Die Vorratsdatenspeicherung 3.0

Arwed Schmidt, 15.05.2026

KI-Illustration

Talk

- Eigene Recherchen im Kontext v.a. des Regierungsentwurfes

  „Entwurf eines Gesetzes zur Einführung einer IP-Adressspeicherung und Weiterentwicklung der Befugnisse zur Datenerhebung im Strafverfahren“ (22.04.2026)

- Disclaimer: I am not a lawyer (IANAL) & do your own research!

- Ziel: gemeinsamer Wissensstand, was aktuell genau geplant wird

- ⚠ Stream & Aufzeichnung!

  Wenn Ihr Euch währenddessen meldet gebt Ihr die Einwilligung zur freien Veröffentlichung unter CreativeCommons.

Flut neuer Gesetzesnormen

digitale biometrische Rasterfahndung	Bund
„Automatisierte Datenanalysen“ („Lex Palantir“)	Bund
Alterskontrollen („Social Media-Verbot“)	Bund
BND-Gesetz	Bund
Bundespolizeigesetz	Bund
(Polizei- & VS-)Gesetze der 16 Länder	Länder
E-Evidence	EU-weit
Chatkontrolle 2.0	EU-weit
parallel: EU-Vorratsdatenspeicherung	EU-weit
„Grenzpartnerschaften“ mit USA & Co.	EU-weit
…	

VDS 3.0-Entwurf (Hubig/Dobrindt)

1. „IP-Adressspeicherung“

- Verpflichtung zur Speicherung bestimmter Daten für 3 Monate

2. „Weiterentwicklung der Befugnisse zur Datenerhebung …“

- u.a. „Sicherungsanordnung“ (DE) &
- EU-“Sicherungs- und Herausgabeanordnung“

3. Funkzellenabfragen *(heute leider keine Zeit für)*

RegE_IP_Speicherung.pdf
vom 22.04.26 (9ac7711cef)

Öffentliche Darstellungen

- gegen „Straftaten im digitalen Raum“
- EuGH habe „eine IP-Adressspeicherung 2024 ausdrücklich erlaubt“
- stehe „im Einklang mit Verfassungs- und Europarecht“
- „Aufklärungsquote bei internetbezogener Kriminalität erhöhen“
- BMJV will den eigenen, noch 2024 entwickelten Quick-Freeze-Gesetzesentwurf „weiterentwickelt haben“ und behauptet tlws. es sei „*eben keine Vorratsdatenspeicherung*“

⚠ Aussagen der BReg

1. IP-Adressspeicherung

- soll **anlasslos** für verpflichtende Datenbestand bei ca. 3.000 verpflichteten Diensteanbietern sorgen, damit zukünftig „keine Ermittlungen mehr ins Leere laufen“ (sinngemäß)

- Verordnung mit technischen & organisatorischen Anforderungen vorgesehen, Gesetz selbst fordert nur „*Stand der Technik*“.

- **Kein** explizites Verbot zur Speicherung/Verarbeitung im Ausland (!)

- Bundesnetzagentur (wieder) für Überwachung und Durchsetzung verantwortlich, planen allein dafür mit **25-30 Stellen**.

§ 177

Pflicht zur Speicherung und Befugnis zur Verwendung von Verkehrsdaten zur Identifizierung von Anschlussinhabern

(1) Wer Internetzugangsdienste erbringt, ist verpflichtet, mit der Zuweisung einer öffentlichen Internetprotokoll-Adresse an einen Anschlussinhaber folgende Daten zu speichern:

1. die dem Anschlussinhaber für eine Internetverbindung zugewiesene, öffentliche Internetprotokoll-Adresse,

2. die der Internetprotokoll-Adresse zugehörigen Portnummern und weitere Verkehrsdaten, soweit diese für eine Identifizierung des Anschlussinhabers anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse erforderlich sind,

3. eine eindeutige Kennung des Anschlusses, über den die Internetverbindung erfolgt, sowie eine zugewiesene Benutzerkennung und

4. das Datum und die sekundengenaue Uhrzeit von Beginn und Ende der Zuweisung der öffentlichen Internetprotokoll-Adressen sowie der zugehörigen Portnummern und weiterer Verkehrsdaten, soweit diese nach Nummer 2 zu speichern sind, an einen Anschlussinhaber unter Angabe der jeweils zugrunde liegenden Zeitzone.

