearbeitung dieser Sache zur Verfügung stehende Zeit war viel zu kurz bemessen. Man kann so weder die nötige Tiefe, noch die nötige Qualität erreichen.

Wenn selbst mir als jemandem, der

- Informatiker ist,
- bereits über Berufserfahrung in der Vorratsdatenspeicherung verfügt,
- sich zufällig gerade fast 100% seiner Zeit dafür freinehmen konnte,

die Zeit viel zu knapp ist, wie sollen dann Fachfremde, Laien mit diesem Thema ernstlich zurande kommen können?

Dies alles erweckt bei mir den Eindruck, dass der Bundestag die Komplexität und das Gewicht dieses Antrags weit unterschätzt.

31.2 Gesetzgebungsverfahren ungeeignet

Ich halte schon die Vorgehensweise per se, einen solchen Gesetzentwurf von Laien schreiben zu lassen, und ganz zum Schluss mal draufschauen zu lassen, wen die Fraktionen gerade vorschlagen, für völlig ungeeignet. Das Ergebnis ist richtig schlecht.

Ich hatte Bundestag und Bundesregierung bereits 1997 zum Kryptoverbot, 2009 zur Kinderpornosperrung und 2023 bei der ersten Anhörung deutlich gesagt, dass das in IT-Themen so nicht funktioniert, dass Sie bereits vor dem ersten Entwurf innerhalb der Fraktionen professionelle Hilfe und Sachkunde benötigen.

In der Stellungnahme von 2023 hatte ich Ihnen bereits einen Katalog von Erkenntnissen aus der Praxis vorgelegt, sehe aber nicht, dass man das irgendwie beachtet habe.

Wenn der Regierung und den Regierungsfractionen aktenkundig und nachweislich eine Darstellung der praktischen Probleme vorliegt, und sie diese völlig übergeht, auch

in drei Jahren nicht in der Lage ist, ihr Gesetzvorhaben daran auszurichten, ist das eine Mischung aus Inkompetenz und Ignoranz.

31.3 Darstellungsform mangelhaft

Schon die reine Darstellung dieses Gesetzentwurfes ist eine Zumutung.

- Es gibt kein Inhaltsverzeichnis.
- Es gibt trotz einer unendlichen Flut von Querverweisen keine Hyper- und keine Dokumentlinks.
- die einzelnen Paragraphen sind nicht auf separaten Seiten, damit man sie trennen und leicht finden kann. Das ist einfach alles sehr unübersichtlich untereinander gekleistert.
- Die Begründung ist wischi waschi und blabla, letztlich nur eine Nacherzählung, was in den Paragraphen steht, als müsste man die nochmal vorlesen.

Eine „Begründung“ im Wortsinn ist das nicht. Man merkt deutlich, dass ja jemand einfach die Paragraphennummern wiederholt und zu allem pro forma etwas Blabla einfüllt.

- Wichtige Teile wie Abwägungen Verhältnismäßigkeit, angestellte Erwägungen, Gefahren fehlen.
- Die Darstellung ist sehr unübersichtlich: Manchmal steht da nur „Zu Absatz 4“ und dann man muss mehrere Seiten zurückblättern um zu erkennen, auf welchen Paragraphen sich der Text bezieht, und wiederum suchen, um den Paragraphen zu finden.

Das ist nicht gemacht, um gelesen, geprüft und bearbeitet zu werden.

Dieser ganze Gesetzentwurf schreit „Lies mich nicht! Fass mich nicht an!“.

In der IT wurden Texte schon aus weit geringerem Anlass weggeworfen und neu geschrieben.

32 Ausblick und weiteres Vorgehen

32.1 Europäischer Gerichtshof

Sollte dieser Gesetzentwurf in Kraft treten, wird es zweifellos erneut Klagen bzw. Vorlagen beim Europäischen Gerichtshof geben.

Es wird nicht ohne Wirkung bleiben, dass die Bundesregierung sich nachweislich und – spätestens hiermit – auch wissentlich über die Rechtsprechung und die Anforderungen des EuGH hinwegsetzt und ein ebenso fehlerhaftes wie gefährliches, schlampig erstelltes Gesetz vorlegt, das Missbrauch nicht nur fördert, sondern geradezu wie dafür gemacht erscheint.

32.2 USA

32.2.1 Handelsrecht

Datenschutz ist das große Argument Deutschlands und vor allem der EU im Handelswettbewerb mit den USA. Immer wieder kommt es zu Ablehnungen von Bewerbungen in Ausschreibungen oder sogar Geldstrafen durch die EU.

