

Stellungnahme als Sachverständiger

für den Deutschen Bundestag

zum Antrag der Fraktion der CDU/CSU

**„IP-Adressen rechtssicher speichern und
Kinder vor sexuellem Missbrauch schützen“**

vom 27.9.2022, BT-Drucksache 20/3687

Anhörung am 11. Oktober 2023

– Rechtsausschuss –

Dipl.-Inform. Hadmut Danisch

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

Stand: 9. Oktober 2023

Inhaltsverzeichnis

1 Auftrag	5
1.1 Fragestellung	5
1.2 Gegenstand	5
1.3 Maßstab	5
1.4 Sachkunde	6
2 Erfahrungen zugunsten einer Vorratsdatenspeicherung	7
3 Fehler und Rechtswidrigkeiten des Antrags	9
3.1 „Portnummern“	9
3.1.1 Erläuterung	9
3.1.2 Technische Fehler	12
3.1.2.1 Keine Port-Speicherung auf dem Server	12
3.1.2.2 Das Uhrzeit-Problem	14
3.1.2.2.1 Halbstatisches Port-NAT	15
3.1.2.2.2 Dynamisches Port-NAT	15
3.1.2.2.3 Dynamisches Port-NAT mit langer Persistenz	18
3.1.2.3 Technische Umsetzbarkeit	18
3.1.3 Datenschutzrechtliche Hindernisse	19
3.1.3.1 Unzulässige Verkehrsprotokollierung	19
3.1.3.2 Verletzung des Post- und Fernmeldegeheimnisses (Art. 10 GG)	19
3.2 Die Entscheidung des EuGH	21
3.2.1 Keine „Eröffnung von Möglichkeiten“	22
3.2.2 Kinderpornographie keine ausreichende Bedrohung	22
3.3 Trugschluss „Rechtssicherheit“	25
3.3.1 Es gibt keine „Rechtssicherheit“ im Internet	25
3.3.2 Fälschung der IP-Adresse	25
3.3.3 Fehler kommen vor	26
3.3.4 Angriff auf Router	26
3.3.5 Beispiel BGP Hijack, ARP Spoofing u.ä.	26
3.3.6 Unsicheres Logging	27
3.3.7 „Jeder kann programmieren!“	28
3.3.8 Unbeherrschbarkeit der Software	28
3.3.9 Unsichere Endgeräte	28
3.3.10 Ende der Route?	29
3.3.11 „Cyberkrieg“	29
3.3.12 Antifa	30

3.3.13 Naive Vorstellung	30
3.4 Mangelhafte Qualität des Antrags	31
4 Insuffizienz der Staatsgewalten	32
4.1 Legislative und Regierung	32
4.1.1 Kinderpornosperrung 2009 (Ursula von der Leyen)	32
4.1.2 Die frühere Auffassung der Bundesregierung von „IT-Sicherheit“	34
4.1.3 Die personelle Besetzung des Bundestags als Gesetzgeber	34
4.1.4 Fehlkonstruktion Auskunftsgestattungsverfahren	35
4.1.4.1 Negativbeispiel Causa Renate Künast	36
4.2 Judikative	38
4.2.1 Das Bundesverfassungsgericht	38
4.2.1.1 Vorratsdatenspeicherung	38
4.2.1.2 Rundfunkbeiträge	40
4.2.1.3 Die Causa Renate Künast	41
4.2.1.4 Personelle Defizite	42
4.2.1.5 Die „Strategische Prozessführung“	43
4.2.1.6 Dysfunktionales Scheingericht	43
4.2.2 Das Vieraugenprinzip der Blinden	44
4.2.3 Mangelnde Sachkunde	45
4.2.3.1 Das Juristenkonzept des 18. Jahrhunderts	45
4.2.3.2 Das Prinzip der zielführenden Ignoranz	45
4.2.3.3 Positive Ausnahme Landgericht: Auskunft nach § 101 UrhG	46
4.3 Exekutive	47
4.3.1 Bundeskriminalamt 2009	47
4.3.2 Polizei	47
4.3.2.1 Fehlende Ausbildung und Einweisung	47
4.3.2.1.1 Datenübertragung per Blaulicht	48
4.3.2.1.2 Fallbeispiel datenschutzwidrige Anfrage aus Unkenntnis	48
4.3.2.2 Provider als Hilfsermittler der Polizei	49
4.3.2.2.1 Blutanhaftungen auf Augenhöhe	49
5 Missbrauch	51
5.1 Private Nutzung	51
5.2 Fehlende Authentizität der Anfragen	51
5.3 Geschäftsmodelle und Geheimdienstschnittstellen	52
5.4 2023: Schwerer Missbrauch beim Landeskriminalamt Berlin	53
6 Sonstige Bedenken	61
6.1 Verhältnismäßigkeit als Verfassungsgrundsatz	61
6.1.1 Mangelnde Eignung	61
6.2 Fehlender Rechtsweg	62
6.3 „Schutz der Kinder“ – Frühsexualisierung	62
6.4 Bürokratiewut	64

7 Ergebnis	65
7.1 Zusammenfassung	65
7.2 Empfehlung	66

1 Auftrag

1.1 Fragestellung

Ich wurde am 4.10.2023 vom Rechtsausschuss des Deutschen Bundestages zur Teilnahme an der Anhörung über den Antrag der Fraktion der CDU/CSU „IP-Adressen rechtssicher speichern und Kinder vor sexuellem Missbrauch schützen“, BT-Drs. 20/3687, am 11.10.2023 eingeladen.

Eine explizite Frage- oder Problemstellung wurde nicht vorgegeben. Die Stellungnahme erfolgt deshalb als freie Äußerung.

1.2 Gegenstand

Es wurden zur Betrachtung herangezogen:

1. Der Antrag der Fraktion der CDU/CSU.
2. Das Urteil des EuGH in den verbundenen Rechtssachen C-793/19 und C-794/19, auf das sich der Antrag bezieht, in der deutschsprachigen Übersetzung.

1.3 Maßstab

Neben Technik, Erfahrung, den Grundrechten und allgemeinem Recht habe ich die Anforderung des EuGH aus seinem o.g. Urteil an eine Vorratsdatenspeicherung als Maßstab angelegt:

„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.“

1.4 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
- 8 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 Kinderpornosperrung der Regierung (Ursula von der Leyen) involviert. Die Sperrung 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
- Über 20.000 Blogartikel zu Rechts- und Medienpolitik und anderen Themen

Ich beantworte die vorliegende Fragestellung – insbesondere wegen der kurzen zur Verfügung stehenden Zeit und weil mich der Auftrag am Urlaubsort ohne Zugriff auf Literatur erreicht hat – vollständig aus meinem bestehenden Wissen aus meiner Ausbildung, meiner Berufserfahrung – insbesondere der Tätigkeit in der Vorratsdatenspeicherung im Jahr 2009 – und vielen Recherchen für Blog-Artikel.

2 Erfahrungen zugunsten einer Vorratsdatenspeicherung

Ich war als der Informatiker in der Rechtsabteilung eines großen Telefon- und Internet-Providers in Deutschland über das Jahr 2009 – nicht in meiner eigentlichen Tätigkeit, sondern als Vertretung eines länger erkrankten Kollegen – leitend für die Aufsicht über die damals neu eingeführte Vorratsdatenspeicherung und sonstige Beauskunftung und für die Eingangsprüfung der Auskunftersuchen zuständig, und habe in dieser Zeit eine Größenordnung von ungefähr 2.000 Fällen bearbeitet.

Ganz grob und aus der lange zurückliegenden Erinnerung geschätzt würde ich

- ein Drittel der Anfragen als ungerechtfertigt, unverhältnismäßig, sach- oder rechtsfehlerhaft, oder sogar missbräuchlich und zweckfremd (dazu später mehr),
- mindestens ein weiteres Drittel als entweder fragwürdig oder mangels Begleitinformation als nicht einzuordnen,
- höchstens ein Drittel, eher weniger, als für mich rechtlich nachvollziehbar, verfassungsrechtlich haltbar und begründet

einstufen.

Es gab jedoch einige Fälle schwerer und schwerster Kriminalität, die durch – und den Umständen nach oft *nur* durch – die Vorratsdatenspeicherung aufgeklärt oder in denen wohl sogar Menschenleben gerettet werden konnten.

Dazu gehören nicht nur – soweit aus der Anfrage erkennbar allerdings seltene – Fälle von Waffen- und Drogenhandel, Bandenkriminalität, Erpressung, Menschenhandel, Verstöße gegen Kriegswaffenverbote, sondern auch Morde und Fälle von höchster Gefahr im Verzuge. Man freut sich dann regelrecht, dass man endlich mal „richtige“ Fälle hat und nicht immer nur endlose Fälle von Beleidigung, Urheberrechtsverstößen und dem sonstigen Bereich des Äußerungsrechts.

Zwei Fälle sind mir dabei besonders in Erinnerung geblieben, weil sie von solcher Dringlichkeit waren, dass ich – entgegen der Regel und Rechtsanforderung, dass Ersuchen und Auskunft ausschließlich schriftlich erfolgen können – in Abwägung der Rechtsgüter ausnahmsweise und vorab telefonisch beauskunftet habe.

In einem Fall war morgens ein Kind ermordet und tot aufgefunden worden. Nach der Sachlage, der Art der Tötung und anderen Erkenntnissen ergab sich der äußerst dringende Verdacht, dass es sich beim Täter um einen Berufsverbrecher handelte, der an diesem Tag unterwegs war, um mehrere Kinder zu töten. Es waren eine Reihe dringender Auskunftsersuchen zu beantworten, um sowohl den Vorfall aufzuklären, als auch die noch gefährdeten Kinder ausfindig zu machen und in Sicherheit zu bringen.

In einem anderen Fall hatte jemand in einem Forum anonym/pseudonym äußerst und ausfällige Wut über eine örtliche Filiale eines Unternehmens geäußert, dass er im Besitz einer Bombe sei und jetzt sofort losfahre, um die da alle in die Luft zu sprengen.

Leser des Forums hatten direkt die Polizei alarmiert, welche sofort mit Blaulicht und mehreren Fahrzeugen zur Filiale eilte. Der Administrator des Forums hatte dazu die IP-Adresse mitgeteilt, zu der das Polizeipräsidium telefonisch bei mir anfragte und mich in einer Dreierkonferenz zum Einsatzleiter im Fahrzeug durchschaltete, um die Beauskunftung schnellstmöglich zu erteilen. Name und Anschrift wurden von mir beauskunftet. Das Präsidium lieferte dazu aus der Halterabfrage die Fahrzeugbeschreibung und die Erkenntnis, dass der Täter nach seinem Wohnort vermutlich dieselbe Hauptstraße benutze, auf der auch die Polizei zur Filiale unterwegs war. Tatsächlich wurde dann – live am Telefon mitgehört – auf dieser Straße das Fahrzeug des Täters entdeckt, abgedrängt, zum Halten gebracht, der Täter überwältigt und festgenommen. Im Fahrzeug wurde ein mutmaßlicher Sprengkörper gefunden. Ob echt oder Attrappe habe ich nicht mehr erfahren, weil die Polizei dann auflegte um das Bombenkommando zu rufen.

Dazu kamen einige wenige weitere Fälle angekündigter *erweiterter* Suizide.

Ich hatte außerdem für die Dauer meiner Tätigkeit in diesem Unternehmen ein Dankschreiben einer Polizeidienststelle aus einem weiteren Fall dafür an der Wand hängen, dass der Mörder aufgrund der Auskunft (und Beratung) gefasst werden konnte. (Was alle Kollegen sehr beeindruckte.)

Ich weise aber darauf hin, dass dies *Einzelfälle* waren und kein durchgängiges Muster darstellen, deshalb nicht ohne weiteres geeignet sind, die Bedingungen des EuGH (vgl. Kapitel 3.2 auf Seite 21) zu erfüllen.

3 Fehler und Rechtswidrigkeiten des Antrags

3.1 „Portnummern“

Auf Seite 2 Mitte des Antrags heißt es

„Dem dient auch die Befristung der Speicherpflicht auf einen Zeitraum von sechs Monaten. Zudem müssen die Portnummern mitgespeichert werden, um eine rechtssichere Zuordnung der IP-Adresse auch dann zu ermöglichen, wenn Provider eine Adresse mehrfach vergeben.“

Dem liegt ein mangelhaftes technisches Verständnis zugrunde, das in der Folge zu Rechtsfehlern führt.

3.1.1 Erläuterung

Das Internet beruht darauf, kleine Datenpakete von einer Zwischenstation zur anderen und mit unterschiedlichen Transportmitteln entlang von Routen durch die Welt zu schicken, und dabei – ähnlich wie die Postleitzahl beim Briefversand oder die Paketmarke beim Fluggepäck – den Weg bis zum Ziel anhand von sogenannten „IP-Adressen“ (IP = Internet Protocol) zu finden. Diese IP-Adressen ermöglichen es, auf allen Ebenen vom Internkontinentalverkehr bis zur WLAN in der eigenen Wohnung den Weg zum Zielrechner zu finden. IP-Adressen und Routing ermöglichen es zusammen, für jedes IP-Paket, das eine kleine Datenportion als Nutzlast mit sich schleppt, den Weg von einem „Umsteigebahnhof“ zum nächsten zu finden.

Nach dem ursprünglichen und immer noch üblichen IP, Protokollversion 4, das sogenannte IPv4 (eins bis drei waren experimentell und nicht im großen Einsatz) hat eine IP-Adresse 32 Bit, womit theoretisch $2^{32} = 4.294.967.296$ verschiedene Adressen möglich sind. Davon fallen aber einige Bereiche für technische Zwecke weg. Außerdem gibt es gehörigen „Verschnitt“, weil IP-Adressen immer in Kontingenten (aus technischen Gründen meist in Zweierpotenzen) vergeben werden. Ähnlich wie Postleitzahlen werden IP-Adressen hierarchisch vergeben und können nicht beliebig und nach Bedarf verteilt werden. Somit ist die Zahl der tatsächlich nutzbaren IP-Adressen nicht nur deutlich geringer als 4 Milliarden, sie lassen sich auch nicht mit der nötigen Granularität verteilen. Außerdem hat man etliche Adressbereiche zu großzügig vergeben, als

noch nicht absehbar war, wie groß das Internet werden würde.

Bei inzwischen rund 8 Milliarden Menschen, dazu unzähligen Servern im Internet, und dem Zeitalter der Smartphones reicht die Zahl der IPv4-Adressen längst nicht mehr, um allen Menschen und allen Geräten und Rechnern eine eigene IPv4-Adresse zuzuweisen, wie es technisch eigentlich erforderlich wäre. Und selbst da, wo noch IPv4-Adressen verfügbar sind, sind sie knapp und werden damit teuer wie Mietwohnungen in deutschen Großstädten.

Deshalb hat man schon vor rund 30 Jahren angefangen, Lösungsansätze zu suchen und zwei praktikable Ansätze gefunden:

IPv6 als neues Protokoll, das ähnlich dem IPv4 funktioniert und dessen Rolle übernimmt, sogar parallel dazu verwendet werden kann, aber statt nur 32 sogar 128 Bit Adressraum bietet, also theoretisch 340.282.366.920.938.463.463.374.607.431.768.211.456 verschiedene Adressen. Man nimmt an, dass das auch auf absehbare Zukunft für alle Menschen und Rechner der Welt reicht, weil es so viele Atome in unserem Sonnensystem nicht gibt.

IPv6 hat sich aber nicht so sehr durchgesetzt, dass es IPv4 verdrängt hätte. Noch immer laufen viele Rechner an Internet mit IPv4, und in manchen Ländern (Beispiel: Zypern) kam man zu der Erkenntnis, dass alle Server, die man im normalen Leben braucht, mit IPv4 zu erreichen sind und Internet Provider deshalb normalen Kunden zur Fehlervermeidung nur IPv4 anbieten. IPv6 wird erst auf ausdrückliche Anforderung und Problemstellung vergeben.

Noch immer können viele Geräte mit Anschluss an das Heimnetz nur IPv4 sprechen.

NAT Die sogenannte „Network Address Translation“ bezeichnet eine seit langem übliche und bewährte Technik, die jeder – auch ohne es zu merken – in seinem Firmen- oder Heimnetz verwendet.

Genauer gesagt, handelt es sich um eine Sammlung *ähnlicher, aber unterschiedlicher* Verfahren, es gibt verschiedene Arten von NAT.

Statt, wie eigentlich technisch erforderlich, jedem Gerät im lokalen Netz (Firma, Wohnung, Behörde, ...) eine eigene offizielle Adresse zu vergeben, und damit viel Adressen für den jeweiligen Anwender vergeben zu müssen, verwendet man den äußeren, an das Internet angeschlossenen Router als eine Art Stellvertreter, und gibt nur diesem eine offizielle IP-Adresse, benötigt also nur eine. Diese Konstellation wird als „Hide-NAT“ bezeichnet, weil sie ein ganzes Netzwerk hinter einer einzelnen IP-Adresse versteckt. Auch die Bezeichnung „Masquerade“ ist für diese Betriebsarbeit gebräuchlich, weil es nach außen hin eine Maskerade hinter der IP-Adresse des Routers darstellt.

Allen anderen Geräten im Netz gibt man Adressen aus einem Kontingent (defi-

niert in RFC 1918) von Bereichen (nämlich 10/8, 172.16/12 und 192.168/16), die nicht öffentlich verwendet und geroutet werden dürfen, und deshalb innerhalb lokaler Netze auch mehrfach verwendet werden können. Der äußere Router oder die Firewall des Netzwerkes müssen dann diese IP-Adressen immer durch die öffentliche IP-Adresse des Routers ausgetauscht werden.

Deshalb haben Rechner im Wohnungsnetz immer Adressen etwa wie 192.168.*.*, und das selbst dann, wenn der Nachbar in seiner Wohnung dieselben Adressen verwendet, weil die Router, mit denen man an das Internet angeschlossen ist, diese Adressen hinter ihrer eigenen, offiziellen Adresse verstecken. Auf diese Weise werden Mehrdeutigkeiten verhindert, obwohl viele Haushalte dieselben IP-Adressen verwenden.

Um das tun und eingehende Pakete auch wieder richtig rückübersetzen und dem einzelnen Gerät zuordnen zu können, müssen sich die Router den Kontext, die Verbindungen merken, und das – bei den Protokollen wie TCP und UDP – indem sie sich die sogenannten Portnummern merken, mit denen der Rechner verschiedenen Verbindungen auseinanderhält und man auswählt, welchen Dienst man auf dem Zielrechner ansprechen will. Beispielsweise sind das 80 für HTTP (Webseiten), 443 für HTTPS (verschlüsselte Webseiten) oder 25 für SMTP (E-Mail). Aber auch auf der Seite des Clients (Nutzers) werden solche Portnummern verwendet, allerdings zufällig gewählte. Die muss der Router sich für eine Verbindung merken, um die Pakete, die als Antwort zurückkommen, richtig zuordnen zu können.

Sehr leistungsstarke Firewalls können diese Zuordnungen auch protokollieren. In der Regel werden sie aber nicht protokolliert, weil sie eine riesige Menge von Daten liefern.

Dieses Konzept ist seit rund 30 Jahren erfolgreich im Einsatz und hat sich bewährt (vgl. RFC 1631).

Der Einsatz von NAT bei IPv4 ist der Grund, warum man bei Abfragen der IP-Adresse nur den Anschlussinhaber, nicht aber das einzelne Gerät abfragen kann, weil man die NAT-Zuordnung von äußerer, offizieller IP-Adresse zum jeweiligen Gerät von außen nicht ersehen kann.

Viele IP-Provider bieten heute sogenannte „Dual-Stack“-Anschlüsse, auf denen man beides, IPv4 und IPv6 bekommt.

Seit 2019 sind alle IPv4-Adressen, die man international noch auf Vorrat hatte, vergeben und verkauft, ebenso seit 2020 in Lateinamerika und der Karibik („IPv4 address exhaustion“).

Innerhalb der Kontinente, der Länder und der Provider sind noch kleine Kontingente verfügbar, aber sehr knapp und teuer. Manche Internet-Provider können nicht mehr genug IPv4-Adressen für ihren Betrieb erhalten oder bezahlen.

Deshalb hat man als Ausweg den sogenannten „Dual Stack light“ ersonnen, also einen Anschluss mit IPv4 und IPv6, bei dem aber nur der IPv6-Anschluss vollwertig ist und offizielle Adressen zugewiesen erhält. Beim IPv4-Anschluss wiederholt man auf Provider-Ebene dieselbe NAT-Technik (sog. „Provider-NAT“), die ich oben für das private Netz (Wohnung, Firma, Behörde,...) beschrieben habe, auf Ebene des ganzen Internet-Providers: Auch die Anschlüsse für Wohnungen erhalten keine offizielle IP-Adresse mehr, sondern nur noch eine nicht-offizielle Adresse aus dem Bereich der privaten RFC1918-Adressen, die dann vom Router des Internet-Providers in offizielle IP-Adressen übersetzt und die Antworten rückübersetzt werden müssen. Somit kommt man mit sehr viel weniger offiziellen IPv4-Adressen aus.