Regierungsentwurf 24.04.26

Die Daten nach Satz 1 sind jeweils für drei Monate zu speichern. Inhalte der Kommunikation sowie Daten über den Aufruf oder die Nutzung von anderen Telekommunikationsdiensten oder digitalen Diensten dürfen nicht aufgrund dieser Vorschrift gespeichert werden.

„Internetzugangsdienst“

bb) Internetzugangsdienst

Der Begriff des **Internetzugangsdiensts** ist in § 3 Nr. 23 TKG legaldefiniert. Die Definition entspricht der Begriffsbestimmung des Artikels 2 Absatz 2 Nummer 2 der Verordnung (EU) 2015/2120 des Europäischen Parlaments und des Rates vom 25. November 2015 über Maßnahmen zum Zugang zum offenen Internet und zu Endkundenentgelten für regulierte intra-EU-Kommunikation sowie zur Änderung der Richtlinie 2002/22/EG und der Verordnung (EU) Nr. 531/2012 (ABl. L 310 vom 26.11.2015, S. 1), die zuletzt durch die Verordnung (EU) 2018/1971 (ABl. L 321 vom 17.12.2018, S. 1) geändert worden ist.

Nach der Verordnung (EU) 2015/2120 ist ein **Internetzugangsdienst**

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

Gemäß Auslegungshinweise BNetzA (2024)

§ 177

Pflicht zur Speicherung und Befugnis zur Verwendung von Verkehrsdaten zur Identifizierung von Anschlussinhabern

(1) Wer Internetzugangsdienste erbringt, ist verpflichtet, mit der Zuweisung einer öffentlichen Internetprotokoll-Adresse an einen Anschlussinhaber folgende Daten zu speichern:

1. die dem Anschlussinhaber für eine Internetverbindung zugewiesene, öffentliche Internetprotokoll-Adresse,

2. die der Internetprotokoll-Adresse zugehörigen Portnummern und weitere Verkehrsdaten, soweit diese für eine Identifizierung des Anschlussinhabers anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse erforderlich sind,

3. eine eindeutige Kennung des Anschlusses, über den die Internetverbindung erfolgt, sowie eine zugewiesene Benutzerkennung und

4. das Datum und die sekundengenaue Uhrzeit von Beginn und Ende der Zuweisung der öffentlichen Internetprotokoll-Adressen sowie der zugehörigen Portnummern und weiterer Verkehrsdaten, soweit diese nach Nummer 2 zu speichern sind, an einen Anschlussinhaber unter Angabe der jeweils zugrunde liegenden Zeitzone.

Regierungsentwurf 24.04.26

Die Daten nach Satz 1 sind jeweils für drei Monate zu speichern. Inhalte der Kommunikation sowie Daten über den Aufruf oder die Nutzung von anderen Telekommunikationsdiensten oder digitalen Diensten dürfen nicht aufgrund dieser Vorschrift gespeichert werden.

§ 177

Pflicht zur Speicherung und Befugnis zur Verwendung von Verkehrsdaten zur Identifizierung von Anschlussinhabern

(1) Wer Internetzugangsdienste erbringt, ist verpflichtet, mit der Zuweisung einer öffentlichen Internetprotokoll-Adresse an einen Anschlussinhaber folgende Daten zu speichern:

Anschlussinhaber aus § 172 TKG?

1. die dem Anschlussinhaber für eine Internetverbindung zugewiesene, öffentliche Internetprotokoll-Adresse,

2. die der Internetprotokoll-Adresse zugehörigen Portnummern und weitere Verkehrsdaten, soweit diese für eine Identifizierung des Anschlussinhabers anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse erforderlich sind,

„und weitere Verkehrsdaten soweit für eine Identifizierung erforderlich“

3. eine eindeutige Kennung des Anschlusses, über den die Internetverbindung erfolgt, sowie eine zugewiesene Benutzerkennung und

4. das Datum und die sekundengenaue Uhrzeit von Beginn und Ende der Zuweisung der öffentlichen Internetprotokoll-Adressen sowie der zugehörigen Portnummern und weiterer Verkehrsdaten, soweit diese nach Nummer 2 zu speichern sind, an einen Anschlussinhaber unter Angabe der jeweils zugrunde liegenden Zeitzone.

Regierungsentwurf 24.04.26

Die Daten nach Satz 1 sind jeweils für drei Monate zu speichern. Inhalte der Kommunikation sowie Daten über den Aufruf oder die Nutzung von anderen Telekommunikationsdiensten oder digitalen Diensten dürfen nicht aufgrund dieser Vorschrift gespeichert werden.

