

# Information Governance

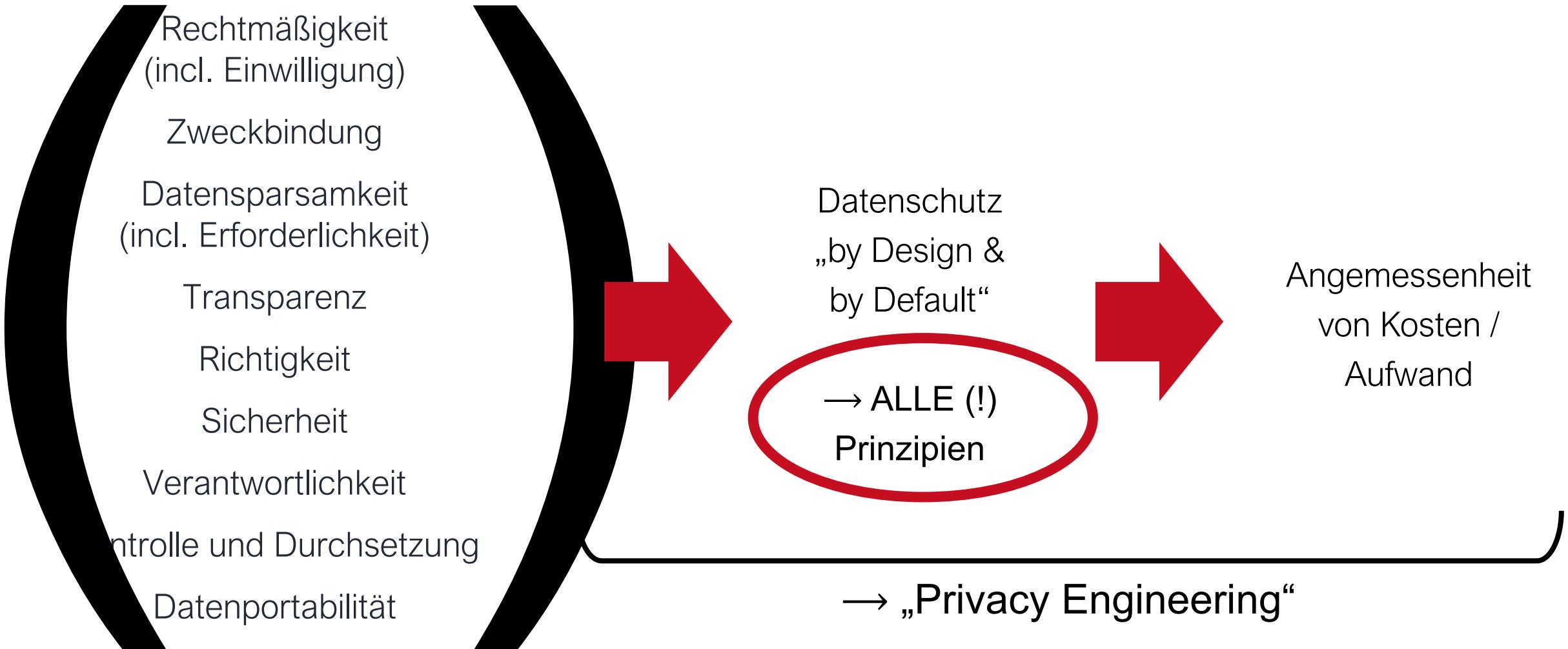
## Lesson 10: Datenschutz 3 – Surveillance



Frank Pallas

*Information Systems Engineering*  
TU Berlin

# „by Design & by Default“



9+1 Prinzipien – „Privacy by Design“ / „Privacy Engineering“

Technische Umsetzung von Datensparsamkeit

Wieviel Security ist angemessen? Experimente

Technische Ansätze für Transparenz (und Zweckbindung)

Technische Datenschutz-Mechanismen existieren (insb. in der wissenschaftlichen Diskussion) vor allem für die Prinzipien Sicherheit und Datensparsamkeit („Anonymisierung“ etc.)

Tatsächlich sind aber technische Ansätze **für alle Prinzipien** notwendig

→ „Privacy Engineering Beyond Anonymization and Security“

# 9 Kernprinzipien des Datenschutzes

Rechtmäßigkeit (incl. Einwilligung)

Zweckbindung

Datensparsamkeit (incl. Erforderlichkeit)

## Transparenz

Richtigkeit

Sicherheit (insb. Vertraulichkeit, Integrität, Verfügbarkeit)

Verantwortlichkeit (incl. nachweisbare Rechtskonformität)

Kontrolle und Durchsetzung

Datenportabilität

# GDPR: „Transparenz“

Werden personenbezogene Daten bei der betroffenen Person erhoben, **so teilt der Verantwortliche der betroffenen Person** zum Zeitpunkt der Erhebung dieser Daten **Folgendes mit:**

- a) den Namen und die Kontaktdaten des Verantwortlichen [...]
  - b) gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten;
  - c) die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung;
  - d) [...]
  - e) gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten und
  - f) gegebenenfalls die Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln [...]
- [...]

Art. 13 DSGVO (s.a. Art. 14, 15, 30)

# GDPR: „Transparenz“

The screenshot shows a web browser window displaying the PayPal 'List of Third Parties' document. The title is 'List of Third Parties (other than PayPal Customers) with Whom Personal Information May be Shared'. It is effective as of 1 January 2018. A red arrow points to the top right corner of the page. Below the table, there is a note about previous versions and a 'Print' button.

>> [View all legal agreements](#)

## List of Third Parties (other than PayPal Customers) with Whom Personal Information May be Shared

Effective as of 1 January 2018

[Print](#)

The previous "List of Third Parties (other than PayPal Customers) with Whom Personal Information May be Shared" is available [here](#).

Category	Party Name and Jurisdiction (in brackets)	Purpose	Data Disclosed
<b>1. Payment Processors</b>	Barclays Bank Plc (UK), HSBC Bank Plc (UK, Ireland), HSBC Merchant Services LLP (UK), Bank of America N.A. (EMEA, USA), BA Continuum India Private Limited (India), Discover Financial Services (USA), JPMorgan Chase Bank (UK, USA), BNP Paribas (France), Netgiro (Sweden), StarFinanz (Germany), Wells Fargo (Ireland, USA), American Express (USA),	To allow payment processing settlement services, and fraud	Name, address, details of user funding instruments, and details of payment



# GDPR: „Transparenz“

products and devices to provide a more tailored and consistent experience on all Facebook products you use, wherever you use them. For example, we allow one Facebook Product when you sign up for an account on a different Product, location-related information: We use location-related information such as check-ins or events you attend. Product over whether we use this technology for you. Ads and other sponsored content: We use the information we have about you—including information about Settings and Instagram Settings. Provide measurement, analytics, and other business services. We use the information we have (including your activity and services. Learn how we share information with these partners: Promote safety, integrity and security. We use the information we have to verify account terms or policies, or when we need help from our users. We use the information we have to help you stay safe. For example, we use Facebook Security Help Center and Instagram Security Tips. Consider following our Safety and Privacy Best Practices. People and accounts you share and communicate with. Your network can also help you share or download things you've shared or downloaded through your profile on Facebook; and

# We Read 150 Privacy Policies. They Were an Incomprehensible Disaster.

**By Kevin Litman-Navarro**

In the background here are several privacy policies from major tech and media platforms. Like most privacy policies, they're verbose and full of legal jargon — and opaquely establish companies' justifications for collecting and selling your data. The data market has become the engine of the internet, and these privacy policies we agree to but don't fully understand help fuel it.

# We Read 150 Privacy Policies. They Were an Incomprehensible Disaster

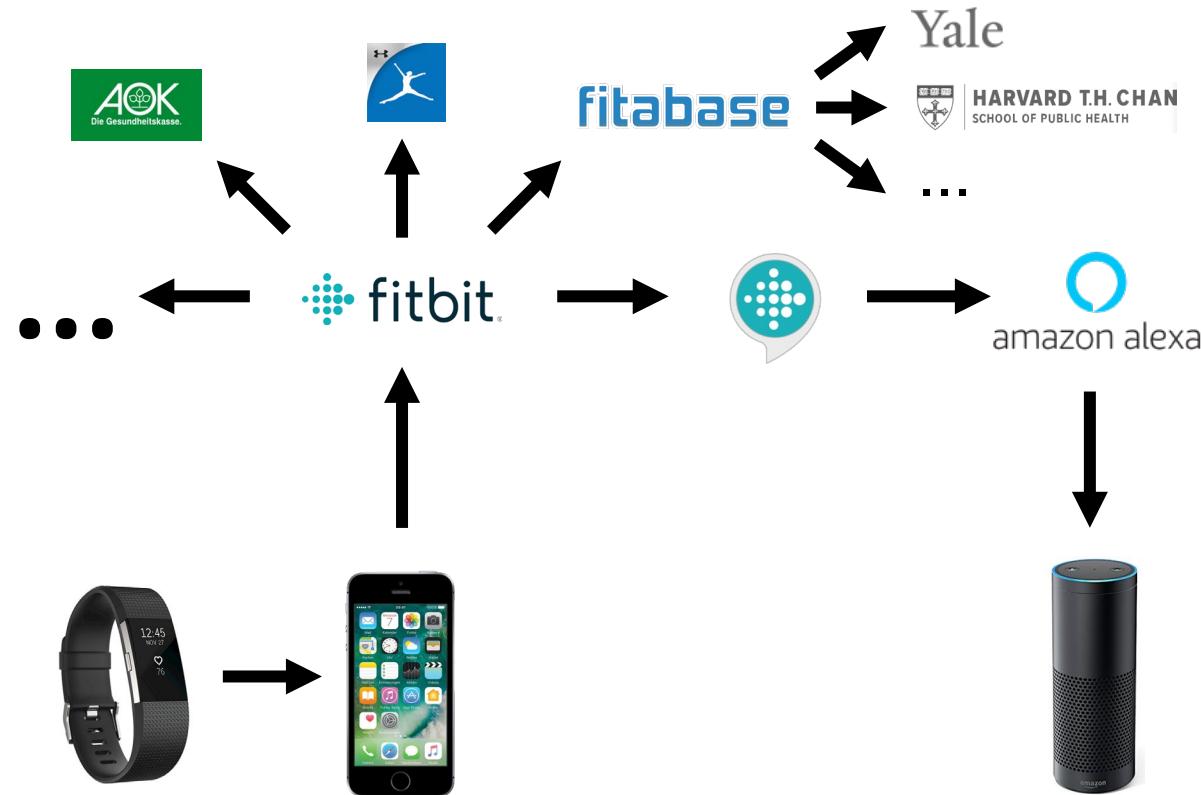
**By Kevin Litman-Navarro**

**In the background here are several privacy policies from major tech and media platforms. Like most privacy policies, they're verbose and full of legal jargon — and opaquely establish companies' justifications for collecting and selling your data.**

**The data market has become the engine of the internet, and these privacy policies we agree to but don't fully understand help fuel it.**



# Transparenz in aktuellen Szenarien



Wer bekommt welche Daten auf welcher Rechtsgrundlage?

Auch hier:  
Aufwände für Individuum zu hoch  
(und Darstellung zu kompliziert/unverständlich), als dass Informationen in der Realität tatsächlich rezipiert würden

→ Technische Repräsentation von Transparenzinformationen?

# GDPR: „Transparenz“

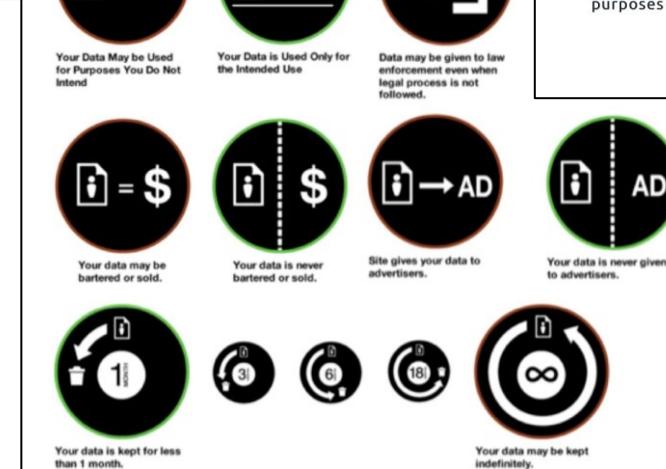
## **Transparent information, communication and modalities for the exercise of the rights of the data subject**

1. The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

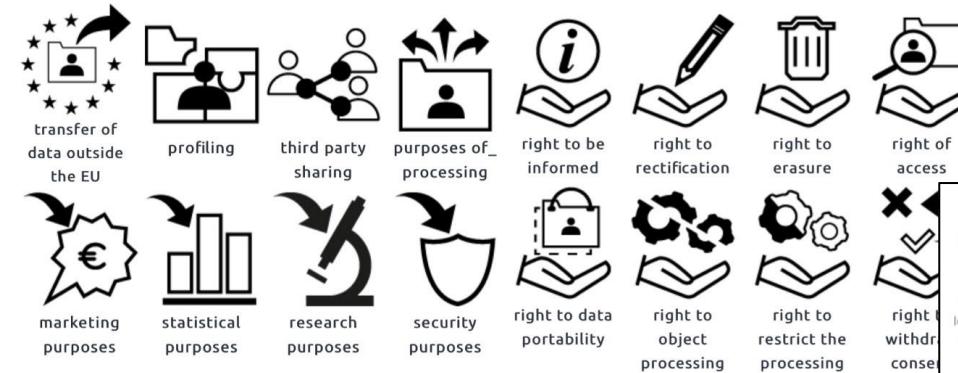
7. The information to be provided to data subjects pursuant to Articles 13 and 14 may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing. Where the icons are presented electronically they shall be machine-readable.

# GDPR: Transparenz und Icons

TYPE OF DATA COLLECTED	GENERAL DATA PRACTICES	DATA SHARING
contact: name, mailing address, email, or phone number	ad customization: user data may be used for the purpose of customizing advertising	affiliates: affiliates and subsidiaries bound by the same privacy practices
computer: IP address, browser type, or operating system	third party tracking: she allows third parties to place advertisements that may track user behavior	contractors: third party contractors bound by the same privacy practices
interactive: browsing behavior or search history	public display: service allows users to contribute information which may be displayed publicly	third parties: third parties not subject to same data practices
financial: account status or activity, credit information, or purchase history	user control: users allowed to access and correct personal data collected	
content: contents of personal communications, stored documents or media	data retention: explicitly stated duration of retention for personal data collected	



## DaPIS: The Data Protection Icon Set



**PRIVACY NOTICE**

If you create an account, Fitbit will collect:

- Your location, when location features, such as maps, are active
- Your name, height, and weight
- When and how long you walk
- Your heart rate throughout the day

You do not need a Fitbit account to use the basic functions of your Fitbit, such as distance and heart rate monitoring, and step count.

What data do we share and with whom?

- Companies providing services to Fitbit
- Organizations you specifically direct Fitbit to share data with (e.g. Facebook)
- Fitbit friends you've listed (opt-out of sharing with friends in your profile settings)

Fitbit may share or sell aggregated information that does not identify you.

How long do we keep your data?