Das funktioniert, führt aber zu erheblichen Einschränkungen und Störungen. Damit kann man noch auf Dienste wie Webseiten usw. zugreifen, die nur per IPv4 erreichbar sind, die volle Funktionalität eines Internet-Anschlusses erhält man aber nur noch für IPv6. Schön ist das nicht, aber aufgrund der Erschöpfung des IPv4-Adressen nicht anders zu machen.

Unseriöse Anbieter haben auch nur IPv4-NAT ohne IPv6 angeboten.

An dieser Stelle ist es wichtig zu verstehen, dass der technische Plan der Internet-Architekten vorsah, dass IPv4 längst abgeschaltet ist und nur noch IPv6 verwendet wird, und damit alle diese Problem gar nicht mehr bestehen. Die Welt hat sich aber als viel zu träge und der Aufwand als zu hoch erwiesen, um in überschaubarer Zeit von IPv4 wegzukommen, ähnlich dem Umstieg von UKW auf DAB+ oder von Fax auf Internet. Es geht hier um Altlasten.

Forensisch führt Provider-NAT zu dem Problem, dass die IP-Adresse aus dem Internet nicht mehr bis zum Endanschluss, sondern nur bis zum nächsten NAT-Punkt zurückverfolgbar ist, und hier deshalb nicht mehr bis zum Anschlussinhaber und dessen Wohnung oder Firmenräume, sondern nur noch bis zum NAT-Punkt – also dem Router – *des Providers*, und damit die Zuordnung zum Endkundenanschluss nachträglich nicht mehr möglich ist.

Der Antrag der CDU/CSU zielt nun darauf ab, die Provider, die Provider-NAT einsetzen, dazu zu verpflichten, diese NAT-Zuordnungen aller Verbindungen zu protokollieren und zu speichern, um anhand dieser Logs nachträglich auf den Anschlussinhaber zu schließen, also nachträglich die NAT-Zuordnungen nachvollziehen zu können.

Dieser Gedanke unterliegt technischen und rechtlichen Fehlern.

3.1.2 Technische Fehler

3.1.2.1 Keine Port-Speicherung auf dem Server

Das Internet arbeitet nicht verbindungs-, sondern paketorientiert. Da man aber Verbindungen benötigt, werden sie durch Ströme von kleinen Datenpaketen simuliert, wozu

Protokolle zuständig sind, die auf dem Internet-Protokoll aufsetzen. Die bekanntesten Aufsatzprotokolle heißen TCP und UDP. TCP (Transmission Control Protocol, standardisiert 1981) hat eben diese Aufgabe, einen Datenstrom beim Absender in kleine Datenpakete zu zerlegen und diese beim Empfänger fehlerfrei wieder zu diesem Datenstrom zusammensetzen. Deshalb wird das Internet oder dessen Protokollfamilie auch mit ihrem alten, historischen Namen „TCP/IP“ bezeichnet, obwohl der eigentlich falsch ist, denn TCP ist nicht *Teil* des Internets, sondern ein Protokoll, um das Internet *zu gebrauchen*. Das Internet selbst kennt kein TCP (abgesehen von der Protokollnummer im IP-Header), TCP ist aus Sicht des Internet nur eine Nutzlast. Gängige Datenprotokolle wie HTTP und HTTPS zum Zugriff auf Webseiten oder SMTP zur Übermittlung von E-Mail beruhen auf TCP.

Jede solche TCP- oder UDP-Verbindung wird *zu jedem Zeitpunkt* durch ein sogenanntes 5-Tupel (also 5 Daten) eindeutig beschrieben und identifiziert:

- Protokoll (TCP, UDP, ...)
- Quell-IP
- Quell-Port
- Ziel-IP
- Ziel-Port

Neben dem Zeitpunkt des Zugriffs sind also auch diese fünf Daten erforderlich, um eine Verbindung zu identifizieren.

Die NAT-Tabellen in Routern und Firewalls beruhen dabei auf 7-Tupeln, nämlich zusätzlich die NAT-IP und der NAT-Port, die nach außen hin die Funktion von Quell-IP und Quell-Port übernehmen.

Bei ins Internet ausgehenden Paketen werden dann die Quell-IP und der Quell-Port durch NAT-IP und NAT-Port ersetzt. Und bei aus dem Internet hereinkommenden Paketen das ganze umgekehrt (dann mit der Ziel-IP und Ziel-Port, weil nun der Rechner im versteckten Netz Empfänger ist).

Soll nun diese Zuordnung nachträglich forensisch aufgeklärt werden, muss im Prinzip das 7-Tupel oder zumindest dessen Teile, die es identifizieren und die Auskunft ermöglichen, gespeichert werden.

Was ist dazu erforderlich?

- Das Protokoll ist nun anzugeben. Man muss also nun angeben, ob es um ein TCP-, UDP- oder sonstiges Protokoll geht.
- Die Ziel-IP (in der Regel irgendeines Servers) ist meist statisch vergeben oder bei forensischen Untersuchungen bekannt.

Auch diese müsste nun als Teil der Anfrage angegeben werden.

- Der Ziel-Port ist durch die Art der Anwendung meistens auch vorgegeben (z. B. Webserver auf Port 80 für HTTP oder 443 für HTTPS).

Auch dieser müsste nun in der Anfrage angegeben werden.

- Die Quelladresse wird auf Webservern u.ä. normalerweise erfasst und geloggt, weil für Zugriffsrechte, Fehlersuche, Angriffsanalyse u.ä. erforderlich.

Diese entspräche der NAT-IP.

- Der Quell-Port wäre erforderlich und entspräche dem NAT-Port wird jedoch in der Regel nicht geloggt, weil normalerweise nutz- und bedeutungslos.

Das heißt, dass im Auskunftersuchen weit mehr Daten angegeben werden müssten als bei einer normalen IP-Adress-Anfrage. Diese Daten – nämlich die Quell-Port-Adresse, die der NAT-Port-Adresse entspricht, normalerweise nicht bekannt ist, weil sie normalerweise nicht geloggt wird. Man kann das bei manchen Servern zwar konfigurieren, dass auch diese geloggt wird, in der Regel wird diese aber nicht geloggt.

Das heißt, dass die erforderlichen Informationen zur Stellung einer Auskunftsanfrage bei Provider-NAT in der Regel nicht vorliegen.

Es wäre also zunächst zu klären, woher die Information des Quell-Ports kommen soll, um diese überhaupt beim Provider abfragen zu können, denn in der Regel wird diese nicht geloggt und kann damit auch nicht beschlagnahmt werden.

Dass ausländische Betreiber von etwa Kinderpornoseiten sich dabei an die Log-Vorstellungen deutschen Rechts halten, ist nicht zu erwarten, denn wenn sie sich nach deutschem Recht richten würden, würden sie ja erst gar keine Kinderpornos hosten.

3.1.2.2 Das Uhrzeit-Problem

Es gibt grundsätzlich zwei Arten von NAT: Statisch und Dynamisch.

Bei statischem NAT wird die Ersatz IP-Adresse vorher fest konfiguriert, etwa bei Server-Maschinen. Bei dynamischem NAT wird jeweils zur Laufzeit eine Adresse neu zugewiesen.

Aus technischen Gründen eignet sich statisches NAT (für IP-Adressen) auf Server-Seite, also das Ziel einer Verbindung, während dynamisches NAT auf der Client-Seite, also der Quelle einer Verbindung verwendet wird, weil der NAT-Server bei einem Verbindungsaufbau aus dem NAT-Netz ersehen kann, was die interne Adresse ist, während er das bei einem Verbindungsaufbau aus dem Internet selbst wissen muss.

Bezüglich der Port-Adressen ist dies komplexer, weil ein statisches Ausgangs-NAT hier nicht möglich wäre.

3.1.2.2.1 Halbstatisches Port-NAT Denkbar wäre ein halbstatisches Port-NAT, in dem jedem Endkunden auf dem NAT-Server ein fester Port-Bereich zugewiesen wird, innerhalb dessen NAT-Verbindungen zugewiesen werden.

Das wäre aber nicht praktikabel, weil

- es den Zweck des NAT konterkariert und das Zahlenverhältnis zwischen Endkunden und IPv4-Adressen stark beschränkt, also praktisch nicht oder kaum einsetzbar wäre,
- es mit erheblichem Verwaltungsaufwand verbunden wäre.

Mir wäre jetzt kein Provider bekannt, der das so machte.

3.1.2.2.2 Dynamisches Port-NAT Da es sich um ein Quell-NAT handelt, dürfte die NAT-Methode rein dynamisch erfolgen, also jeder Verbindung eine gerade freie Kombination aus NAT-IP und NAT-Port zugewiesen werden.

Damit läuft man aber in das Problem eine nicht ausreichend genauen und fein granularen Zeitmessung.

Im Gegensatz nämlich zu den IPv4- und IPv6-Adressen, die den Anschlüssen in der Regel für 24 Stunden, je nach Anbieter auch mehrere Tage oder Wochen zugewiesen werden, und bei denen es auf Ungenauigkeiten in der Zeit nicht so ankommt, werden dynamische NAT-Verbindungen nur für die Dauer einer TCP-Verbindung zugewiesen, **und damit im Sekunden oder sogar Millisekunden-Bereich.**

Zwar werden NAT-Zuordnungen auch nach Schließen der Verbindung – je nach Implementierung – bei manchen Geräten noch für gewisse Zeit belegt, um nachlaufende IP-Pakete aufzufangen. (Im Internet ist nicht spezifiziert und deshalb auch nicht sichergestellt, dass IP-Pakete ankommen, dass sie nicht mehrfach ankommen, und dass in der richtigen Reihenfolge ankommen.)

Es gibt aber im Allgemeinen auf Internet-Geräten keine hinreichend genaue und zuverlässige Zeitmessung dafür.

1. Es gibt keine Verpflichtung der Server-Betreiber, eine genaue oder richtige Zeiteinstellung zu haben.

Mir wurde auch kein einziges Strafermittlungsverfahren bekannt, in dem die Genauigkeit der Serverzeit geprüft wurde.

2. Server-Hardware-Uhren sind erfahrungsgemäß oft sehr ungenau und müssen ständig per Software korrigiert oder nachgezogen werden, weil sie oft mehrere Sekunden pro Monat driften. Das hat mehrere Gründe, etwa Kosten- und Platzgründe. Sie enthalten keine oder nur sehr billige Quarze, und sind Temperaturschwankungen und Alterung ausgesetzt, können durch leere Pufferbatterien

ganz ausfallen und bieten oft nur eine Granularität von einer Sekunde.

Als Server bezüglich der Uhrzeit noch auf sich selbst gestellt waren, war es noch üblich, auf den Rechnern die Drift der Hardwareuhr zu messen und dann rechnerisch auszugleichen. Auch heute noch ist das erforderlich, wenn sie keine Netzwerkverbindung zu einem Zeitserver oder -empfänger haben.

Server-Uhren sind nicht spezifiziert, eine Genauigkeit im Sekunden- oder Millisekundenbereich zu leisten. Aufgabe der Server-Uhren ist in erster Linie, die strenge Monotonie der Zeit beim Booten zu gewährleisten, aber nicht, eine echtzeitfähige Präzision zu liefern.

3. Normalerweise – aber nicht zwingend – werden die Rechner per NTP an eine Zeitquelle gebunden. Das funktioniert in der Regel, aber nicht immer und nicht permanent, und Ausfälle werden nicht bemerkt oder gar geloggt.

Es ist also möglich und passiert gelegentlich, dass Rechner wegen irgendeiner Störung im NTP die Synchronisation verlieren, langsam driften, und um mehrere 10 Sekunden oder sogar Minuten „falsch gehen“, dann aber durch Neustart o.ä. wieder synchronisiert werden und die Abweichung nie bemerkt wird, und auch nicht nachvollziehbar ist.

4. NTP erfolgt in der Regel über mehrere Stufen hinweg (Stratum) und erreicht über das Internet hinweg im günstigen Fall eine Genauigkeit von bestenfalls einigen zehn Millisekunden.
5. Typische Server-Systeme wie Linux oder Windows geben die Uhrzeit zwar in Milli- oder sogar Mikrosekunden an, **aber nicht mit dieser Genauigkeit und Granularität.**

Rechner-Uhren sind nicht darauf spezifiziert, genau zu sein, weil in der Informationstechnik eine hohe Genauigkeit weder erforderlich ist, noch sinnvoll umgesetzt werden kann. Die Uhrzeit dient eher dazu, die Reihenfolge zu gewähren, weshalb die formale Spezifikation für die Zeit auf Rechnersystemen ist, dass

- Keine Zeit übersprungen wird, also jede Uhrzeit vorkommt (damit Cron-Jobs nicht übergangen werden)
- Keine Zeit doppelt vorkommt, also nicht wiederholt wird,
- Zeit in der richtigen Reihenfolge abläuft, als 16:00 Uhr nicht vor 15:00 Uhr kommt.

Es gibt keine Spezifikation, wonach Systemuhren mit einer bestimmten Genauigkeit oder Toleranz mit der gesetzlichen Zeit übereinzustimmen haben. Die systemübergreifende Genauigkeit von Systemuhren dient vor allem dem Zweck, die spezifizierten Anforderungen an die Systemuhren auch bei systemübergreifenden Systemen, wie auf Fileservern oder verteilten Prozessen konsistent zu halten.

Deshalb wird auf Servern, etwa Datenbankservern und ähnlichen, auf denen die Uhrzeit nicht stimmt, bei sorgfältiger Administration die Uhrzeit nicht neu gestellt, weil damit möglicherweise Uhrzeiten ausgelassen oder wiederholt würden. Stattdessen beschleunigt oder bremst man die Uhr, damit sie schneller oder langsamer läuft, und über einen gewissen Zeitraum die richtige Zeit erreicht, dabei aber alle Uhrzeiten vollständig, ohne Doppel und in der richtigen Reihenfolge durchläuft.

Die Uhren auf Computersystemen entsprechen deshalb nicht dem intuitiven Verständnis einer Uhr.

6. Serversoftware ist nicht dazu geschrieben, die Uhrzeit in definierter Präzision zu loggen. Da die Log-Einträge von Webservern u.ä. normalerweise auch das Ergebnis der Transaktion und die Menge der übertragenen Daten umfasst, wird die Uhrzeit oft erst bei der Erstellung des Logeintrags *nach Ende der Verbindung* genommen, was auf einem Multitasking-System aber zu einer undefinierten Verzögerung führt.

Das ist unkritisch, solange es nicht auf ein paar Sekunden ankommt. Wenn aber ein Port-NAT forensisch aufgelöst werden soll, wären Genauigkeiten im Millisekunden-Bereich erforderlich.

7. Typische Server-Systeme wie Linux oder Windows sind **nicht echtzeitfähig**. Sie können Vorgänge nicht in dieser Genauigkeit erfassen.

Zwar sind heute viele Zeiteinträge bei Unix-Systemen, etwa die Modifikationszeiten bei Dateien, in Mikrosekunden angegeben. Das heißt aber nicht, dass sie diese Genauigkeit auch erreichen. Es bedeutet nur (vgl. Spezifikation oben) dass auch bei schnellen Datenverarbeitungsvorgängen *die Reihenfolge* gewahrt bleibt. Man hat dies eingeführt, weil dies für Build-Chains (Make usw.) erforderlich war, weil schnelle Prozessoren viele Vorgänge innerhalb einer Sekunde durchführen können und dann bei einer Granularität von Sekunden die Reihenfolge nicht mehr klar ist.

8. Serversysteme laufen heute typischerweise nicht direkt auf der physikalischen Maschine, sondern in virtuellen Maschinen. Je nach Virtualisierungstechnik kommt es dabei zu erheblichen Fehlern in der Maschinenzzeit.
9. Es können Fehler in der Zeit entstehen, wenn Maschinen nicht gründlich aktualisiert werden, weil gelegentlich Schaltsekunden an Sylvester eingelegt werden oder sich Veränderungen bei Zeitzonen und Sommerzeiteinstellungen ergeben, die in der Software berücksichtigt werden müssen.
10. Es gibt Systeme, die manuell auf Sommer- und Normalzeit umgestellt werden müssen, was aber dann oft vergessen oder verspätet durchgeführt wird.
11. Viele Systeme werden erst gar nicht auf eine genau Zeit oder NTP eingestellt, weil es den Betreiber nicht interessiert, ob die Uhrzeit stimmt. Nicht wenige „Ad-

ministratoren“ wissen auch nicht, wie das geht.

12. Erfahrungsgemäß sind auf vielen Servern die Zeitzonen falsch eingestellt, und werden dann durch falsche Zeiteinstellungen kompensiert. Wenn also ein System auf 16:00 MEST eingestellt sein sollte (Mittleuropäische Sommerzeit), kommt es nicht selten vor, dass es auf UTC (Universal Time) oder GMT (Greenwich Mean Time) steht, und dann 14:00 zeigen müsste, der Administrator es dann aber auf 16:00 UTC stellt, um "16:00 Uhr zu sehen, und die Uhr damit um zwei Stunden falsch geht. Windows-Systeme sind berüchtigt für Verwerfungen zwischen der Hardware-Uhr und der Systemzeit.
13. Erfahrungsgemäß (Wissensstand 2009) werden solche Zeitzoneneinstellungen und -fehler bei forensischen Untersuchungen und IP-Abfragen durch die Polizei nicht richtig oder gar nicht berücksichtigt.

Eine Abweichung von 1 oder 2 Stunden muss bei einer langfristig zugewiesenen IP-Adresse noch nicht zwangsläufig zu Fehlern führen, bei dynamischem NAT führt es aber zu völligen Fehl-Antworten.

3.1.2.2.3 Dynamisches Port-NAT mit langer Persistenz Man könnte auf den Gedanken kommen, ein dynamisches NAT mit sehr langer Persistenz der Zuordnung der NAT-Ports zu bauen, die gegenüber der erreichbaren Genauigkeit der Uhren hinreichend lange besteht, um die Ungenauigkeiten zu überbrücken.

Auch das würde aber den Zweck eines NAT zumindest teilweise vereiteln, weil es den Nutzen begrenzt.

Zudem müsste man eine verbindliche und verlässliche Genauigkeit der Uhren herstellen.

Es darf bezweifelt werden, dass die IT-Technik sich dabei so weit nach deutschem Gesetzeswunsch richtet und richten muss, dass solche Besonderheiten berücksichtigt werden.

3.1.2.3 Technische Umsetzbarkeit

Davon ganz abgesehen wären es enorme Datenmengen, die hier anfallen, und es ist zweifelhaft, ob die bestehenden NAT-Geräte der Provider überhaupt in dieser Informationsdichte aufzeichnen können.

Zwar können das größere Firewall-Systeme, die Firmennetze absichern, aber schon da sind erhebliche Anforderungen an Rechenleistung und Speicherplatz erforderlich.

Firewall- und NAT-Geräte, die einen solchen Datendurchsatz erreichen, dass sie einen ganzen Internet-Provider bedienen können, machen das normalerweise nicht per Software, sondern in Hardware. Es ist fraglich, zumindest nicht selbstverständlich, dass

diese dies auch in dieser Dichte protokollieren können, denn die Zahl der Verbindungen, die ein ganzer Internet-Provider herausleiten muss, ist beträchtlich.

3.1.3 Datenschutzrechtliche Hindernisse

3.1.3.1 Unzulässige Verkehrsprotokollierung

Bisher, bei normalen IPv4-Auskunftsersuchen, musste die Polizei die strafbare Handlung beobachten oder aus Logs ermitteln. Man fand also beispielsweise einen Zugriff auf den Kinderpornoserver K zum Zeitpunkt Z von der IP-Adresse A und fragte dann:

Wer hatte zum Zeitpunkt Z die IP-Adresse A?

Hat man aber die kompletten NAT-Zuordnungen protokolliert – und damit weitaus mehr Daten als nur bei der IP-Adress-Zuordnung – werden gänzlich andere Anfragen möglich, ob im Wege des Auskunftersuchens oder der Beschlagnahme:

Der Kinderpornoserver K hat die IP-Adresse a.b.c.d. Listen Sie uns alle Ihre Kunden samt den Zeitpunkten auf, die schon einmal auf diese IP-Adresse zugegriffen haben.

Und das ist nach EU-Recht und der EuGH-Entscheidung unzulässig.

In Verbindung mit dem unten in Abschnitt 5.4 ab Seite 53 geschilderten Missbrauch von hoheitlichen Befugnissen durch heimliche unzulässige Abfragen aus politischen Motiven ergibt sich daraus ein völlig unvertretbares Missbrauchspotential.

Denn genauso könnte man – heimlich – abfragen: *Listen Sie uns alle Kunden, die das Blog von Hadmut Danisch lesen.*

Man muss nur aus den NAT-Logs diejenigen heraussuchen und auflösen, bei denen die IP-Adresse meines Blogs als Ziel-IP enthalten ist.