Erläuterungen zu § 177 Abs. 1

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

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

Bei mehreren Beteiligten wie z.B. Resellern

… zu WLAN & „Freifunk“

Nicht verpflichtet zur vorsorglichen Speicherung sind daher etwa nummernunabhängige interpersonelle Telekommunikationsdienste (OTT-1-Dienste, etwa Messenger- und E-Mail-Dienste).

Chatanbieter etc.

Passagen zu WLANs & „Freifunk“

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

WLAN allgemein (Hotel, Firmen, ...)

Passagen zu WLANs & „Freifunk“

Nicht verpflichtet zur vorsorglichen Speicherung sind daher etwa nummernunabhängige interpersonelle Telekommunikationsdienste (OTT-1-Dienste, etwa Messenger- und E-Mail-Dienste). Auch Bereitsteller von lokalen drahtlosen Netzwerken (wie etwa der Hotelbetreiber, der seinen Gästen WLAN zur Verfügung stellt, oder eine Initiative, die die vorübergehende Mitnutzung von privaten lokalen Netzwerken ermöglicht) gehören nicht zum Kreis der Verpflichteten. Denn gemäß Artikel 2 Absatz 2 Nummer 2 der Verordnung (EU) 2015/2120, auf die § 3 Nummer 23 Bezug nimmt, ist Internetzugangsdienst „ein öffentlich zugänglicher elektronischer Kommunikationsdienst, der unabhängig von der verwendeten Netztechnologie und den verwendeten Endgeräten Zugang zum Internet und somit Verbindungen zu praktisch allen Abschlusspunkten des Internets bietet“. Lokale drahtlose Netzwerke bieten aber selbst keinen Zugang „zum Internet und somit Verbindungen zu praktisch allen Abschlusspunkten des Internets“, sondern vermitteln – bildlich gesprochen – nur einen Weg dorthin. Sie sind nämlich ihrerseits auf eine Verbindung zu einem Internetzugangsdienst und dessen Telekommunikationsdienstleistung angewiesen. Erst dieser gewährt den eigentlichen „Zugang zum Internet“ (also zu Internet-Knoten oder den Netzen von anderen Internetdienstanbietern). Entsprechend weisen die lokalen drahtlosen Netzwerke auch keine öffentlichen Internetprotokoll-Adresse zu, sondern allenfalls netzwerk-/routerinterne IP-Adressen. Ferner unterfallen auch Freifunkvereine nicht der Verpflichtung nach Absatz 1, da sie weder dem Inhaber des Freifunkrouters noch dem Freifunknutzer eine Rufnummer oder Anschlusskennung, also keine öffentliche IP-Adresse an Anschlussinhaber vergeben. Aus Nutzersicht verhält sich die Erbringung des Dienstes wie eine Mitnutzung in einem Hotel, bei dem keine Registrierung erfolgt und eine IP-Adresse einem Endgerät zugewiesen wird. Der Dienst beruht dabei immer auf einem Internetzugangsdienst eines anderen Internetzugangsanbieters, **der selbst nach Absatz 1 verpflichtet ist.**

explizit „Freifunk“

Detailliert nachzulesen: S. 66

RegE_IP_Speicherung.pdf
vom 22.04.26 (9ac7711cef)

2. Befugnisse zur Datenerhebung

- zu einer VDS gehört immer auch eine Erhebungsregelung
  - Erhebung von Bestandsdaten (z.B. Personalien)
  - Erhebung von Nutzungsdaten (z.B. IP/Port zu einem Posting)

Bestands-daten-auskunft

§ 100j (bisher)	§ 100j
Bestandsdatenauskunft	**Erhebung von Bestandsdaten**
(1) Soweit dies für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes eines Beschuldigten erforderlich ist, darf Auskunft verlangt werden	(1) Soweit dies für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes eines Beschuldigten erforderlich ist, darf Auskunft verlangt werden
1. über Bestandsdaten gemäß § 3 Nummer 6 des Telekommunikationsgesetzes und über die nach § 172 des Telekommunikationsgesetzes erhobenen Daten *(§ 174 Absatz 1 Satz 1 des Telekommunikationsgesetzes) von* demjenigen, der *geschäftsmäßig* Telekommunikationsdienste *erbringt* oder daran mitwirkt, und	1. über Bestandsdaten gemäß § 3 Nummer 6 des Telekommunikationsgesetzes und über die nach § 172 **Absatz 1** des Telekommunikationsgesetzes erhobenen Daten **bei** demjenigen, der **öffentlich zugängliche** Telekommunikationsdienste **anbietet** oder daran mitwirkt, und
2. über Bestandsdaten gemäß § 2 Absatz 2 Nummer 2 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes *(§ 22 Absatz 1 Satz 1 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes) von* demjenigen, der *geschäftsmäßig eigene oder fremde* digitale Dienste *zur Nutzung bereithält oder den Zugang zur Nutzung vermittelt*.	2. über Bestandsdaten gemäß § 2 Absatz 2 Nummer 2 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes **bei** demjenigen, der digitale Dienste **anbietet**.