- Until you delete your Fitbit account (even if you remove it from your profile)

# Transparenz: Trennen von Bereitstellung und Darstellung (Provision vs. Presentation)

Controller A

```

15   "controller": {
      "name": "Green Company AG",
      "division": "Product line e-mobility",
      "address": "Wolfsburger Ring 2, 38440 Berlin",
      "country": "DE",
      "representative": {
        "name": "Jane Super",
        "email": "contact@greencompany.de",
        "phone": "0049 151 1234 5678"
      }
    },
    "dataProtectionOfficer": {
      "name": "Jane Super",
      "address": "Wolfsburger Ring 2, 38440 Berlin",
      "country": "DE",
      "email": "contact@greencompany.de",
      "phone": "0049 151 1234 5678"
    },
    "dataDisclosed": [
      {
        "_id": "f1424ff6-ca0f-4f0c-9438-43cc000509931",
        "category": "E-mail address",
        "purposes": [
          ...
        ]
      }
    ]
  }
}

```

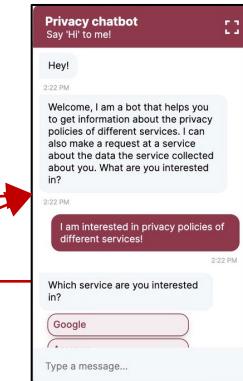
Provision      Presentation

Controller B

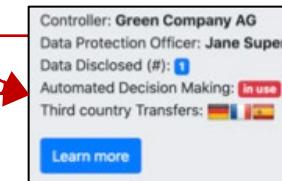
```

15   "controller": {
      "name": "Green Company AG",
      "division": "Product line e-mobility",
      "address": "Wolfsburger Ring 2, 38440 Berlin",
      "country": "DE",
      "representative": {
        "name": "Jane Super",
        "email": "contact@greencompany.de",
        "phone": "0049 151 1234 5678"
      }
    },
    "dataProtectionOfficer": {
      "name": "Jane Super",
      "address": "Wolfsburger Ring 2, 38440 Berlin",
      "country": "DE",
      "email": "contact@greencompany.de",
      "phone": "0049 151 1234 5678"
    },
    "dataDisclosed": [
      {
        "_id": "f1424ff6-ca0f-4f0c-9438-43cc000509931",
        "category": "E-mail address",
        "purposes": [
          ...
        ]
      }
    ]
  }
}

```



Chatbots



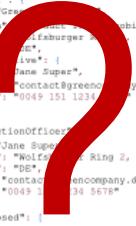
Browser plugins



# Transparenz: Bereitstellung in maschinenlesbarer Form

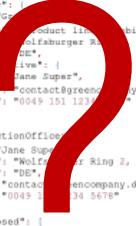
Provision | Presentation

Controller A



```
15   "controller": {
16     "name": "Green Company",
17     "division": "Product Line Mobility",
18     "address": "Wolfsburger Ring 2, 38440 Berlin",
19     "country": "DE",
20     "representative": {
21       "name": "Jane Super",
22       "email": "contact@greencompany.de",
23       "phone": "0049 151 123 45678"
24     }
25   },
26   "dataProtectionOfficer": {
27     "name": "Jane Super",
28     "address": "Wolfsburger Ring 2, 38440 Berlin",
29     "country": "DE",
30     "email": "contact@greencompany.de",
31     "phone": "0049 151 123 45678"
32   },
33   "dataDisclosed": [
34     {
35       "_id": "f142af0f-4f0c-9438-43cc00509931",
36       "category": "B",
37       "address": "",
38       "purposes": []
39     }
40   ],
41   ...
42 }
```

Controller B

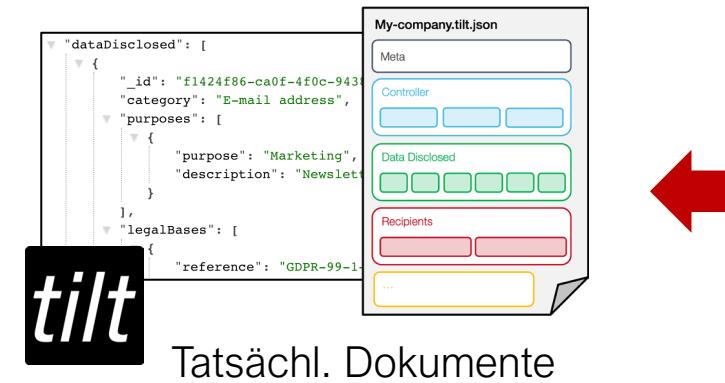


```
15   "controller": {
16     "name": "Green Company",
17     "division": "Product Line Mobility",
18     "address": "Wolfsburger Ring 2, 38440 Berlin",
19     "country": "DE",
20     "representative": {
21       "name": "Jane Super",
22       "email": "contact@greencompany.de",
23       "phone": "0049 151 123 45678"
24     }
25   },
26   "dataProtectionOfficer": {
27     "name": "Jane Super",
28     "address": "Wolfsburger Ring 2, 38440 Berlin",
29     "country": "DE",
30     "email": "contact@greencompany.de",
31     "phone": "0049 151 123 45678"
32   },
33   "dataDisclosed": [
34     {
35       "_id": "f142af0f-4f0c-9438-43cc00509931",
36       "category": "B",
37       "address": "",
38       "purposes": []
39     }
40   ],
41   ...
42 }
```

# Transparenz: Bereitstellung in maschinenlesbarer Form

## Transparency and modalities

Rechtliche Anforderungen (z.B. DSGVO)

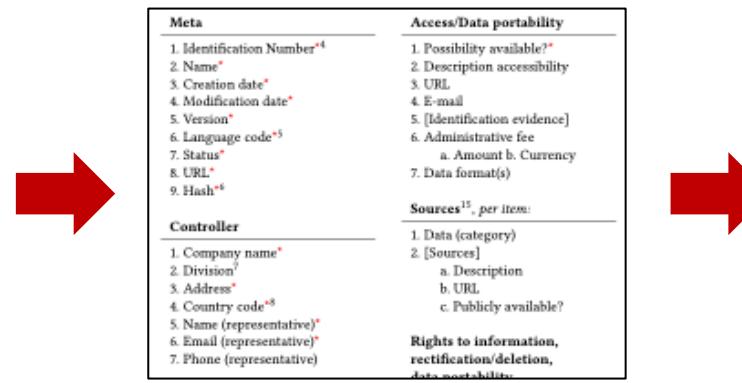


```
    "controller": {
        "name": "Green Company AG",
        "division": "Product line e-mobility",
        "address": "Wolfshburger Ring 2, 38440 Berlin",
        "country": "DE",
        "representative": {
            "name": "Jane Super",
            "email": "contact@greencompany.de",
            "phone": "0049 151 1234 5678"
        }
    },
    "dataProtectionOfficer": {
        "name": "Jane Super",
        "address": "Wolfshburger Ring 2, 38440 Berlin",
        "country": "DE",
        "email": "contact@greencompany.de",
        "phone": "0049 151 1234 5678"
    },
    "dataDisclosed": [
        {
            "_id": "f1424f86-ca0f-4fd0-9438-43cc00509931",
            "category": "E-mail address",
            "purposes": [
                {
                    "name": "Marketing"
                }
            ]
        }
    ]
}
```

Rechtlich abgeglichene,  
maschinenlesbare Repräsentation

Reference(s)		Transparency information		
13 (1a)	14 (1a)	30 (1a)	Controller	
13 (1b)	14 (1b)	30 (1a)	Data protection officer	
13 (1c)	14 (1c)	15 (1a)	30 (1b)	Purposes
13 (1c)	14 (1c)			Legal basis
13 (1d)	14 (2b)			Legitimate interests
13 (1e)	14 (1e)	15 (1c)	30 (1d)	Recipient (categories)
13 (1f)	14 (1f)	15 (1c)	30 (1e)	Third country transfer
13 (1f)	14 (1f)	15 (2)	30 (1e)	Adequacy (third country)
13 (1f)	14 (1f)	15 (2)	30 (1e)	Access and Data portability
13 (2a)	14 (2a)	15 (1d)	30 (1f)	Retention or storage criteria

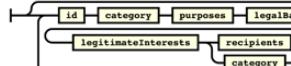
## Kategorisierung



Detaillierte Analyse benötigter Ausdrucksmächtigkeit

```
dataDisclosed := {
  id,
  category,
  purposes,
  legalBases,
  legitimateInterests,
  (recipients | category),
  storage,
  nonDisclosure,
  [addProp]
};

65
70
```



# Formale Sprachspezifikation

# Technische Repräsentation von Transparenzinformationen im Einklang mit GDPR-Anforderungen

**TILT: A GDPR-Aligned Transparency Information Language and Toolkit for Practical Privacy Engineering**

Anonymous Author(s)

**ABSTRACT**  
In this paper, we present TILT, a transparency information language and toolkit explicitly designed to represent and process transparency information in line with the requirements of the GDPR and allowing for a more automated and adaptive use of such information than established, legalistic data protection policies do.

We provide a detailed analysis of transparency obligations from the GDPR to identify the expressiveness required for a formal transparency language intended to meet specific legal requirements. In addition, we identify a set of further, non-functional requirements that need to be met to foster practical application in real-world (web) information systems engineering. On this basis, we specify our formal language and present a respective, fully implemented toolkit around it. We then evaluate the practical applicability of our language and toolkit and demonstrate the additional prospects it unlocks through two different use cases: a) the inter-organizational analysis of persons' data-related practices allowing, for instance, to uncover data sharing networks based on explicitly announced transparency information and b) the presentation of formally represented transparency information to users through novel, more comprehensible, and potentially adaptive user interfaces, heightening data subjects' actual informedness about data-related practices and, thus, their sovereignty.

Altogether, our transparency information language and toolkit allow – differently from previous work – to express transparency information in line with actual legal requirements and practices of modern (web) information systems engineering and thereby pave the way for a multitude of novel possibilities to heighten transparency and user sovereignty in practice.

**CCS CONCEPTS**  
• Applied computing → Law; • Information systems → Information systems applications; • Web data description languages; • Software and its engineering → Formal language definitions; • Context specific languages; • Security and privacy → Privacy protections;

**KEYWORDS**  
Data transparency, GDPR, data protection, privacy by design, legal informatics, privacy engineering

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without prior permission or fee. This permission does not extend to other kinds of copying, such as copying for general distribution for profit, for advertising or promotional purposes, for creating new collective works, or for resale. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Contact permissions@acm.org.  
FACIT, 2021, 10 months, Canada  
© 2021 Association for Computing Machinery.  
ACM ISBN 978-1-4503-8888-8...\$xx.00  
<https://doi.org/xx.xxx/xxx>

**grünwald und pallas (2021)**

<https://github.com/Transparency-Information-Language>

```

15      "controller": [
20        "name": "Green Company AG",
25        "division": "Product line e-mobility",
30        "address": "Wolfsburger Ring 2, 38440 Berlin",
35        "country": "DE",
        "representative": [
          "name": "Jane Super",
          "email": "contact@greencompany.de",
          "phone": "0049 151 1234 5678"
        ]
      },
      "dataProtectionOfficer": [
        "name": "Jane Super",
        "address": "Wolfsburger Ring 2, 38440 Berlin",
        "country": "DE",
        "email": "contact@greencompany.de",
        "phone": "0049 151 1234 5678"
      ],
      "dataDisclosed": [
        {
          "_id": "f1424f86-ca0f-4f0a-943",
          "category": "E-mail address",
          "purposes": [
            ...
          ]
        }
      ]
    }
  }
}

```

Formale, maschinenlesbare  
Repräsentation

**Privacy chatbot**  
Say 'Hi' to me!

Hey!  
2:22 PM

Welcome, I am a bot that helps you to get information about the privacy policies of different services. I can also make a request at a service about the data the service collected about you. What are you interested in?

2:22 PM

I am interested in privacy policies of different services!

Which service are you interested in?  
Google

Type a message...

**Controller: Green Com**  
**Data Protection Officer: Jane Super**  
**Data Disclosed (#): 1**  
**Automated Decision Making: IN USE**  
**Third country Transfers: DE, ES**

**Learn more**

**Neue Darstellungsmöglichkeiten**

# Zweckbindung: Technische Umsetzung

**Towards Application-Layer Purpose-Based Access Control**

— Preprint ACM SAC 2020 —

Frank Pallas TU Berlin Information Systems Engineering Research Group Berlin, Germany fp@ise.tu-berlin.de	Max-R. Ulbricht TU Berlin Information Systems Engineering Research Group Berlin, Germany mu@ise.tu-berlin.de	Stefan Tai TU Berlin Information Systems Engineering Research Group Berlin, Germany st@ise.tu-berlin.de
Thomas Peikert TU Berlin thomas.peikert@campus.tu-berlin.de	Marcel Reppenagen TU Berlin marcel.reppenagen@campus.tu-berlin.de	Daniel Wenzel TU Berlin daniel.wenzel@campus.tu-berlin.de
Paul Wille TU Berlin paul.wille@campus.tu-berlin.de	Karl Wolf TU Berlin karl.wolf@campus.tu-berlin.de	

**Preprint, to appear in: The 35th ACM/SIGAPP Symposium On Applied Computing (ACM SAC 2020), Brno, Czech Republic, March 30-April 3, 2020.**  
**Final version available at:**  
<https://doi.org/10.1145/3341105.3375764>

**ABSTRACT**

In this paper, we propose an architecturally novel approach to implementing purpose-based access control in practice. Different from previous proposals, our approach resides on the application instead of the data(base) layer. This allows for significantly better integration with established architectures and practices of real-world application engineering and to achieve database independence.

To validate practical applicability, we provide two exemplary implementations and briefly assess the introduced overhead in matters of achievable throughputs. Results significantly depend on data and query type but basically suggest bearable overheads for realistic applications even though possible performance optimizations have not been implemented in our proofs-of-concept yet. Our approach thus proposes significantly better practical feasibility than previous ones and exhibits reasonable overheads. It therefore paves the way for purpose-based access control to be actually adopted in practice.

**KEYWORDS**

Privacy, data protection, purpose limitation, access control, PBAC, privacy by design, privacy engineering, web engineering

**1 INTRODUCTION**

Privacy by Design<sup>1</sup> (PbD) is one of the core concepts of modern privacy legislation, aiming at the effective implementation of privacy principles through concrete technologies and their design. For instance, the European General Data Protection Regulation (GDPR) requires data controllers to "implement appropriate technical and organisational measures [...] designed to implement principles [...] in an effective manner and to integrate safeguards into the processing" [10, Art. 25 (1)].

Noteworthy, this obligation refers to "data purposes" in general. Even though (academic) discussions largely revolve around data minimization (pseudonymization, etc.) and security, other principles also need to be addressed properly.

Of the various established privacy principles at those codified in Art. 5 of the GDPR, we herein consider principle of purpose limitation and the possibility to it technically, "by Design". Basically, purpose limitation is codified in Art. 5 of the GDPR.

Personal data shall be [...] collected for specific and legitimate purposes and not further processed in a manner that is incompatible with those purposes [10, Art. 5 (1 b)]

Other examples vividly illustrating the particular purpose limitation throughout the regulatory regime include the limitation of individually provided for more specific purposes" (Art. 6 (1)), the rigorous pursuit for processing special categories of personal data in Art. 9, or the obligations to inform data subjects about which data is collected and processed given in Art. 15. The track of the purposes that certain pieces of personal information are used for and ensuring these limitations to actually be met is thus a core obligation for any party collecting personal data under the regime of the GDPR.

Related work on purpose limitation, however, has mostly focused at data-at-rest, that is, data persisted in a database and accessed (for a particular purpose) later on. Respective technical mechanisms are typically subsumed under the term "purpose-based access control (PBAC)". Concrete implementations proposed include low-level database extensions often referred to as "Hippocratic Databases" [2]-[4] as well as higher-level approaches integrating PBAC into established programming abstractions for database access such as object-relational-mappers (ORMs) [5].

Surprisingly, little attention has been paid on purpose limitation and PBAC for data-in-transit, that is, data traveling through the network by means of communication middleware. With event-driven architectures and stream-based processing, data may not necessarily be persisted anymore, but runs

<sup>1</sup>Being well aware of the slightly different notions between "Privacy" and "Data Protection", we use these terms interchangeably herein.

2021 IEEE 25th International Enterprise Distributed Object Computing Conference (EDOC)

**Messaging with Purpose Limitation – Privacy-Compliant Publish-Subscribe Systems**

Karl Wolf Information Systems Engineering TU Berlin Berlin, Germany kw@ise.tu-berlin.de	Frank Pallas Information Systems Engineering TU Berlin Berlin, Germany fp@ise.tu-berlin.de	Stefan Tai Information Systems Engineering TU Berlin Berlin, Germany st@ise.tu-berlin.de
--	---	---

**Abstract**—Purpose limitation is an important privacy principle to ensure that personal data may only be used for the declared purposes it was originally collected for. Ensuring compliance with respective privacy regulations like the GDPR, which codify purpose limitation as an obligation, consequently, is a major challenge in real-world enterprise systems. Technical solutions usually focus on data being held always in databases, while PBAC for communication and publish-subscribe messaging in particular has received only little attention. In this paper, we argue for PBAC to be also applied to data-in-transit and introduce and study a concrete proof-of-concept implementation, which extends a popular MQTT message broker with purpose limitation. On this basis, purpose limitation as a core privacy principle can be applied in enterprise IoT and message-driven integration architectures that do not focus on databases but event-driven communication and integration instead.

**Index Terms**—purpose limitation, publish-subscribe, messaging, GDPR, privacy, privacy engineering

**I. INTRODUCTION**

Privacy is of key importance to any enterprise. Regulations like the GDPR [1] in the EU specifically prescribe how personal information is (not) to be used by organizations. Among the core principles of regulations like the GDPR is the principle of purpose limitation. This privacy principle requires purposes for the processing of data to be specified and that compliance to declared purposes must be ensured.