3.1.3.2 Verletzung des Post- und Fernmeldegeheimnisses (Art. 10 GG)

Im Internet gibt es keine „Portnummern“. Sie kommen im Internet-Protokoll nicht vor.

Sie kommen erst in den Nutzlast-Protokollen wie TCP und UDP vor.

In der Netzwerktechnik und anderen Bereichen der Informatik verwendet man sogenannte „Schichtenmodelle“, um die verschiedenen Funktionen wie Hierarchieebenen oder Zwiebelschalen zu trennen und zu abstrahieren.

Bei Netzwerken kommt dabei in der Regel das ISO-OSI-Modell mit 7 Schichten zur

Anwendung, obwohl es zwar gut, aber nicht exakt auf das Internet passt, weil es erst nach der Erfindung des Internet eingeführt wurde und zum – erfolglosen und längst weitgehend gestorbenen – Konkurrenzmodell der ISO-Protokolle gehörte. Nach dieser Einteilung liegt das Internet-Protokoll auf Schicht 3, während TCP und UDP auf Schicht 4 liegen. Grundsätzlich aber wurde auch schon bei der Konstruktion des Internet in Schichten gedacht, das ist Stand der Technik in der Informatik.

IP einerseits und TCP und UDP andererseits sind deshalb verschiedene Protokolle. TCP und UDP sind Nutzlast und nicht Teil des Internet-Protokolls.

In der Analogie eines Paketes: Die IP-Adresse eines Paketes steht als Adresse außen drauf, während die Port-Nummer bereits zum Inhalt des Paketes gehört. Es verhält sich nicht, wie gelegentlich intuitiv-laienhaft, aber irreführend und falsch beschrieben wird, dass die Port-Nummer eine Art Nebenstellenummer als Teil einer Telefonnummer sei.

Den Internet-Provider geht grundsätzlich nur der IP-Header eines IP-Paketes etwas an, weil er dies zum Transport braucht (Schicht 3). Alles oberhalb von Schicht 3 ist Nutzlast, und geht den Provider nichts an. Ein Zugriff ist eine Verletzung des Post- und Fernmeldegeheimnisses. Und damit auch die Protokollierung von Port-Nummern.

Jeder Zugriff des Providers auf Informationen in der Nutzlast fällt unter den Begriff der „Deep Packet Inspection“ und ist damit eine Verletzung des Fernmeldegeheimnisses.

Prinzipiell ist damit auch das Provider-NAT, wie oben beschrieben, eine solche Verletzung, aber gerade noch vertretbar, weil das Problem der „IPv4 address exhaustion“ anders nicht mehr zu lösen ist, und die fraglichen Daten nur für die Dauer der Verbindung, meist nur Millisekunden oder Sekunden, mitunter auch Stunden, im NAT-System gehalten und zu keinem anderen Zweck verwendet werden.

Werden diese aber, wie hier, protokolliert und über die Nutzungsdauer hinaus aufbewahrt, für andere Zwecke als die Erbringung der Telekommunikation verwendet, liegt darin eine erhebliche Verletzung des Fernmeldegeheimnisses.

Es lässt sich dabei auch nicht argumentieren, dass man nur analog der IP-Adressen bei ausreichender Verfügbarkeit ohne NAT protokolliert, um zum selben Ergebnis zu kommen. Denn die IP-Adresse wird für einen längeren Zeitraum zugewiesen und sagt nichts über die konkrete Nutzung, den konkreten Verkehr.

Die NAT-Protokollierung tut dies aber. Denn die NAT-Daten müssen die 7-Tupel jeder einzelnen TCP-Verbindung speichern und damit genaue Verbindungsdaten über jede einzelne Webseite, die besucht wurde, also – anlasslos – die gesamten Aktionen im Internet aufzeichnen. Das wäre eine totale Überwachung jeder einzelnen Aktion. Es würde Auskunft geben, wann jemand zuhause, wach, im Internet ist, welche Webseiten er besucht.

Hat man eine solche Liste, kann man damit eben nicht nur die von der CDU/CSU-Fraktion dargestellte Auflösung der Zugriffe auf Webseiten betreiben, sondern umgekehrt auch alle Aktionen eines Anschlussinhabers über einen Zeitraum auflisten,

auch wenn die Angaben zum Server damit auf IP-Adressen beschränkt sind und keine Hostname oder URLs o.ä. enthalten. Es läuft auf eine komplette Verkehrsaufzeichnung zwar nicht der Inhalte, aber der Verbindungen hinaus.

Das Ansinnen der CDU/CSU ist damit verfassungs- und EU-rechtswidrig und geht weit über eine Vorratsdatenspeicherung hinaus.

Die Begründung im Antrag, dass

Entgegen der Speicherung von sonstigen Verkehrs- und Standortdaten handelt es sich dabei um einen deutlich geringfügigeren Eingriff in die Grundrechte.

ist dann falsch, wenn man, wie es im Antrag ausdrücklich gefordert wird, auch die Portnummern im dynamischen NAT speichert, weil dann jede einzelne TCP- und UDP-Verbindung protokolliert werden muss. Es widerspricht sich.

3.2 Die Entscheidung des EuGH

Aus dem Antrag der CDU/CSU-Fraktion:

Deshalb müssen die durch den Europäischen Gerichtshof eröffneten Möglichkeiten vollumfänglich genutzt werden.

[...]

Der Europäische Gerichtshof hat am 20. September 2022 in den verbundenen Rechts-sachen C-793/19 (SpaceNet) und C-794/19 (Telekom Deutschland) gesetzgeberische Handlungsmöglichkeiten aufgezeigt. Er hat u. a. entschieden, dass das Unionsrecht nationalen Rechtsvorschriften nicht entgegenstehe, die

- zum Schutz der nationalen Sicherheit, zur Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit einen auf das absolut Notwendige begrenzten Zeitraum eine allgemeine und unterschiedslose Vorratsspeicherung der IP-Adressen, die der Quelle einer Verbindung zugewiesen sind, vorsehen;
- zum Schutz der nationalen Sicherheit, zur Bekämpfung der Kriminalität und zum Schutz der öffentlichen Sicherheit eine allgemeine und unterschiedslose Vorratsspeicherung der die Identität der Nutzer elektronischer Kommunikationsmittel betreffenden Daten vorsehen;
- es zur Bekämpfung schwerer Kriminalität und zum Schutz der nationalen Sicherheit gestatten, den Betreibern elektronischer Kommuni-

kationsdienste aufzugeben, während eines festgelegten Zeitraums die ihnen zur Verfügung stehenden Verkehrs- und Standortdaten umgehend zu sichern. Der durch den Europäischen Gerichtshof ausdrücklich festgestellte gesetzgeberische Handlungsspielraum zur Speicherung von IP-Adressen muss nun unverzüglich genutzt werden.

Auch das ist so nicht haltbar, die Formulierungen sind suggestiv verändert.

3.2.1 Keine „Eröffnung von Möglichkeiten“

Der EuGH hat keine „Möglichkeiten eröffnet“, sondern lediglich festgestellt, wann die Europäische Datenschutzrichtlinie nationalen Vorschriften für eine Vorratsdatenspeicherung entgegensteht und wann nicht.

Eine Eröffnung von Vorratsdatenspeicherung gegen nationales Recht ist da nicht gegeben. Das ist keine EU-Erlaubnis. Andere Rechtshindernisse werden dadurch nicht beseitigt.

3.2.2 Kinderpornographie keine ausreichende Bedrohung

Es ist festzustellen, dass der EuGH feststellt, dass EU-Datenschutzrecht die Vorratsdatenspeicherung im Allgemeinen verbietet, dann aber einen Katalog von besonderen Ausnahmen davon mit besonderen Bedingungen aufstellt, der Ausnahmen vom Verbot rechtfertigt.

Darin findet sich durchgängig als Bedingung die Formulierung

zum Schutz der nationalen Sicherheit, zur Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit

wobei in einem Ausnahmebestand nur von Kriminalität, statt von schwerer Kriminalität die Rede ist und in der Kürze der mir zur Verfügung stehenden Zeit nicht zu klären war, ob Absicht oder Versehen. Gegen eine Absicht spricht aber, dass dann der Tenor des allgemeinen Verbots mit Ausnahmen unter besonderen Bedingungen hinfällig wäre.

Es erscheint jedoch überaus fraglich, ob der bloße Besitz von Kinderpornographie in Form von Dateien auf einem Computer bereits eine so schwere Straftat ist, dass die vom EuGH gezogene Grenze überschritten ist. Denn der EuGH gibt eine Schwelle vor, die mit der *nationalen Sicherheit und der Verhütung schwerer Bedrohungen der öffentlichen Sicherheit* auf einer Stufe stehen müssen.

Eine derartige Bedrohung der Allgemeinheit, wie sie der EuGH voraussetzt, ist für mich aus dem bloßen Besitz oder Verschaffen von Kinderpornographie – auf einem Computer gespeicherte Dateien, das Anordnen von Nullen und Einsen – beim besten

Willen, so verwerflich und geächtet dies auch sein mag, nicht zu entnehmen. Zwar stellt § 184b Absatz 3 StGB schon den Besitz unter ein Strafmaß von einem bis zu fünf Jahren Haft und ordnet ihn damit in den Verbrechen ein. Die Beweggründe sind aber moralischer und politischer Natur und auf Schutz des Einzelnen, nämlich der betroffenen Kinder ausgelegt.

Man kann keine Bedrohung fingieren, indem man eine Straftat, die für sich betrachtet keine Bedrohung darstellt, mit hohem Strafmaß belegt. Der EuGH verlangt ernste Bedrohungen, nicht hohe Strafen.

Der EuGH sagt ausdrücklich, dass EU-Recht die Vorratsdatenspeicherung grundsätzlich verbietet, und nur unter gewissen Bedingungen Ausnahmen zulässt. Das Vorliegen dieser Ausnahmebedingungen muss sachlich und nachvollziehbar begründet werden. Man kann das Vorliegen nicht fingieren, indem man sich einfach irgendeine, willkürlich mit hoher Strafe belegt aber ansonsten nicht unter die Bedingungen fallende Straftat als Vorwand vorschiebt.

Dies gilt umso mehr, als der § 184b ja nicht nur den Besitz *echter* Kinderpornographie von *echten* Kindern, sondern auch solche Darstellungen unter Strafe stellt, denen kein konkreter Kindesmissbrauch zugrundeliegt und die nur gezeichnet oder durch Bildmanipulation oder Künstliche Intelligenz erzeugt wurden, also gar niemand unmittelbar geschädigt wird, das Verbot also nur noch einem abstrakten, mittelbaren Schutz dient.

Es steht Deutschland als souveränem Staat frei, Kinderpornographie als verwerflich einzustufen und mit hohem Strafmaß zu belegen. Das kann man tun, es spricht nichts dagegen. Darüber besteht auch zweifellos ein gesellschaftlicher Konsens und es entspricht im demokratischen Sinne dem Wunsch einer überragenden Bevölkerungsmehrheit. Aber dieser Akt der Gesetzgebung legt nur das Verbot und das Strafmaß fest. Er konstituiert keine Bedrohung im beschriebenen Ausmaß. Der Gesetzgeber kann nur Gesetze machen, aber keine Bedrohungen herstellen.

Anders ausgedrückt:

Der EuGH setzt die Schwere der Bedrohung als Bedingung für den Eingriff in den Datenschutz an. Der Antrag dagegen versucht rein durch Rhetorik, aber ohne Begründung, die Höhe des Strafmaßes und die Empörungsdichte an deren Stelle zu setzen.

Das ist medientauglich, aber nicht revisionsfest. Der Antrag ist ein Täuschungsmanöver. Er verletzt das EuGH-Urteil und hält der Überprüfung nicht stand.

Damit will ich ausdrücklich nicht sagen, dass es keine Bedrohungen Deutschlands und seiner Sicherheit gibt, die eine Vorratsdatenspeicherung nach dem EuGH-Urteil rechtfertigen. Aber dieser Antrag genügt dem nicht.

Ob die Herstellung von Kinderpornographie ausreichend ist, kann ich in der knappen Zeit, die mir zur Verfügung steht, nicht klären, und das ist hier auch nicht Teil des Antrages und damit des Auftrages. Dazu fehlen Informationen zum Umfang und Ausmaß,

außerdem zur Abgrenzung.

Ich halte es beispielsweise für überaus problematisch und im Sinne der Begründung schwerer Kriminalität für kontraproduktiv, dass man Kindern und Jugendlichen die Verbreitung von Kinder- und Jugendpornographie vorwirft, wenn sie sich gegenseitig Nacktfotos *von sich selbst* schicken, weil man grundsätzlich keine Straftaten gegen sich selbst begehen kann. Auch sehe ich darin keine substantielle Bedrohung der Gesellschaft. Ich halte dieses gegenseitige Zusenden von Nacktfotos in der Schulklasse für eine doppelte enorme Dummheit, erstens der Kinder und zweitens des Gesetzgebers, diese zu betrafen. Ich halte es für völlig verfehlt, Kindern und Jugendlichen wegen solcher Jugendummheiten Straftaten anzuhängen.

Ebenso fragwürdig ist es, gezeichnete oder KI-erzeugte Bilder, selbst wenn sie nur Kinderpornographie-ähnlich sind und fiktive Phantasiewesen zeigen, auf eine Stufe mit tatsächlichem Kindesmissbrauch und gequälten Kindern zu stellen. Denn damit verharmlost man die Straftat und nimmt sich die Möglichkeit, die Schwere der Tat herauszustellen.

Und durch diese Unschärfen und Widersinnigkeiten nimmt sich der Gesetzgeber auch selbst das nötige Gewicht des Straftatbestandes, wenn die Grenzen derart in Bereiche verschwimmen, die nicht mehr glaubwürdig sind und die sich dem Gefühl aussetzen, dass der Staat hier unzulässig in die Handlungsfreiheit aus Artikel 2 Abs. 1 Grundgesetz eingreift, der als Grenze hauptsächlich die Rechte *anderer* vorsieht, aber Handlungen hart bestraft, die keinen anderen betreffen, und damit dann ins Post- und Fernmeldegeheimnis eingreifen will.

Auf weitere Probleme in diesem Zusammenhang verweise ich im Abschnitt 6.3 auf Seite 62.

Man sollte sich dringend erst einmal um die Schärfung des Straftatbestandes selbst kümmern, bevor man derartige Kapriolen zu dessen Strafverfolgung unternimmt. Sonst ist man nicht in der Lage nachzuweisen, dass die Schwere der Bedrohung, die der EuGH fordert, tatsächlich vorliegt.

Solange man 14-Jährige verfolgt, die Bilder von sich selbst verschicken, und Phantasielbilder tatsächlich erfolgter Gewalt gleichsetzt, wird man die Schwere des Straftatbestandes nicht halten können.

Es ist auch nicht nachvollziehbar, dass man 14-Jährigen gestattet, sich mit Geschlechtsumwandlungen lebenslang körperlich zu ruinieren und unfruchtbar zu machen, 16-Jährigen das Wahlrecht geben will, aber beiden Straftaten unterstellt und sie als Sexualstraftäter führt, wenn sie ihren Freunden aus Jux ein Nacktfoto von sich selbst schicken. Das ist willkürlich.

Dieser Gesetzgeber ist nicht in der Lage – und auch nicht willens – eine konsistente Rechtslage herzustellen.

3.3 Trugschluss „Rechtssicherheit“

Der Antrag unterstellt, schon im Titel, dass durch eine Vorratsdatenspeicherung eine „rechtssichere“ Speicherung von IP-Adressen möglich wäre.

Das ist aus mehreren Gründen falsch.

3.3.1 Es gibt keine „Rechtssicherheit“ im Internet

Man kann IP-Adressen nicht „rechtssicher“ speichern, weil das Internet selbst nicht „rechtssicher“ ist, und auch nie dafür gebaut wurde. Das ist nicht Teil der Spezifikation und damit auch keine durch Konstruktion und Aufbau hergestellte Eigenschaft.

Das Internet ist nicht dafür gebaut, rechtssicher zu sein. Es wurde nicht als rechtssicher bestellt, und deshalb auch nicht als rechtssicher geliefert. Insbesondere wurde es nicht an deutschen Rechtsvorstellungen ausgerichtet.

Die „rechtssichere Speicherung von IP-Adressen“ ist nur Juristenfolklore.

Wäre das Internet rechtssicher, müsste man nicht großem Aufwand zusätzliche Maßnahmen treffen, um Rechtssicherheit herzustellen.

3.3.2 Fälschung der IP-Adresse

Man kann IP-Adressen nicht rechtssicher speichern, weil sie (ohne zusätzliche Maßnahmen) nicht authentisch sind.

Das Internet-Protokoll leistet keine Authentizität, und es ist auch keine solche spezifiziert.

Es gibt auf IP-Ebene keinerlei Sicherstellung darüber, dass die IP-Adresse, die beim Server als Absender ankommt, auch mit der übereinstimmt, die vom Client kam.

Lediglich die Sequence-Number im TCP, die ein Angreifer nicht wissen kann, und der Umstand, dass der echte Inhaber der IP-Adresse ein Ablehnungspaket senden würde, wenn die IP-Adresse lediglich gefälscht wäre, und die Daten den Angreifer nicht erreichen könnten, bieten ein gewisses Maß an Sicherheit gegen gefälschte IP-Adressen, *wenn und solange Integrität für das Routing der Rückrichtung besteht und keine Angriffe auf den Schichten 1 und 2 im Zielnetz stattfinden*. Auch das ist nicht sichergestellt und nicht nachträglich überprüfbar.

Kurioserweise erwähnt die CDU/CSU-Fraktion selbst die Möglichkeit des Provider-NAT, ohne aber intellektuell zu verstehen, dass das ja eine Änderung der IP-Adresse durch einen Dritten – in der Sicherheitstechnik strukturell eine „man in the middle“-Attacke – ist. Obwohl die CDU/CSU selbst schreibt, dass es

Systeme gibt, die im Internet IP-Adressen austauschen, versteht sie es nicht und hält an der Fiktion und dem Postulat einer rechtssicheren Speicherung fest.

Im Internet sind zwischen den beiden Seiten einer Kommunikation eine Vielzahl von Systemen in vielen unterschiedlichen Ländern mit unterschiedlichen Rechtssystemen involviert, die in die IP-Adressen und das Routing eingreifen können.

3.3.3 Fehler kommen vor

Das Internet ist nicht fehlerfrei. Es kommen immer wieder Fehler, Fehlkonfigurationen und dergleichen vor.

3.3.4 Angriff auf Router

Ich habe 1999 firmenintern eine Prozedur zur Fehlerbehebung entwickelt, weil die Abteilung, die Firewall-Hardware an Kunden verschickte, die wir dann zu konfigurieren hatten, Fehler gemacht und diese mit falschen, fremden, und deshalb nicht erreichbaren Internet-Adressen ausgeliefert hatte. Um Aufwand und Spesen für Reisen zum Kunden und peinliche Entschuldigungen zu ersparen, habe ich eine Vorgehensweise spezifiziert, um mittels GRE-Tunneln zwischen einem Linux-Rechner und einem CISCO-Router beim Kunden den Verkehr für die falschen IP-Adressen zu ermöglichen, bis die Maschinen auf die richtigen IP-Adressen umkonfiguriert waren.

Dasselbe Prinzip taugt auch zum Angriff, falls man Kontrolle über einen Router auf der Wegstrecke hat. Man kann damit jede beliebige IP-Adresse vorgaukeln.

3.3.5 Beispiel BGP Hijack, ARP Spoofing u.ä.

Es gibt eine Vielzahl von Angriffen gegen das Routing, etwa gegen Routing-Protokolle oder innerhalb von LANs durch gefälschte Router-Advertisings, falsche ARP-Responses, ICMP-Redirects, Router-Advertisings, DHCP-Spoofing und ähnliches. Solche Angriffe habe ich vor 20 Jahren in Sicherheits-Workshops live vorgeführt. *Damals war das noch neu, vor 20 Jahren wussten das noch nicht alle.*

Solche Angriffe gibt es auch im großen Stil auf Internet-Ebene. Beispielsweise landete im März 2022 der Verkehr zu Twitter (USA) durch einen BGP-Fehler etwa 45 Minuten lang bei einem russischen Internet-Provider statt bei Twitter. Zwar wurde letztlich nicht klar, ob es ein Fehler oder ein absichtlicher Angriff war, aber ein absichtlicher Angriff hätte auf dieselbe Weise funktioniert.

Stellen Sie sich vor, ein Angreifer leitet an einem hohen Feiertag die IP-Adressen des Bundestags für wenige Sekunden um, vielleicht auch nur in einem kleinen Teil des Internet, um mit den IP-Adressen unliebsamer Politiker Kinderpornos herunterzuladen,

um sie damit zu erledigen. (Stichwort: Tauss, Edathy) Aus Sicht des Bundestages würde das, wenn überhaupt bemerkt, höchstens für einen normalen Internet-Ruckler gehalten. Monate später würde mit „beweissicheren“ IP-Adressen ein Verfahren eröffnet.