2. Befugnisse zur Datenerhebung

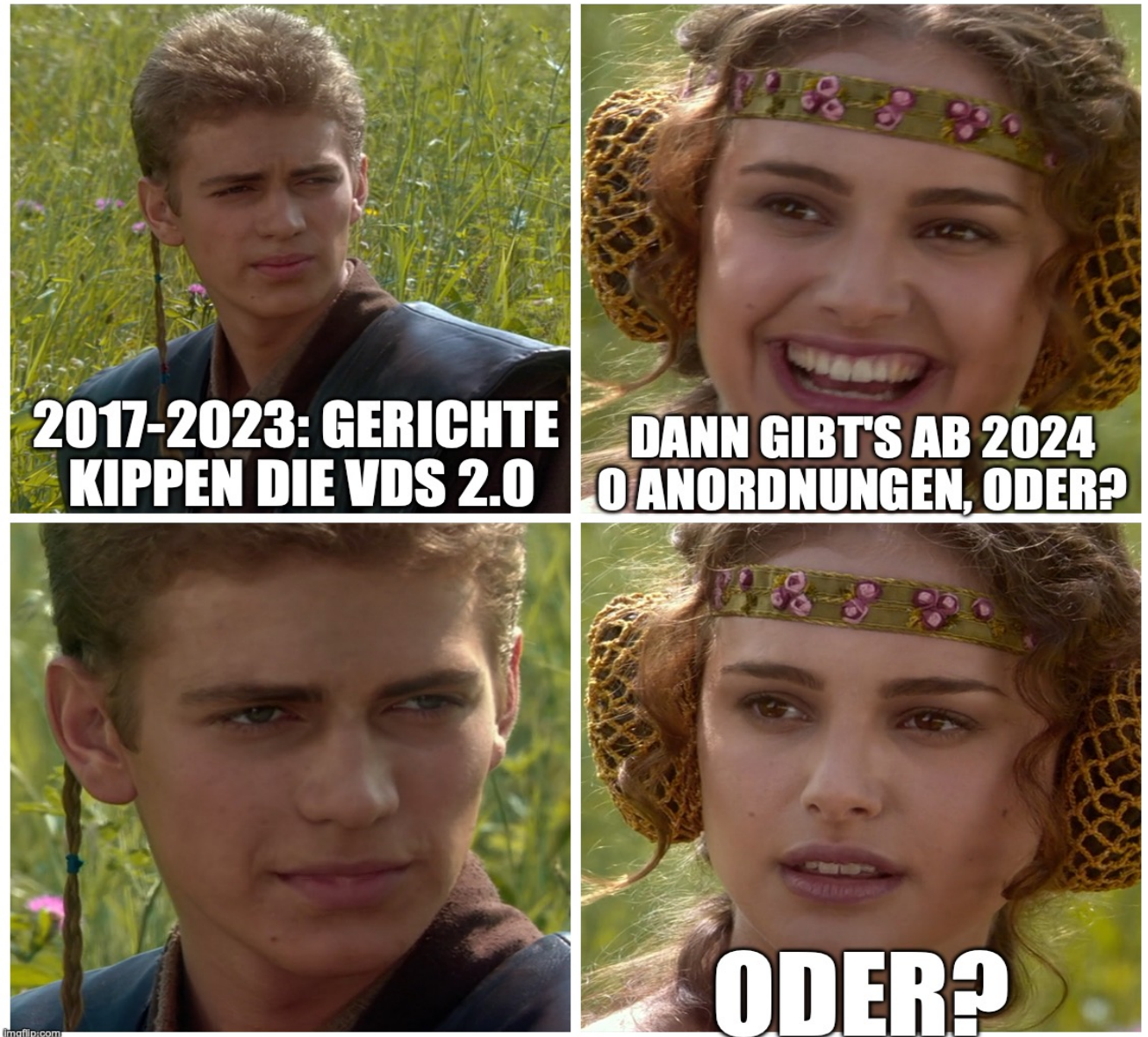
- zu einer VDS gehört immer auch eine Erhebungsregelung
  - Erhebung von Bestandsdaten (z.B. Personalien)
  - Erhebung von Nutzungsdaten (z.B. IP/Port zu einem Posting)
  - Erhebung von Verkehrsdaten (z.B. zu Abrechnungs- oder Werbezwecken gespeichert)

- Diesem Teil auch zugeordnet: Sicherungsanordnung(en).