In particular, our contributions are:

- An in-depth analysis of requirements and prerequisites to be taken into account when introducing purpose-awareness to publish-subscribe systems,
- A model and design to introduce purpose-related functionalities – particularly allowing the publication of data to be bound to sets of hierarchically structured allowed (AIP) and prohibited intended purposes (PIP) and subscriptions to be made for explicitly specified access purposes (APs) – to existing MQTT brokers while still providing backward compatibility for clients without dedicated purpose-related functionality,
- A proof-of-concept implementation for a purpose-aware MQTT broker, enforcing said purpose restrictions against APs at different filtering points in time (on publish, on subscribe, etc.),
- An easy-to-use Python client library allowing to integrate respective purpose-related capabilities into sending and receiving clients with low effort, and

**Examiners:** Prof. Dr.-Ing. Stefan Tai, TU Berlin  
**Prof. Dr.-Ing. David Bermbach, TU Berlin**

**Advisors:** Dr.-Ing. Frank Pallas, TU Berlin  
**M. Sc. Karl Wolf, TU Berlin**

**Submitted by**

**2022-09-20**

Information Governance  
 22

ISEngineering

# Beispiele: PEng@ISE

## YaPPL - A Lightweight Privacy Preference Language for Legally Sufficient and Automated Consent Provision in IoT Scenarios\*

Max-R. Ulbricht<sup>[0000-0001-7134-4351]</sup> and Frank Pallas<sup>[0000-0002-5543-0265]</sup>

## RedCASTLE: Practically Applicable $k_s$ -Anonymity for IoT Streaming Data at the Edge in Node-RED

Frank Pallas  
fp@ise.tu-berlin.de  
TU Berlin, Information Systems Engineering  
Berlin, Germany

Niklas Amslgruber  
n.amslgruber@campus.tu-berlin.de  
TU Berlin  
Berlin, Germany

Julian Legler  
julian.legler@campus.tu-berlin.de  
TU Berlin  
Berlin, Germany

Elias Grünewald  
eg@ise.tu-berlin.de  
TU Berlin, Information Systems Engineering  
Berlin, Germany

## Hawk: DevOps-driven Transparency and Accountability in Cloud Native Systems

Elias Grünewald, Jannis Kiesel, Siar-Remzi Akbayin, and Frank Pallas  
Information Systems Engineering, Technische Universität Berlin  
{gruenewald, kiesel, s.akbayin, frank.pallas}@tu-berlin.de

Lawfulness  
(incl. consent)

Purpose Limitation

Data minimization  
(incl. necessity)

Transparency

Accuracy

Security

Accountability

Data Access & Portability

Enforcement

## Messaging with Purpose Limitation – Privacy-Compliant Publish-Subscribe Systems

Karl Wolf  
Information Systems Engineering  
TU Berlin  
Berlin, Germany  
kw@ise.tu-berlin.de

Frank Pallas  
Information Systems Engineering  
TU Berlin  
Berlin, Germany  
fp@ise.tu-berlin.de

Stefan Tai  
Information Systems Engineering  
TU Berlin  
Berlin, Germany  
st@ise.tu-berlin.de

## TILT: A GDPR-Aligned Transparency Information Language and Toolkit for Practical Privacy Engineering

Elias Grünewald  
Technische Universität Berlin  
Information Systems Engineering Research Group  
Berlin, Germany  
gruenewald@tu-berlin.de

Frank Pallas  
Technische Universität Berlin  
Information Systems Engineering Research Group  
Berlin, Germany  
frank.pallas@tu-berlin.de

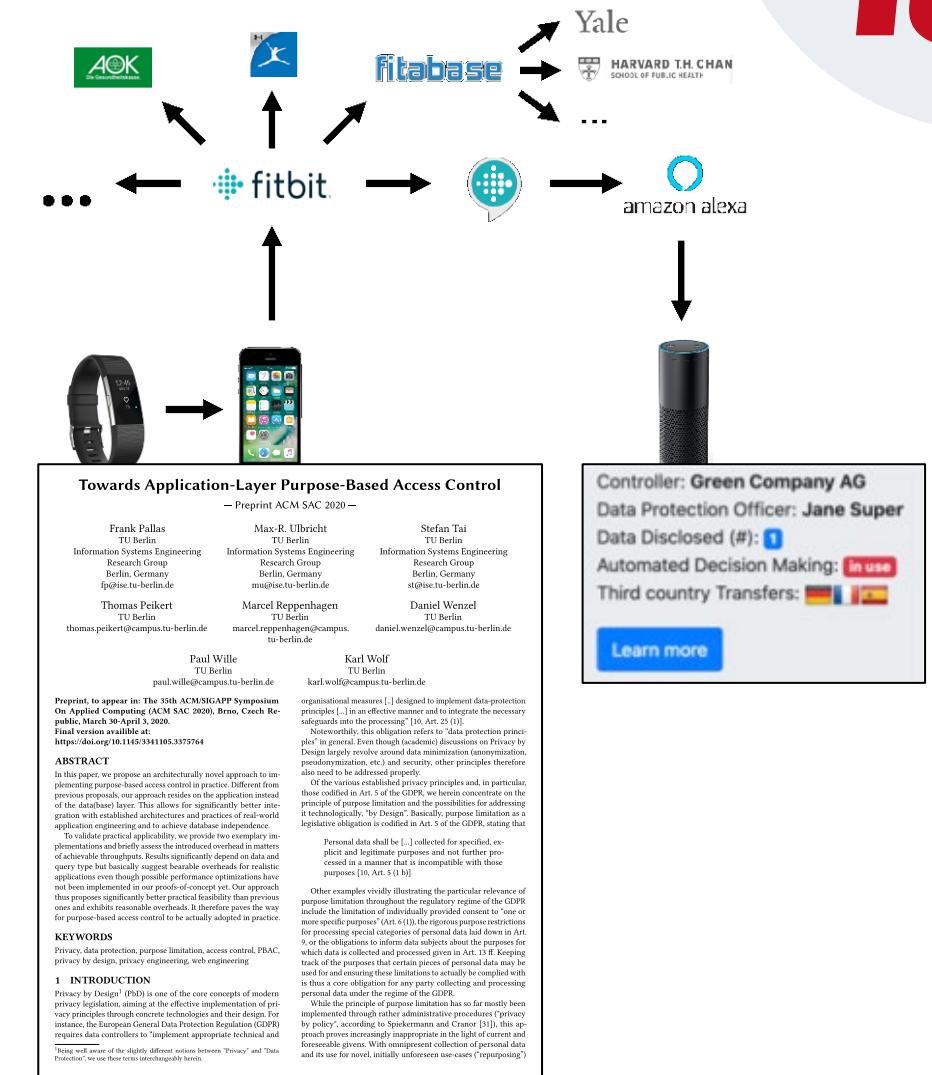
**Streamlining personal data access requests:  
From obstructive procedures to automated web workflows**

Nicola Leschke<sup>[0000-0003-0657-602X]</sup>, Florian Kirsten<sup>[0000-0002-9202-6640]</sup>,  
Frank Pallas<sup>[0000-0002-5543-0265]</sup>, and Elias Grünewald<sup>[0000-0001-9076-9240]</sup>

...

# Privacy Engineering: Jenseits von Sicherheit und Minimierung

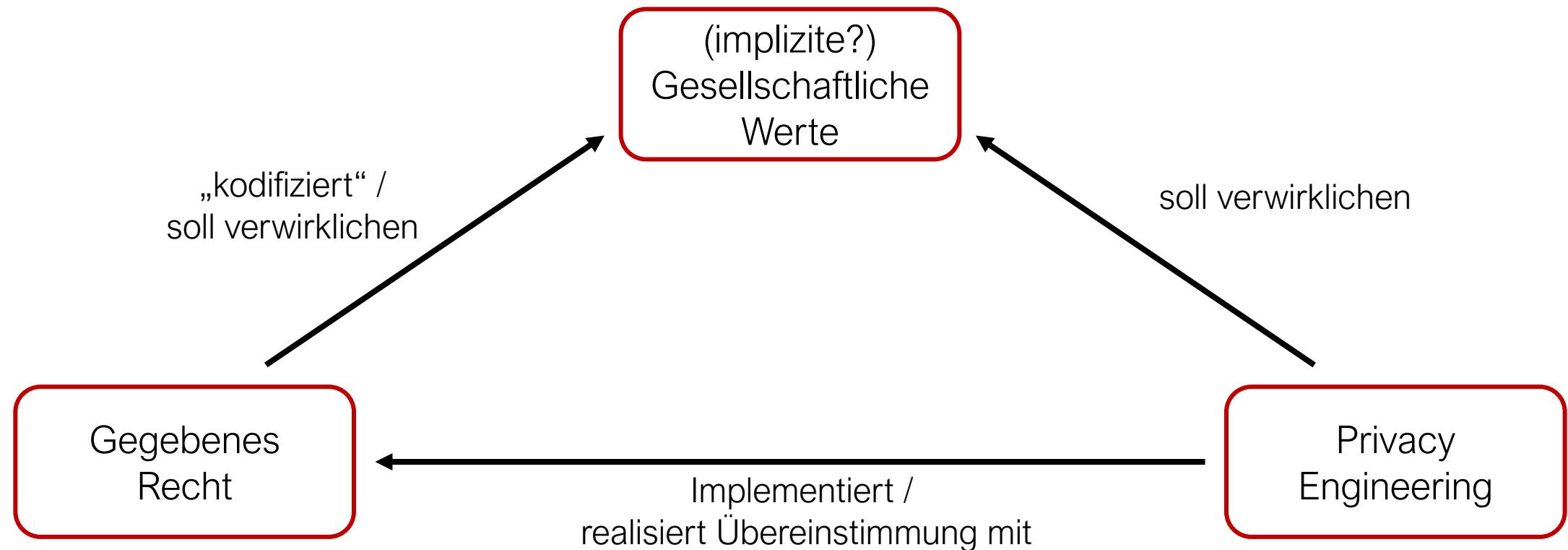
- Technische Mechanismen für Privacy / Data Protection by Design derzeit vor allem für Datensparsamkeit / -minimierung und Sicherheit
- Tatsächlich sind aber technische Ansätze für **alle Prinzipien** notwendig
- Auch Prinzipien wie Transparenz oder Zweckbindung lassen sich technisch abbilden
- Wichtig dabei: **Tatsächliche** rechtliche Anforderungen und **Implementierungsaufwand** in aktuellen Technologiestacks etc. von Beginn an mitdenken!



# „Privacy Engineering“



# „Privacy Engineering“?

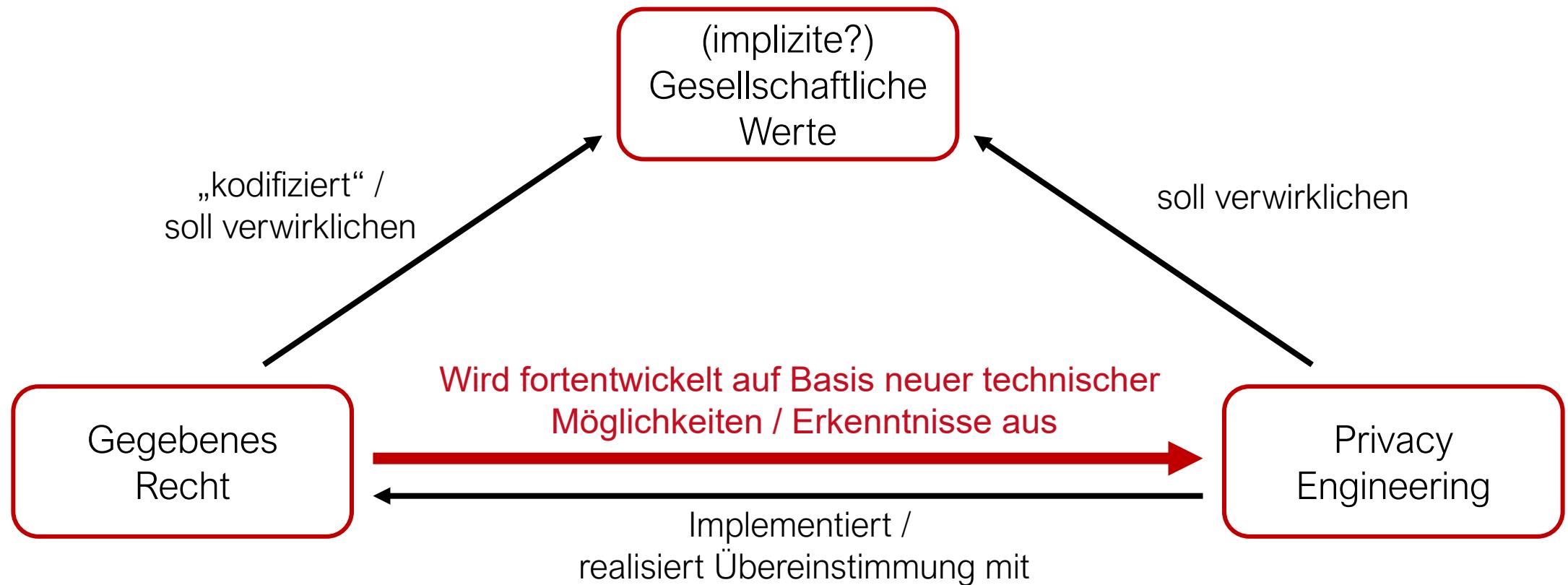


## **Transparent information, communication and modalities for the exercise of the rights of the data subject**

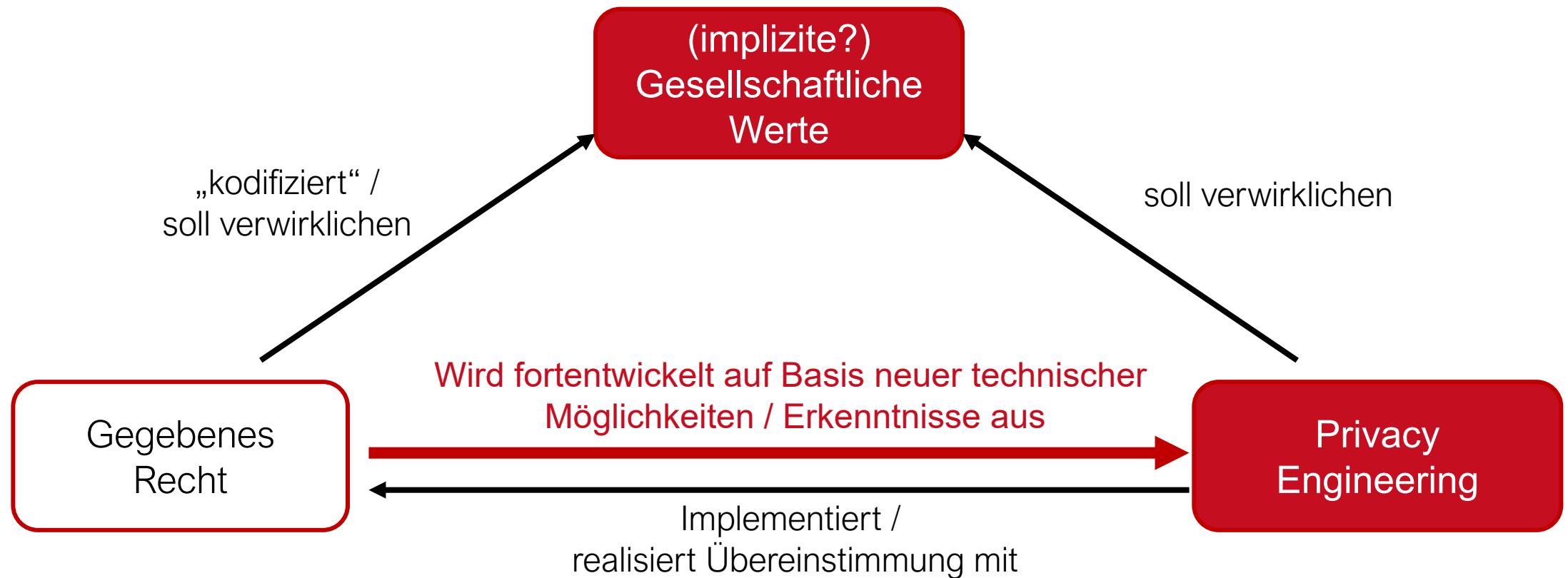
1. The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

7. The information to be provided to data subjects pursuant to Articles 13 and 14 may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing. Where the icons are presented electronically they shall be machine-readable.

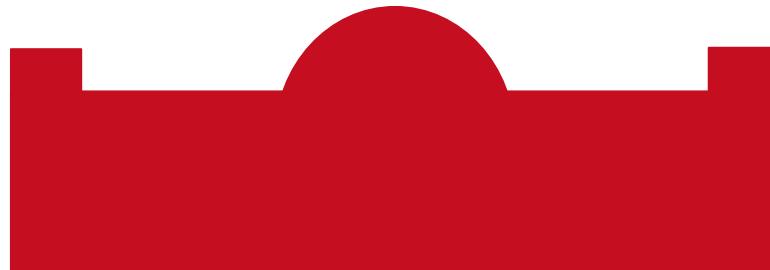
# „Privacy Engineering“?