3.3.6 Unsicheres Logging

Auch ein rechtssicheres Logging ist im Allgemeinen nicht gegeben.

Das liegt schon daran, dass über die Integrität des loggenden Serversystems nichts bekannt ist. Es gibt heute praktisch keine vollständig angriffssichere Serversoftware und kein hinreichend sicheres, geeignetes Betriebssystem mehr, und viele Server sind nicht aktuell und nicht sehr gepflegt. *Woher will man wissen, ob die Software tatsächlich die wahrheitsgemäße IP-Adresse eines echten Vorgangs geloggt hat, und nicht falsche Log-Einträge erzeugt hat?*

Woher weiß man, dass die Log-Dateien tatsächlich das zeigen, was der Server geloggt hat, also Integrität herrscht, und nicht jemand böswillig falsche Log-Einträge hinzugefügt oder bestehende verändert hat? Was hindert einen Administrator oder Angreifer daran, in einer Logdatei IP-Adressen auszutauschen? Oder die Programmbibliothek für das Logging zu manipulieren?

Ich habe vor 20 Jahren schon in Sicherheitsworkshops live vor Publikum vorgeführt, wie ich auf triviale Weise falsche Log-Einträge erzeugen kann, ohne den Server selbst zu kompromittieren. Der Server war so eingestellt, dass er versucht, IP-Adressen nach DNS in Hostnamen aufzulösen, und wenn das nicht funktioniert, die IP-Adresse selbst zu loggen.

Ich habe von der IP-Adresse 1.2.3.4 aus zugegriffen, ihr aber im DNS die Rückwärtsauflösung in den Hostnamen „5.6.7.8“ eingetragen. Der IP-Adresse also einen DNS-Namen zugeordnet, der nur so aussieht wie eine IP-Adresse. In den Logfiles stand dann der Hostname „5.6.7.8“, sah aber so aus, als hätte man von der IP-Adresse 5.6.7.8 zugegriffen. Solche Konfigurationsfehler sollten heute nicht mehr vorkommen, weil die DNS-Auflösung beim Logging abgeschaltet sein sollte und solche Rückwärtsauflösungen durch anschließende Vorwärtsauflösungen verifiziert werden müssten, aber sicher ist das nicht.

Und selbst wenn das Logging heute zuverlässig ist – es werden fast jeden Tag Systemaktualisierungen eingespielt. Das kann morgen schon anders und übermorgen schon wieder anders aussehen.

3.3.7 „Jeder kann programmieren!“

In diesem Zusammenhang ist daran zu erinnern, dass – auch in Deutschland politisch propagiert und durchgedrückt – Slogans wie „jeder kann programmieren“ publiziert werden, durch Quoten kompetenzdefizitäre Quereinsteiger installiert werden, Political Correctness und „Codes of Conduct“ Kritik verbieten und es unmöglich machen, minderwertigen Code abzulehnen.

Das Ergebnis ist eine signifikant sinkende Softwarequalität.

3.3.8 Unbeherrschbarkeit der Software

Software hat heute einen Grad der Komplexität erreicht, der nicht mehr zu beherrschen ist. Moderne Softwaresysteme setzen den Code aus Flickwerk von hunderten oder tausenden kleinen Bibliotheken aus allen Bereichen der Welt zusammen, und keiner weiß mehr, was alles an Stückchen in seiner Software steckt und darin eigentlich passiert.

2021 gab es im vermeintlich sicheren Java-System, auf dem viele Serverdienste weltweit beruhen, ein Sicherheitsleck von katastrophalem weltweitem Ausmaß: Log4Shell.

Miserable Software aus verschiedenen Quellen sorgte erst im Zusammenspiel in einer nicht vorhergesehenen Weise zu einem Totalausfall der Sicherheit. Server-Dienst, die in Java geschrieben waren, verwendeten in der Regel die Logging-Funktionen von Java. Diese unterlag einer funktionalen Stringsstitution. Weil der Angreifer aber Teile der Daten, die geloggt werden, frei bestimmen konnte und die Stringsstitution dazu führen konnte, dass Programmcode von einem externen LDAP-Server nachgeladen wird, und es hat über Jahre niemand bemerkt, weil die Komplexität zu hoch war, die Programmstücke von verschiedenen Leuten kamen, die Dokumentation unzureichend und zu unübersichtlich war, und niemand das unheilvolle Zusammenspiel und schon gar nicht den fatalen Fehler bemerkt hat, dass Programmcode von beliebigen LDAP-Servern, und damit auch einem Server des Angreifers, heruntergeladen und ausgeführt wird.

Und solche Logging-Systeme will man hier für „rechtssicher“ halten?

3.3.9 Unsichere Endgeräte

Es gibt heute im Allgemeinen keine sicheren Endgeräte mehr, insbesondere nicht im privaten Haushaltsbereich. Die Dichte der Angriffe ist enorm hoch. Ich selbst bekomme durchschnittlich mindestens einen Angriffsversuch per Mail-Zusendung, in denen man versucht, mich auf irgendeine Weise dazu zu bringen, Malware (meist für Windows) auszuführen. In aller Regel werden damit Systeme installiert, mit denen man den ganzen Rechner samt Netzwerkverkehr fernsteuern kann. Der Angreifer kann damit mit der IP-Adresse seines Opfers auftreten und in deren Namen, deren IP-Adresse, wenn

er sie findet auch mit der Kreditkarten- oder Kontonummer Dinge bestellen – oder eben Kinderpornos herunterladen.

3.3.10 Ende der Route?

Nur weil eine IP-Adresse eines Haushaltes angegeben ist, bedeutet das noch lange nicht, dass das das Ende der Route war, die die IP-Pakete nahmen. Wenn sich ein Angreifer beispielsweise Zugang zum Wohnungsrouter oder zur Unternehmensfirewall verschafft, und beispielsweise einen VPN-Tunnel einrichtet und später wieder löscht, werden die Pakete nach außen weitergeroutet.

Jeder Radiowecker, jeder Fernseher, jeder Kühlschrank mit Internetanschluss und unsicherer Firmware könnte heute als Relay missbraucht werden, um einen Kinderporno- oder sonstigen strafbaren Netzwerkzugriff als von dieser IP-Adresse vorgenommen vorzugaukeln.

Man muss nur in seinen Spam-Folder sehen, um unzählige Spam-Mails zu finden, die von „gehijackten“ Systemen ohne Wissen ihrer Nutzer und Eigentümer versandt worden sind.

3.3.11 „Cyberkrieg“

Es ist geradezu grotesk, dass die Bundesregierung gerne warnt, dass wir im „Cyberkrieg“ seien und „Cyberarmeen“ brauchten, wiewohl man das Wort „Cyber“ anscheinend auch sehr liebt, die sofort zurückschießen sollten, und dass wir gerade jetzt, in Zeiten des Ukraine-Krieges und des hochkochenden Wirtschaftsstreits mit China steigenden Gefahren durch „Cyberangriffe“ ausgesetzt wären.

Das ist soweit richtig.

Seltsamerweise aber geht man dabei immer davon aus, dass „Cyberkrieger“ ganze Kraftwerke abschalten oder alles Wasser ablassen.

Seltsamerweise aber kommt man nicht auf die Idee, dass eine feindliche Macht, die einen „Cyberkrieg“ führt, gezielt einzelne Personen abschießen könnte, indem sie vorgaukelt, diese Person habe auf Kinderpornos zugegriffen, indem sie entsprechendes Material auf dessen Rechner kopiert und dafür sorgt, dass es passende Log-Einträge mit der IP-Adresse gibt und diese gefunden werden. Oder eben, um die Zielperson zu erpressen.

Das ist umso fragwürdiger, als es in Zeiten des kalten Krieges eine bekannte Masche war, Politiker und Geschäftsleute in eine „Venusfalle“ zu locken, bei Sex mit Agentinnen zu filmen und hinterher zu kompromittieren oder zu erpressen.

Würde man heute einen Politiker beim Sex mit einer Fremden filmen und die Aufnah-

men veröffentlichen, würde vermutlich nicht mehr passieren, als dass er für gute Performance beachtliche viele Likes bekäme. Es ist naheliegend, dass man diese Angriffsmethode heute auf Kinderpornographie hocheskaliert hat. Der Angriff folgt der gesellschaftlichen Tabuisierung.

Es ist nicht nur bekannt, dass auf der Sex-Insel von Jeffrey Epstein die Räume mit versteckten Videokameras geradezu gespickt waren, also von jedem, der sich zum Sex mit Minderjährigen auf die Insel begab, danach kompromittierende Videos entstanden. Es ist ebenfalls bekannt, dass FBI und CIA ausgehobene Webserver mit Kinderpornos nicht abschalten, sondern weiterbetreiben.

Dazu kommt, dass gängige Betriebssysteme heute so eng und dicht mit der „Cloud“ verbunden sind, dass ein Laie dies nicht mehr trennen kann, oder die Trennung zu erheblichen Funktionsbeeinträchtigungen führt. Fast jedes Handy lädt heute alles und jedes in die Cloud hoch und auch wieder runter.

Es ist damit für Cloud-Betreiber ein Leichtes, ohne Wissen und Mitwirkung des Inhabers Kinderpornos auf jedes Gerät zu kopieren.

3.3.12 Antifa

Wir haben heute eine enorme Zahl von „Aktivisten“, oft in scheinbar unabhängigen, aber manchmal von der Bundes- oder einer Landesregierung beauftragten und bezahlten „NGO“, deren Ziel es ist, Kritiker zu diffamieren.

Ich habe das selbst in den letzten Jahren erlebt: Diffamierung, Drohbriefe, Beschimpfungen an den Arbeitgeber, Beschimpfungen im Internet, Schmiererei am Haus, Diffamierungsschreiben in die Briefkästen der Nachbarschaft. Sabotage von Geschäftsverbindungen und Bankkonten.

Jede Art von Diffamierung wird eingesetzt, nicht nur deckungsgleich mit der „Zersetzung“-Methodik der Stasi, sondern zweifellos von denen übernommen.

Es steht außer Frage, dass man auch den Zugriff auf Kinderpornografie vortäuschen würde, um jemanden politisch und gesellschaftlich zu erledigen.

3.3.13 Naive Vorstellung

Die Vorstellung, dass IP-Adressen überhaupt im Internet „rechtssicher“ zu erfassen und zu speichern wären, ist damit naiv.

3.4 Mangelhafte Qualität des Antrags

Ich kann nicht umhin, meiner Missbilligung des Antrags Ausdruck zu verleihen. Es ist mir unverständlich, warum man einen solchen Antrag stellt, und ihn nicht vorher fraktionsintern durch Sachkundige prüfen und bereinigen lässt.

Dies umsomehr, als dies ja nicht meine erste Qualitätsrüge gegenüber der Fraktion der CDU/CSU ist.

Ich war 2009 als Vertreter eines großen Interner-Anbieters zunächst im Familienministerium und dann im Bundeskriminalamt in die Diskussion um die Kinderpornosperrung Ursula von der Leyens involviert.

Das Bundeskriminalamt hat damals die Internetsperre abgesagt, nachdem ich dort aufzeigte, dass die vom Ministerium und Frau von der Leyen verfolgte Linie nicht nur fehlerhaft und nicht umsetzbar ist, sondern auf einem katastrophal falschen Verständnis vom Internet beruhte. Man hielt das DNS für den Verteildienst von Webseiten, die Internet-Provider für eine Art Webseiten-Broker, und Webseiten für monolithische Dokumente. So, wie früher BTX aufgebaut war. Man dachte, man könnte Webseiten aus dem DNS einfach löschen, womit sie dann weg wären, und könnte den Internet-Providern wie einem Einzelhändler einfach untersagen, gewisse Webseiten durchzuführen. Man hatte überhaupt gar nichts verstanden, aber versucht, etwas durchzusetzen, indem man alle als „krachend unfähig“ beschimpfte (214. Sitzung des Deutschen Bundestages vom 26. März 2009), die nicht lieferten, was man wollte.

Schon damals hatte ich die Vorgehensweise der CDU/CSU in aller Deutlichkeit gerügt, weil man keine Internetgesetze machen kann, wenn man nicht wenigstens über ein gewisses Minimum an Sachkunde und Kenntnis der tatsächlichen Abläufe verfügt. Man hatte damals versucht, die Situation politisch und von der Leyen vor einer Blamage zu retten, indem man öffentlichkeitswirksam einen – substanzlosen – „Vertrag“ mit den Providern schloss, obwohl die Kinderpornosperrung längst abgesagt und tot war.

Heute, 14 Jahre später, hat sich die Situation nicht wesentlich gebessert.

Das ist umso erstaunlicher, als der Antrag immer noch nach der Handschrift Ursula von der Leyens aussieht und sich in Versuche der EU, eine Chatkontrolle zu etablieren, einfügt.

4 Insuffizienz der Staatsgewalten

Der Staat türmt einen immer größeren Stapel an Anforderungen, Pflichten, Berichtszwängen, Formalismen auf, die immer schwieriger zu erfüllen sind, und die Unternehmen vor immer größere Aufgaben, Probleme und Kosten stellen.

Dabei ist als symptomatisch zu beobachten, dass vor allem der Gesetzgeber sein Handeln selbst immer weniger versteht, und immer mehr davon auf andere, auf die Judikative, die Exekutive, die Privatwirtschaft, die Bürger abwälzt, obwohl unserer Staatskonstruktion von Demokratie wegen die Pflicht innewohnt, dass der Gesetzgeber alle wesentlichen Entscheidungen selbst treffen muss (Wesentlichkeitstheorie).

In einem demokratischen Staat ist der Gesetzgeber ein Macher. In dieser Bundesrepublik ist der Gesetzgeber ein Wünscher und Verlanger.

Ich werde in diesem Kapitel darlegen, dass der Staat durch eine immer weiter steigende Komplexität des Rechts nicht nur die Bürger und Rechtsverpflichteten, sondern auch sich selbst, alle drei Staatsgewalten, überfordert und nicht in der Lage ist, eine Überwachungsstruktur wie die Vorratsdatenspeicherung noch zu verstehen und adäquat und „rechtssicher“ zu behandeln.

Und das geht nicht nur rechtsstaatlich schief, sondern bleibt dann auch formal an einer höheren Instanz hängen, wenn es diese, wie hier den EuGH, oberhalb von Staaten ausnahmsweise doch gibt.

Ich werde nachfolgend darlegen, warum die drei Staatsgewalten der Bundesrepublik Deutschland nicht in einem Zustand sind, um den hier als Maßstab gewählten verbindlichen qualitativen Anforderungen des EuGH zu genügen.

4.1 Legislative und Regierung

4.1.1 Kinderpornosperrung 2009 (Ursula von der Leyen)

Im Jahr 2009 betrieb Ursula von der Leyen das Vorhaben, eine Kinderpornosperrung im Internet zu etablieren.

Ich war damals in meiner Rolle als Informatiker einer Rechtsabteilung eines großen Internetproviders involviert und beteiligt, und habe festgestellt, erläutert und 2011 auch publiziert, dass Regierung und Bundestag bereits am elementaren Verständnis des

Internet scheiterten und man mit administrativer Gewalt, politischen Intrigen und öffentlicher Beschimpfung durchzusetzen versucht, was nicht umzusetzen ist. In der damaligen 214. Sitzung des Deutschen Bundestages vom 26. März 2009 beschimpfte Ursula von der Leyen alle als „krachend unfähig“, die hinter verschlossenen Türen sagten, dass dies technisch nicht möglich sei. Damit bezog sie sich auf die Sitzung im Bundeskriminalamt vom Februar 2009, in der ich technisch erläutert hatte, warum die Forderungen von der Leyens, ihres Ministeriums, der Regierung und das geplante Gesetzesvorhaben auf einem völligen Fehlverständnis des Internet und technischer Unfähigkeit beruhten.

Man verhielt sich damals als Regierung wie ein ungezogenes, trotziges Kind, das schreit und tobt, wenn es nicht bekommt, was es will.

Auf Seiten des Ministeriums und von der Leyens, auch des Innenministeriums und sogar in Teilen des BKA stellte man sich das Internet in einer Art und Weise vor, die dem früheren BTX nahe kommt, nämlich dass das Internet nur aus der Bereitstellung monolithischer Webseiten bestehe – man hatte nicht einmal verstanden, dass Internet und Webseiten verschiedene Dinge sind – und dachte, dass das DNS ein Art gigantisches Webseitenlager und der Internetprovider eine Art Einzelhändler ist, der diese Webseiten an seine Kunden verkauft, und dem man die Auslieferung bestimmter Webseiten verbieten könne wie einem einem Verlag und einem Buchhändler ein bestimmtes Buch.

Es war völlig unmöglich, dem Ministerium irgendetwas zu erklären, weil sie einfach gar nichts, aber immer alles besser wussten, völlig beratungsresistent und unfähig waren, jemand anderem als sich selbst zuzuhören, und alles aus feministischer Perspektive ohnehin nur für finstere Machenschaften chauvinistischer pornoliebender alter Männer hielt. Es herrschte der Grundsatz, dass Frauen Männern stets mit herablassendem Gehabe ins Wort zu fallen, dasselbe abzuschneiden haben, unfähig zuzuhören. In völliger Unkenntnis festgefahren, durch Feminismus besserwisserisch und völlig informationsresistent gemacht. Die grenzenlose Überheblichkeit blanker Unkenntnis. Der Dunning-Kruger-Effekt als Regierungsform. Ich kenne Zehnjährige, die weit verständiger sind, als es die Regierung damals in dieser Sache war, und denen ich das Internet erklären kann.

Oder, um es mit den Worten und den Darstellungen einer damaligen Gender-Beraterin von der Leyens auszudrücken, von denen sie offenbar stark beeinflusst wurde: „Quality is a myth“. Sachkunde könne von Frauen nicht verlangt werden, weil es sie nicht gibt und nur ein Konstrukt böser Männer zur Ausgrenzung anderer sei.

Außerdem war nicht zu übersehen, dass der Kindesmissbrauch nur als Aufhänger, Vorwand, als rhetorisch-moralische Dampfmaschine dient, es tatsächlich aber um den Aufbau einer viel größeren Zensurmaschine ging.

Während das Bundeskriminalamt zu Anfang der Sitzung noch darauf aus war, den Widerstand der Provider durch Druck und konfrontative Sitzordnung (man hatte eine lange Tisch- und zwei Stuhlreihen darum aufgebaut; auf einer Seite saßen die Provi-

der, auf der anderen Seite direkt gegenüber und in konfrontativer „Manndeckung“ das BKA) weichzuklopfen, sah das BKA nach den Ausführungen der Provider, insbesondere meinen Ausführungen als Informatiker, selbst ein, dass das so nicht funktioniert, wie es verlangt wurde, und sagte die Sperre ab.

Von der Leyen versuchte dann, den Gesichtsverlust zu vermeiden, indem sie die Provider beschimpfte und zum Schein völlig substanz- und wirkungslose „Verträge“ vereinbarte. Faktisch war die Sperre da längst tot und es ging nur noch um Täuschung der Öffentlichkeit (und Rache).

4.1.2 Die frühere Auffassung der Bundesregierung von „IT-Sicherheit“

2008 geriet ich auf einer Konferenz mit dem damaligen Chef des BSI, Udo Helmbrecht, aneinander, weil der – unfreiwillig, gezwungenermaßen, merklich unwohl – konferenzöffentlich das offizielle Verständnis der Bundesregierung unter Angela Merkel von „IT-Sicherheit“ vertrat: *„IT Security Business is growing up.“*

„IT Sicherheit“ sei – völlig sinnentleert und beliebig austauschbar – wenn die Branche für „IT Sicherheit“ steigende Umsätze melde. Nicht mehr, nicht weniger. So kann man jede beliebige Branche behandeln, ohne auch nur im Ansatz verstehen zu müssen, worum es eigentlich geht. Völlig austauschbare Begriffshülsen, die nicht mehr beeinhalteten, als dass für jede Kategorie die gleichnamige Branche Zufriedenheit meldet: X ist, wenn die X-Branche zufrieden ist.

Der Bundesregierung fehlte damals jedes Verständnis für Informationstechnik und das Internet, und sie bezeichnete es 2013 als „Neuland“. Danach faselte man zur Digitalisierung von „Flugtaxi“ und setzte eine Autobahnmaut, De-Mail und einiges andere in den Sand.

Mir liegen heute, 2023, bei Redaktionsschluss keine Informationen vor, dass sich daran wesentlich etwas gebessert hätte.

4.1.3 Die personelle Besetzung des Bundestags als Gesetzgeber

Im Gegenteil sehe ich heute sogar noch eine Verschlechterung.

Im Bundestag wimmelt es von Studienabbrechern, Leuten ohne jede Berufsausbildung und -erfahrung, TikTok-Prinzessinnen, Quotenexistenzen, Lebenslaufartisten, Diätenempfängern, Dissertationsplagiatoren und Ghostwriterbeauftragern. Das parlamentarische Auftreten und Benehmen gleicht oft einem Schulhof, und die Qualität der Reden ist auch nur selten besser. Die schier endlose Liste der entzogenen Doktorgrade und als Ghostwriterwerke aufgeflögerten Bücher sagt wohl alles.