2017-2023: GERICHTE
KIPPEN DIE VDS 2.0


DANN GIBT'S AB 2024
0 ANORDNUNGEN, ODER?

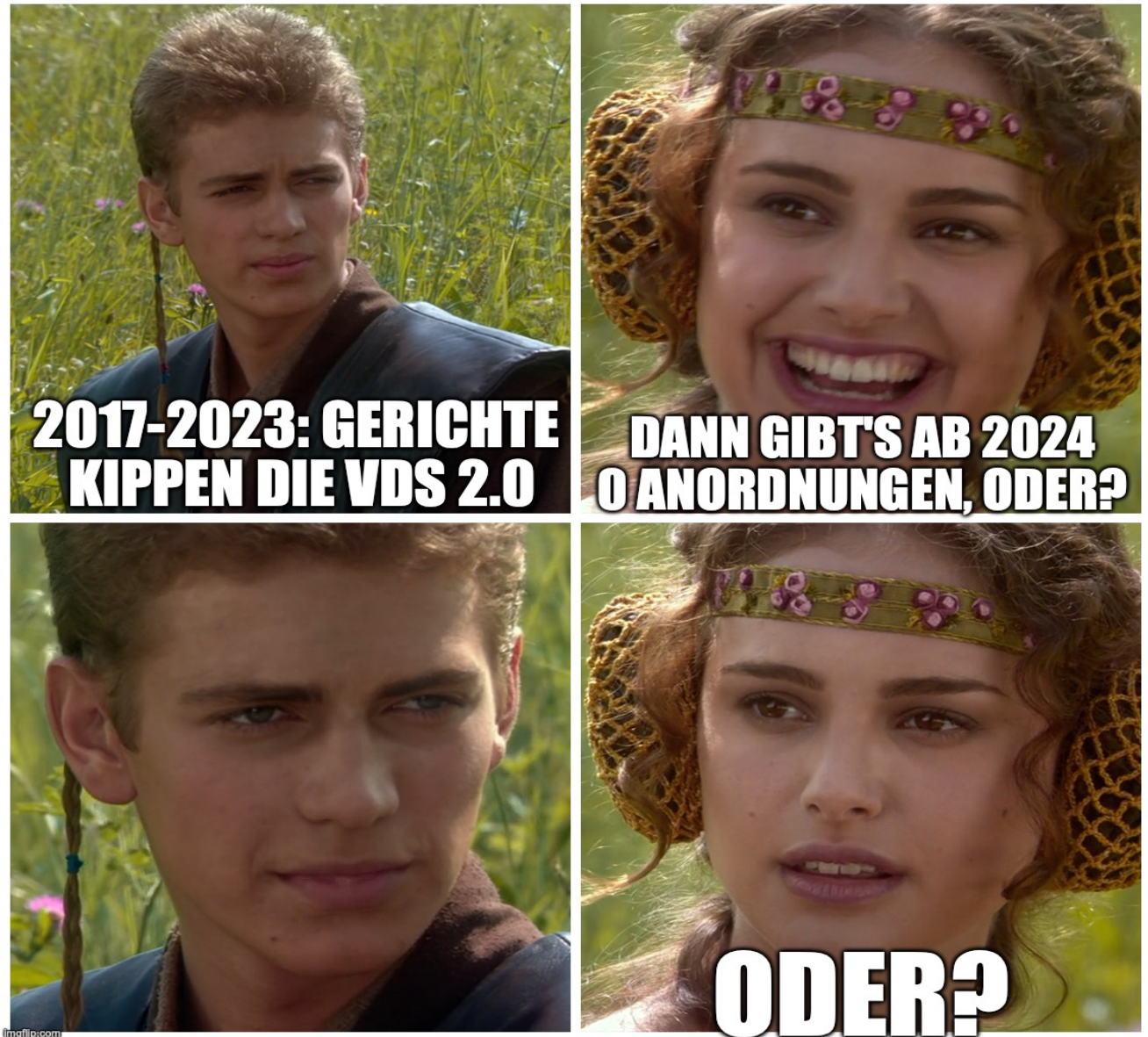

ODER?