# „Privacy Engineering“?



# Information Governance – The Horizontal Policy Elevator



- Technische Fortentwicklung des „Stands der Technik“ und des „mit angemessenem Aufwand Umsetzbaren“
- Neue explizite und implizite Verpflichtungen zur Umsetzung

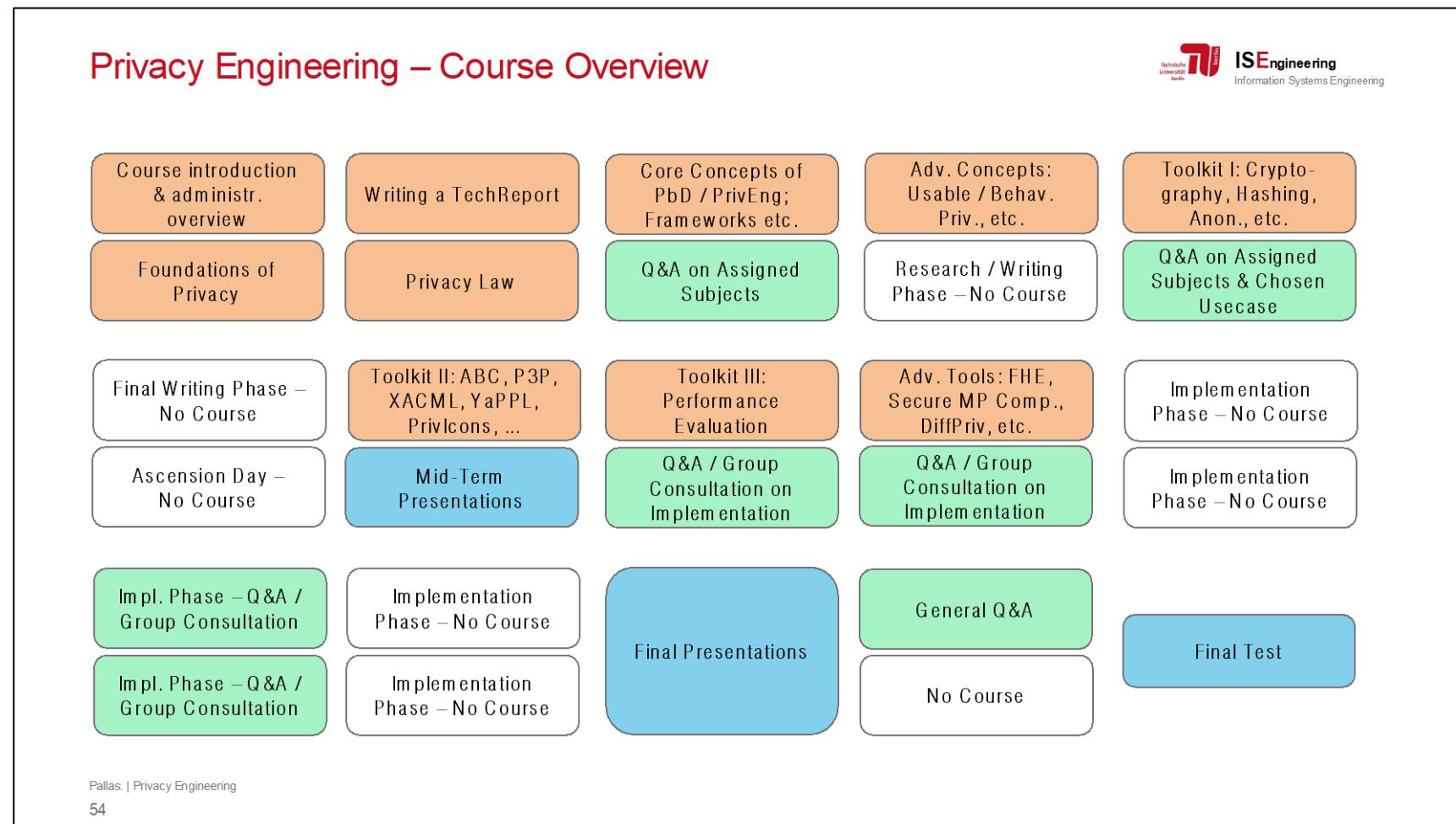
# More Privacy Engineering?

## Privacy Engineering

Lesson 1: Kick-Off / Introduction / Domain Overview “Privacy Engineering”

A large, stylized red starburst graphic containing the text "PEng" in white. The starburst has several points and is set against a yellow background.

# More Privacy Engineering?



→ Inter-/transdisziplinär, Implementierungsfokus, SoSe, Master

## Das Verhältnis von „Datenschutz“ und „Überwachung“

Benthams „Panopticon“ – now and then

Konflikte mit (anderen) staatlichen Aufgaben

Freiheit vs. Sicherheit? Zum Umgang mit sich  
widersprechenden Grundrechten

## Recap: Datenschutz

→ Ohne personenbezogene (oder „personenbeziehbare“)  
Daten keine Anwendbarkeit der DSGVO

(und des Datenschutzrechts im Allgemeinen)

Missing:

# Datenschutz? Privacy?

## 1. Lesung

Keine Unterstützung für Forderung nach IP-Adressen-Speicherung



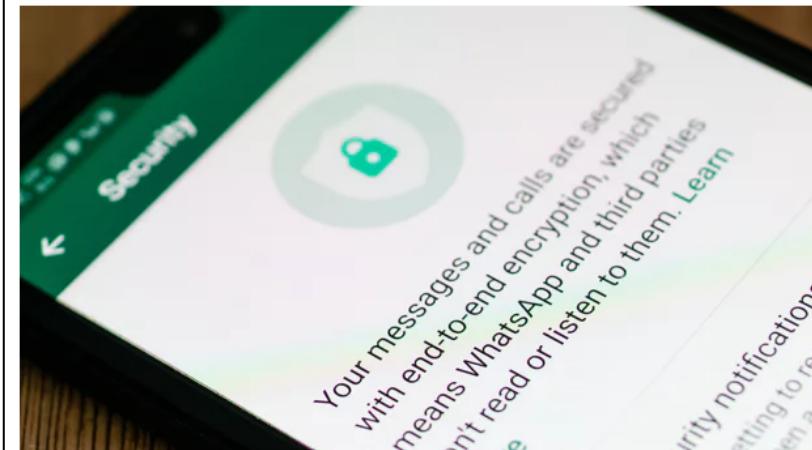
Der Bundestag hat am **Donnerstag, 29. September 2022**, erstmals über einen Antrag der Unionsfraktion mit dem Titel „**IP-Adressen rechtssicher speichern und Kinder vor sexuellem Missbrauch schützen**“ (20/3687) beraten. Im Anschluss der Aussprache wurde der Antrag zur federführenden Beratung an den Rechtsausschuss überwiesen. In ihrem Antrag, der von den anderen Fraktionen scharf kritisiert wurde, bezieht sich die Unionsfraktion auf ein Urteil des Europäischen Gerichtshofs (EuGH) zur deutschen Vorratsdatenspeicherung und begrüßt, dass **Bundesinnenministerin Nancy Faeser (SPD)** die Möglichkeiten aus dem EuGH-Urteil nutzen wolle.

## Messenger-Überwachung: Faesers Position zu Chatkontrolle stößt auf viel Kritik

Der SPD-nahe Verein D64 schlägt Alarm: Die Position des Innenministeriums zu einem EU-Entwurf laufe "auf das Ende der Privatheit von Kommunikation hinaus".

Lesezeit: 6 Min.  In Pocket speichern

64



# Vorratsdatenspeicherung, Quellen-TKÜ & Co

**EU-Staatschefs und Innenminister drängen auf neue Vorratsdatenspeicherung**

**Europäischer Rat der Europäischen Union**

Die Innenminister von Bund und Ländern halten es für nötig, vorläufiger Messanger-Überwachung: Faesers Position zu Chatkontrolle stößt auf viel Kritik

Messenger-Überwachung: Faesers Position zu Chatkontrolle stößt auf viel Kritik

Der SPD-nahe Verein D64 schlägt Alarm: Die Position des Innenministeriums zu einem EU-Entwurf laufe "auf das Ende der Privatheit von Kommunikation hinaus".

Rat der EU | Pressemitteilung | 14. Dezember 2017

**Verschlüsselung: durch Verschlüsselung an**

**WhatsApp-Überwachung**

**Die Bundesregierung sollbruchstellen**

Ein Gastbeitrag von Sven H.

Deutschland treibt auf EU-Ebene Sicherheitsbehörden Einblicke in verschlüsselte Kommunikationen. Das würde die IT-Sicherheit aller Bürger schwächen.

(Bild: Lenscap Photography/Shutterstock.com)

03.12.2020, 12:25 Uhr

**Bundesverfassungsgericht**

**Posteo muss Kunden überwachen können**

Ermittler wollten von Posteo die IP-Adressen eines Kunden abrufen. Diese Daten gab Posteo nicht. Muss er aber können, hat nun der BVerfG entschieden.

Von Patrick Beuth

**Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens**

Vom 17. August 2017

Der Bundestag hat das folgende Gesetz beschlossen:

- 2. In § 129 Absatz 4 wird die Angabe „100c“ durch die Angabe „100b“ ersetzt.
- 3. § 266a Absatz 4 Satz 2 wird wie folgt geändert:

**Artikel 1**

**EuGH bestätigt: keine anlasslose Vorratsdatenspeicherung – mit Ausnahmen**

Vorratsdatenspeicherung ist unter bestimmten Voraussetzungen möglich – wenn die nationale Sicherheit bedroht ist. Ohne Anlass widerspricht sie EU-Recht.

Die Innenminister von Bund und Ländern haben Maßnahmen gegen Rechtsextremismus beschlossen. Die Beschlüsse gehen Politikern von CDU und CSU nicht weit genug.

Datenschutz?

Privacy?

Anzuwendendes Recht?

### Art. 10 GG:

- „(1) Das **Briefgeheimnis** sowie das **Post- und Fernmeldegeheimnis** sind unverletzlich.
- (2) **Beschränkungen** dürfen nur **auf Grund eines Gesetzes** angeordnet werden.  
Dient die Beschränkung dem Schutze der freiheitlichen demokratischen  
Grundordnung [...]“

# Fernmeldegeheimnis

§3, Abs. 1 TTDSG („Telekommunikation und Telemedien“):

Dem **Fernmeldegeheimnis** unterliegen der **Inhalt** der **Telekommunikation** und ihre **näheren Umstände**, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche.

# Fernmeldegeheimnis

§170, Abs. 1 TKG (**Telekommunikationsgesetz**):

(1) Wer eine Telekommunikationsanlage betreibt, [...] hat [...] ab dem Zeitpunkt der Betriebsaufnahme auf eigene Kosten technische Einrichtungen zur Umsetzung **gesetzlich vorgesehener Maßnahmen zur Überwachung** der Telekommunikation vorzuhalten [...]

# Fernmeldegeheimnis

... usw. usf. ...

# Rechtliche Fragen von Überwachung & Co.



# „Privatheit“ von Telekommunikation im Recht

Überwachung insb. von Telekommunikation ist rechtlich nicht das Gleiche wie das Erheben und Verarbeiten personenbezogener Daten.

Telekommunikation (-überwachung) ist in eigenen rechtlichen Vorgaben (insb. TKG, TTDSG) geregelt

Verfassung statuiert grundsätzliches Fernmeldegeheimnis, sieht aber gesetzliche Ausnahmen explizit vor.

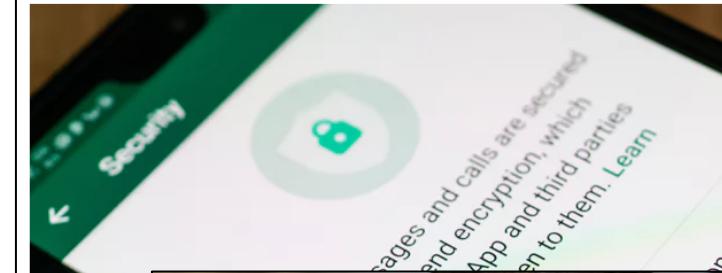
Materialisiert z.B. in Pflicht zur Vorhaltung von Überwachungseinrichtungen in §170 TKG (oder auch in Regelungen der StPO)

Messenger-Überwachung: Faesers Position zu Chatkontrolle stößt auf viel Kritik

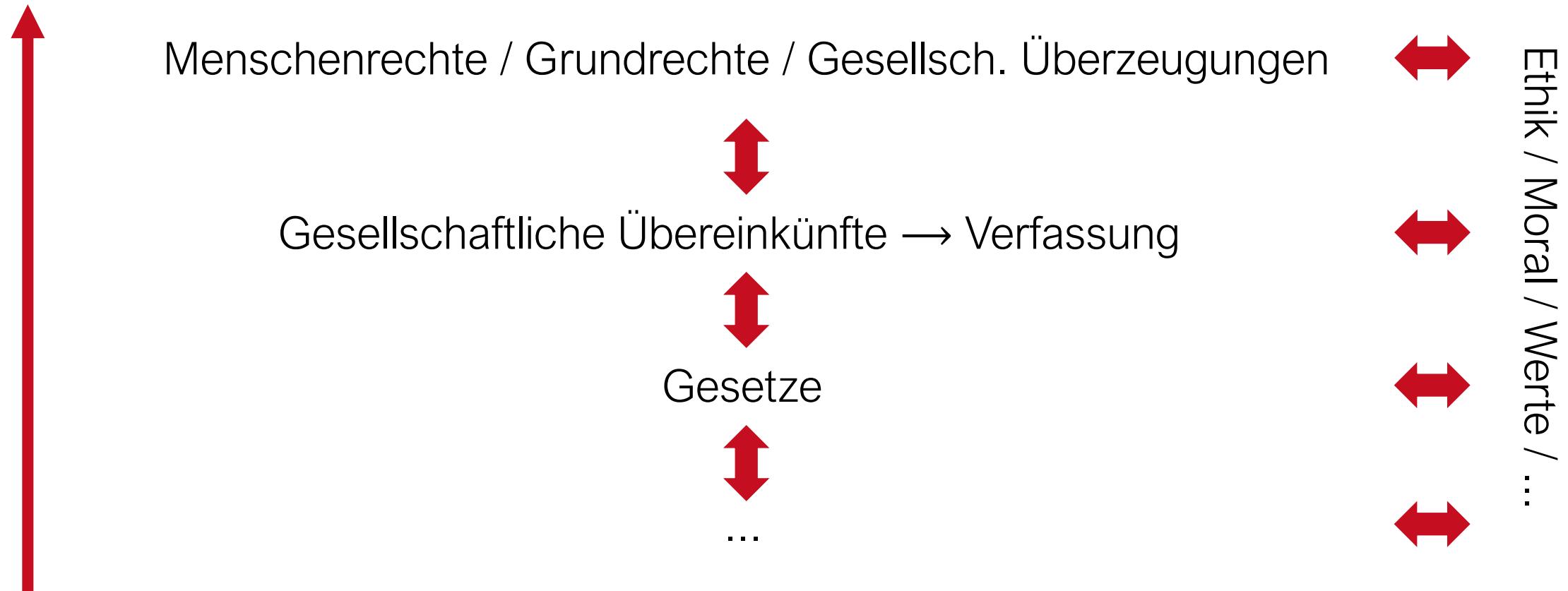
Der SPD-nahe Verein D64 schlägt Alarm: Die Position des Innenministeriums zu einem EU-Entwurf laufe "auf das Ende der Privatheit von Kommunikation hinaus".

Lesezeit: 6 Min. In Pocket speichern

64



# „Normenhierarchie“



# „Privatheit“ als Grundrecht

Grundrechtecharta der EU, Art. 7:

„Everyone has the right to respect for his or her **private and family life, home and communications.**“

Grundrechtecharta der EU, Art. 8:

„Everyone has the right to the **protection of personal data** concerning him or her [...]“

# „Privatheit“ als Grundrecht

Mit Dokumenten wie der allg. Erklärung der Menschenrechte, der EU-Grundrechtecharta etc. haben wir uns als „Weltgemeinschaft“ darauf verständigt, dass alle Menschen ein Grundrecht auf Privatheit / Datenschutz / „Privacy“ haben.

Dass der Begriff semantisch unterschiedlich verstanden wird, sei dahingestellt.

Verständnis zuallererst als „Recht des Individuum“, dass etwas nicht geschieht (→ sog. „Abwehrrecht“, dazu später mehr)

Rolle von „Privatheit“ jenseits moralischer Ansprüche des Individuums?



Das Verhältnis von „Datenschutz“ und „Überwachung“

Benthams „Panopticon“ – now and then

Konflikte mit (anderen) staatlichen Aufgaben

Freiheit vs. Sicherheit? Zum Umgang mit sich  
widersprechenden Grundrechten

# Benthams Panopticon



- Gefängnisarchitektur
- Nur ein (oder wenige) Überwacher\*innen im Zentrum
- Überwacher\*in kann alle Insass\*innen sehen
- Insass\*innen können Überwacher\*innen nicht sehen
- Insass\*innen wissen, dass sie überwacht werden **können**
- Effekt: Insass\*innen verhalten sich entsprechend („als ob“)

Caroline Haskins Nov 10, 2023, 10:58 PM CET



The former de Koepel prison in Haarlem has been converted into office spaces. Hanneke Luijting/Getty Images

- In 2022, Amazon opened office space in de Koepel, a former prison in Haarlem, the Netherlands.
- The prison, which is built in a panopticon design, was active from 1901 to 2016.