Die Parteien huldigen der Kompetenzlosigkeit geradezu bei der Besetzung ihrer Mandatsposten. Es ist erschreckend, dass in einem so wichtigen Thema wie Digitalisierung

und Vernetzung anscheinend gar keine Kompetenz vorhanden ist.

Das erweist sich dann als fatal, wenn auf Ebene des EU-Rechts in solch wichtigen Dingen wie Eingriffen in den Datenschutz und das Fernmeldegeheimnis gewisse gesetzgeberische Qualitäten gefordert sind, die der Gesetzgeber in seiner derzeitigen Form nicht aufbringt.

Der Bundestag wäre besser beraten, wenn er seine Quoten nicht nach Geschlechtsbefinden und Herkunft, sondern nach Sachkunde, Beruf und Berufserfahrung auslegen würde, um die erforderliche Befähigung herzustellen.

4.1.4 Fehlkonstruktion Auskunftsgestattungsverfahren

Der Gesetzgeber hat – ursprünglich § 101 UrhG und § 14 TMG alte Fassung, inzwischen über § 21 TTDSG – zivilrechtliche Auskunftsansprüche geschaffen, um etwa bei Urheber- oder Persönlichkeitsrechtsverletzungen den Nutzer einer IP-Adresse zu identifizieren. Ich habe 2009 eine Reihe solcher Auskunftersuchen bearbeitet.

Nach meiner Beobachtung werden diese Auskunftsverfahren besonders häufig missbraucht, weil zum Zeitpunkt der Gestattung eine Prüfung des Rechtsanspruches nur schwer möglich ist und praktisch gar nicht erfolgt, und auch die Betroffenen nie davon erfahren. In der Realität heißt das, dass jeder, der auch nur eine Verletzung *behauptet*, Zugriff auf die Daten erhält.

Dass derjenige, der die Auskunft ersucht, dann auch tatsächlich privatrechtlich gegen die Betroffenen vorgeht oder diese überhaupt je davon erfahren, ist in keiner Weise sichergestellt. Es wird nicht geprüft.

Dabei beruht das Gestattungsverfahren auf einer juristischen Hilfskonstruktion, denn verfassungsrechtlich wäre es eigentlich nicht zulässig. Grund ist nämlich, dass der Betroffene Anspruch auf rechtliches Gehör aus Artikel 103 Absatz 1 GG dazu hat, ob seine Daten herausgegeben werden. Nach der Rechtsprechung des Bundesverfassungsgerichts kann ein rechtliches Gehör aber nicht nachträglich gewährt werden, weil es die Entscheidung nicht mehr beeinflussen kann. Vor der Auskunftserteilung an Privatpersonen kann rechtliches Gehör aber auch nicht gewährt werden, weil man den Betroffenen noch nicht kennt und nicht informieren und laden kann.

Die juristische Hilfskonstruktion läuft deshalb darauf hinaus, dass das Gericht und der Anwalt des Antragstellers – ähnlich einer Geschäftsführung ohne Auftrag – eine fiktive Rechtsvertretung der Betroffenen und eine Interessenabwägung vornehmen müssen. Das kann in der Praxis kaum funktionieren, denn ein Anwalt kann – und darf – (außer in Scheidungssachen u.ä.) nicht beide Seiten vertreten. Aufgabe des Anwaltes und des Gerichts ist es deshalb, fiktiv zu ergründen, wie ein anwaltlich ordentlich vertretener Betroffener in diesem Fall verteidigt würde, und dann entsprechend darauf zu antworten. Eine Art Schachspiel oder Boxkampf gegen sich selbst.

Das Verfahren ist deshalb weder praxistauglich, noch stellt es das wirksame rechtliche Gehör sicher. Das ganze Verfahren ist deshalb im Grunde verfassungswidrig. Richtig wäre es, wenn die Daten nur an das Gericht herausgegeben würden und das Gericht direkt rechtliches Gehör gewährt. Das können die Gerichte aber quantitativ nicht leisten.

Die Quintessenz ist, dass der Gesetzgeber es nicht vermochte, ein gleichermaßen praktikables und grundrechtskonformes Auskunftsverfahren zu konstruieren. Es geht immerhin um Eingriffe in das Post- und Fernmeldegeheimnis aus Artikel 10 GG, das dort als **unverletzlich** geschützt ist, in der Praxis aber wie auf dem Rummelplatz behandelt wird.

Bereits die bisherige Konstruktion und die Praxis der Gestattungsverfahren genügen den Anforderungen, die der EuGH hier stellt, nicht. Einen Rechtsschutz für die Betroffenen gibt es nicht, und es ist nicht einmal gewährleistet, dass die Betroffenen von dem Eingriff überhaupt erfahren. Eine Missbrauchskontrolle findet praktisch nicht statt (vgl. Abschnitt 5.3 auf Seite 52).

4.1.4.1 Negativbeispiel Causa Renate Künast

Im Jahr 2019 machte ein solches Gestattungsverfahren die große Runde durch Medien und öffentliche Empörung. Die Politikerin Renate Künast von den Grünen hatte einen Gestattungsantrag gestellt, weil sie im Internet „Schlampe“, „Drecksfotze“ und ähnliches genannt worden sei.

Eine Recherche der Medien, ob diese Aussagen – mit Hinblick auf die inzwischen verbreitete Methodik der „strategischen Prozessführung“ – überhaupt echt oder fingiert waren, fand meines Wissens nicht statt. Bei früheren Recherchen über andere Personen, die im politischen Umfeld und medial auftraten und im Internet übel beleidigt worden sein wollten, hatte ich den starken Verdacht, dass die kritischen Äußerungen von ihnen selbst oder politischen Aktivisten als „False Flag“ vorgetäuscht wurden. Es hat den Anschein, als gäbe es regelrechte Agenturen, die solche Kampagnen produzieren.

Hier erwachsen Zweifel auch daraus, ob die Angelegenheit überhaupt echt war, weil in den Medien (Süddeutsche) gesagt wurde, dass die Sache nicht von Renate Künast selbst ausging, sondern sich eine Organisation namens „Hate Aid“ den Fall als „Testballon gesucht und an sie herangetreten“ sei, und sie den Fall dann Hate Aid „überlassen“ habe, als könne man eine Aktivlegitimation spenden. Das entspricht nicht nur dem Schema der „strategischen Prozessführung“, sondern ist meines Erachtens unzulässig und als Prozessbetrug strafbar, und nährt natürlich den Verdacht, dass die – oder zumindest einige der – Äußerungen von Klägerseite lanciert und nicht von Beschuldigten- und Beklagtenseite getätigt wurden und die Sache zumindest teilweise inszeniert und aufgebauscht wurde. Dazu trägt auch der Umstand bei, dass die Kanzlei die Sache öffentlichkeitswirksam skandalisierte, indem man beim Mordfall Walter

Lübcke auftritt.

Das Landgericht Berlin hatte den Antrag unter anderem mit Hinweis auf die Meinungsfreiheit abgelehnt.

Daraus entstand eine öffentliche Diskussion mit hochgekochter Empörung darüber, dass das Landgericht geurteilt habe, dass man Politikerinnen „Drecksfotze“ nennen dürfe.

Das war in mehrfacher Hinsicht unrichtig, denn es war kein Urteil, sondern ein Beschluss, und das Gericht hat auch nicht über die Bezeichnungen, sondern über den Antrag entschieden. Eine Entscheidung über die Strafbarkeit der Bezeichnungen kann eine Zivilkammer nicht treffen, schon gar nicht ohne Anhörung der Beschuldigten, und das hat sie auch nicht getan. Die komplette – und anscheinend von den Grünen lancierte und in Teilen von Pressenhäusern in anteiligem Besitz der SPD – Kampagne war Fake News.

Das Gericht hatte seinen Beschluss – offenbar unter Arbeitsdruck und auch nicht in so genauer Kenntnis des Gestattungsverfahrens – zwar ungeschickt und sperrig formuliert, in der Sache aber wohl richtig entschieden¹.

Dann das Gericht hat in der Sache (möglicherweise, ohne es selbst ganz zu verstehen) nichts anderes getan, als genau das, was im Gestattungsverfahren seine Aufgabe ist: *Nämlich den noch unbekanntem und nicht geladenen Betroffenen fiktives rechtliches Gehör zu gewähren. Das Gericht ist exakt seiner Aufgabe gefolgt, nämlich die Verteidigung der Betroffenen durch einen fiktiven Anwalt zu übernehmen. Dabei spielt es nicht einmal eine Rolle, ob diese Verteidigung juristisch „richtig“ ist. Es genügt schon, wenn ein verständiger und pflichtbewusster Anwalt sie für seinen Mandanten vortragen würde. Und in diesen Fällen würde sich ein Anwalt für seinen Mandanten selbstverständlich auf die Meinungsfreiheit berufen.*

Soweit sich der Formulierung des Beschlusses entnehmen ließ, beruhte die Entscheidung darauf, dass Frau Künast und ihr Anwalt es schlicht und einfach unterlassen oder versäumt hatten, den Gestattungsantrag richtig zu stellen und die fiktive Verteidigung der Gegenseite vorwegzunehmen und zu behandeln.

Verfahrensrechtlich betrachtet hat das Gericht deshalb nicht entschieden, dass solche Bezeichnungen zulässig wären, sondern nur, dass eine *fiktive* Verteidigung das pflichtgemäß, aber die Antragstellerin dazu nichts vorgetragen hat. Der Antrag war so schlecht gestellt, dass er gegen einen Anwalt verloren hat, der gar nicht da war. Der Antrag hätte Ausführungen enthalten müssen, warum die Bezeichnungen nicht unter die Meinungsfreiheit fallen, und das hat er wohl nicht.

Unklar ist, ob Frau Künast und ihr Anwalt den Antrag, der so nur abgelehnt werden konnte, nur aus Unkenntnis des Verfahrens nicht richtig gestellt hatten, oder in der Absicht, die Sache entsprechend der „strategischen Prozessführung“, für die die rot-grüne Juristenszene notorisch ist, zum Bundesverfassungsgericht hochzueskalieren,

¹<https://www.danisch.de/blog/2019/09/21/schlampenmassstaebe/>

um darüber dann im Bundesverfassungsgericht außerdemokratisch parteipolitisch entscheiden zu lassen.

Zur Fehlerhaftigkeit der Entscheidung des Bundesverfassungsgerichts unten in Abschnitt 4.2.1.3 auf Seite 41.

In der Gesamtsicht diene das Verfahren in meinen Augen nur der medial aufgeblasenen Attacke gegen die Rechte von Betroffenen von Auskunftersuchen und der Beseitigung dieser Rechte, also einem Angriff auf die Substanz genau der Grundrechte, die zu schützen der EuGH hier verlangt.

Ich empfinde es als ebenso frappierend wie irritierend, dass Frau Künast einerseits das Gestattungsverfahren anscheinend nicht verstanden hat, andererseits aber im Rechtsausschuss sitzt und damit „die Federführung bei der Gesetzgebung im deutschen Straf- und Zivilrecht sowie in Fragen des Prozessrechtes (Straf- und Zivilprozessordnung)“ innehat. Das erscheint mir als unvereinbar.

4.2 Judikative

4.2.1 Das Bundesverfassungsgericht

Ich werde nachfolgend darlegen, warum ich erhebliche Zweifel daran habe, dass das Bundesverfassungsgericht befähigt ist, adäquaten Grundrechtsschutz in IT- und Medien Themen zu leisten.

4.2.1.1 Vorratsdatenspeicherung

Parallel zu meiner Tätigkeit in der Vorratsdatenspeicherung im Jahr 2009 fand vor dem Bundesverfassungsgericht das Verfahren über Verfassungsbeschwerden gegen die Vorratsdatenspeicherung statt. Zunächst wurde die Anwendung über eine einstweilige Anordnung vom 11. März 2008 geregelt, die jeweils verlängert wurde, und schließlich am 2. März 2010 geurteilt (1 BvR 256/08).

Ich war damals nicht nur bezüglich der Befolgung dieser einstweiligen Anordnung in der Vorratsdatenspeicherung mit dem Verfahren befasst, sondern habe die wesentlichen Teile der Stellungnahme des Branchenverbands Bitkom e.V. zu einem Fragenkatalog des Bundesverfassungsgerichts verfasst.

Dabei zeigte sich das Verfahren des Bundesverfassungsgerichts als reine Operettenveranstaltung ohne Sachkunde.

Im gesamten Verfahren war (außer zufällig und indirekt mir, weil der Bitkom intern angefragt und ich gerade Zeit hatte), soweit erkennbar, kein Einziger beteiligt, der konkrete Kenntnisse und Erfahrungen mit der Vorratsdatenspeicherung hatte.

Die mündliche Verhandlung war, soweit darüber berichtet wurde, ein Witz, weil man, wie beim Bundesverfassungsgericht üblich, die parteinahe und medienbekannte Meinungsprominenz auftreten ließ, um denen Publizität zu verschaffen und eine Anhörung der Öffentlichkeit vorzugaukeln, sich das aber auf allgemeinplätzlichen Hokus-Pokus beschränkte, wie etwa, wieviele Daten auf eine Micro-SD-Karte passen und man die unbemerkt heraustragen konnte. Immer wieder zeigt sich, dass das Bundesverfassungsgericht kein juristisches Gericht ist, sondern ein nach Parteienproporz besetzter Rat der gesellschaftlichen politischen Strömungen, der lediglich in juristischer Verkleidung auftritt.

Tatsächliche Probleme der Vorratsdatenspeicherung wurden nicht erkannt, nicht erfasst, nicht verstanden, nicht behandelt. Es war ein Laienkonzil, das einen Laienkonsens gefasst und sich dann gefeiert hat.

Der Fragenkatalog ging meilenweit an der Sache vorbei, beruhte auf Unkenntnis und war im Wesentlichen nutzlos. Es war aber auch nicht gestattet, davon abzuweichen und zu sagen, was nicht gefragt war. Und es war nichts gefragt, was wichtig war.

Die einstweilige Anordnung war verfehlt und fast völlig wirkungslos, weil laienhaft und schlecht formuliert.

Die abfrageberechtigten Behörden wie Polizei, Kriminalämter, Zoll und so weiter haben sie überhaupt nicht beachtet, weil die Formulierung der Anordnung – außer in den Ausnahmen schwerer Katalogstraftaten – verbot, Daten *aus* der Vorratsdatenspeicherung abzufragen.

Damit aber lief sie völlig fehl, denn die Behörden standen auf dem – kaum abzuweisenden – Standpunkt, dass mit der Frage, wer Nutzer einer IP-Adresse zu einem Zeitpunkt war, ja gar *keine Vorratsdaten, sondern nur Bestandsdaten abgefragt* würden (Text der Anordnung: „das sich auf allein nach § 113a des Telekommunikationsgesetzes gespeicherte Telekommunikations-Verkehrsdaten bezieht“), die geschützten Verkehrsdaten also nicht etwa abgefragt, sondern im Gegenteil schon bekannt seien und von der Polizei angeliefert würden, und abgefragt nur Bestandsdaten würden.

Vereinfacht gesagt: Das Bundesverfassungsgericht hat laienhaft beschlossen, dass man nicht abfragen darf, welche IP-Adresse ein namentlich genannter Kunde zum gegebenen Zeitpunkt verwendete, was praktisch nie vorkam, während die Polizei in der Realität fragte, wer der Nutzer einer IP-Adresse zum gegebenen Zeitpunkt war.

In der gesamten Zeit meiner Tätigkeit (1 Jahr, ungefähr 2.000 Fälle) gab es insgesamt nur einen eindeutigen und einen Zweifelsfall, der überhaupt von der Anordnung erfasst wurde. Ich hatte deshalb gemäß der Anordnung nur zwei Kuverts im Tresor liegen. Von etwa 2.000 Auskunftersuchen und einer nicht erfassten Zahl von abgefragten Daten, vielleicht 10.000 oder 20.000. Also ein Effekt unterhalb des Promillebereichs.

Die einstweilige Anordnung war damit nahezu wirkungslos, unbeachtlich und fand nur in der Einbildung des Gerichts statt. Und es gab keinen zulässigen Weg, das Bundesverfassungsgericht darauf hinzuweisen. Die als Sachverständige geladene Meinungs-

prominenz hatte keine Ahnung davon.

Das Urteil vom 2.3.2010 ist wirr und unlogisch. Zwar lässt die Nr. 6 darauf schließen, dass man inzwischen bemerkt hatte, dass es Abfragen gibt, die andersherum laufen als gedacht, nämlich den Namen zur IP-Adresse abfragen, aber verstanden hat man es nicht. Die Nummern 2 bis 4 der Entscheidung sind „soll-sich-jemand-anderes-damit-herschlagen-Blabla“. Die Nummer 5 schränkt Abfragen, die in der Praxis so gut wie gar nicht vorkommen, stark ein. Erst die Nummer 6 betrifft die tatsächlich vorkommenden Abfragen („wer war Nutzer der IP x?“), schränkt sie aber fast nicht, nur für einige Ordnungswidrigkeiten ein.

Also wurde effektiv fast nichts geschieden. Der Berg kreißte mit viel Getöse und gebar eine Maus.

Das Bundesverfassungsgericht hat die Vorratsdatenspeicherung nicht verstanden, eine Operette statt einer Gerichtsverhandlung aufgeführt, an der Sache völlig vorbei und damit im Ergebnis eigentlich gar nichts entschieden. Aber man kam sich sehr gut vor.

2014 erlebte ich auf einer Veranstaltung der Juristen in der Humboldt-Universität zu Berlin den Auftritt des damaligen Präsidenten und Vorsitzenden des Bundesverfassungsgerichts, Hans-Jürgen Papier, der da einen polternden Vortrag hielt und dazu anscheinend von Veranstaltung zu Veranstaltung tingelte, eine Worthülsenkanonade ohne Inhalt. Und sich dabei unter Beifall der anwesenden Juristen eben jener Entscheidung brüstete.

Es hatte noch immer niemand verstanden, dass die Entscheidung und vor allem die einstweilige Anordnung, ebenso die Verhandlung und Fragen, völlig an der Sache vorbei gingen und das Bundesverfassungsgericht nicht verstanden hatte, wie die Vorratsdatenspeicherung funktioniert.

Es gab viel Beifall.

4.2.1.2 Rundfunkbeiträge

2020 war ich als Sachkundiger in der Frage der Erhöhung der Rundfunkbeiträge vor dem Landtag in Sachsen zur Anhörung geladen, und stellte u.a. fest, dass eine Erhöhung schon aus formalen Gründen nicht möglich ist, weil § 3 Absatz 1 Satz 1 und 2 RFinStV verlangt, dass die KEF einen Bericht zum Rundfunkbedarf erstellen muss, auf dessen Grundlage die Erhöhung nur erfolgen kann, und dieser Bericht auch die Überprüfung enthalten muss, ob sich die Programmentscheidungen im Rahmen des Rundfunkauftrages halten.

Mit anderen Worten: Es reicht nicht, wenn die KEF nur prüft, was es kostet, 24 Stunden am Tag zu senden, sondern sie muss auch prüfen, ob der Rundfunkauftrag erfüllt ist und die in Rechnung gestellten Tätigkeiten diesen auch nicht überschreiten.

Was faktisch nicht der Fall ist, weshalb ein korrekter, vollständiger KEF-Bericht *unabhängig vom Finanzbedarf* eine Erhöhung unmöglich gemacht hätte, weil die Nichterfüllung und die Abweichung vom Rundfunkauftrag hätten festgestellt werden müssen.

Das aber enthielt der Bericht der KEF nicht nur nicht, sondern sogar die Aussage, schriftlich und mündlich in der Stellungnahme, dass die KEF das nicht machen wolle, um nicht in die Autonomie des Rundfunks und des Landtages einzugreifen.

Es waren also schon die formalen Anforderungen an die Erhöhung des Rundfunkbeitrages nicht erfüllt, eigentlich nicht einmal dessen Fortsetzung in gleicher Höhe möglich.

Trotzdem entschied das Bundesverfassungsgericht am 20. Juli 2021, 1 BvR 2756/20, dass das Bundesland Sachsen-Anhalt der Erhöhung auf Grundlage des KEF-Berichts zustimmen muss. Dass im KEF-Bericht ein wesentlicher Teil fehlt und deshalb formal kein wirksamer KEF-Bericht vorliegt, hat das Bundesverfassungsgericht nicht bemerkt. Oder sich nicht dafür interessiert und es bewusst übergangen.

4.2.1.3 Die Causa Renate Künast

Ich hatte oben die Causa um das Gestattungsverfahren der Politikerin Renate Künast beschrieben (Abschnitt 4.1.4.1 auf Seite 36).