Zu § 100g Abs. 2 StPO:

In 2024 mindestens

- 2.000 Ernstanordnungen
- 170 Verlängerungen



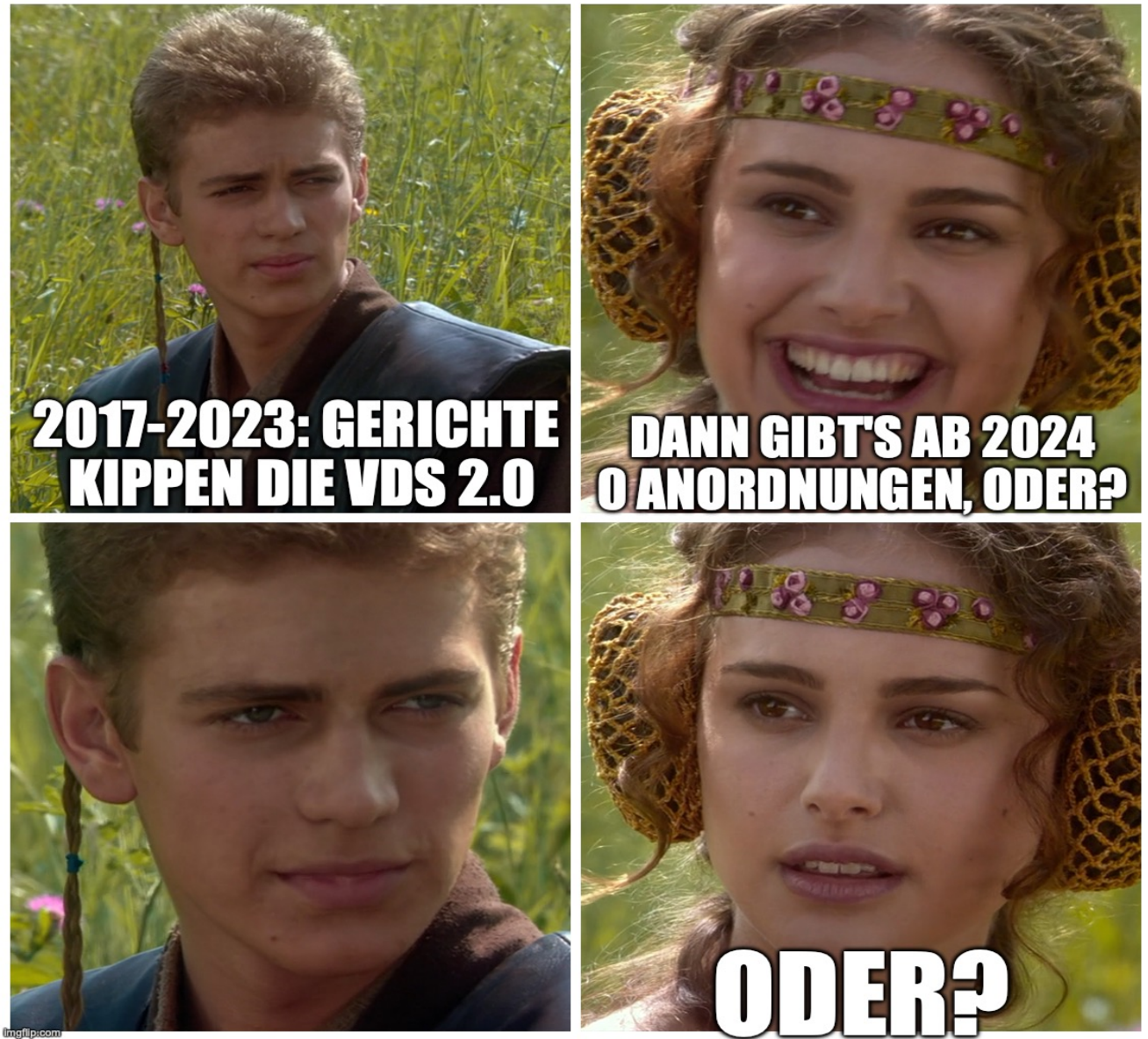
Zu § 100g Abs. 2 StPO:

In 2024 mindestens

- 2.000 Ernstanordnungen
- 170 Verlängerungen

Dabei abgefragte Daten:

- 903x bis zu eine Woche alt,
- 1.213x über eine Woche alt
- 1.019x über vier Wochen alt
- 894x über zehn Wochen alt



Zu § 100g Abs. 2 StPO:

In 2024 mindestens

- 2.000 Ernstanordnungen
- 170 Verlängerungen

Dabei abgefragte Daten:

- 903x bis zu eine Woche alt,
- 1.213x über eine Woche alt
- 1.019x über vier Wochen alt
- 894x über zehn Wochen alt

- min. 128x „Abruf ausschließlich künftig anfallende Verkehrsdaten“

Buschmann wollte 2024 §100g Abs. 2 entfernen, aber gab “Verabredung mit 1 Koalitionspartner“..

