How to Design a Surveillance Barometer

Model for the Regular Monitoring and Assessment of Statutory Powers and Practices in State Surveillance

Michael Kilchling, Sabrina Ellebrecht *

eucrim
European Law Forum: Prevention • Investigation • Prosecution

Article

ABSTRACT

The surveillance of citizens by government agencies is an issue that can affect many areas of everyday life. It regularly provokes controversy, particularly in public discourse. Strikingly, in discussions about the existing powers of security authorities, their possible extension, or even the introduction of entirely new and additional surveillance powers, little or nothing is usually known about which surveillance measures are actually used in daily practice, how often they are used, and under what circumstances. Surveillance of any kind always has a high degree of social relevance and touches the very core of the liberal constitution. The execution of such measures is therefore relevant not only to those directly affected, but – due to their potential intrusiveness – can affect a large number of persons. As the frequency of these (often covert) measures increases, so does the actual and perceived risk of becoming a target of police, prosecutorial, or other security authorities.

The Max Planck Institute for the Study of Crime, Security and Law (MPI-CSL) in Freiburg has developed an innovative concept for a surveillance barometer that facilitates the mapping and systematic assessment of the level of surveillance in Germany. For the first time, this tool provides a scientifically sound basis for an overall account and assessment of surveillance practices. It is to be continued and gradually expanded in the coming years. A prototype for a dynamic online information system is currently under development. It will serve as a blueprint for similar projects in other countries and, on this foundation, enable comparative analyses across EU Member States. This exercise is an indispensable stepping stone on the path towards greater transparency and provides a solid basis for evidence-based security policies. In the longer term, it can also help reduce constitutional misconceptions in the debate on security law, both on the part of the security agencies and civil society.

AUTHORS

Michael Kilchling

Senior Researcher; Lecturer at the Faculty of Law of the University of Freiburg, Germany
Max Planck Institute for the Study of Crime, Security and Law, Freiburg

Sabrina Ellebrecht

Sociologist and expert in police research; member of the Surveillance Barometer research team at the MPI-CSL (until March 2026)

CITATION SUGGESTION

M. Kilchling, S. Ellebrecht, "How to Design a Surveillance Barometer", 2025, Vol. 20(4), eucrim, pp311–323. DOI: https://doi.org/10.30709/eucrim-2025-023

Published in
2025, Vol. 20(4) eucrim pp 311 – 323
ISSN: 1862-6947
https://eucrim.eu

I. Introduction

The production, retention, seizure, and processing of a variety of sensitive data about citizens and their activities in everyday life,[1] together with other forms of surveillance carried out by state agencies, have been at the centre of democratic discourse – in politics, juristic and other academic circles, NGOs, the media, and civil society – for decades. Driven by the steady expansion of such powers – technically facilitated by digitalisation, and politically propelled by EU legislative demands – some critical observers have even predicted nothing short of the end of privacy.[2] One of the key turning points in this development was the introduction of the groundless temporary retention of telecommunications metadata from all citizens, stored as a standard resource at the disposal of prosecution agencies. Notwithstanding the erstwhile lack of legislation powers in penal matters[3] the instrument was pushed by the European Union (EU), regardless of opposing positions in some of the Member States and the established case law of their constitutional courts. Even after the nullification of the original directive[4] by the European Court of Justice,[5] *data retention* has remained on the agenda in most Member States and continues to be one of the most powerful trigger words in the critical security policy discourse.[6] It has become a metaphor of today's "surveillance society,"[7] a phenomenon that is particularly evident in the German context.[8]

II. Assessment of the Impact of Surveillance from a Supra-individual Perspective

Academic discussion about surveillance and its constitutional limits in Germany was largely stimulated by the Federal Constitutional Court's (FCC, *Bundesverfassungsgericht – BVerfG*) 2010 landmark ruling on the limits of telecommunications metadata retention under constitutional law.[9] As one of its key arguments, the Court held that excessive precautionary surveillance of citizens would be incompatible with the constitutional identity of the Federal Republic of Germany, which implies that the state must not record and register citizens' exercise of their freedoms in its entirety. In a side note, the judges in Karlsruhe further held:

> "[W]ith the precautionary retention of telecommunications traffic data in place, there is considerably less leeway for allowing other types of data gathering not based on specific grounds, including for measures originating at EU level."[10]

The FCC had further emphasised that these constitutional principles require *"greater restraint by the legislature"* when considering introducing additional data retention powers.[11]