In der Sache entschied 2021 das Bundesverfassungsgericht (1 BvR 1073/20), verfehlte dabei aber das Thema. Denn das Gericht behandelte die Vorinstanzen, als ginge es um ein Strafrechts- oder Unterlassungsurteil.

Dass es hier um eine Gestattung ging, und im Gestattungsverfahren, wie oben beschrieben, andere Regeln gelten, es noch gar nicht um die Hauptsache gehen kann, weil der Betroffene noch nicht angehört wurde, sondern um die Frage, ob der Gestattungsantrag richtig gestellt wurde und durchgreift.

Man spult zwar das übliche Programm zur Abwägung von Meinungsfreiheit und Beleidigung ab, aber dass es hier – noch – nicht um die Hauptsache geht, sondern den formalen Vorgang des Gestattungsverfahrens und den Schutz von Personen, die ihr rechtliches Gehör noch nicht wahrnehmen können, kommt darin nicht vor. Auch die Frage, ob der Gestattungsantrag formal richtig gestellt ist, kommt nicht vor.

Das Bundesverfassungsgericht hat nicht verstanden, was Gegenstand des Verfahrens ist. Das Bundesverfassungsgericht kennt das Gestattungsverfahren nicht.

Wer nur den Hammer kennt, für den sieht alles wie ein Nagel aus.

4.2.1.4 Personelle Defizite

Ich hatte zweimal beruflich mit Verfassungsrichtern außerhalb derer gerichtlichen Tätigkeit zu tun und dabei verblüfft festgestellt, dass sie außerstande waren, Grundrechte in dienstlichen Angelegenheiten anzuwenden, sie völlig übergingen und missachteten, und zwar selbst dann, wenn die Anwendung durch Rechtsprechung des BVerfG bereits geklärt ist. Als ob sie sie nicht kennen und verstehen würden.

Auch in den außergerichtlichen Schriften von Richtern, sogar in deren Entscheidungen, entstand schon der Eindruck, dass sie mit den Grundrechten jenseits von Artikel 3 nicht bekannt sind, und sich rhetorisch damit durchschlagen, alles als Diskriminierung, und wenn das nicht geht, über die Menschenwürde aus Artikel 1 abzuhandeln, während sie wichtige Grundrechte oder grundrechtsgleiche Rechte wie 5, 10, 12, 19 IV, 33 II weder anwenden können noch wollen, weil sie 1 und 3 für eine Art überraschende Universalgummiparagrafen halten, die ohnehin alle anderen überflüssig und obsolet machen.

Ich habe vor einigen Jahren eine Auskunftsklage gegen den Wahlausschuss des Deutschen Bundestags bezüglich eines bestimmten Verfassungsrichters betrieben, der besonders zweifelhaft erschien.

Dabei stellte sich heraus und wurde in der Verhandlung durch den Wahlausschuss eingeräumt, dass man den Kandidaten bei seiner Wahl überhaupt nicht kannte, die Person nie gesehen hatte, keine Aussprache durchgeführt hatte, nicht einmal eine Personalakte hatte, und völlig blind nach Parteienproporz eine dem Ausschuss völlig unbekannt Person blind durchgewinkt hatte.

Dass die Person über keinerlei richterliche Erfahrung verfügte und sich eigentlich auch nicht um Recht, sondern um Soziologie kümmert, bemerkte man nicht. Dass der Lebenslauf nicht korrekt war, und darin ein Posten genannt wurde, den es nicht gibt, übersah man auch.

Und das Sahnehäubchen: Weil man die Person fälschlich für einen *ordentlichen Professor des Rechts* hielt, und deshalb annahm, dass nach dem Richtergesetz schon damit die Befähigung zum Richteramt vorliege, vergaß man sogar die Überprüfung, ob die Person überhaupt das juristische Staatsexamen und die Befähigung zum Richteramt hat.

Das Bundesverfassungsgericht wird mit Hinz und Kunz besetzt, solange sie nur parteinah sind. Und solche Personen lässt man dann außerdemokratische Entscheidungen treffen, die sogar die Regierung binden und auf demokratischem Weg nicht mehr beseitigt werden können. Die dann natürlich die Parteiziele als Maßstab nehmen und nicht die Grundrechte.

Eine Befähigung, die Aufgaben der jeweiligen Richterstelle zu erfüllen und die Themen innerhalb der zugewiesenen Zuständigkeit zu beherrschen, ist nicht mehr gefordert. Quality is a myth.

4.2.1.5 Die „Strategische Prozessführung“

Im deutschen Recht sollte eigentlich der Grundsatz „Wo kein Kläger, da kein Richter“ gelten.

Ich habe als Blogger einige Entscheidungen des Bundesverfassungsgerichts untersucht, die der Methode der „Strategischen Prozessführung“ entsprechen. Dabei werden aus dem Freundes-, Bekannten-, Kollegen-, Ex-Kollegenkreis der Verfassungsrichter nach politischen Wünschen fingierte Rechtsstreitigkeiten entworfen, um bestehendes Recht, mit dem man nicht einverstanden ist, unter dem Vorwand einer Verfassungsbeschwerde zu ändern.

Danach castet man einen Grundrechtsverletztendarsteller, der als Strohmann, Namens- und Aktivlegitimationsspender auftritt, dem man die Prozesskosten bezahlt und alle Schriftsätze schreibt. Man führt systematisch einen aussichtslosen Prozess, um formal den gesamten Rechtsweg mit ablehnenden Entscheidungen ausgeschöpft zu haben und schließlich mit der Verfassungsbeschwerde beim „eigenen“ Verfassungsrichter zu landen, der dann unter dem Anschein einer Verfassungsbeschwerde eigene oder vom Freundeskreis entworfene Scheinbeschwerden entscheiden und außerdemokratische politische Entscheidungen durchsetzen kann.

Dabei fällt vor allem die „Gesellschaft für Freiheitsrechte“ auf, deren Geschäftsstelle im selben Haus wie die grüne Jugend sitzt, auf der Rückseite der Parteizentrale der Grünen. Nach ungeprüften Behauptungen sollen beide Gebäude Eigentum der Grünen sein.

Gleichzeitig fällt die „Gesellschaft für Freiheitsrechte“ durch eine Affinität zu von den Grünen vorgeschlagenen Verfassungsrichtern auf, was den Eindruck einer geschlossenen grünen Produktionsstraße für vorgetäuschte Verfassungsentscheidungen zum Umgehen und Brechen demokratischer Entscheidungsprozesse entstehen lassen könnte.

Durch die richterliche Konzentration auf diese „eigenen“ Fälle und als Richter in quasi eigener Sache kommen normale Beschwerden und andere Themen zu kurz oder werden übergangen.

4.2.1.6 Dysfunktionales Scheingericht

In der Gesamtsicht halte ich das Bundesverfassungsgericht zunehmend für ein Scheingericht, das lediglich durch seinen Namen, seine Abläufe, den Gebrauch juristischer Sprache und gelegentliche echte Entscheidungen den Eindruck vermittelt, ein Grundrechtengericht zu sein.

Nach meinen Recherchen der letzten 11 Jahre komme ich zu der Überzeugung, dass das Bundesverfassungsgericht eine Art außerdemokratischer Parteienrat, eine Lobby für Parteiinteressen ist, der das unter dem Anschein einer Verfassungsentscheidung

durchsetzt, was auf demokratischem und rechtsstaatlichem Weg nicht zu erreichen ist.

Insbesondere habe ich den Eindruck, dass das Bundesverfassungsgericht dazu dient, Parteiinteressen im Wege der Gerichtsentscheidung so durchzusetzen, dass sie gegen Wahlen und damit gegen den demokratischen Einfluss des Souveräns verriegelt werden.

4.2.2 Das Vieraugenprinzip der Blinden

Ein zentrales rechtsstaatliches Sicherheitselement des Strafverfahrensrechtes ist es, dass bei den Überwachungen, die in das Post- und Fernmeldegeheimnis eingreifen, von denen aber der Betroffene nichts erfahren darf, ein Vieraugenprinzip verankert ist, damit kein Fehler oder Missbrauch eines einzelnen oder einer Behörde möglich ist: *Die Staatsanwaltschaft muss es beantragen, und der Richter muss es beschließen.* Keiner von beiden soll allein ohne den anderen in das Grundrecht eingreifen können.

Es ist immer wieder passiert, dass ein „dringender“ Gerichtsbeschluss hereinkam, dem zwar zu entnehmen war, dass er unverzüglich umzusetzen sei, gerne auch mit Strafandrohung, aber in dem nicht stand, was denn angefragt wird. Meist lag das daran, dass die Gerichte aus Gründen der Rechtssicherheit und um Rechtsmittel und Revision standzuhalten, Formulierungen direkt aus dem Gesetz übernahmen, und etwa wie in § 100a StPO formuliert, anordneten, „die Telekommunikation“ aufzuzeichnen, ohne dies näher zu beschreiben.

Ich habe dann immer den Richter des Beschlusses angerufen und gefragt, was es denn heute sein dürfe. Eher was Telefonisches, oder doch das Internet. Wenn er beide nähme, könnte ich ihm auch noch eine e-Mail-Ausleitung oder Mobilfunkzellenabfrage draufpacken, wir hätten gerade Angebotswochen. Drei zum Preis von zweien. Einen gibt's gratis dazu.

Die Antwort war stets die gleiche: *Das wisse er doch nicht.*

Ermittlungsrichter müssten 20 Fälle am Tag abarbeiten und hätten die Akten dabei *höchstens* für eine halbe Stunde auf dem Tisch, könnten diese nicht lesen, und schon gar nicht hinterher sagen, worum es gehe. Es sei unmöglich, danach Fragen zur Sache zu beantworten oder zu klären, worauf sich ihr Beschluss eigentlich beziehe. Ich müsse mich an den Staatsanwalt wenden, der sei Herr des Verfahrens und im Besitz der Akte. *Der habe doch den Beschluss beantragt.*

Der ach so heilige „Richtervorbehalt“ heißt in der Realität, dass Beschlüsse völlig ungeprüft und unverstanden am Fließband einfach durchbeschlossen, und dabei unklar und mehrdeutig formuliert werden, weil man das dann für „Rechtssicherheit“ hält.

Frage ich aber die Staatsanwälte, kam auch von denen die immer gleiche Antwort: *Woher solle er wissen, was der Richter sich dabei gedacht habe. Das müsse ich doch den Richter fragen, der habe das doch beschlossen. Es sei doch dessen Beschluss.*

Jeder zeigt nur auf den anderen.

Der Einzige, der am Ende weiß, was eigentlich gebraucht und verlangt wird, ist der ermittelnde Polizist. Im Rahmen seiner – unten beschriebenen – arg begrenzten Sachkunde. Der sagt einem das dann am Telefon, was der Beschluss beinhalten soll, obwohl er das eigentlich nicht zu entscheiden hat und Entscheidungen schriftlich zu erfolgen haben. In den Akten ist später nichts nachvollziehbar.

Damit sind der Rechtsschutz, der Richtervorbehalt und das Vieraugenprinzip völlig wertlos, völlig ad absurdum geführt.

4.2.3 Mangelnde Sachkunde

4.2.3.1 Das Juristenkonzept des 18. Jahrhunderts

Das Konzept der Juristen beruht noch immer auf der Weltsicht des 18. Jahrhunderts, als man noch den Universalgelehrten wie in Goethes Faust kannte, der alles studiert hatte und alles wusste, was es damals zu studieren und zu wissen gab, und deshalb über alles urteilen konnte.

Die Welt ist inzwischen weitaus komplexer, aber noch immer halten wir an dem Weltbild fest, dass der Jurist über alles entscheiden kann, auch wenn es weit außerhalb seiner Ausbildung liegt.

Es gibt etwa keine Fachgerichte, die mit Spezialisten besetzt sind, die beides beherrschen, Recht und IT. (Oder Medizin oder ähnliches.)

4.2.3.2 Das Prinzip der zielführenden Ignoranz

Besonders im Bereich der Informationstechnik, des Unterlassungsrechts und der Internetstraftaten findet sich immer wieder das Prinzip der juristischen zielführenden Ignoranz.

Statt deduktiv aus dem Sachverhalt auf die rechtliche Bewertung zu schließen, wird umgekehrt die gewünschte Entscheidung vorgegeben, und dann der Sachverhalt so lange durch Wegignornieren von Bestandteilen zurechtgeschnitzt, bis die gewünschte Entscheidung möglich wird. Die meisten Gerichte betreiben keine Rechtsfindung mehr, sondern entscheiden willkürlich politisch und betreiben dann nur eine Begründungsfindung.

Typisches Beispiel ist die Störerhaftung. Ähnlich dem amerikanischen Prinzip, nicht den Mörder zu hängen, sondern den, der sich am wenigsten dagegen wehren kann, damit irgendeiner gehängt ist und der Staatsanwalt wieder gewählt wird, wird hier oft einfach irgendeiner verurteilt, damit der vermeintliche Rechtsfrieden hergestellt ist und

„das Internet kein rechtfreier Raum ist“.

Das Internet ist kein rechtsfreier Raum.

Aber er wird durch den Zustand unserer Rechtsprechung zum rechtswillkürlichen Raum gemacht. Man ist nicht in der Lage, einzusehen, zu verstehen, wann etwas einfach nicht durchsetzbar ist, sondern geht immer den Weg des geringsten Widerstandes. Rechtsdurchsetzung auf politischen Wunsch, koste es, was es wolle.

4.2.3.3 Positive Ausnahme Landgericht: Auskunft nach § 101 UrhG

Ich möchte bei aller Schelte auch eine – seltene – positive Ausnahme erwähnen. Ein Landgericht hat sich meine Achtung und meinen Respekt verdient.

Ich hatte als Informatiker in einer Rechtsabteilung einen Rechtsstreit übernommen, in dem das Unternehmen auf Auskunft nach § 101 UrhG verklagt wurde. Die Juristen der Rechtsabteilung hatten den Streit als aussichtslos aufgegeben, weil zuvor ein anderer Provider von derselben Kammer in gleich liegender Sache verurteilt worden war (sich aber technisch unterschied).

Zu Beginn der Verhandlung erklärte der Vorsitzende, dass er für diese Fragen um das Internet zu alt sei, und diese nicht in der nötigen Tiefe verstehe, und deshalb das Wort und die Verhandlungsführung seinen beiden jungen Beisitzern überlasse, weil diese privat sehr internetaffin und -interessiert seien.

Ich führte mit ihnen ein fast zweistündiges technisches Fachgespräch, um im Detail von vorne bis hinten zu erläutern, wie ein Internetprovider, die Beauskunftung, die Vorratsdatenspeicherung funktionieren, und wo die Unterschiede liegen, warum der vorliegende Fall aufgrund technischer Unterschiede anders zu beurteilen ist.

Ergebnis: Die Richter haben durchverstanden, wie ein Internetanbieter funktioniert. Und ich habe den Prozess gewonnen, weil sie auch die technischen Unterschiede verstanden haben und in der Urteilsfindung anwenden konnten.

Es war aber eine seltene Ausnahme, für die sich die Richter besonders viel Zeit nahmen, und bei der der Vorsitzende die Qualität hatte, das Wort den Beisitzern zu überlassen, dazu zwei internetaffine Beisitzer hatte, und alle drei es wirklich wissen wollten und viele Fragen stellten.

Es zeigt aber, welchen Nutzen es hätte, wenn man Fachgerichte mit Richtern hätte, die neben der juristischen Befähigung auch über die fachliche des Streitfalles verfügten.

Man könnte auch überlegen, gerichtsübergreifende Fachbeisitzer zu schaffen, die in Streitfällen an Stelle eines Beisitzers oder zusätzlich als Teil des Spruchkörpers oder als eine Art Berater hinzugezogen werden.

Im Zeitalter der elektronischen Kommunikation, der Videokonferenz und des Homeof-

fice und der steigenden Komplexität und fachlichen Spezialisierung der Streitfälle sollte man prüfen, ob das Konzept der örtlichen Zuständigkeit der Gerichte noch tragfähig ist.

4.3 Exekutive

4.3.1 Bundeskriminalamt 2009

Im Zusammenhang mit der bereits erwähnten Kinderpornosperrung und den Besprechungen im Bundesfamilienministerium und dem Bundeskriminalamt im Jahr 2009 zeigte sich, dass die Sachkunde im Bundeskriminalamt sehr ungleichmäßig und nicht herausragend ist.

Besonders die Abteilung, die die Ermittlungen im Bereich Kinderpornographie durchführt, hatte zwar große Sachkunde und Fertigkeiten bei der forensischen Beurteilung von Bildern, deren kriminalistischer Einstufung und der Erfassung von Informationen, die man den Aufnahmen entnehmen kann.

Sachkunde über die und Verständnis der Funktionsweise des Internet und des World Wide Web waren aber unzureichend, und für die Diskussion der Probleme der Sperre musste eine andere Abteilung hinzugezogen werden, die sich besser auskannte.

Letztlich ist damit eine „rechtssichere“ Erfassung nicht gegeben.

4.3.2 Polizei

4.3.2.1 Fehlende Ausbildung und Einweisung

Als Anfang 2009 die Vorratsdatenspeicherung eingeführt wurde, war ich etwa das erste Vierteljahr praktisch täglich damit beschäftigt, Polizisten Einweisungen und Erklärungen zu geben, die anriefen um sich erklären zu lassen, was das jetzt eigentlich sei und wie man das benutze.

In vielen Polizeidienststellen wurde einer ausgesucht, der die Aufgaben dann „an der Backe“ hatte. Manchmal war es der Jüngste, weil man sagte, er sei am Internet-affinsten. Manchmal der Älteste, weil der nicht mehr außendiensttauglich war.

Es fiel immer wieder auf, dass man die Polizei überhaupt nicht aufgeklärt, angeleitet, eingewiesen hatte, was für ein Werkzeug das ist und wie es zu gebrauchen war.

Ich habe damals überlegt, eine Broschüre oder ein Buch herauszugeben.

Es ist unverständlich, warum niemand in der Lage war, gegenüber den eigenen Polizisten den Umgang, die Anwendung, die Rechtsgrenzen darzulegen.

4.3.2.1.1 Datenübertragung per Blaulicht In einem Fall brauchte die Polizei dringend Daten in sehr großem Umfang und in elektronischer Form, und wollte diese per E-Mail, ohne die Möglichkeit zur TLS-Verschlüsselung. Ich bestand darauf, dass die Daten nur stark verschlüsselt übertragen werden können und dürfen. Die Polizei übermittelte mir ihren öffentlichen PGP-Schlüssel und wir verifizierten diesen am Telefon. Im Lauf des Tages meldeten sie sich, und beklagten sich, dass sie die Daten nicht entschlüsseln können. Wir gingen die Schritte am Telefon zusammen durch. Das Ergebnis der Fehlersuche war, dass sie den private key nicht hatten und nicht wussten, dass zu einem öffentlichen Schlüssel ein privater gehört, mittels dessen man entschlüsselt.

Das Ende vom Lied war, dass die Daten auf eine CDROM gebrannt und von einem Streifenwagen mit Blaulicht abgeholt wurden.

4.3.2.1.2 Fallbeispiel datenschutzwidrige Anfrage aus Unkenntnis Mir ist unter den Fällen unsachgemäßer, zu weit gehender und datenschutzwidriger Auskunftsersuchen ein Fall in besonderer Erinnerung geblieben.

Frau A hatte einen sehr kurzen anonymen Anruf erhalten. Ein Mann trug in unterer, gerade noch schlafzimmergängiger Ausdrucksweise den Wunsch nach gemeinsamer praktischer Ausübung einer bestimmten Sexualtechnik an sie heran. Ihre Zustimmung fand er damit indes nicht. Im Gegenteil unterstrich Frau A die kategorische Natur ihrer Ablehnung durch eine Strafanzeige.

In der Vernehmung durch eine Polizistin gab Frau A den Inhalt des Anrufs wieder und grenzte dessen Zeitpunkt auf etwa 20 Minuten ein. Andere Anrufe habe sie an diesem Tag nicht erhalten. Sie sei mit der Abfrage der Anrufe einverstanden. *Auf die Frage, ob sie einen Verdacht habe, sagte sie, es könne vielleicht der B gewesen sein. Sicher sei sie aber nicht.*

Die Polizistin stellte deshalb beim Anbieter des B das Auskunftsersuchen nach der Liste aller Anrufe, die B an diesem ganzen Tag getätigt hätte. Das Ersuchen wurde von mir als viel zu weit gehend und außerhalb des Ermittlungszwecks liegend abgelehnt.

Dies brachte mir umgehend den wütenden Anruf der – zunächst – überaus aufgebrachten Polizistin ein, der dazu führte, dass mir die Sache in Erinnerung geblieben ist.