„Sicherungsanordnung“ in VDS 3.0

- StA kann gegenüber Diensteanbietern **anordnen...**

  Verkehrsdaten für 3 Monate zu speichern
- „wenn zureichende tatsächliche Anhaltspunkte dafür vorliegen, dass eine Straftat begangen worden ist“
- Optional: **Verlängerung** (+3 Monate) oder **Abruf der Daten**
- Eingeschränkt in Regierungsentwurf: „betroffene Person muss in persönlichen oder räumlichen Bezug zu der Straftat stehen“
- ⚠ Vorsicht, ist **nicht** „Quick-Freeze“!

Exkurs: E-Evidence-Verordnung

- ab 18.08.2026 gültig, sieht harte Fristen vor (Notfälle: 6 Stunden)

- Speicher- und/oder Herausgabeanordnungen, für vier Arten:

  Subscriber Data
  Identitäts- und Adressdaten von Kunden, welche Dienste gebucht wurden und wie gezahlt wird, also Bestandsdaten

  Access Data
  Metadaten zur konkreten Inanspruchnahme eines Dienstes: Datum und Uhrzeit, IP-Adresse, User-ID

  Transactional Data
  Metadaten zur Art der Nutzung von Diensten: Absender und Empfänger von E-Mails, Geolokation der Endgeräte, genutzte Protokolle.

  Content Data
  gespeicherte Inhaltsdaten, also Text, Bild, Ton oder Video.

- Diensteanbieter müssen Rechtmäßigkeit selbst prüfen!

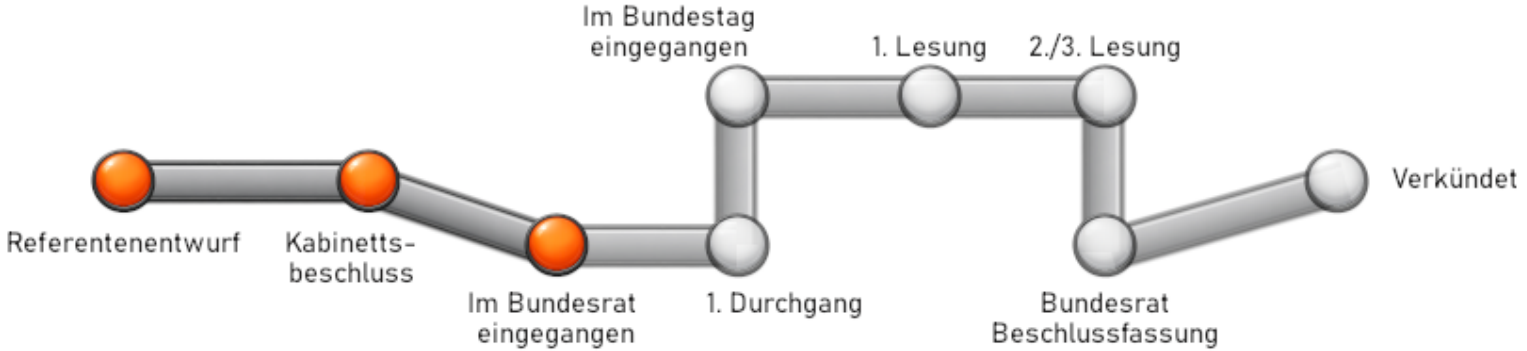
„EU-Sicherungsanordnung“

- Knüpft an E-Evidence an
- Jede Staatsanwaltschaft darf diese anordnen
- In „begründeten Notfällen“ auch Ermittler, Finanzbehörden (und Zollbehörden)
- Hierdurch wohl Öffnung für EU-weite Anordnung (siehe Art. 6 Abs. 3 E-Evidence-Verordnung)
- ..weitere Varianten: § 52 Abs. 3 BkaG, § 25a Abs.1 BPolG-Entwurf

Kritik am VDS 3.0-Entwurf

- totalitärer Ansatz eines Generalverdachts (gegen **alle** Bürger)
- Grundrechtsschonende Alternativen (wie Quick-Freeze) möglich
- unzulässig hohe Dauer der Speicherung (z.B. BfDI-Kritik)
- Hohe Kosten & Aufwände für Verpflichtete, kaum Entschädigung
- bei Symmetric NAT nur mit Ziel-IP eindeutig → extremer Eingriff
- in Kombination mit anderen Gesetzen sehr kritisch!