<https://www.businessinsider.com/amazon-office-former-prison-de-koepel-netherlands-2023-11>

## Benthams „Weisheiten“

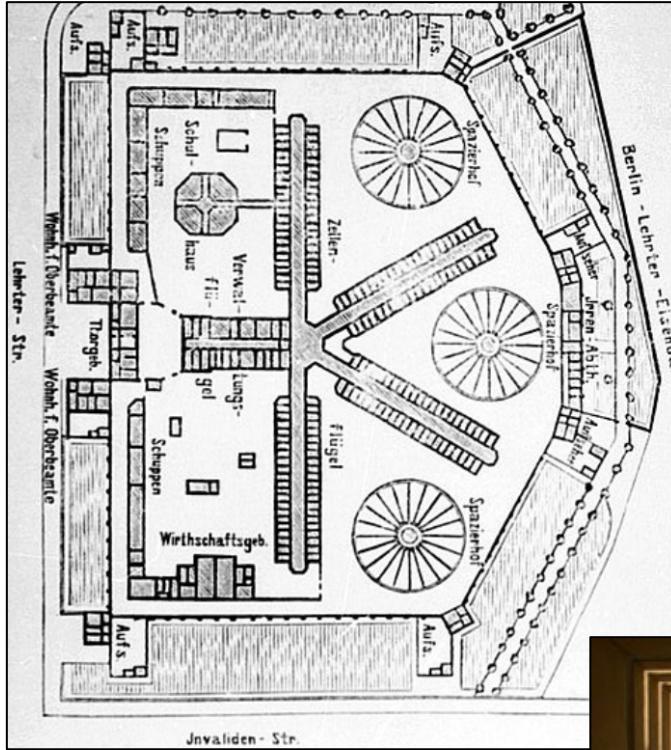
„[S]eeing without being seen“

„[T]he persons to be inspected should always feel themselves  
as if under inspection“

„A new mode of obtaining power of mind over mind, in a quantity  
hitherto without example“

→ Allein die **Möglichkeit des Überwachtwerdens** führt zu verändertem Verhalten

# Zellengefängnis Moabit



# Bentham heute



Videoüberwachung am Berliner Südkreuz

27.07.2018, 15:39 Uhr

## Technik erkennt "abweichendes Verhalten"

Nach der automatischen Gesichtserkennung wird die Videoüberwachung am Bahnhof Südkreuz ausgebaut. Sie soll mehr Szenarien beherrschen als bisher bekannt. VON [HANNES HEINE](#)



## Die sichere GPS-Telefonuhr für Ihr Kind

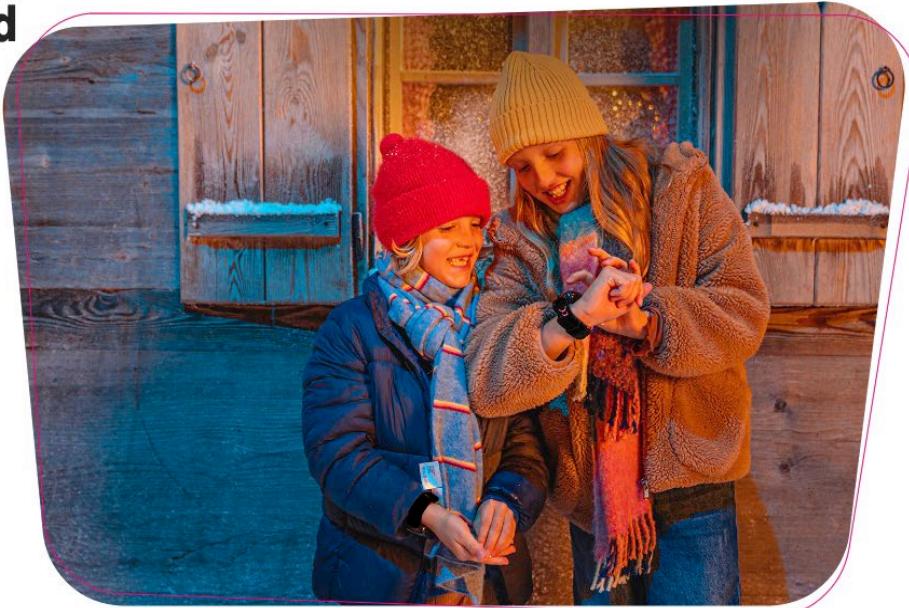
Kids Watch XPLORA X5 Play eSIM



Für die Nutzung der Kids Watch XPLORA X5 Play eSIM benötigen Sie einen Tarif. Unsere Empfehlung: Tarif Smart Connect S mit Top-Gerät.

Kids Watch XPLORA X5 Play eSIM für **1 € einmalig** bei einer Laufzeit von 24 Monaten.

Bis zum 31.12. sparen Sie 3 Monate lang den Grundpreis im Tarif Smart Connect S mit Top-Gerät **für 0 € statt 9,95 € mtl.**



## Kaufempfehlung: PAJ GPS – Easy Finder



Marke: PAJ GPS

Farbe: Schwarz

Größe: 7,8 x 4,0 x 2,7 cm

Gewicht: 93 g

Telefonfunktion: Nein

SOS-Funktion: Ja

GPS Standortbestimmung: Ortung über Smartphone-App

Folgekosten durch Sim-Karte: Sim Karte inklusive, Jährliche Abokosten

**ELTERN AKTUELL**

**KAUFTIPP**

[www.eltern-aktuell.de](http://www.eltern-aktuell.de)

**48,99 EUR** ✓Prime

Bei Amazon kaufen

Der PAJ GPS ist eine günstige Lebensversicherung für Sie und Ihre Lieben. Als Rundum-Sorgenlos-Paket aus integrierter M2M SIM-Karte und einem monatlichen Abonnement, kann das Gerät kinderleicht installiert und in Betrieb genommen werden. Neben der eingebauten SOS-Taste, gibt es zusätzliche Extras wie ein Erschütterungsalarm, einen Geschwindigkeitsalarm, 100-Tage-Streckenspeicher sowie die Möglichkeit einen Geozaun einzustellen. Das Gerät verfügt über eine Ausschaltssicherung und kann vielseitig eingesetzt werden – eignet sich jedoch besonders für Kinder oder Demenzerkrankte.

# Bentham heute

... usw. usf. ...

# Problem?

# „Volkszählungsurteil“

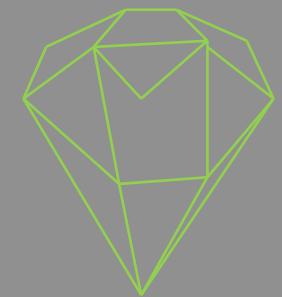
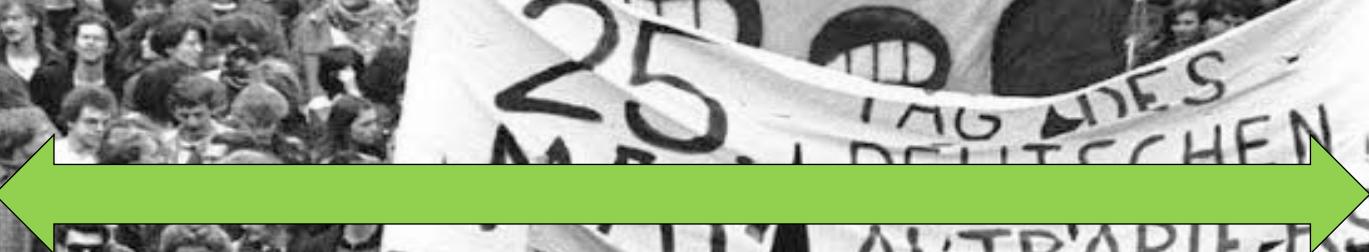
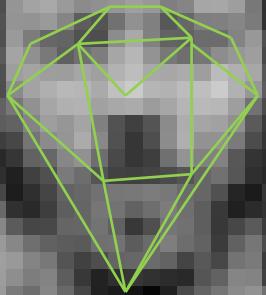


„Wer damit rechnet, daß etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird [...], wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte [...] verzichten. Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, [...].“

BVerfGE 65,1 – „Volkszählung“

Anonymität kann gesellschaftlich wünschenswertes  
Handeln fördern / überhaupt erst ermöglichen

„Georg Schwalzach“



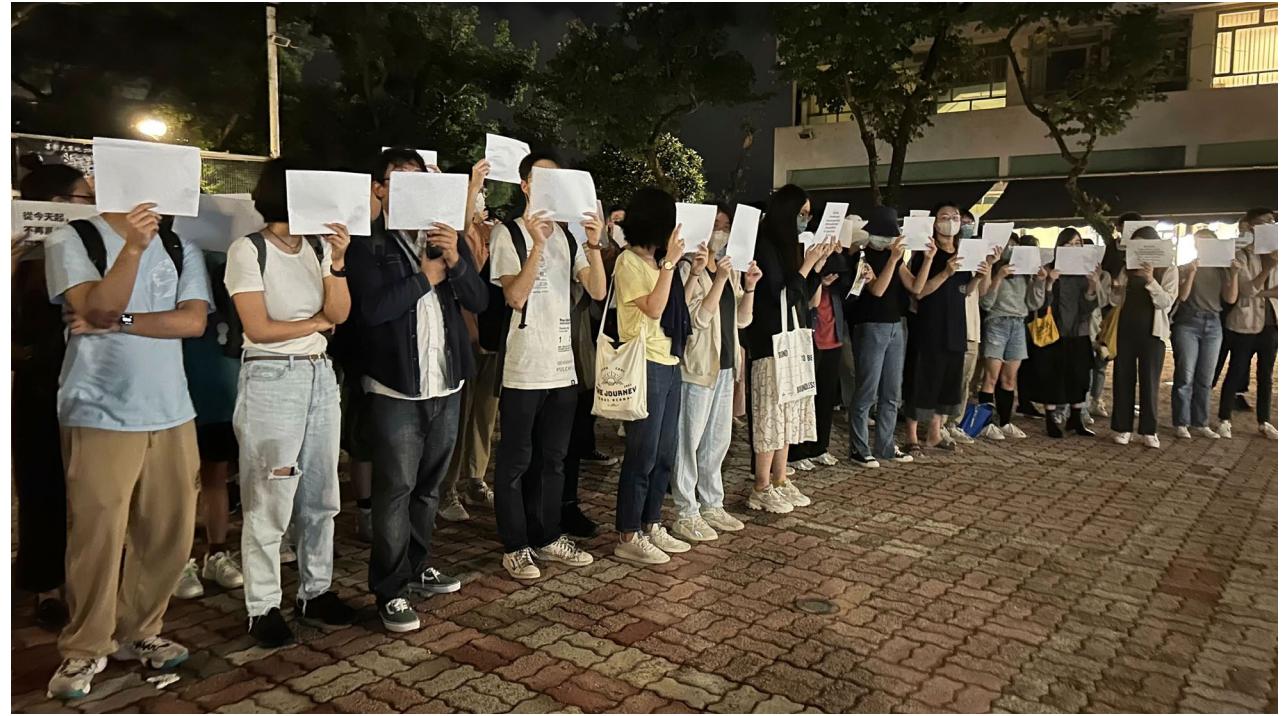
Bildquelle: <http://ais.badische-zeitung.de/piece/00/8d/22/e3/9249507.jpg>

# Bentham heute




<https://www.nytimes.com/2022/06/25/technology/china-surveillance-police.html>

Die Anonymität „in der Masse“ kann  
„unter den Bedingungen moderner Datenverarbeitung“  
nicht mehr angenommen werden.



Gesellschaftliche Fortentwicklung ohne (praktische und als solche empfundene) Möglichkeit zu Widerspruch und Nonkonformität?



Gesellschaftliche Fortentwicklung ohne (praktische und als solche empfundene) Möglichkeit zu Widerspruch und Nonkonformität?



Gesellschaftliche Fortentwicklung ohne (praktische und als solche empfundene) Möglichkeit zu Widerspruch und Nonkonformität?



Gesellschaftliche Fortentwicklung ohne (praktische und als solche empfundene) Möglichkeit zu Widerspruch und Nonkonformität?

■ ■ ■

Gesellschaftliche Fortentwicklung ohne (praktische und als solche empfundene) Möglichkeit zu Widerspruch und Nonkonformität?

„Privatheit“ als notwendige Vorbedingung  
gesellschaftlicher Fortentwicklung!

Wenn das aber so ist...

# „Privatheit“ gesellschaftlich wünschenswert?

## 1. Lesung

Keine Unterstützung für Forderung nach IP-Adressen-Speicherung



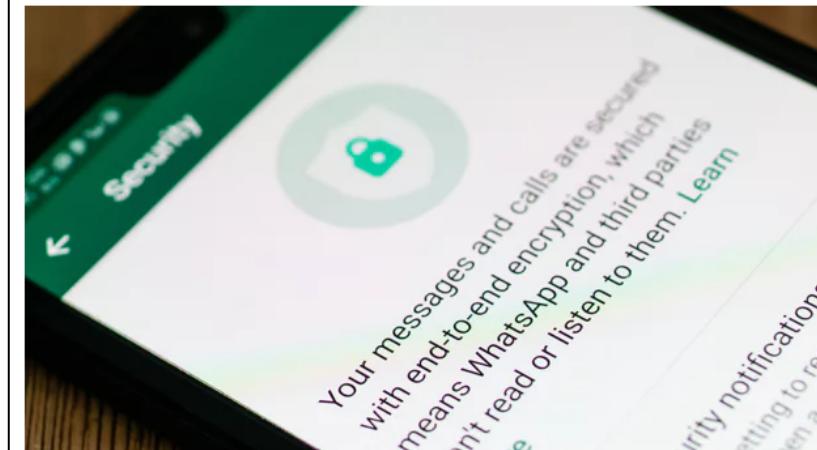
Der Bundestag hat am **Donnerstag, 29. September 2022**, erstmals über einen Antrag der Unionsfraktion mit dem Titel „**IP-Adressen rechtssicher speichern und Kinder vor sexuellem Missbrauch schützen**“ (20/3687) beraten. Im Anschluss der Aussprache wurde der Antrag zur federführenden Beratung an den Rechtsausschuss überwiesen. In ihrem Antrag, der von den anderen Fraktionen scharf kritisiert wurde, bezieht sich die Unionsfraktion auf ein Urteil des Europäischen Gerichtshofs (EuGH) zur deutschen Vorratsdatenspeicherung und begrüßt, dass **Bundesinnenministerin Nancy Faeser (SPD)** die Möglichkeiten aus dem EuGH-Urteil nutzen wolle.

## Messenger-Überwachung: Faesers Position zu Chatkontrolle stößt auf viel Kritik

Der SPD-nahe Verein D64 schlägt Alarm: Die Position des Innenministeriums zu einem EU-Entwurf laufe "auf das Ende der Privatheit von Kommunikation hinaus".

Lesezeit: 6 Min.  In Pocket speichern

64



# „Privatheit“ gesellschaftlich wünschenswert?

**EU-Staatschefs und Innenminister drängen auf neue Vorratsdatenspeicherung**

**Europäischer Rat der Europäischen Union**

Die Innenminister von Bund und Ländern halten es für nötig, vorläufiger Messanger-Überwachung: Faesers Position zu Chatkontrolle stößt auf viel Kritik

Der SPD-nahe Verein D64 schlägt Alarm: Die Position des Innenministeriums zu einem EU-Entwurf laufe "auf das Ende der Privatheit von Kommunikation hinaus".

Lesezeit: 6 Min.  In Pocket speichern

Startseite > Presse > Pressemitteilungen

Rat der EU | Pressemitteilung | 14. Dezember 2017

**Verschlüsselung: durch Verschlüsselung an**

**WhatsApp-Überwachung**

**Die Bundesregierung sollbruchstellen**

Ein Gastbeitrag von Sven H.

Deutschland treibt auf EU-Ebene Sicherheitsbehörden Einblicke in verschlüsselte Kommunikationen, was würde die IT-Sicherheit aller Bürger schwächen.

(Bild: Lenscap Photography/Shutterstock.com)

03.12.2020, 12:25 Uhr

**Bundesverfassungsgericht**

**Posteo muss Kunden überwachen können**

Ermittler wollten von Posteo die IP-Adressen eines Verdächtigen, die dieser nicht mehr benutzt. Diese Daten gab Posteo nicht. Muss er aber können, hat nun der BVerfG entschieden.