Ich erläuterte ihr, dass ich die Beauskunftung nicht schlechthin ablehnte, sondern ihr Auskunftsersuchen falsch gestellt war. Ich erklärte ihr das – ihr bis dahin völlig unbekannte – Konzept der CDRs (Call Data Records, gelegentlich auch Call Detail Records genannt). Außerdem dass

eine bessere Abfrage wäre, die Telefonnummer der A anzugeben und nur nach den Anrufen vom Anschluss des B an diese Nummer zu fragen, weil damit keine Anrufe erfasst werden, die nichts mit der Tat zu tun haben.

die richtige Abfrage wäre, beim Provider von Frau A zu fragen, wer in diesem Zeit-

raum ihren Anschluss angerufen habe, und dann zu diesen Telefonnummern die Bestandsdaten abzufragen.

Dies schütze nicht nur B im Falle seiner Unschuld, sondern führe sie auch – gänzlich verdachtsunabhängig – direkt zum Anschluss, von dem der Anruf erfolgt war.

Die Polizistin gab zu, dass dies einleuchtend, überzeugend und richtig sei.

Das habe sie aber nicht gewusst, das sei ihr alles unbekannt gewesen, weil sie ohne jegliche Schulung und Unterweisung einfach angewiesen wurde, sich irgendwie um Auskunftersuchen zu kümmern, sie deshalb nicht wusste, wie sie das anfangen sollte. Sie hätten schlicht keine Anleitung und keine Informationen darüber, was das alles eigentlich ist und wie man es benutzt.

Mir ist nicht bekannt, ob der Anruf von B kam. Da ich aber nichts mehr in der Sache hörte, nahm ich an, dass B nicht der Täter war und die Abfrage einen Unschuldigen getroffen hätte.

4.3.2.2 Provider als Hilfsermittler der Polizei

Eine Folge der mangelnden Ausbildung und Einweisung der Polizei war, neben den Problemen mit der Stellung der Anfragen, auch, dass die Polizeien regelrecht Hilfe suchten und die Provider quasi als Hilfsermittler einsetzten.

Besonders in den ersten Monaten kam es häufig vor, dass keine Anfrage gestellt wurde, sondern mehr oder weniger die gesamte Ermittlungsakte mit der Bitte um Hilfe und Beratung durchgefaxt wurde, um aus dem Sachverhalt auf mögliche und erfolgversprechende Anfragen zu kommen und geeignete Anfragen zu formulieren.

Diese Akten waren mitunter sehr unterhaltsam, führten gelegentlich zu Gelächter, aber es kann bei Lichte betrachtet nicht angehen, dass die Provider damit indirekt zu Hilfssheriffs der Polizei werden und hoheitliche Aufgaben so völlig ohne Rechtsgrundlage in die Privatwirtschaft ausgelagert werden.

4.3.2.2.1 Blutanhaftungen auf Augenhöhe Der Kettensägenmörder hatte tagesaktuell eine Familie per Hausmassaker dahingerafft.

Die Polizei schickte die gesamte Ermittlungsakte im Stand des ersten Ermittlungstages per Fax an uns als Provider der Familie mit einer Anfrage und der Bitte um Beratung und allgemeine Unterstützung bei der Suche nach Ermittlungsansätzen.

Mit forensischer Liebe zum Detail war in diktiergerätiger Tatortprosa unter anderem beschrieben, wo, wie und in welcher Höhe welche früheren Bestandteile von Mutti an den – laut Feststellungen leider nicht hoch genug gekachelten – Wänden der Küche klebten, und wie, warum und von wo aus sie wohl dahin gekommen sein könnten.

Eine Kollegin, die die Anfrage zuerst hatte, erklärte sich knapp am Nervenzusammenbruch vorbei für außerstande, den Text zu lesen. Sie wollte nicht einmal mehr das Papier der Anfrage anfassen, obwohl es aus dem abteilungseigenen Faxgerät stammte und Blutanhaftungen damit sicher ausgeschlossen werden konnten.

Ich versuchte nach Kräften, behilflich zu sein und Beratung zu leisten. *Doch was haben solche Akten beim Telefonanbieter verloren?*

Nichts.

5 Missbrauch

Ich werde in diesem Kapitel vier Kategorien von Missbrauch beschreiben.

Die ersten drei Kategorien beruhen auf meinen Erfahrungen in der Vorratsdatenspeicherung und Beauskunftung im Jahr 2009. Mir wäre derzeit nicht bekannt, dass sich hier Verbesserungen ergeben hätten, ich bin aber seit 2009 auch nicht mehr in diesem Bereich tätig und mit der aktuellen Praxis nicht vertraut.

Die vierte Kategorie beschreibt die missbräuchliche Abfrage von Personen- und Zahlungsdaten durch das Landeskriminalamt Berlin vor wenigen Monaten im Jahr 2023.

5.1 Private Nutzung

Während meiner Tätigkeit in der Vorratsdatenspeicherung im Jahr 2009 habe ich zweimal (echte) Polizisten bei dem Versuch ertappt, Anfragen für rein private Zwecke zu stellen.

Das Erkennen dieser Versuche war aber nur möglich, weil sie sich dabei besonders auffällig und ungewöhnlich angestellt haben und seltsam bedächtig per Telefon angefragt hatten, um keine Spuren zu hinterlassen. Sie dabei anhörten wie Kinder, die Kekse geklaut haben. Anfragen dürfen aber (außer in Fällen allerhöchster und dringender Gefahr im Verzuge) weder telefonisch gestellt noch beauskunftet werden. Beide klappten bei kritischer Rückfrage zusammen.

Bei den normalen Anfragen per Fax bestand keine Möglichkeit, Missbrauch und Zweckentfremdung zu erkennen.

5.2 Fehlende Authentizität der Anfragen

Es gab im Jahr 2009 keinen praktikablen Weg, die Echtheit einer Anfrage zu prüfen. Irgendwer schickte ein Fax, und das musste beauskunftet werden, ohne dass dabei zuverlässig klar wurde, ob die Anfrage echt ist und es die angegebene Polizeidienststelle überhaupt gab.

Erschwerend hinzu kam, dass nur manche Dienststellen Anschreiben mit richtigen Briefköpfen verwendeten. Die waren zwar mitunter liebevoll aufwendig gestaltet, aber

von jedem durch einfaches Kopieren zu kopieren und fälschen, der jemals ein Schreiben dieser Polizeidienststelle erhalten hatte. Viele Dienststellen setzten einfach ein primitives, auf Excel beruhendes Formular ein, auf dem nicht einmal stand, dass es sich um Polizei handle und das Wort „Polizei“ nicht vorkam, man also einem Fälscher nicht einmal Urkundenfälschung oder Amtsanmaßung vorwerfen könnte. Stattdessen stand da oft nur „PI“ für „Polizeiinspektion“. „PI“ ist aber nicht geschützt und könnte alles bedeuten – Private Investigator, Pistazienimporteur, Freundeskreis der Zahl 3,1415926...

Ich kann mich an einen Fall erinnern, in dem schon die Anfrage selbst daherkam wie Falschgeld. Zwar gab es eine solche Polizeidienststelle, die auch die angegebene Telefonnummer hatte, aber die Faxnummer wich vom Nummernschema und sogar in der Vorwahl ab. Ich hatte dies zunächst für eine Fälschung gehalten, und wollte eben diese Polizeidienststelle darüber informieren. Es stellte sich aber heraus, dass die Anfrage echt war, und die Faxnummer darauf beruhte, dass man einen externen Faxdienstleister einsetze, der Fax in Mail wandelt. Man sagte mir, ich sei der erste gewesen, dem das aufgefallen sei.

Im Prinzip stand die Vorratsdatenspeicherung für jeden offen, der wusste, wie die Anfragen aussehen und formuliert werden müssen. Man hätte dabei die Angaben von Polizeidienststellen und Orten, die es nicht gibt, frei erfinden können, es wäre nicht bemerkt worden, weil die Beauskunftung damals nicht abgerechnet wurde, der Aufwand hätte die Einnahmen überstiegen. Jeder, der eine Kopie des oft verwendeten Formulars erhalten oder die Chuzpe besessen hätte, eine Polizeidienststelle frei zu erfinden, hätte Auskunft erhalten.

Es wäre später noch nicht einmal nachvollziehbar oder gar beweisbar gewesen, weil alle Anfragen und Auskünfte nach einer kurzen Vorhaltefrist zum Nachweis der Beauskunftung, für Übertragungsfehler und für Abrechnungszwecke gelöscht wurden.

5.3 Geschäftsmodelle und Geheimdienstschnittstellen

Es gab eine Reihe von Anfragen wegen Urheberverletzungen. Diese sind nach § 101 UrhG nach Einholung eines Gestattungsbeschlusses vom Landgericht zu beauskunften.

Ein Anbieter einer gewissen Art von urheberrechtlich geschützten Produkten umging dieses Verfahren indem er massenweise Strafanzeigen stellte, die allesamt eingestellt werden mussten, für die die Staatsanwaltschaften aber zunächst Auskunft einholen mussten, um dann Akteneinsicht zu nehmen und die Leute teuer abzumahnen. Die Frage kam auf, ob das Kerngeschäft dieses Herstellers in seinen Produkten oder doch eher im Abmahngeschäft besteht und die Produkte nur der Köder dafür sind.

Auffälliger waren aber oft die Auskunftersuchen, die mit korrektem Gestattungsbeschluss eingereicht wurden. Es ist äußerst dubios, wenn jemand behauptet, dass sei-

ne Urheberrechte in exakt 500 oder 1500 Fällen verletzt worden seien. Oder wenn die anfragende Kanzlei in England sitzen will, auf Google Street View unter der angegebenen Adresse aber keine Kanzlei zu sehen, und auch sonst über die Kanzlei nichts zu finden ist.

Ich bin damals aufgrund verschiedener Seltsamkeiten und Ungereimtheiten zu dem Schluss gekommen, dass § 101 UrhG eine getarnte Abfrageschnittstelle für Geheimdienste ist, die sich als Kanzlei ausgeben, eine fingierte Urheberrechtsverletzung behaupten, und die tatsächliche Anfrage in einer Liste von 500 Anfragen verstecken, damit man nicht erkennt, nach wem sie wirklich fragen.

5.4 2023: Schwerer Missbrauch beim Landeskriminalamt Berlin

Ich bin gerade selbst unmittelbar Betroffener eines schweren Datenschutzskandals beim Landeskriminalamt Berlin, dessen datenschutz- und strafrechtliche Aufarbeitung gerade erst anfängt.

In meinem Blog habe ich auch regierungs- und genderkritische Artikel, außerdem schreibe ich zu Grundrechten. Im Dezember 2021 erschien in der WELT als Teil einer Kampagne, die in vielen Medien erschien, ein Artikel des Chefredakteurs Ulf Poschardt, es sei tabu, die Adipositas der Grünen-Politikerin Ricarda Lang anzusprechen.

Darauf hatte ich eine längere Replik verfasst und darin erklärt, warum es sachlich und rechtlich möglich ist, warum man sich da selbst widerspricht, und dass es von Lang selbst zum Dauerthema gemacht wird. Es ist bisher auch nicht geklärt, warum Grüne zu Veganer Ernährung aufrufen, zucker- und fetthaltige Lebensmittel verbieten wollen, das sogar zum Gegenstand ihres Wahlprogramms machen, dann aber eine Vorsitzende wählen, zu deren Eigendarstellung es gehört, sich provokativ mit fetten und zuckerhaltigen Süßigkeiten wie Torten und Eisportionen in den Social Media zu zeigen.

Es erweckt den Eindruck, als ob die Grünen der arbeitenden Bevölkerung schmale, karge Kost verordnen, sich aber selbst fette Portionen gönnen. Ähnlich wie bei Flugreisen und Einfamilienhäusern.

Unmittelbar nach der Wahl Langs zur Vorsitzenden erstattete die in Stuttgart ansässige und von den Grünen geführte und finanzierte „Meldestelle REspect!“ beim Landeskriminalamt Berlin Strafanzeige wegen § 188 StGB gegen mich, unter der Behauptung, ich hätte Ricarda Lang beleidigt, indem man aus dem langen Text per Screenshot einen einzigen Satz ausstanzte, daraus fünf Wörter entnahm und – wider erweislich besseres Wissen – eine Aussage aus dem gesamten Kontext und damit dem Sachzusammenhang und der Sachdiskussion riss.

Erst kurz zuvor hatte die CSU im Benehmen mit eben dieser Meldestelle den § 188 um

Beleidigung erweitert. Die Sache landete bei der – ebenfalls von den Grünen eingerichtete – „Zentralstelle Hasskriminalität“ der Staatsanwaltschaft Berlin. Die ermittelte über ein Jahr gegen mich.

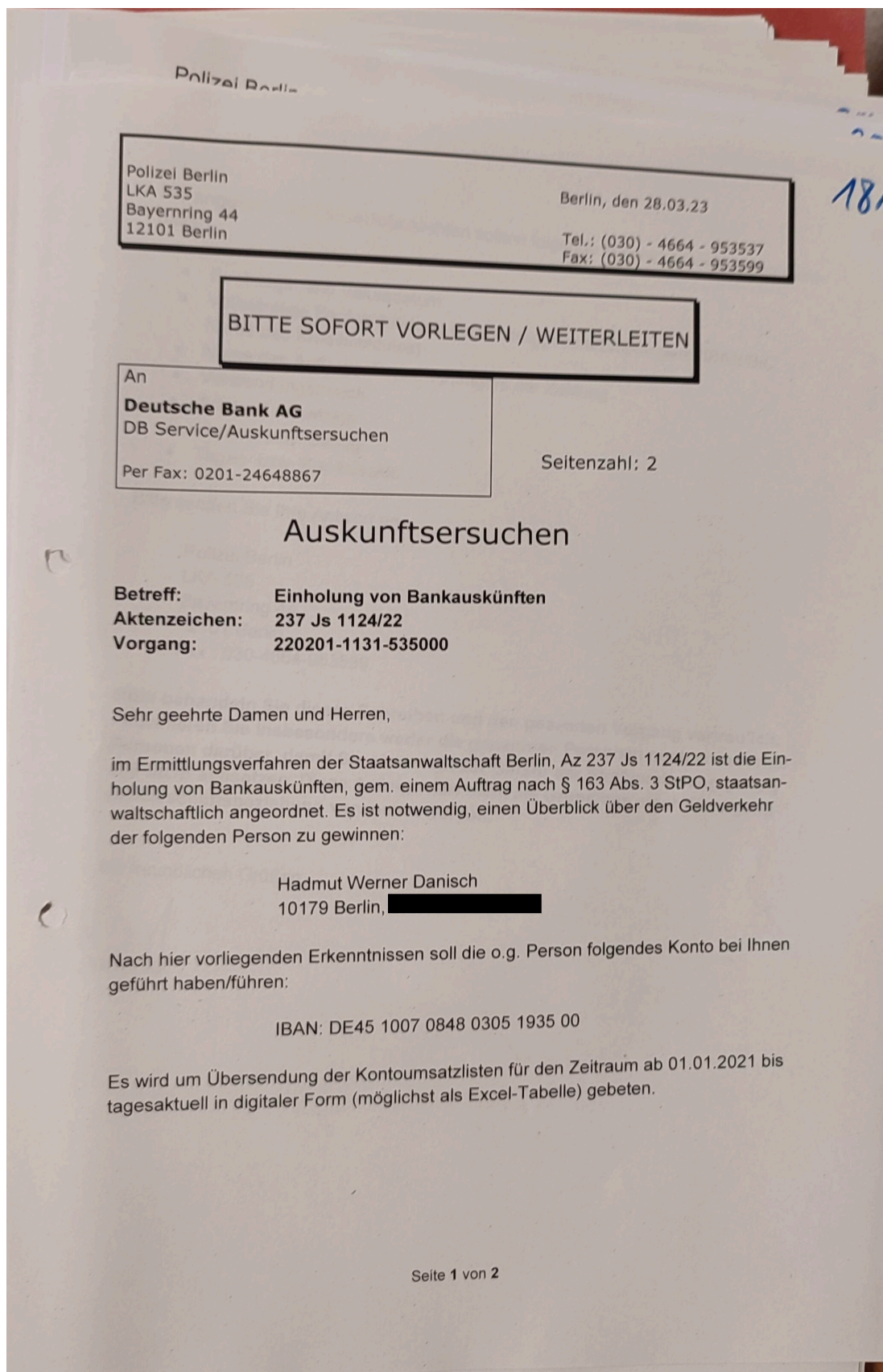
Der Vorwurf war aber nicht haltbar. Mein Blogartikel unterliegt vollumfänglich dem Schutz der Meinungsfreiheit, wie durch bestehende Entscheidungen des Bundesverfassungsgericht belegt werden kann. Die erforderliche Anbindung der „Tat“ an die Rechtsmerkmale der vorgeworfenen Straftat gelang der Staatsanwaltschaft nicht. Das Amtsgericht hat das Verfahren im August 2023 eingestellt.

Während des Ermittlungsverfahrens, im Frühjahr 2023, kam es zur Kündigung eines Girokontos durch die Deutsche Bank, das ich auf dem Blog sein 10 Jahren als Spendenkonto angegeben hatte. Die Deutsche Bank gab keinen Grund an und verweigert auch auf mehrere Datenschutzanfragen die Herausgabe von Informationen oder erklärte wahrheitswidrig, es gäbe keine.

Erst eine Akteneinsicht im September 2023 brachte Licht ins Dunkel. Die Staatsanwaltschaft hatte zuvor verfügt, dass eine „Kontostaffel“ (also nur die Beträge und Salden, aber keine Einzahler, Kontonummern, Verwendungszwecke) einzuholen sei. Der Ermittlungszweck war schon da nicht ersichtlich.

Die Sache kam zur – ebenfalls von den Grünen eingerichteten – Stelle beim Landeskriminalamt für „Hasskriminalität“, wurde dort als „Politisch Motivierte Kriminalität“ eingestuft, *obwohl gar keine Straftat vorlag*. Und diese Stelle stellte nun ein Auskunftsersuchen an die Deutsche Bank,

- obwohl das Konto und der Zahlungsverkehr in gar keinem, nicht einmal von der Polizei selbst behaupteten, Zusammenhang mit der vorgeworfen Tat stehen, also von der Ermittlungsbefugnis der §§ 160,161 StPO nicht erfasst wird,
- in einem Auskunftsverfahren, das es rechtlich und strafprozessual nicht gibt (Bankauskünfte müssen als Zeugenvernehmung einer konkreten natürlichen Person eingeholt werden)
- ohne Angabe der Rechtsgrundlage (die es auch nicht gibt),
- ohne Angabe, um welchen Vorwurf es überhaupt geht (was bei Zeugenvernehmungen und damit auch Bankauskünften zwingend angegeben werden muss, damit der Zeuge die Grenzen der Aussagepflicht erkennen kann und weil die Bank die Verhältnismäßigkeit prüfen muss, hier also hätte erkennen können und müssen, dass der Vorwurf einer Beleidigung diese Auskunft nicht trägt),
- einfach mit der willkürlichen Behauptung, es sei „erforderlich“,
- unter Verletzung des § 500 StPO und § 48 BDSG neu,
- unter der Vortäuschung, das Konto und die Zahlungen seien Gegenstand laufender, anhaltender schwerer Straftaten, gegen die das Landeskriminalamt verdeckt ermittle,



182

Die angeforderten Umsatzübersichten sollten folgende Mindestvoraussetzungen enthalten:

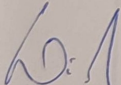
- Buchungs- und Valutadatum
- Vollständige Bankverbindung des Auftraggebers/Empfängers (IBAN/BIC, Name des Kreditinstitutes)
- Name des Auftraggebers/Empfängers der Zahlung
- Verwendungszweck
- Art der Transaktion
- Umsatz bzw. Betrag
- Tages- bzw. Kapitalsaldo

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

- dazu eine rechtswidrige und frei erfundene Drohung gegen die Deutsche Bank, sie würde wegen Strafvereitelung verfolgt, wenn sie mich darüber informiere,
- und der „Wink mit dem Zaunpfahl“ bezüglich der Kündigung des Kontos.

Ausgeforscht und abgeschossen.

Die Deutsche Bank kündigte daraufhin das Konto und gab rechtswidrig die Beauskunftung samt Namen, Kontonummern und Verwendungszwecken **einer mittleren dreistelligen Zahl von Personen**.

Darin liegt nicht nur eine schwere Verletzung von Datenschutzrecht, denn weil hier politisch ermittelt wurde, wurden besonders geschützte Daten in Form der politischen Meinung erhoben (Verstoß gegen Art. 9 DSGVO bzw. § 48 BDSG neu).

Und weil man darin keine Straftaten und keine Auffälligkeiten fand, gab man die Daten gleich noch an den Zoll weiter, ob die nicht irgendwas finden könnten. Und nach Aktenlage wurde die gesamte Akte anscheinend auch an die Rechtsanwälte von Ricarda Lang weitergegeben, und damit steht zu vermuten und befürchten, dass er auch den parteiinternen „Geheimdienst“ der Grünen namens „Gegneranalyse“ weitergegeben wurde, die die politische Position von Menschen im großen Stil erfassen.

Außerdem bestehen Anhaltspunkte, dass die Daten an den Verfassungsschutz weitergegeben wurden, denn der Verfassungsschutz hat erweislich Kenntnis des Verfahrens und seiner Aktenzeichen, und verweigert weitergehende Auskünfte.