Hier wird es für die USA beachtlich sein, dass dieser „Datenschutz“ in der Realität gar nicht existiert und nur eine Attrappe ist, die als Handelshemmnis aufgestellt wurde. Wie man – insbesondere an Hessen und Baden-Württemberg – überdeutlich sieht, gibt es Datenschutz in der Realität gar nicht, und die Landesdatenschutzbeauftragten sind nicht nur nutzlos, sondern kontraproduktiv, weil sie den Datenschutz aus politischen Gründen torpedieren und aushebeln.

32.2.2 US State Department

Ein zentraler Akteur der deutschen Zensursuppe, zu der ich auch diesen Gesetzesentwurf rechnen muss, sind Organisationen wie die „Meldestelle RESpect!“ und „HateAid“.

Das US State Department hat – aus gutem Grunde – bereits Sanktionen gegen die HateAid-Chefinnen Ballon und von Hodenberg **verhängt**. Auch der amerikanische Kongress beschäftigt sich damit (vgl. **Bericht** und **Pressemitteilung**).

Deutschland selbst ist nicht nur nicht mehr in der Lage, sondern auch nicht mehr willens, die epidemieartig wuchernde Zensur in den Griff zu kriegen und zu begrenzen, Grundrechte wie die Meinungsfreiheit zu schützen.

Hier müssen weitere, stärkere Sanktionen bewirkt und diese ausgedehnt werden, insbesondere gegen die Förderer und Finanziere von Organisationen wie HateAid, wie etwa die Milliardärsfamilie Reimann mit ihrer Alfred Landecker Foundation.

Das muss richtig von außen krachen.

32.2.3 US-Börsenaufsicht

Was wir hier sehen, ist eine Datenschutzkatastrophe: Ein Unternehmen wie die Deutsche Bank stellt nicht nur alle Fenster auf Durchzug, damit die Regierung – heimlich und rechtswidrig – alle Kritiker erfassen und durchleuchten kann, sondern das Land Hessen protegiert und fördert diese Praxis auch noch, und treibt gleichzeitig die IP-Adressspeicherung voran.

Die Deutsche Bank ist in den USA tätig, und ihre Aktien werden an US-Börsen gehandelt.

Damit unterliegt die Deutsche Bank auch der US Börsenaufsicht.

Wenn hier nun nicht nur Regierungskritiker in großem Umfang ausspioniert werden, sondern auch noch Konten durch anonyme Unbefugte – möglicherweise Hacker, Geheimdienstagenten, Parteimitglieder usw. – als gekündigt in der Datenbank eingetragen werden, **und die Deutsche Bank selbst, nicht einmal ihre Datenschutzabteilung, sagen kann, wer dieses Konto wie und warum gekündigt habe, und sie das nicht einmal stört, jegliche Reaktionen darauf ausbleiben, es nicht als Datenschutz- und IT-Sicherheitsvorfall behandelt wird**, dann liegt eine erhebliche Verletzung etwa des Sarbanes-Oxley Acts vor.

The Sarbanes-Oxley Act (SOX) is a 2002 U.S. federal law designed to protect investors and the public from corporate accounting fraud. It establishes strict standards for financial reporting, mandates that executives personally certify financial accuracy, **and imposes harsh penalties for destroying or falsifying records.**

Und die US-Behörden sind bei solchen Strafen nicht zimperlich. Was die EU bei ihren Datenschutzstrafen gegen US-Unternehmen ja auch nicht ist.

Freuen wir uns also auf unterhaltsame Nachrichten.

33 Persönliche Anmerkung

Nach meiner Stellungnahme für den Bundestag vom 9. Oktober 2023 und kurz nachdem mich die Bundestagsfraktion der AfD aufgrund meiner Sachkunde für den DSC-Beirat vorgeschlagen hatte, kam es zu einem Vorfall.

Eine Redakteurin der Stuttgarter „Kontext Wochenzeitung“, eines mir bis dahin unbekannten und anscheinend nur politisch und durch Spenden betriebenen Schein-Blattes ohne realen Geschäftsbetrieb, wohl regelmäßig vertreten durch einen den Grünen Baden-Württemberg sehr nahestehenden Rechtsanwalt, kontaktierte mich unter dem Vorwand, ein Interview zur damaligen Stellungnahme mit mir führen zu wollen.