Von Patrick Beuth

3202 Bundesgesetzblatt Jahrgang 2017 Teil I Nr. 58, ausgegeben zu Bonn am 23. August 2017

**Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens**

Vom 17. August 2017

Der Bundestag hat das folgende Gesetz beschlossen:

- 2. In § 129 Absatz 4 wird die Angabe „100c“ durch die Angabe „100b“ ersetzt.
- 3. § 266a Absatz 4 Satz 2 wird wie folgt geändert:

Artikel 1

**EuGH bestätigt: keine anlasslose Vorratsdatenspeicherung – mit Ausnahmen**

Vorratsdatenspeicherung ist unter bestimmten Voraussetzungen möglich – wenn die nationale Sicherheit bedroht ist. Ohne Anlass widerspricht sie EU-Recht.

Die Innenminister von Bund und Ländern haben Maßnahmen gegen Rechtsextremismus beschlossen. Die Beschlüsse gehen Politikern von CDU und CSU nicht weit genug.

Wenn das aber so ist...

... wie werden dann staatliche Überwachungsmaßnahmen / -gesetze gerechtfertigt und in Einklang mit „Privatheits-“ Grundrechten gebracht?

Wie erklären sich dann staatliche Maßnahmen, die denen zu widersprechen scheinen?

# Lesson 10: Datenschutz 3 – Surveillance

Das Verhältnis von „Datenschutz“ und „Überwachung“

Benthams „Panopticon“ – now and then

Konflikte mit (anderen) staatlichen Aufgaben

Freiheit vs. Sicherheit? Zum Umgang mit sich  
widersprechenden Grundrechten

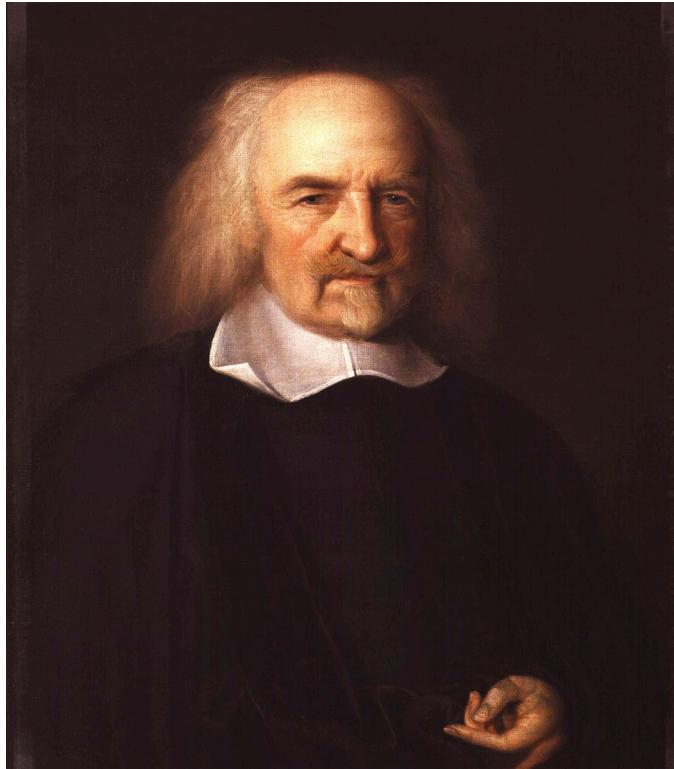
# Was wäre, wenn...



Was wäre, wenn...



# „State of Nature“ und Rolle „des Staates“ – Thomas Hobbes

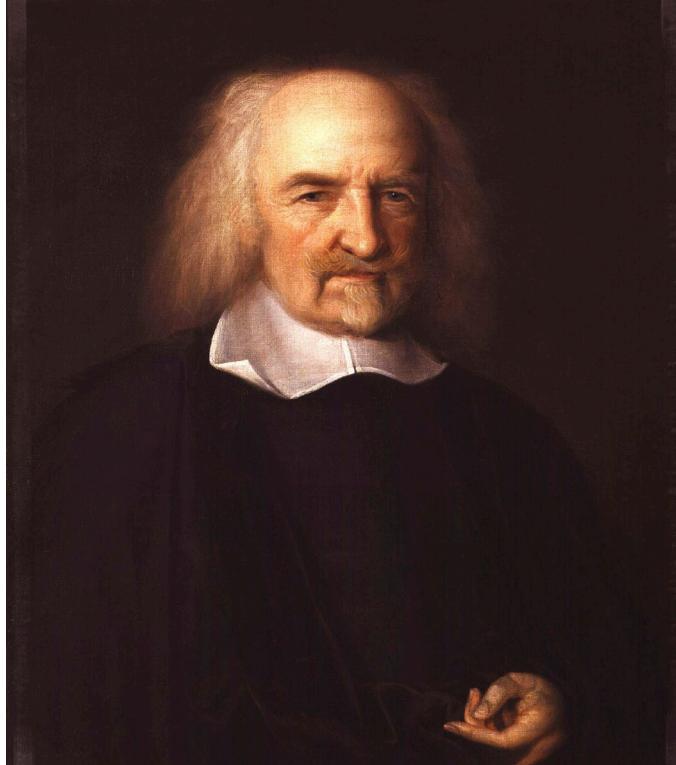


Thomas Hobbes

Whatsoever therefore is consequent to a time of war, where **every man is enemy to every man** [...]. In such condition there is no place for industry, because the fruit thereof is uncertain: and consequently no culture of the earth [...] no knowledge of the face of the earth; no account of time; no arts; no letters; no society; and which is worst of all, continual fear, and danger of violent death; and the life of man, solitary, poor, nasty, brutish, and short.

Hobbes (1651): Leviathan or the Matter...

# „State of Nature“ und Rolle „des Staates“ – Thomas Hobbes



→ „Homo homini lupus est“

Thomas Hobbes

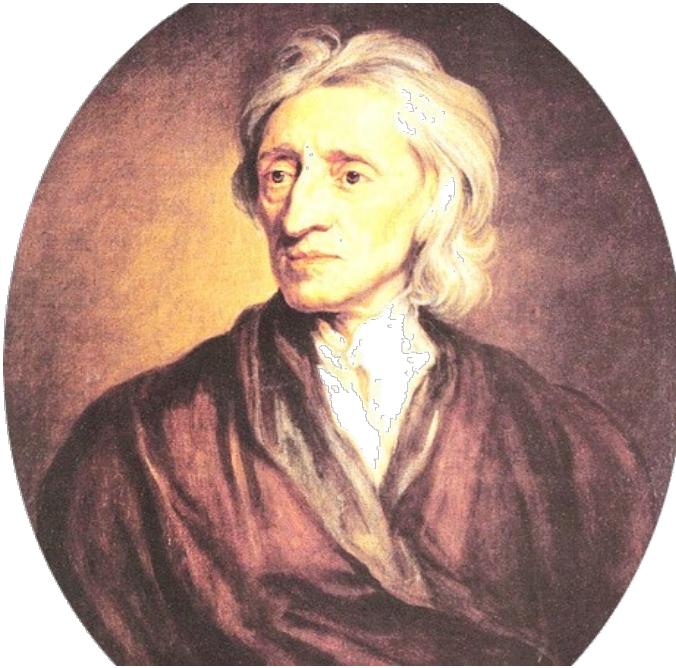
# Hobbes' Antwort: Leviathan



Stark vereinfacht:

- Im „Naturzustand“ haben alle Menschen absolute (Handlungs-) Freiheit
- Menschen sind eigennützig und rational
- Aus Eigennutz tendieren sie dazu, anderen Gewalt anzutun, Dinge wegzunehmen etc., wenn sie keine Bestrafung fürchten müssen → „Der Mensch ist dem Menschen ein Wolf“
- Alternative: Menschen schließen einen „Gesellschaftsvertrag“ auf Gegenseitigkeit: Alle verpflichten sich, Freiheit abzugeben und sich einem Leviathan zu „unterwerfen“ – zum allseitigen Vorteil
- Leviathan gewährt individuelle (Sicherheits-) Rechte und setzt sie durch – Er beschützt Menschen voreinander

# „State of Nature“ und Rolle „des Staates“ – John Locke

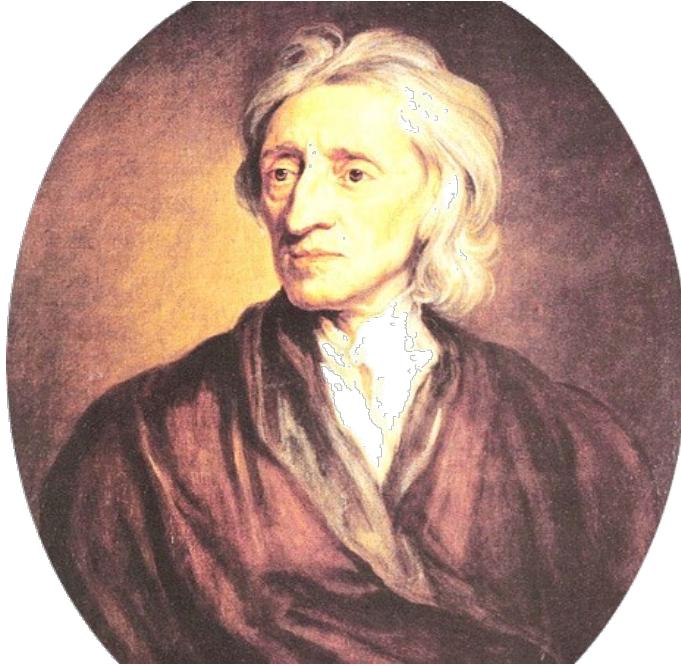


John Locke

The state of nature has a law of nature to govern it, which obliges every one: and reason, which is that law, teaches all mankind, who will but consult it, that being all equal and independent, no one ought to harm another in his life, health, liberty, or possessions: [...] Every one, [...], ought he, as much as he can, to preserve the rest of mankind, and may not, unless it be to do justice on an offender, take away, or impair the life, or what tends to the preservation of the life, the liberty, health, limb, or goods of another.

Locke (1689): Two Treatises of Government

# „State of Nature“ und Rolle „des Staates“ – John Locke



John Locke

→ The right to life, liberty, and property

# Sicherheit als Staatsaufgabe? Grundgesetz

Art. 2, Abs. 2 GG:

„Jeder hat das **Recht auf Leben und körperliche Unversehrtheit**. Die **Freiheit der Person** ist unverletzlich. In diese Rechte darf nur auf Grund eines Gesetzes eingegriffen werden.“

# Sicherheit als „Supergrundrecht“?

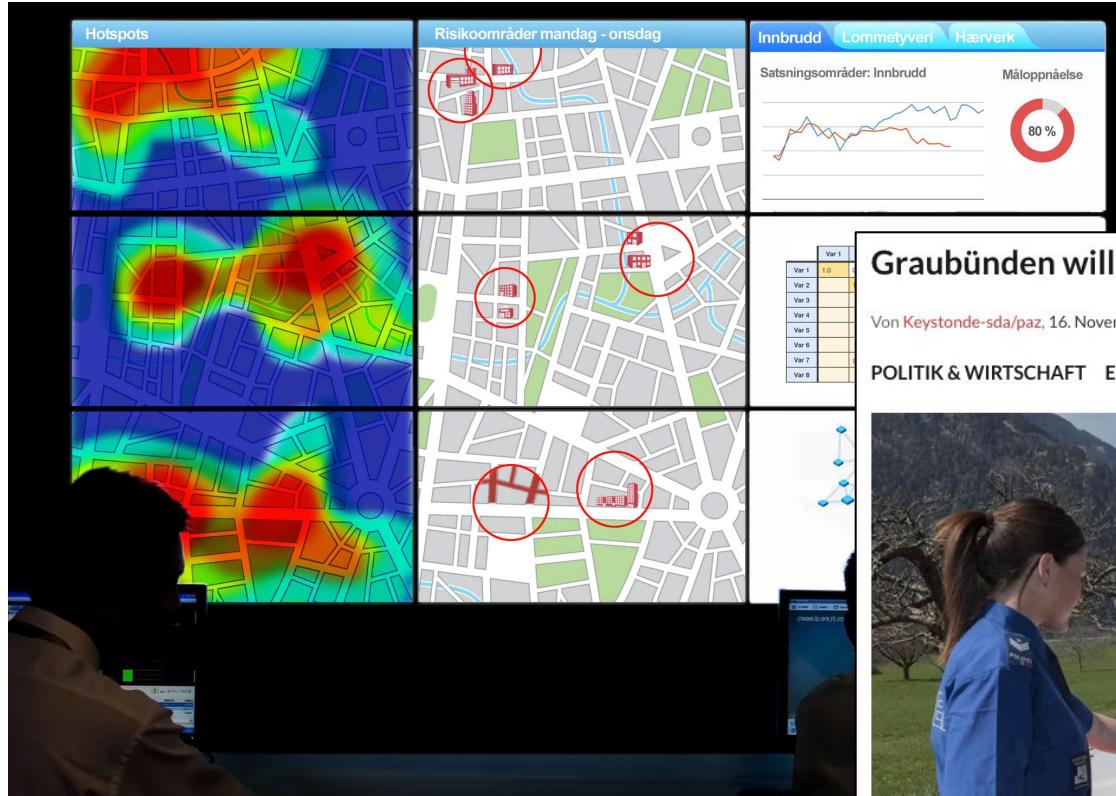


Hans-Peter Friedrich (u.A.)

Die Logik:

- Um von Grundrechten überhaupt „Gebrauch“ machen zu können, muss man sich erst einmal „seines Lebens sicher sein“
- Sicherheit ist daher zwingend notwendige Vorbedingung für alles weitere
- Daher muss der Staat zuallererst Sicherheit gewährleisten
- Andere Grundrechte müssen daher „zurückstehen“

# „Predictive Policing“



## Graubünden will Predictive Policing einführen

Von Keystone-dsa/paz, 16. November 2022 um 16:05

POLITIK & WIRTSCHAFT E-GOVERNMENT VERWALTUNG KANTON



Foto: Kantonspolizei Graubünden

Der Bündner Regierungsrat spricht sich für ein kantonales Bedrohungsmanagement aus. Dabei soll auch Software für Predictive Policing zum Einsatz kommen.

KI in der Polizeiarbeit: EU-Grundrechteagentur warnt vor verzerrten Algorithmen

Voreingenommenheit in Algorithmen kann im Laufe der Zeit durch Feedback-Schleifen verschlimmert werden. Das ist ein Problem etwa bei der Strafverfolgung.

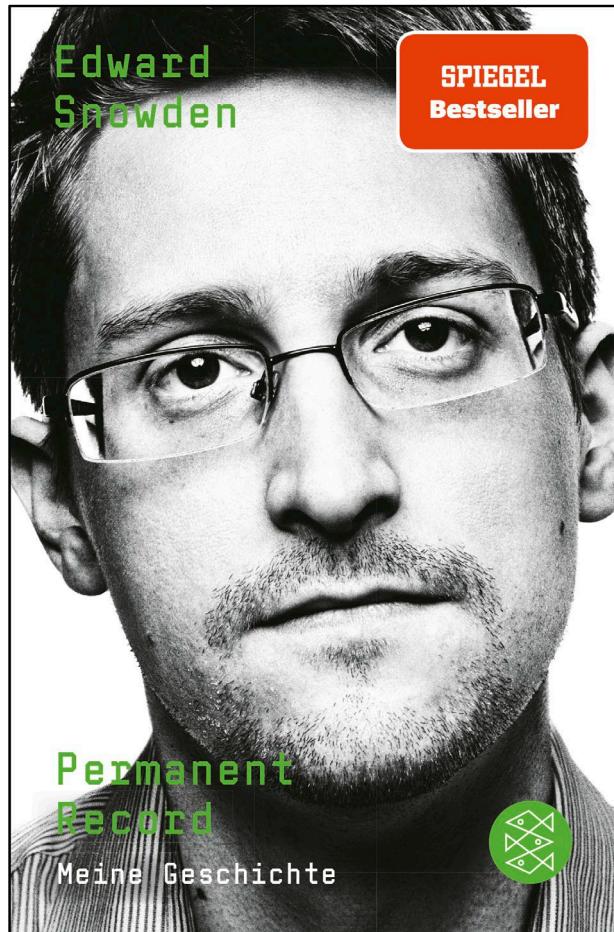
Lesezeit: 4 Min.  In Pocket speichern

Speaker icon, Print icon, 6



(Bild: Zapp2Photo / Shutterstock.com)

08.12.2022 19:24 Uhr



usw.

usw.

usw.

usw.

...  
...

# Sicherheit im Grundgesetz

Art. 2, Abs. 2 GG:

„Jeder hat das **Recht auf Leben und körperliche Unversehrtheit**. Die **Freiheit der Person** ist unverletzlich. In diese Rechte darf nur auf Grund eines Gesetzes eingegriffen werden.“

→ „Supergrundrecht Sicherheit“ als Verpflichtung des Staates, Überwachung zu betreiben?