Dieses Vorgehen ist auch strafbar, es erfüllt die Straftatbestände der

- Verfolgung Unschuldiger (§ 344 StGB)
- Politische Verdächtigung (§ 241a StGB)
- Nötigung (§ 240 StGB)

Mindeststrafe 1 Jahr Gefängnis und damit die Entfernung aus dem Dienst.

In der Gesamtsicht waren die Strafanzeige und das Ermittlungsverfahren – entlang einer komplett von den Grünen eingerichteten Falschbeschuldigungs- und Strafverfolgungsstraße – nur fingiert, um den Vorwand für den Zugriff auf das Konto und dessen Sperrung zu liefern.

Hier geht es um Spionage für den Verfassungsschutz – der Verfassungsschutz Berlin hätte auf direktem Wege keine Auskunft von der Deutschen Bank einholen können, weil diese in einem anderen Bundesland sitzt – und den parteieigenen Geheimdienst „Gegneranalyse“.

Auch die Heinrich-Böll-Stiftung der Grünen hatte früher schon einen „Steckbrief“ in ihrem Projekt „agentin.org“ auf mich ausgestellt. Dies ist inzwischen strafbar (§ 126a StGB).

In Folge dieses „Steckbriefes“ kam es zu massiven Diffamierungen gegen mich, wie Verleumdung im Internet, Schmähschriften an Arbeitgeber, Diffamierungsschreiben in Briefkästen der Nachbarn, Schmiererei an der Hauswand, mit mehrfachem Bezug auf eine Richterin des Bundesverfassungsgerichts, an der ich Kritik geäußert hatte. Es erweckt den Anschein, als gäbe es da Querverbindungen in das linke, kriminelle Antifa-Milieu.

Das Landeskriminalamt ist ausweislich des vorliegenden Falles selbst mit linkem Aktivismus und Antifa verwoben. Strukturell haben sich hier linke Aktivisten unter Steuerung der damaligen grünen Landesregierung hoheitliche Befugnisse von Polizei und Staatsanwaltschaft verschafft, die sie für ihre Zwecke missbrauchen.

Hier stehen großangelegte Strukturen im Raum, denn das Thema „De-Banking“, also das Wegschießen von Konten als Mittel politischer Kriegführung, um Kritiker und jeden, der nicht gleicher Meinung ist, zu ruinieren, kocht gerade international hoch. In England gab es einen Skandal um Kontenkündigungen gegen Nigel Farage, was zu öffentlicher Empörung führte. Man fertigt gerade ein Gesetz, um jeder Bank, die aus politischen Gründen Konten kündigt, die Banklizenz zu entziehen.

Hier in Deutschland dagegen sind Organisationen wie der Bayerische Rundfunk und ein „Thinktank“ namens CeMAS aktiv, die im großen Stil jedem, der irgendeine Kritik äußert, die Konten wegschießen. Nach deren Auftritt bei der re:publica halte ich CeMAS für eine kriminelle Vereinigung zur Begehung von Straftaten (§ 241a StGB).

Eine Spur führt dabei zur Bundesinnenministerin Nancy Faeser, über die die Tagesschau berichtete¹:

Rechtsextreme Gruppen finanziell äustrocknen das ist erklärtes Ziel von Bundesinnenministerin Nancy Faeser. Die SPD-Politikerin schrieb dies in ihrem im März 2022 veröffentlichten Aktionsplan gegen Rechtsextremismus an die erste Stelle. "Denn ohne Finanzmittel gibt es keine Propaganda und keine Aktivitäten, um Menschen zu radikalisieren und zu rekrutieren", sagte Faeser, als sie den Plan mit den Chefs von Verfassungsschutz und Landeskriminalamt vorstellte. Die Maßnahmen im Aktionsplan sollten schnell umsetzbar sein, so interne Unterlagen aus dem Innenministerium, die BR-Recherche vorliegen.

Doch es gibt Zweifel an der Wirksamkeit: In der Praxis müssen wir sagen: Wir haben bisher nicht festgestellt, dass sich da viel geändert hat", sagt Miro Dittrich vom "Center für Monitoring, Analyse und Strategie"(CeMAS). Die Forscher der gemeinnützigen Organisation mit Sitz in Berlin beobachteten rechtsextreme Aktivitäten systematisch.

Dabei gilt schon jeder als „rechtsextrem“, wenn er sich marxistischer Weltansicht und grüner Ideologie *nicht unterwirft*. Jegliche Form von Kritik oder Nichtzustimmung gilt

¹<https://www.tagesschau.de/investigativ/br-recherche/rechtsextreme-spenden-finanzdienstleister-100.html>

schon als „rechtsextrem“.

Der Bericht der Tagesschau legt Verbindungen zwischen Nancy Faeser und CeMAS nahe, und das Verhalten des LKA Berlin folgt dem Muster, das CeMAS auf der re:publica vorgestellt hat. Bindeglied zwischen dem Aktionsplan und dem vorliegenden Fall ist der Verfassungsschutz.

Die Methodik entspricht dabei dem Prinzip der Zersetzung und Agitation der Stasi in der DDR. Anscheinend erhoffte sich Frau Faeser, damit schöne Wahlergebnisse in Hessen zu schaffen.

Das gesamte Ermittlungsverfahren war nach Lage der Dinge nur vorgetäuscht, um als Vorwand für den Zugriff auf die Kontodaten und die Sperrung des Kontos herzuhalten.

Doch was war eigentlich der Grund für diese Aktion?

Warum werde ich als Informatiker, gegen den noch nie ein Strafverfahren lief, der mehrfach sicherheitsüberprüft ist, plötzlich und ohne nachvollziehbaren oder den Akten zu entnehmenden Grund als „rechtsextrem“ geführt und unter „Politisch Motivierte Kriminalität“ eingestuft, obwohl keine Straftat vorliegt und aus der Akte auch keine Begründung hervorgeht?

Die Antwort liegt im Zeitraum der abgefragten Daten.

Ich bin der Blogger, der 2021 die öffentliche Diskussion über den aufgeblasenen Lebenslauf von Annalena Baerbock losgetreten hat, weil mir damals auffiel, dass ihr in einem Jubelartikel der Süddeutschen ein Bachelor attestiert wurde, den es an dieser Hochschule in diesem Zeitraum noch nicht gab.

Mehrere Insider und Politologen kamen zu der Einschätzung, dass die folgende öffentliche Diskussion die Grünen so viele Stimmen gekostet hat, dass sie den Ausgang der Wahl und die Besetzung des Kanzlerpostens verändert hat, und deshalb nun Olaf Scholz und nicht Annalena Baerbock Kanzler ist.

Einige Politiker der Grünen und manche Medien setzten damals die Legende in Umlauf, dass nur die Russen wegen Nord Stream 2 hinter der Kritik an Baerbock stecken könnten, weil die marxistische Ideologie das Individuum negiert und sie der Überzeugung sind, dass kein Einzelner von sich aus Kritik an ihrer heiligen Weltsicht äußern könne, sondern immer finstere Mächte dahinterstecken müssten, die Leute beeinflussen, und die es ausfindig zu machen gelte.

Offenbar wurde das Strafermittlungsverfahren inszeniert, weil man herausfinden wollte, wer meine „Auftraggeber“ seien, und mich von ihnen abschneiden. Anscheinend hatte man sich das wohl so vorgestellt, dass der russische Geheimdienst mir Geld überweist und im Verwendungszweck Aufträge wie „Erledigen Sie Annalena Baerbock“ oder „Beleidigen Sie Ricarda Lang“ erteilt.

Blödsinniger geht es wohl kaum.

Der Fall legt aber offen, dass hier Strafermittlungsverfahren fingiert und polizeiliche Befugnisse und Amtsstellungen missbraucht werden, um unter dem Vorwand von Ermittlungen rechtswidrige Spionage zu betreiben und politische Gegner auszuschalten, also eine verbotene politische Verfolgung von Regierungskritikern zu betreiben und die Presse- und Meinungsfreiheit auszuhebeln.

Nach Lage der Dinge dienen die kürzlich erfolgten Erweiterungen des § 188 StGB dazu, solche Verfahren als Vorwand zu fingieren, weil die Beleidigung nicht durch Rechtsmerkmale definiert ist und immer behauptet werden kann, und hier die Erfordernis eines förmlichen Strafantrages entfällt. Durch Scheinorganisationen wie „Meldestelle REspect!“ und die von den Grünen zur politischen Verfolgung eingerichteten Sonderabteilungen bei Staatsanwaltschaft und Polizei können praktisch beliebige Ermittlungsverfahren inszeniert und gesteuert werden.

Auch der vorliegende und hier zu bewertende Antrag der Fraktion der CDU/CSU erscheint in diesem Licht nur wie die Einrichtung eines Werkzeugs zur Ausspionierung und politischen Verfolgung von Gegnern, und das Argument der Kinderpornographie nur wie ein Vorwand.

Die Missbrauchsstrukturen, die hier zu Tage treten, und eindeutig kein Einzelfall, sondern eben Strukturen sind, schließen unter der Vogabe der hier zugrundegelegten EuGH-Entscheidung eine Vorratsdatenspeicherung in Deutschland kategorisch aus.

Schon die Erkenntnisse aus dem hier vorliegenden Missbrauchsfall genügen, um eine Vorratsdatenspeicherung auf Grundlage der EuGH-Entscheidung wegzuklagen.

6 Sonstige Bedenken

6.1 Verhältnismäßigkeit als Verfassungsgrundsatz

Staatliche Maßnahmen müssen nach Verfassungsrecht verhältnismäßig sein, also geeignet und erforderlich sein und eine innere Verhältnismäßigkeit aufweisen.

Zur Erforderlichkeit trage ich weiter unten vor.

6.1.1 Mangelnde Eignung

Die Eignung des Antrags ist nicht dargetan, sie wird nur insinuiert.

Ich bezweifle, dass die beantragten Maßnahmen geeignet sind, den vorgeblichen Zweck, die Bekämpfung der Kinderpornographie, zu erreichen.

Zweifellos dürfte jeder, der heute Kinderpornographie konsumiert oder weitergibt, wissen, dass dies strafbar ist. Selbst wenn das nicht mehr jedem Einzelnen klar sein dürfte, weil durch die Veränderung der Gesellschaft nicht mehr jeder mit den Grundzügen unserer Kultur und unseres Rechtssystems vertraut ist, ist stark anzunehmen, dass dies in Foren und von denen, die Material verteilen, schon im eigenen Interesse thematisiert wird.

Deshalb ist damit zu rechnen, dass die große Mehrheit der Konsumenten Verdunklungsmaßnahmen ergreifen wird, die immer dem aktuellen Ermittlungsverfahren einen Schritt voraus sind.

So ist damit zu rechnen, dass Verfahren wie Tor-Browser und VPN verwendet werden, um sich hinter außereuropäischen IP-Adressen zu verstecken.

Inzwischen gibt es längst eine Vielzahl von Möglichkeiten, anonym und ohne Identifikation Internet-Dienste zu nutzen, weil in jedem Flughafen, in vielen Läden und Restaurants „Hot Spots“ bestehen, die kostenloses Internet anbieten. Gerade in Touristengebieten bekommt man an jeder Ecke anonym und kostenlos Internet. Oft muss man die Läden und Restaurants noch nicht einmal betreten, sondern es reicht, sich in deren Nähe aufzuhalten.

Es bestehen also reichlich Ausweichwege, um einer Vorratsdatenspeicherung zu entgehen, und diese werden auch genutzt werden.

Kurz vor Fertigstellung dieser Stellungnahme tauchte die Meldung auf¹, aus Frankreich werde der Versuch unternommen, den Gebrauch von VPN-Software zu verbieten, um Anonymität zu unterbinden. Ein überaus törichtes Unterfangen, weil VPNs nicht nur ein äußerst wichtiges Mittel der Sicherheitstechnik und für gewerblichen Gebrauch dringend erforderlich sind, sondern einige Techniken auch nicht zu blockieren sind.

6.2 Fehlender Rechtsweg

Es gibt keine Ausführungen zum erforderlichen Rechtsweg für die Betroffenen.

6.3 „Schutz der Kinder“ – Frühsexualisierung

Es erscheint überaus widersprüchlich und nicht nachvollziehbar, wenn man einerseits Kinderpornographie als so großes gesellschaftliches Problem hinstellt, dass es mit derartigen Eingriffen bekämpft werden müsse, andererseits aber eine permanente Frühsexualisierung betreibt und Kinder schon in Kindergärten und Schulen an sexualisierte Tänze, Praktiken, Trans- und Homosexualität, Masturbation herangeführt werden und sich mit Themen wie Transsexualität, Prostitution, Sexualpraktiken, Dildos beschäftigen müssen.

So hat Berlin das Buch „Rosi sucht Geld“ von gefördert und im Internet frei publiziert, das Kinder im Alter von 6 bis 12 Jahren **mit teils pornographischen Abbildungen und konkreten Adressangaben zu zwei Berliner Straßenstrichzonen und einer nahe gelegenen Grundschule, mit der jedes Kind hinfindet** über die Nöte von Prostituierten des Straßenstrichs aufklären soll und speziell auch migrantische Kinder ansprechen soll.

Erzählt wird die Geschichte des syrischen Mädchens Mayram und des deutschen Martin, die sich zusammen am Straßenstrich herumtreiben, um den Prostituierten zuzuschauen und mit einer, Rosi, über ihre Tätigkeit zu sprechen.

Autos fahren ganz langsam, halten plötzlich an. Der Fahrer spricht mit einer Frau, sie beugt sich zum Autofenster.

[...]

Deshalb suchen wir Rosi woanders. Sie geht oft zum Gleisdreieck, wo es grün ist. Das ist in der Nähe des Mädchentreffs in den U-Bahnbögen in der Pohlstrasse, wo ich Hausaufgaben mache.

[...]

¹<https://www.heise.de/news/Online-Ausweis-und-VPN-Verbot-Streit-ueber-Anonymitaet-im-Netz-kocht-wieder-hoch-9327812.html>

Rosi arbeitet wieder. Sie ist auch eine von den Frauen auf der Strasse. Sie nennt es Arbeit, wenn sie mit einem Auto wegfährt. In dem Auto sitzen immer Männer.

[...]

Es ist ein Geheimnis, dass wir Rosi ansprechen. Unsere Eltern sagen, wir sollen einen großen Bogen um die Frauen auf der Straße machen.

[...]

Heute aber haben wir uns vorgenommen, Rosi endlich einmal zu fragen, was sie mit den Männern so macht. Eigentlich wissen wir es schon. Sie geben ihr Geld und wollen Liebe machen. „Aber ist das denn 'Liebe' ?“, frage ich Martin.

„Es ist anders als bei Mama und Papa. Mama macht Liebe mit Papa, aber die Männer bei Rosi machen nicht Liebe, sondern Sex wie im Fernsehen.“

[...]

„Was soll ich euch sagen? Meistens ist es doch so: Die Männer wollen ihren Penis in meine Vagina stecken. Ein paar Mal rein und ein paar Mal raus – und fertig. Mehr ist da gar nicht dran.“

Man kommt unwillkürlich zu dem Eindruck, dass das Buch versucht, Prostitution zu verharmlosen, als normale Geldquelle zu beschreiben – nicht zu teuer – und Mädchen im Kindesalter, auch aus Syrien, an die Prostitution heranzuführen und sich auf dem Straßenstrich herumzutreiben.

Das Buch ist eine regelrechte Anleitung für Kinder,

- wo sie den Straßenstrich finden,
- was man dort macht,
- wie man das Geschäft anbaut,
- worin die Dienstleistung besteht und dass „nichts dabei“ wäre,
- sich über die Anweisungen und Verbote der Eltern hinwegzusetzen und dabei
- heimlich zu handeln,
- mit Prostituierten zu sprechen,
- dass man für ein kurzes harmloses rein-raus oder auch manchmal nur für Reden Geld bekommt.

Als wollte man systematisch – vor allem migrantische – Grundschulkinder, die sich Geld wünschen, für den Straßenstrich anwerben.

Im Juli wurde über eine „Kita“ in Hannover berichtet, dass man dort einen „Körpererkundungsraum“ für „sexuelle Spiele“ eröffnen wollte, und erst das Jugendamt dies auf Betreiben entsetzter Eltern gestoppt habe.

Gleichzeitig werden Kinder mit unfassbarem Druck mit Themen der Transsexualität bombardiert, als gebe es Bedarf an Knaben in Mädchenaufmachung und solchen ohne Eintritt der Pubertät, die länger im Kindeszustand bleiben.

Solange es zu solchen Vorgängen kommt und Kinder damit systematisch als Frischfleisch an Pädophile/Pädokriminelle herangeführt werden, ist es sehr seltsam und unglaubwürdig, vorgeblich Kinderpornographie zum Schutz vor Kindern mit derart drastischen Grundrechtseingriffen verfolgen zu wollen.

Der Verfassungsgrundsatz der Verhältnismäßigkeit setzt voraus, dass der Staat zunächst geringere Mittel ausschöpft. Und das würde zunächst einmal darin bestehen, die staatliche Frühsexualisierung und die verharmlosende zwangsweise Heranführung von Kindern an Sexualität und Prostitution einzustellen, um die Verankerung der Pädophilie und des Kindesmissbrauchs in Gesellschaft und Zeitgeist zu verhindern. Auch das Problem der Kinderehen gehört in diesen Themenbereich.

Es ist nicht zu verstehen, nicht zu begründen, dass man auf der einen Seite Kinderpornographie mit Eingriffen in Grundrechte verfolgen will, um Kinder vor Pädophilen zu schützen, andererseits aber Kinder im Kindergarten- und Grundschulalter mit staatlichen Mitteln und hoheitlichen Befugnissen an den Straßenstrich und sexuelle Handlungen heranführt, sie permanent mit Sexualität konfrontiert, einen regelrechten Babystrich aufbaut.

Es wirkt nicht glaubwürdig.

6.4 Bürokratiewut

Eigentlich war es doch erklärtes Ziel der Regierung, auch der Partei der CDU/CSU, Bürokratie abzubauen.

Warum beantragt man dann aber wieder neue Schikanen und Pflichten?

7 Ergebnis

7.1 Zusammenfassung

Es gibt zwar gute tatsächliche Gründe für eine Vorratsdatenspeicherung zur Verfolgung und Abwehr schwerster Straftaten. Es ist aber sehr zweifelhaft, ob schon der reine Konsum und Besitz von Kinderpornographie die vom EuGH aufgestellte Schwelle der Bedrohung für die Gesellschaft erreicht.

Es bestehen außerdem **schwere Zweifel** daran, dass Kinderpornographie der wahre Grund für diesen Antrag ist. Ich halte das für einen bloßen Vorwand, der als moralischer Hebel verhindern soll, dass man noch dagegen sein könnte.

Sowohl die politische Entwicklung auf EU-Ebene, als auch der in Abschnitt 5.4 beschriebene massive Missbrauch polizeilich-hoheitlicher Stellung durch das Landeskriminalamt Berlin nach Stasi-Manier, und der Kontext, dass die Fraktion der CDU/CSU auch in die Aufbohrung des § 188 StGB zum Zweck der politischen Verfolgung involviert ist, wecken den starken Verdacht, dass es auch hier um die Verfolgung politisch Andersdenkender geht und der Antrag im Ganzen missbräuchlich gestellt ist.

Schon deshalb wäre er abzulehnen.

Aber auch unabhängig von den Motiven hinter dem Antrag kann er keinen Erfolg haben.

Dieser Staat ist in seinem derzeitigen Zustand in allen drei Staatsgewalten meilenweit davon entfernt, die vom EuGH geforderten rechtsstaatlichen Qualitäten und Garantien aufzubringen. Keine der drei Staatsgewalten ist auch nur annähernd in einem Zustand, der eine Vorratsdatenspeicherung tragen und rechtfertigen könnte.

Angesichts der massiven Mängel und des aufgedeckten strukturellen Missbrauchs dürfte eine Vorratsdatenspeicherung in Deutschland auf absehbare Zeit keine Aussicht auf Bestand vor dem EuGH haben.

Ich erinnere daran, dass der EuGH im Mai 2019 schon die deutschen Staatsanwälte vom Europäischen Haftbefehl ausgeschlossen hat, weil sie nicht politisch unabhängig sind und deshalb die Strafverfolgung politisch ist (C-508/18 und C-82/19).

Deutschland hat

- passende Kriminelle,
- passende Straftaten,
- aber nicht die passende Polizei

für eine Vorratsdatenspeicherung.

7.2 Empfehlung

Der Antrag ist abzulehnen. Eine Vorratsdatenspeicherung ist bis auf weiteres zu unterlassen.

Augenmerk sollte zuvörderst darauf gelegt werden, die drei Staatsgewalten zu ertüchtigen und in einen wenigstens demokratienahen und rechtsstaatsähnlichen Zustand zu versetzen.

Stellen Sie den Missbrauch ab.