Es stellte sich dabei schnell heraus,

- dass sie völlig fachfremd war und das schon das Thema überhaupt nicht verstand,
- dass sie mich überhaupt nicht kannte,
- dass sie mein Blog überhaupt nicht kannte,
- dass sie überhaupt nichts über mich wusste, wer ich bin, was ich mache, und offenkundig keinerlei beruflichen Bezug zu mir hatte,
- sie sich mit solchen Themen sonst überhaupt nicht befasst,
- es überhaupt nicht nachvollziehbar ist, wie sie – Kunstgeschichte studiert – überhaupt dazu kommt, selektiv den Lebenslauf in einem Sachverständigengutachten über Vorratsdatenspeicherung angreifen zu wollen,
- und dringend – und das unter hohem Zeitdruck zur Veröffentlichung und ohne erkennbare oder dargelegte Motivation oder sachliche Grundlage, ohne irgendeinen Grund und aus dem Nichts heraus – darauf aus war, meine in der damaligen Stellungnahme dargelegte Sachkunde (hier gleichlautend Unterkapitel [1.6](#)) als frei erfunden hinzustellen und mich als Hochstapler zu entlarven.

Es war dabei überdeutlich, dass es sich dabei um eine Auftragsarbeit handelte, weil sie selbst nicht wusste, wie sie überhaupt darauf kam, dass an meiner Darstellung irgendetwas nicht stimmen sollte oder könnte, oder wie sie überhaupt dazu kam, sich mit meiner Person oder Stellungnahme zu befassen. Oder wie sie, ohne den Rest der Stellungnahme zu kennen, isoliert auf diese rein formale Nebenangabe gekommen ist, statt sich besser um den Inhalt zu kümmern.

Gleichwohl äußerte sie sich in einer Weise und verfügte über Informationen und Bildmaterial, die auf Insiderwissen aus der damaligen Ausschusssitzung hindeuten.

Es entstand der Eindruck, dass das eine beauftragte Retourkutsche für die Aufdeckung Annalena Baerbocks Lebenslauffrisierungen (vgl. Kapitel 22) werden sollte. Erstaunlich dabei war, dass sie nicht den geringsten Ansatzpunkt für eine Fälschung hatte, sondern es einfach als natürlich und selbstverständlich ansah, dass ein solcher Erfahrungsschatz gefälscht und erfunden sein müsse.

Offenbar geht ein grünennahes Milieu hier von seinen eigenen Verhältnissen aus und unterstellt unzulässig, dass alle anderen sich genau wie sie verhalten. Ein reales Arbeitsleben, noch dazu *mit* einem erlernten und außerdem noch *im* erlernten Beruf, und das noch über Jahre, sogar Jahrzehnte, scheint in grünen Schichten offenbar unvorstellbar und unmöglich. Auch das Konzept eines zutreffenden, tatsächlich erarbeiteten, einfach wahren Lebenslaufs scheint unbekannt. Woher sollte man das auch kennen? Der feministische Schlachtruf lautet ja „Quality is a myth“.

Ich habe der Frau dargelegt, dass alle meine Angaben selbstverständlich wahr **belegbar und nachprüfbar** sind, es dazu Zeugen, Kollegen, Arbeitsverträge, Arbeitszeugnisse, reichlich Schriftstücke, Publikationen, Protokolle und dergleichen gibt. Sie solle einfach damit anfangen, in die Protokolle und Gutachten der damaligen Enquete „Zukunft der Medien in Wirtschaft und Gesellschaft“ zu schauen. Was für eine Redakteurin, die offenbar über Verbindungen in den Bundestag verfügt, nicht zu schwer sein sollte. Oder in meine Publikationen aus dieser Zeit.

Ihren Ärger und ihren Unwillen, einzusehen, warum die AfD ausgerechnet mich vorgeschlagen habe, ob es keine anderen Sachkundigen gäbe, konnte ich auch nicht mit dem Hinweis mildern, dass ich nun einmal einer der sehr wenigen Leute bin, die tatsächlich 2009 eine Vorratsdatenspeicherung geleitet haben, und das ein triftiger – und, wie ich meine, nachvollziehbarer – Grund sei, für sachverständig zum Thema Vorratsdatenspeicherung gehalten zu werden. Wenn es doch so viele andere – bessere – Sachkundige zu diesem Thema gibt, wie das IT- und Forensik-Fachblatt Kontext Wochenzeitung meint, warum haben die anderen Fraktionen sie dann nicht zum Wohle des Ergebnisses vorgeschlagen, statt den Vorwurf zu erheben, dass man *einen* überhaupt eingeladen hat?

Nachdem sie diesen Vorwurf überhaupt nicht belegen konnte und einsehen musste, dass er jeder Grundlage entbehrt und rein spekulativ frei erfunden war, einfach weil sich irgendwer da nicht vorstellen konnte, dass es auch Leute gibt, die so richtig und mit Ergebnis arbeiten, sie aber unter Zeitdruck einen Diffamierungsartikel vorlegen musste, erschien dann kurz darauf ein Artikel, in dem ich – ebenso frei erfunden – als „Holocaust-Relativierer“ beschimpft werde und *das* als Grund hingestellt wird, warum die AfD mich und nicht irgendwen anderen vorgeschlagen habe.