# Sicherheit im Grundgesetz

Art. 2, Abs. 2 GG:

„Jeder hat das **Recht auf Leben und körperliche Unversehrtheit**. Die **Freiheit der Person** ist unverletzlich. In diese Rechte darf nur auf Grund eines Gesetzes eingegriffen werden.“

→ **Status negativus!** („der Staat darf nicht“)

(→ positivus: Ansprüche an den Staat; activus: Beteiligung, z.B. akt. + pass. Wahlrecht)

# Sicherheit im Grundgesetz



Bundeskriminalamt

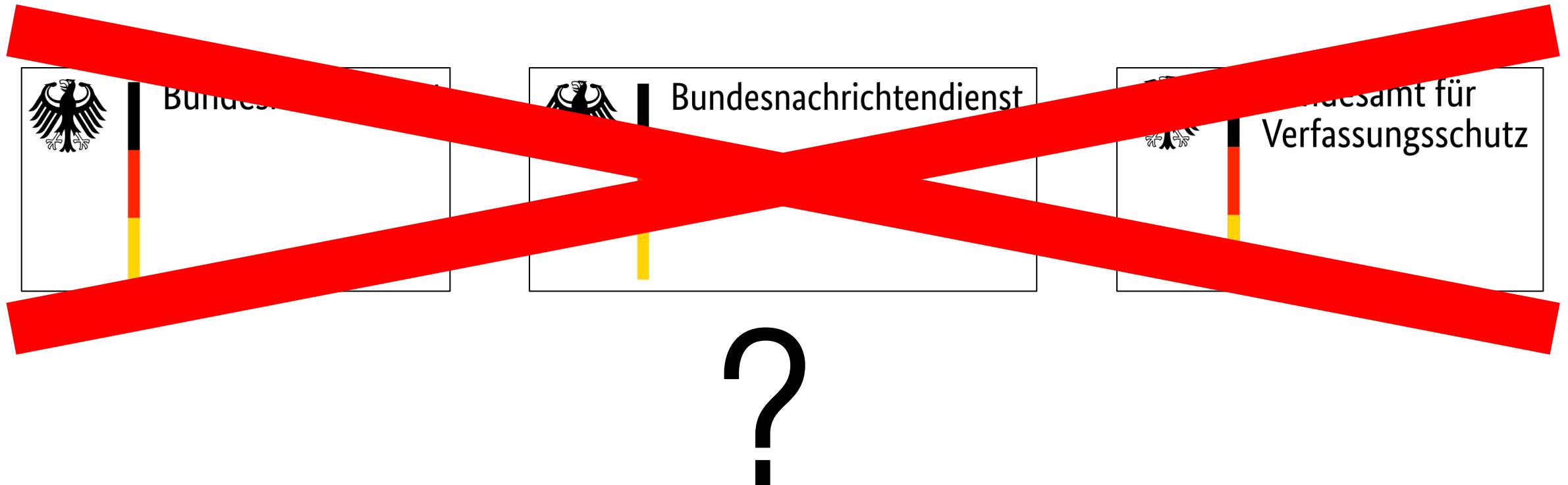


Bundesnachrichtendienst



Bundesamt für  
Verfassungsschutz

# Sicherheit im Grundgesetz



Darf der Staat dann überhaupt Überwachungsbehörden betreiben?

Das Verhältnis von „Datenschutz“ und „Überwachung“

Benthams „Panopticon“ – now and then

Konflikte mit (anderen) staatlichen Aufgaben

Freiheit vs. Sicherheit? Zum Umgang mit sich  
widersprechenden Grundrechten

„Recht auf Leben und körperliche Unversehrtheit“ (Art. 2, 2 GG)

+

„Menschenwürde“ → Schutzpflicht des Staates (Art. 1, 1+2 GG)?

(ähnliche Sichtweise z.B. bei Spinoza, Josef Isensee, ...)

# Sicherheit im Grundgesetz

```
> grep -i Sicherheit gg.txt | wc -l
```

# Sicherheit im Grundgesetz

```
> grep -i Sicherheit gg.txt | wc -l  
6  
>
```

# Sicherheit im Grundgesetz

```
> grep -i Sicherheit gg.txt | wc -l  
6  
> grep -i Freiheit gg.txt | wc -l
```

# Sicherheit im Grundgesetz

```
> grep -i Sicherheit gg.txt | wc -l  
6  
> grep -i Freiheit gg.txt | wc -l  
29  
>
```

# Sicherheit im Grundgesetz

Der Staat **darf** die Sicherheit der Bürger schützen – innerhalb verfassungsrechtlicher Grenzen!

Der Staat **darf** die Sicherheit der Bürger schützen – innerhalb verfassungsrechtlicher Grenzen!

Bei der Bewertung spielt das „**Gewicht**“ des zu schützenden **Gutes** eine zentrale Rolle!

# Sicherheit im GG – Quellen-TKÜ & Onlinedurchsuchung



The screenshot shows the homepage of the Federal Constitutional Court. It features the German eagle logo and the text "Bundesverfassungsgericht". Below is a photograph of the court's modern building with large glass windows. A navigation bar includes links for "Das Gericht", "Richterinnen und Richter", "Verfahren", and "Entscheidungen". The main content area displays a judgment from February 27, 2008, under the heading "Leitsätze" (Principles). The text discusses the general protection of personality rights and the infiltration of information systems. It emphasizes that such infiltration is only permissible if it poses a threat to fundamental rights like life, freedom, or the state's existence.

„Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. [...]

Die heimliche Infiltration eines informationstechnischen Systems [...] ist verfassungsrechtlich nur zulässig, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen. **Überragend wichtig sind Leib, Leben und Freiheit der Person oder [...] Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt. [...]**

BVerfGE 120, 274 – 350 (2008) – **Staatstrojaner** / Onlinedurchsuchung  
→ “Computergrundrecht“

# Quellen-TKÜ & Onlinedurchsuchung (2017)

3202

Bundesgesetzblatt Jahrgang 2017 Teil I Nr. 58, ausgegeben zu Bonn am 23. August 2017

## Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens

Vom 17. August 2017

Der Bundestag hat das folgende Gesetz beschlossen:

### Artikel 1 Änderung des Strafgesetzbuches

Das Strafgesetzbuch in der Fassung der Bekanntmachung vom 13. November 1998 (BGBl. I S. 3322), das zuletzt durch Artikel 1 des Gesetzes vom 17. Juli 2017 (BGBl. I S. 2442) geändert worden ist, wird wie folgt geändert:

2. In § 129 Absatz 4 wird die Angabe „100c“ durch die Angabe „100b“ ersetzt.
3. § 266a Absatz 4 Satz 2 wird wie folgt geändert:
  - a) In Nummer 2 wird das Wort „oder“ am Ende durch ein Komma ersetzt.
  - b) Nach Nummer 2 werden die folgenden Nummern 3 und 4 eingefügt:

„3. fortgesetzt Beiträge vorenthält und sich zur Verschleierung der tatsächlichen Beschäftigungsverhältnisse unrichtige, nachgemachte

Infiltration, um Kommunikation vor Verschlüsselung „abzugreifen“ und Systeme zu durchsuchen

## § 100a Telekommunikationsüberwachung

(1) Auch ohne Wissen der Betroffenen darf die Telekommunikation überwacht und aufgezeichnet werden, wenn

1. bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine in Absatz 2 bezeichnete schwere Straftat begangen, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht, oder durch eine Straftat vorbereitet hat,
2. die Tat auch im Einzelfall schwer wiegt und
3. die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos wäre.

Die Überwachung und Aufzeichnung der Telekommunikation darf auch in der Weise erfolgen, dass mit technischen Mitteln in von dem Betroffenen genutzte informationstechnische Systeme eingegriffen wird, wenn dies notwendig ist, um die Überwachung und Aufzeichnung insbesondere in unverschlüsselter Form zu ermöglichen. Auf dem informationstechnischen System des Betroffenen gespeicherte Inhalte und Umstände der Kommunikation dürfen überwacht und aufgezeichnet werden, wenn sie auch während des laufenden

Übertragungsvorgangs im öffentlichen Telekommunikationsnetz in verschlüsselter Form hätten überwacht und aufgezeichnet werden können.

# Quellen-TKÜ – §100a StPO – „Schwere Straftaten“



(2) Schwere Straftaten im Sinne des Absatzes 1 Nr. 1 sind:

<p>1. aus dem Strafgesetzbuch:</p> <ul style="list-style-type: none"> <li>a) Straftaten des Friedensverrats, des Hochverrats und der Gefährdung des dem Rechtstaates sowie des Landesverrats und der Gefährdung der äußerer Sicherheit bis 82, 84 bis 86, 87 bis 89a, 89c Absatz 1 bis 4, 94 bis 100a,</li> <li>b) Bestechlichkeit und Bestechung von Mandatsträgern nach § 108e,</li> <li>c) Straftaten gegen die Landesverteidigung nach den §§ 109d bis 109h,</li> <li>d) Straftaten gegen die öffentliche Ordnung nach § 127 Absatz 3 und 4 sowie den §§ 129 bis 130,</li> <li>e) Geld- und Wertzeichenfälschung nach den §§ 146 und 151, jeweils auch in Verbindung mit § 145a Absatz 1 sowie nach § 152a Abs. 3 und § 152b Abs. 1 bis 4,</li> <li>f) Straftaten gegen die sexuelle Selbstbestimmung in den Fällen der §§ 176, 176c, 176d und, u. d. in § 177 Absatz 6 Satz 2 Nummer 2 genannten Voraussetzungen, des § 177,</li> <li>g) Verbreitung, Erwerb und Besitz kinder- und jugendpornographischer Inhalte nach § 144b, § 145 Absatz 2,</li> <li>h) Mord und Totschlag nach den §§ 211 und 212,</li> <li>i) Straftaten gegen die persönliche Freiheit nach den §§ 232, 232a Absatz 1 bis 5, den §§ 232b Absatz 2, den §§ 233a, 234, 234a, 239a und 239b,</li> <li>j) Bandendiebstahl nach § 244 Abs. 1 Nr. 2, Wohnungseinbruchdiebstahl nach § 244 Absatz 4 und schwerer Bandendiebstahl nach § 244a,</li> <li>k) Straftaten des Raubes und der Erpressung nach den §§ 249 bis 255,</li> <li>l) gewerbsmäßige Hehlerei, Bandenhehlerei und gewerbsmäßige Bandenhehlerei nach den §§ 260 und 260a,</li> <li>m) Geldwäsche nach § 261, wenn die Vortat eine der in den Nummern 1 bis 11 genannten schweren Straftaten ist,</li> <li>n) Betrug und Computerbetrug unter den in § 263 Abs. 3 Satz 2 genannten Voraussetzungen und im Falle des § 263 Abs. 5, jeweils auch in Verbindung mit § 263a Abs. 2,</li> <li>o) Subventionsbetrug unter den in § 264 Abs. 2 Satz 2 genannten Voraussetzungen und im Falle des § 264 Abs. 3 in Verbindung mit § 263 Abs. 5,</li> <li>p) Sportwettbetrug und Manipulation von berufssportlichen Wettbewerben unter den in § 265e Satz 2 genannten Voraussetzungen,</li> <li>q) Vorenthalten und Veruntreuen von Arbeitsentgelt unter den in § 266a Absatz 4 Satz 2 Nummer 4 genannten Voraussetzungen,</li> <li>r) Straftaten der Urkundenfälschung unter den in § 267 Abs. 3 Satz 2 genannten Voraussetzungen und im Fall des § 267 Abs. 4, jeweils auch in Verbindung mit § 268 Abs. 5 oder § 269 Abs. 3, sowie nach § 275 Abs. 2 und § 276 Abs. 2,</li> <li>s) Bankrott unter den in § 283a Satz 2 genannten Voraussetzungen,</li> <li>t) Straftaten gegen den Wettbewerb nach § 298 und, unter den in § 300 Satz 2 genannten Voraussetzungen, nach § 299,</li> <li>u) gemeinschaftliche Straftaten in den Fällen der §§ 306 bis 306c, 307 Abs. 1 bis 3, des § 308 Abs. 1 bis 3, des § 309 Abs. 1 bis 4, des § 310 Abs. 1, der §§ 313, 314, 315 Abs. 3, des § 315b Abs. 3 sowie der §§ 316a und 316c,</li> <li>v) Bestechlichkeit und Bestechung nach den §§ 332 und 334,</li> </ul> <p>2. aus der Abgabenordnung:</p> <ul style="list-style-type: none"> <li>a) Steuerhinterziehung unter den in § 370 Absatz 3 Satz 2 Nummer 1 genannten Voraussetzungen, sofern der Täter als Mitglied einer Bande, die sich zur fortgesetzten Begehung von Taten nach § 370 Absatz 1 verbunden hat, handelt, oder unter den in § 370 Absatz 3 Satz 2 Nummer 5 genannten Voraussetzungen,</li> </ul>	<p>I) gewerbsmäßige Hehlerei, Bandenhehlerei und gewerbsmäßige Bandenhehlerei nach den §§ 260 und 260a,</p> <p>7. aus dem Betäubungsmittelgesetz:</p> <p>a) Straftaten nach einer in § 29 Abs. 3 Satz 2 Nr. 1 in Bezug genommenen Vorschrift unter den dort genannten Voraussetzungen,</p> <p>29 (3) BtMG: Besonders schwerer Fall z.B. wenn „gewerbsmäßig“ (also wiederholt und mit Absicht zur Gewinnerzielung)</p>	<p>4. aus dem Asylgesetz:</p> <ul style="list-style-type: none"> <li>a) Verleitung zur missbräuchlichen Asylantragstellung nach § 84 Abs. 3.</li> </ul> <p>6. Straftaten nach § 13 Absatz 3,</p> <p>7. aus dem Außenwirtschaftsgesetz:</p> <p>vorsätzliche Straftaten nach den §§ 17 und 18 des Außenwirtschaftsgesetzes,</p> <p>7. aus dem Betäubungsmittelgesetz:</p> <ul style="list-style-type: none"> <li>a) Straftaten nach einer in § 29 Abs. 3 Satz 2 Nr. 1 in Bezug genommenen Vorschrift unter den dort genannten Voraussetzungen,</li> <li>b) Straftaten nach den §§ 29a, 30 Abs. 1 Nr. 1, 2 und 4 sowie den §§ 30a und 30b,</li> </ul> <p>8. aus dem Grundstoffüberwachungsgesetz:</p> <p>Straftaten nach § 19 Abs. 1 unter den in § 19 Abs. 3 Satz 2 genannten Voraussetzungen,</p> <p>9. aus dem Gesetz über die Kontrolle von Kriegswaffen:</p> <ul style="list-style-type: none"> <li>a) Straftaten nach § 19 Abs. 1 bis 3 und § 20 Abs. 1 und 2 sowie § 20a Abs. 1 bis 3, jeweils auch in Verbindung mit § 21,</li> <li>b) Straftaten nach § 22a Abs. 1 bis 3,</li> </ul> <p>9a. aus dem Neue-psychoaktive-Stoffe-Gesetz:</p> <p>Straftaten nach § 4 Absatz 3 Nummer 1 Buchstabe a,</p> <p>10. aus dem Völkerstrafgesetzbuch:</p> <ul style="list-style-type: none"> <li>a) Völkermord nach § 6,</li> <li>b) Verbrechen gegen die Menschlichkeit nach § 7,</li> <li>c) Kriegsverbrechen nach den §§ 8 bis 12,</li> <li>d) Verbrechen der Aggression nach § 13,</li> </ul> <p>11. aus dem Waffengesetz:</p> <ul style="list-style-type: none"> <li>a) Straftaten nach § 51 Abs. 1 bis 3,</li> <li>b) Straftaten nach § 52 Abs. 1 Nr. 1 und 2 Buchstabe c und d sowie Abs. 5 und 6.</li> </ul>
--	---	---

# Onlinedurchsuchung – StPO

## § 100b Online-Durchsuchung

(1) Auch ohne Wissen des Betroffenen darf mit technischen Mitteln in ein von dem Betroffenen genutztes informationstechnisches System eingegriffen und dürfen Daten daraus erhoben werden (Online-Durchsuchung), wenn

1. bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine in Absatz 2 bezeichnete besonders schwere Straftat begangen oder in Fällen, in denen der Versuch strafbar ist, zu begehen versucht hat,
2. die Tat auch im Einzelfall besonders schwer wiegt und
3. die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos wäre.