1. Need for an impact assessment

In scholarship, *Alexander Roßnagel* developed and promoted the idea of the need for a comprehensive review of all existing surveillance powers, called *"Überwachungsgesamtrechnung"* [general surveillance calculus].[12] In the following years, this topos – which appears both catchy and cumbersome – was picked up in legal, political, and societal discussions and referred to as key argument in favour of establishing a critical record of all existing surveillance powers provided to state agencies. The discussions addressed not only the law enforcement sector but also other areas of (interventionist) public administration, including preventive policing, customs and finance, transportation, digital services, and not least the intelligence sector. This broad approach is based on an additive understanding of the impact that the mere existence of the various statutory surveillance powers and their potential use has on the potential infringement of fundamental freedoms.[13]

Contrary to what the term “general surveillance calculus” actually implies, the approach has mainly been discussed theoretically (on a qualitative, doctrinal level) and less from a practical perspective (in that it was only rudimentarily operationalised). By focusing on surveillance powers from an abstract point of view, previous analysis has failed to address whether and to what extent surveillance practices are in fact applied. In this regard, we are still groping in the dark. We are currently unable to quantify whether the “burden of surveillance” in the country has actually changed over the past decade(s), nor can we determine its overall scope. The associated infringement of fundamental rights materialises only when the available legal powers are in fact exercised by the state. Therefore, the key question regarding the – constitutionally acceptable – level of state surveillance is also a quantitative one. This is because, as the frequency of such measures increases, so does the statistical probability of being targeted individually.

The quantity issue, however, is often neglected in critical discussions on surveillance. While the individual risk of actually becoming being targeted by a covert remote computer search (“online search” – *Onlinedurchsuchung*) is virtually close to zero, due to the small number of cases in which it is used,[14] the constant monitoring of financial data affects almost all citizens. From both a qualitative and a quantitative perspective, the mass surveillance of financial data — not least because of its promotion and continuous expansion through EU legislation[15] — is likely one of the most extreme examples of indiscriminate and ubiquitous data retention.[16] This is even more the case than with flight passenger data recording, which has been considered an extreme example of excessive data retention in recent years.[17] Whereas passenger flights are a relatively rare activity in the daily life of the average citizen, financial transactions are carried out regularly and, with the growth of cashless payments, often several times a day. This can be considered a prime example of an excessive precautionary surveillance of citizens, as problematised by the FCC in its 2010 ruling. Surprisingly, this dimension of surveillance has not yet received much public attention, presumably also due to a lack of information.[18]

Indeed, it seems imperative not only to look at surveillance and its impact through a doctrinal lens, but also to incorporate empirical reality into the assessment. The fact that this has not been done in the past can be explained, at least in part, by the fact that reliable statistical information on the frequency of surveillance measures, especially when carried out in a preventive context, has long been only sporadically available or even unavailable. This is a crucial gap that must be gradually closed in the coming years.

The Freiburg Max Planck Institute for the Study of Crime, Security and Law (MPI-CSL) has developed and pretested the model and methodology for establishing a Periodic Surveillance Barometer (*Periodisches Überwachungsbarometer*). It combines two perspectives: an assessment of the normative shape of the various surveillance powers in force (legal perspective) and their application in practice (empirical perspective). This conceptual approach enables the systematic evaluation of the *burden of surveillance* to which citizens are subjected in a specific reference period (e.g., calendar year), based on a standardised set of qualitative and quantitative variables. “Burden” refers to the general risk of being targeted by a surveillance measure, as well as the impact of surveillance practices on the actual level of protection of fundamental rights in society as a whole. From a doctrinal perspective, this touches upon an additional aspect of the nature of fundamental rights, one that more recent contributions have addressed as the objective dimension of fundamental rights[19] protection.[20] *Marcus Löffelmann* published proposals for a concept similar to the MPI-CSL’s Surveillance Barometer, which not only seeks to quantify the societal costs of security-related surveillance measures but also takes into account their potential societal benefits.[21]

2. Traditional assessment models

Concepts for assessing the concrete degree of (potential) infringements on individual rights have been discussed in surveillance studies[22] from a variety of theoretical and practical perspectives. These include

models and proposals for, e.g., impact assessments of human rights violations,[23] privacy impact assessments,[24] data protection impact assessments,[25] and surveillance impact assessments,[26] the latter sometimes with a particular focus on the economic costs of surveillance.[27] Adopting an even broader perspective, *Wright* and *Raab* point to potential social, economic, financial, political, ethical and psychological impacts of surveillance.[28] In some jurisdictions, different types of impact assessments are already in place, also as a standard element in the drafting processes for legislative acts; quite often, however, they are criticised for their lack of any solid empirical background.[29] All such models share, however, a significant shift from an individualist perspective to a systemic risk perspective — one that moves from an *ex post* assessment of individual harm to the evaluation of potential fundamental rights risks for citizens and society as a whole.[30]