Gesetzgebungsverfahren



Vielen Dank an:

- Soll noch vor Sommerpause im Bundestag beschlossen werden!
- Geht dort wsl. in folgende Ausschüsse:
  - Digitales und Staatsmodernisierung
  - Recht und Verbraucherschutz
  - Innen

Bundestagszusammenfasser.de/details?docid=1133

Bonus: Nationaler Normenkontrollrat

- Stellungnahme 17.04.26 zum Entwurf überwiegend not amused:
  - **„Kein Nutzen dargestellt“**
  - **„(liefert) den Entscheidern kein realitätsnahes Bild der Regelungsfolgen“**
  - **„entgegen Beschlusslage keine Angaben zu der One in, one out-Regel“**
  - Haken an „Digitalcheck durchgeführt“
- Auszug der Antwort Bundesregierung 01.05.26:
  - „Die Aufwände, die den Anbietern von Internetzugangsdiensten […] entstehen, **kann die Bundesregierung nicht darstellen**, da die Unternehmen hierzu keine aussagekräftigen Informationen liefern konnten.“

Vielen Dank. Eure Fragen?

- jetzt (im Stream) oder gerne auch später an der Bar

Vielen Dank für Eure Aufmerksamkeit!

Ergänzende Slides

Begriffe nach §3 TKG

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

3. **„Anschlusskennung“** eine Rufnummer oder andere eindeutige und einmalige Zeichenfolge, die einem bestimmten Anschlussinhaber dauerhaft zugewiesen ist und die Telekommunikation über den jeweiligen Anschluss eindeutig und gleichbleibend kennzeichnet;

13. **„Endnutzer“** ein Nutzer, der weder öffentliche Telekommunikationsnetze betreibt noch öffentlich zugängliche Telekommunikationsdienste erbringt;

25. **„Kennung“** einem Nutzer, einem Anschluss oder einem Endgerät zu einem bestimmten Zeitpunkt zugewiesene eindeutige Zeichenfolge, die eine eindeutige Identifizierung des Nutzers, des Anschlusses oder des Endgerätes ermöglicht;

44. **„öffentlich zugängliche Telekommunikationsdienste“** einem unbestimmten Personenkreis zur Verfügung stehende Telekommunikationsdienste;

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

„Anschlussinhaber“

Verpflichtung zur Erfassung von Anschlussinhabern in unter bestimmten Umständen:

Telekommunikationsgesetz (TKG)
§ 172 Daten für Auskunftsersuchen der Sicherheitsbehörden

(1) Wer nummerngebundene interpersonelle Telekommunikationsdienste, Internetzugangsdienste oder Dienste, die ganz oder überwiegend in der Übertragung von Signalen bestehen, erbringt und dabei Rufnummern oder andere Anschlusskennungen vergibt oder Telekommunikationsanschlüsse für von anderen vergebene Rufnummern oder andere Anschlusskennungen bereitstellt, hat für die Auskunftsverfahren nach den §§ 173 und 174 vor der Freischaltung folgende Daten zu erheben und unverzüglich zu speichern, auch, soweit diese Daten für betriebliche Zwecke nicht erforderlich sind:

1. die Rufnummern,
2. andere von ihm vergebene Anschlusskennungen,
3. den Namen und die Anschrift des Anschlussinhabers,
4. bei natürlichen Personen deren Geburtsdatum,
5. bei Festnetzanschlüssen die Anschrift des Anschlusses,
6. in Fällen, in denen neben einem Mobilfunkanschluss auch ein Mobilfunkendgerät überlassen wird, die Gerätenummer dieses Gerätes sowie
7. das Datum der Vergabe der Rufnummer und, soweit abweichend, das Datum des Vertragsbeginns.

Das Datum der Beendigung der Zuordnung der Rufnummer und, sofern davon abweichend, das Datum des Vertragsendes sind bei Bekanntwerden ebenfalls zu speichern. Die Sätze 1 und 2 gelten auch, sofern die Daten nicht in Endnutzerverzeichnisse eingetragen werden. Für das Auskunftsverfahren nach § 174 ist die Form der Datenspeicherung freigestellt.