# Onlinedurchsuchung – §100b StPO – „Schwere Straftaten“



(2) Besonders schwere Straftaten im Sinne des Absatzes 1 Nummer 1 sind:

## I) gewerbsmäßige Hehlerei, Bandenhehlerei und gewerbsmäßige Bandenhehlerei nach den §§ 260, 260a,

o sowie in den Nummern 2 bis 10 genannte besonders schwere Straftaten zu ermöglichen oder zu fördern,

- c) Bildung krimineller Vereinigungen nach § 129 Absatz 1 in Verbindung mit Absatz 5 Satz 3 und Bildung terroristischer Vereinigungen nach § 129a Absatz 1, 2, 4, 5 Satz 1 erste Alternative, jeweils auch in Verbindung mit § 129b Absatz 1,

d) Geld- und Wertzeichenfälschung nach den §§ 146 und 151, jeweils auch in Verbindung mit § 152,

1 und der §§ 176c, ngen, des § 177, 184b Absatz 1 Satz

des § 232a Absatz 1, 3, 4 und 5 zweiter Halbsatz, des § 232b Absatz 1 und 3 sowie Absatz 4, dieser in Verbindung mit § 232a Absatz 4 und 5 zweiter Halbsatz, des § 233 Absatz 2, des § 233a Absatz 1, 3 und 4 zweiter Halbsatz, der §§ 234 und 234a Absatz 1 und 2 sowie der §§ 239a und 239b,

- i) Bandendiebstahl nach § 244 Absatz 1 Nummer 2 und schwerer Bandendiebstahl nach § 244a, j) schwerer Raub und Raub mit Todesfolge nach § 250 Absatz 1 oder Absatz 2, § 251, k) räuberische Erpressung nach § 255 und besonders schwerer Fall einer Erpressung nach § 253 unter den in § 253 Absatz 4 Satz 2 genannten Voraussetzungen, l) gewerbsmäßige Hehlerei, Bandenhehlerei und gewerbsmäßige Bandenhehlerei nach den §§ 260, 260a,
- m) besonders schwerer Fall der Geldwäsche nach § 261 unter den in § 261 Absatz 5 Satz 2 genannten Voraussetzungen, wenn die Vortat eine der in den Nummern 1 bis 7 genannten besonders schweren Straftaten ist,

## 5. aus dem Betäubungsmittelgesetz:

- a) besonders schwerer Fall einer Straftat nach § 29 Absatz 1 Satz 1 Nummer 1, 5, 6, 10, 11 oder 13, Absatz 3 unter der in § 29 Absatz 3 Satz 2 Nummer 1 genannten Voraussetzung,

4. aus dem Außenwirtschaftsgesetz:  
a) Straftaten nach § 17 Absatz 1, 2 und 3, jeweils auch in Verbindung mit Absatz 6 oder 7,

b) Straftaten nach § 18 Absatz 7 und 8, jeweils auch in Verbindung mit Absatz 10,

5. aus dem Betäubungsmittelgesetz:  
a) besonders schwerer Fall einer Straftat nach § 29 Absatz 1 Satz 1 Nummer 1, 5, 6, 10, 11 oder 13, Absatz 3 unter der in § 29 Absatz 3 Satz 2 Nummer 1 genannten Voraussetzung,

b) eine Straftat nach den §§ 29a, 30 Absatz 1 Nummer 1, 2, 4, § 30a,

6. aus dem Gesetz über die Kontrolle von Kriegswaffen:

a) eine Straftat nach § 19 Absatz 2 oder § 20 Absatz 1, jeweils auch in Verbindung mit § 21,

b) besonders schwerer Fall einer Straftat nach § 22a Absatz 1 in Verbindung mit Absatz 2,

7. aus dem Grundstoffüberwachungsgesetz:

Straftaten nach § 19 Absatz 3,

8. aus dem Neue-psychoaktive-Stoffe-Gesetz:

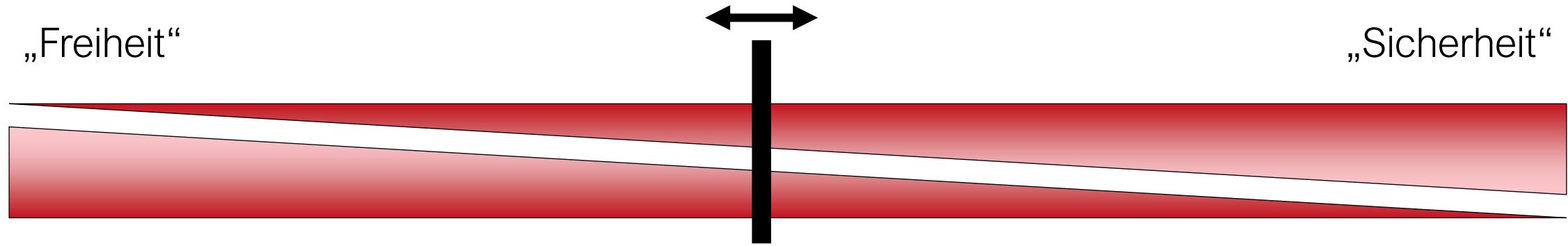
Straftaten nach § 4 Absatz 3 Nummer 1,

9. aus dem Völkerstrafgesetzbuch:

29 (3) BtMG: Besonders schwerer Fall z.B. wenn „gewerbsmäßig“  
(also wiederholt und mit Absicht zur Gewinnerzielung)

Die große Frage – unabhängig vom konkreten Fall:  
Was tun, wenn sich Grundrechte (und staatliche Pflichten)  
widersprechen?

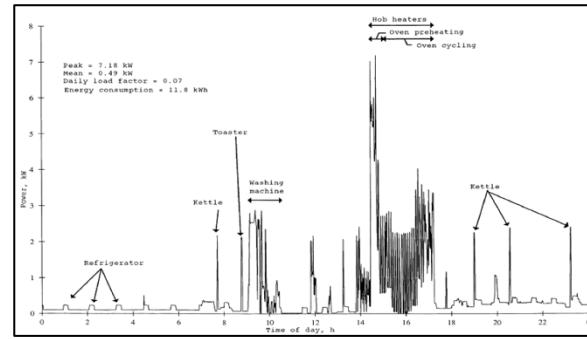
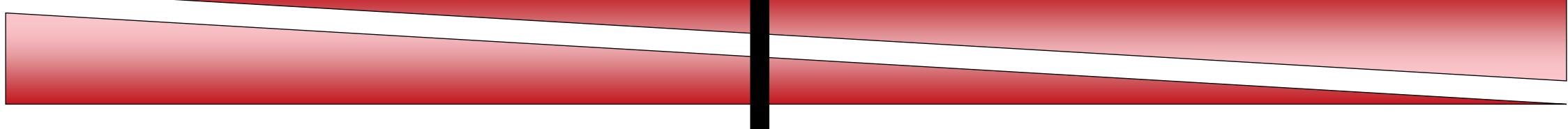
# Was tun, wenn sich Grundrechte (und staatliche Pflichten) widersprechen?



# Was tun, wenn sich Grundrechte (und staatliche Pflichten) widersprechen?

„Privatheit“ /  
informationelle Selbstbestimmung

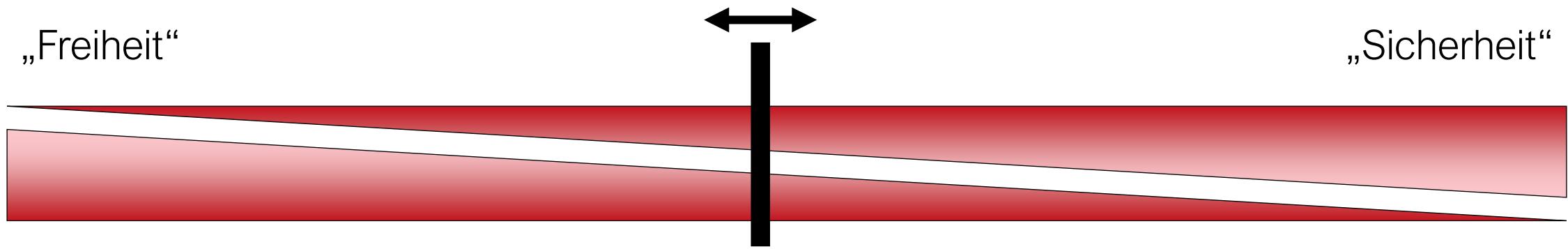
„Schutz der natürlichen  
Lebensgrundlagen“ (Art. 20a GG)



**Long story short:**  
Für mehr Erneuerbare Energien ist  
Smart Metering aus physikalischen  
Gründen zwingend erforderlich



# Was tun, wenn sich Grundrechte (und staatliche Pflichten) widersprechen?



Die Antwort der Jurist\*innen: „Praktische Konkordanz“

Untermaßverbot, Übermaßverbot, beiderseitige Optimierung, angemessener Ausgleich,  
Verhältnismäßigkeit, ....

→ Viel schwieriger als einfacher „Schieberegler“

Wir können es uns natürlich immer auch ganz einfach machen...

Wir können es uns natürlich immer auch ganz einfach machen...

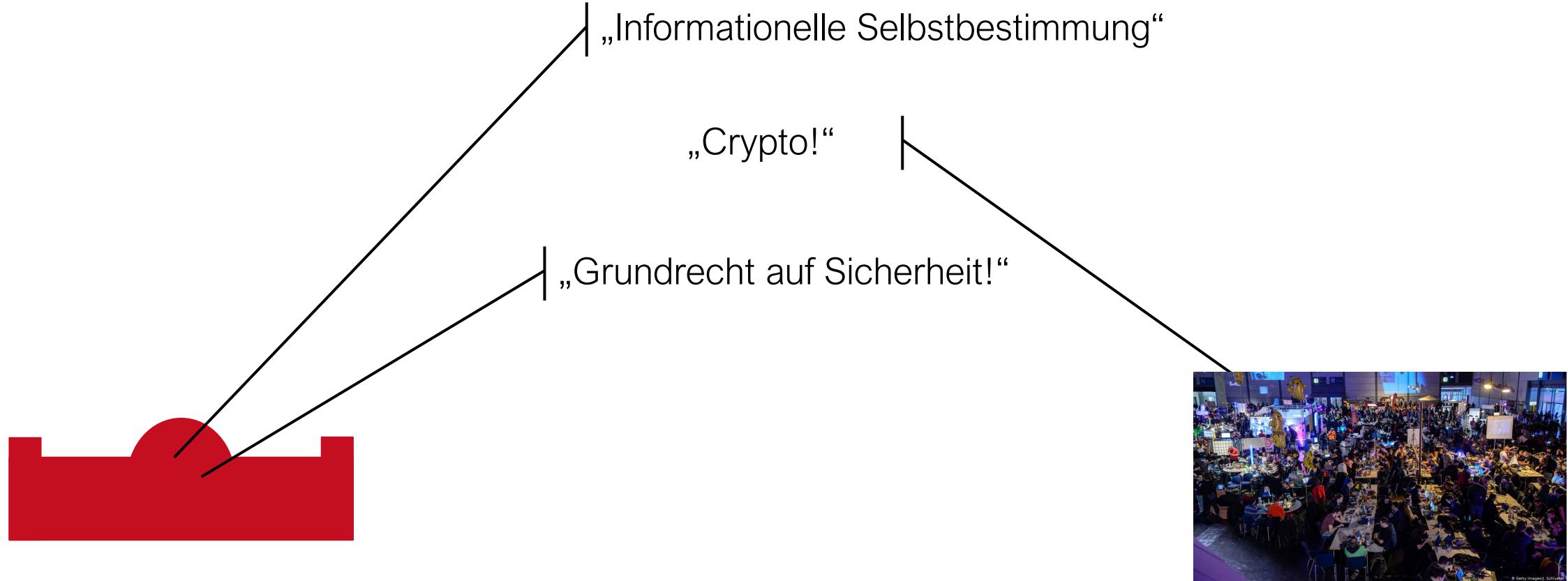
... sollten wir aber besser nicht...

Wir können es uns natürlich immer auch ganz einfach machen...

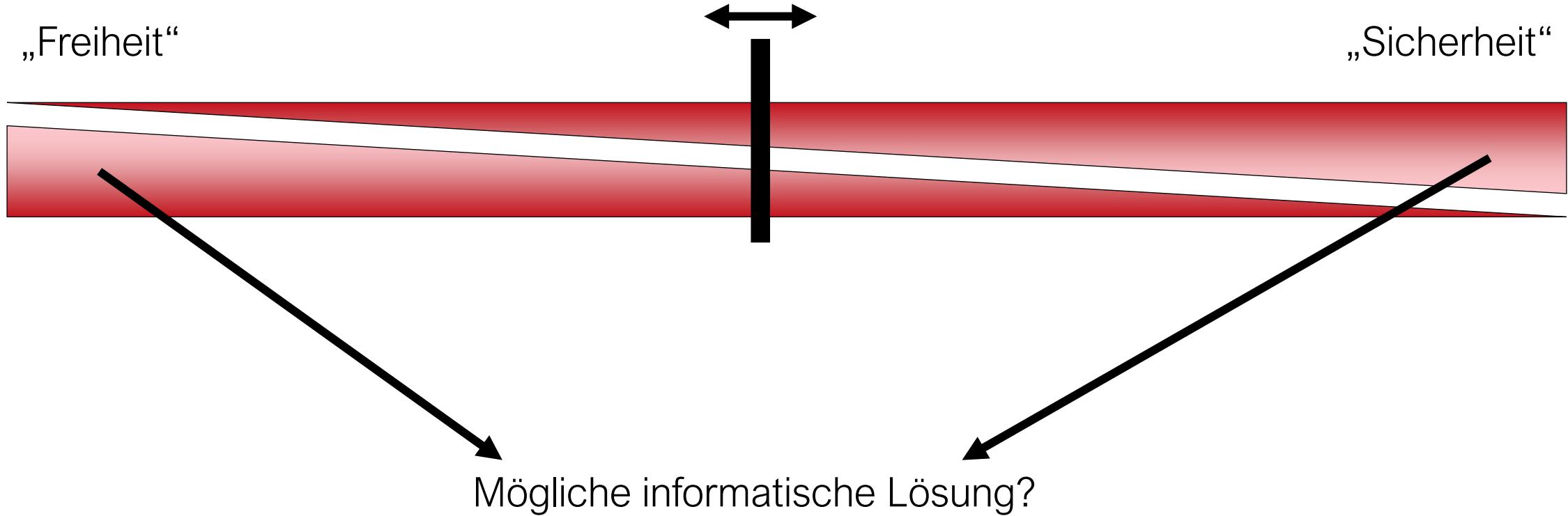
... sollten wir aber besser nicht...

... denn wenn (Top-)Jurist\*innen sich mit Grundrechtsfragen schwertun, dann ist es zumindest unwahrscheinlich, dass die Frage trivial ist.

# Recap: Horizontal Policy Elevator



# Was tun, wenn sich Grundrechte (und staatliche Pflichten) widersprechen?



# Datenschutz- / Privatheits-Roundup

Advanced technologies and implications  
(eg FHE, Hippocr.DBs, ...)

„Regulatory overhead“  
→ Small firms / innovation?

Exerting indiv. preferences  
w/o interfaces (e.g., IoT)

Multi-person data  
(→ invalidates intuitive „owned by“ view)

Better integration  
law ↔ technology

„Data is an asset“  
→ Econ. Approach to Data Prot / Priv.

(D)PIA

Behavioral studies  
on DP/priv

DP-/Priv-Governance in  
massively distributed systems

„choice“ and market power

Alternative modalities (!law)

Process-driven vs. indiv. control

...

# Datenschutz- / Privatheits-Roundup

Datenschutz / „Privacy“ ist Dauerbrenner und wird dies auch auf absehbare Zeit bleiben

Neue Technologien verändern die Rahmen-/ Vorbedingungen ständig

Fragen von Datenschutz und „Privacy“ **von Beginn an** mitdenken

Immerhin geht es hier um **Grund- / Menschenrechte!**

Datenschutz / Privatheit ist (fast) **nie einziges gesellschaftliches Ziel**

→ Abwägungen, Interessenausgleich, ...

→ Frühzeitige Bewertung/Beurteilung von Gestaltungspfaden

→ Implikationen für den Gestaltungsprozess neuer Technologien?

# What's next?

8	11.12.23	Datenschutz 3: Surveillance <b>(in Präsenz)</b> [FP]	1. Datenschutz vs. Überwachung 2. Bentham's Panopticon 3. Gesamtgesellschaftliche Bedeutung 4. Freiheit vs. Sicherheit? Zum Umgang mit sich widersprechenden Grundrechten
	14.12.23	Q&A zu Block C <b>(via Zoom)</b>	

9	18.12.23	Technik & Regulierung: „Code is Law“ and beyond [NL, KW] <b>(in Präsenz)</b>	1. Technik als verhaltensregulierende Modalität 2. Spezifika technischer Regulierung (im Vergleich z.B. mit Recht): ex-ante vs. ex-post, Absolutheit, etc. → untersch. technische Ansätze 3. Paradigmatische Grenzen technischer Regelimplementierung 4. Technologiebasiertes Nudging
	21.12.23	Großübung „How to Essay“ [EG] <b>(via Zoom)</b>	<b>Poster-Einreichung für Druck: Do, 04.01.</b>

fin