Dieser Vorwurf ist frei erfunden. Ich habe nie irgendetwas in dieser Richtung geäußert¹. Dazu kamen auf Diffamierung und Rufmord ausgerichtete Anfragen an den

¹ Im Gegenteil habe ich in meinem Blog mehrmals über ein Gespräch mit meiner Großmutter berichtet,

Bundestag und einen Landtag.

Wie mir Leser berichteten, ist dieser Vorwurf – und das war offenbar die Absicht eines Pseudoblattes, das praktisch keine Leser hat und nicht selbst lebensfähig ist – schnell in KI-Systeme und deren Auskünfte über meine Person eingesickert. Im Gegensatz zu vielen Politikern sind KI-Systeme aber lernfähig, und da geht so etwas nach hinten los, sobald die KI-Systeme dahinter kommen, dass das Fake News waren – und das in alle Sprachen übersetzen. Etwa für US-Politiker.

Im weiteren Verlauf zeigte sich, dass auch dieser Vorwurf jeder Grundlage entbehrt und von einer Antifa-Seite auf der Kriminellen-Webseite Indymedia/Linksunten abgeschrieben war, von denen ich 2020 mit einer Terror-, Diffamierungs- und Verleumdungswelle angegriffen worden war, weil ich Kritik an Gender Studies und der ehemaligen grünen-nahen Verfassungsrichterin Susanne Baer geübt hatte.

Vertreten wurden sie gegenüber der Staatsanwaltschaft dabei von einer den Grünen Baden-Württemberg sehr nahestehenden Anwaltskanzlei, die unter falscher Zitierung eines Urteils die Auffassung vertrat, dass man einen solchen Vorwurf erst gar nicht belegen müsse, weil er eine reine Meinungsäußerung sei. Man könne das eben einfach mal so nach Belieben dahinmeinen, dass jemand Holocaust-Relativierer sei. (Wenn man Auftrag und Abgabefrist hat und einem sonst nichts einfällt. Ohne dieses Thema kommen sie dann auch nicht aus, Godwin's Law. Geistig ist da sonst nichts.)

Und offenbar wird sie darin auch politisch protegiert, denn die Generalstaatsanwaltschaft Stuttgart wies meinen Strafantrag wegen Verleumdung und übler Nachrede mit der seltsamen Begründung ab, dass die Tat nicht mehr verfolgbar, weil nach **§ 24 Abs. 1 Landespressegesetz** kurze Verjährung eingetreten sei. Dass sich diese Vorschrift aber nur auf *Druckwerke* und nicht auf Online-Artikel bezieht, und der Artikel noch immer online war und ist, eine Verjährung noch gar nicht angefangen hatte, interessiert die Stuttgarter Generalstaatsanwaltschaft nicht. Strafrecht ist in Deutschland längst zum völligen Willkürobjekt und zur politischen Verfügungsmasse geworden.

Ich verwahre mich – auch vorsorglich wegen der nun bestehenden Wiederholungsgefahr – in aller Form gegen einen solchen Umgang, ersichtlich auch der Bundestagsfraktionen, mit Sachverständigen. Ein solches Gebaren ist nicht nur einer Demokratie und eines Parlamentes unwürdig. Es wirft auch ein ganz schlechtes Licht auf die – ohnehin schon qualitativ fragwürdige – Gesetzgebung dieses Landes.

Vielleicht sollten Sie überdenken – Stichwort Wahlergebnisse, Politikverdrossenheit – wie Ihre Zusammensetzung und Vorgehensweisen, Ihre Sitten und Gebräuche auf Bürger, Steuerzahler, Wähler – und Sachverständige oder sogar andere Länder wie die USA – wirken.

die mir sagte, dass die Vorgänge unbestreitbar seien und lüge, wer sie bestreite, weil damals „ab der Hälfte der Zeit“ – also ungefähr 1942 – „jeder gewusst habe, was da abläuft“. Denn Soldaten, Wehrpflichtige aus Konzentrationslagern hätten dies in den Dörfern brühwarm erzählt – und man habe es damit unfälschbar und aus erster Hand erfahren. Darauf meldeten sich zwei Historiker der Hochschulen bei mir und bestätigten, dass sie diese Aussage voll und ganz aus ihrer Forschungsarbeit bestätigen können.