Of particular importance is the assessment of the intensity of infringements of fundamental rights. Independent of the concrete terminology referred to – seriousness, severity, gravity, magnitude, etc.[31] – intensity has always been a key parameter of the proportionality test in many legal systems.[32] Following this tradition, the FCC's case law provides an extensive casuistry of categories, ranging from "minor *[gering]*" or "slight *[geringfügig]*" at one end of an imaginary scale to "very intrusive *[tiefgreifend]*" or "particularly serious *[besonders stark]*" at the other end; infringements of a medium degree have been characterised as, e.g., "of considerable weight *[von erheblichem Gewicht]*" or just „weighty *[gewichtig]*."[33] This qualitative assessment technique conveys a certain quasi-empirical appearance. In its very essence, however, it is of an intuitive nature. This carries with it a certain risk of imbalance and uncertainty, which can sometimes even be detected in actual court decisions.

Interestingly, the FCC's 2010 ruling on telecommunications metadata retention itself provides proof of this problem: in the two dissenting opinions, considerable contention about the extent to which data retention practices may interfere with citizens' fundamental rights has been documented. While the majority vote considered the interference to be "particularly serious," the first dissenting judge characterised it as less serious; instead of "particularly serious," his final rating was "particularly weighty."[34] Similar considerations were put forth in the second dissenting opinion, which concluded that "[obviously – *sic!*] the weight of interference [… induced by telecommunication metadata retention …] is *minor* and cannot be compared to the weight of interference resulting from access to communication contents."[35] The disparity between the majority's opinion and the second dissenting opinion could not be more profound, given that "particularly serious" denotes the most severe type of interference conceivable according to the FCC's current scale.[36]

The dissenting opinions reveal a principal shortcoming of the concept as currently applied. What might appear to be an issue of semantics is the result of a lack of consistent and evaluable criteria. What specifically makes the difference between, e.g., an infringement of a "considerable *[erheblich]*" extent and one of a "not inconsiderable *[nicht unerheblich]*" extent, and what is the threshold between them?[37] Instead of a descriptive scaling, developed and continually refined on the basis of emerging case law – which is as selective as it is arbitrary[38] – a more generalised concept based on definite and measurable parameters should be applied.

3. Empirically grounded assessment

As outlined above, a purely normative assessment method is insufficient for capturing the impact of surveillance. What is needed is a theoretically and empirically sound operationalisation of the impact assessment that reveals the true level of surveillance that citizens are exposed to in their daily lives as a result of the *actual* use of various statutory powers by the authorities. Unlike traditional proportionality doctrine, the Surveillance Barometer is not concerned with the abstract (constitutional) legality or illegality of a measure, but with its concrete impact on those affected, considering not only the individual but also the collective of fundamental rights holders.[39] From this perspective, *any single intervention* constitutes a relevant infringe-

ment, including all proportionate and lawful measures. Taken together, these measures minimise the areas in which constitutionally protected freedoms can be exercised – that is (in our context), surveillance-free spaces. This explains why the frequency with which individual surveillance measures are applied is an essential factor in assessing the extent of state surveillance.[40] In its case law, the FCC has traditionally considered prevalence indirectly at most, for example by requiring highly protective statutory restrictions for serious infringements, thereby aiming to curb excessive surveillance. However, concrete figures have not yet been taken into account.

Unlike earlier proposals,[41] the MPI-CSL's Surveillance Barometer systematically includes empirical aspects. The concept applies to the two main elements of its intensity assessment method:

- A determination of the seriousness of the basic rights infringements by means of uniform and measurable criteria;
- A systematic account and classification of how frequently the various surveillance powers are being applied.

Taken together, the concept is both theoretically and empirically sound: all potential surveillance scenarios can be accurately measured and put into relation with each other. This makes it possible, for the first time, to identify trends and draw a wide range of comparisons between specific types of surveillance measures, agency sectors, regional practices, and time periods. As a result, several questions can be addressed, e.g.:

- Has the number of surveillance activities and/or their intensity increased in recent years due to the introduction of new legislation or changes in application practices?
- Has the level of surveillance ever decreased, e.g., in the wake of a crisis such as the COVID-19 pandemic?
- Are fundamental rights holders in federal state A possibly subject to greater surveillance than those in federal state B, because the police in A increasingly resort to telecommunications metadata or digital services, while those in B prefer traditional search and seizure?

In the following section, we will present the methodological concept of the MPI-CSL's Surveillance Barometer, together with some preliminary findings.

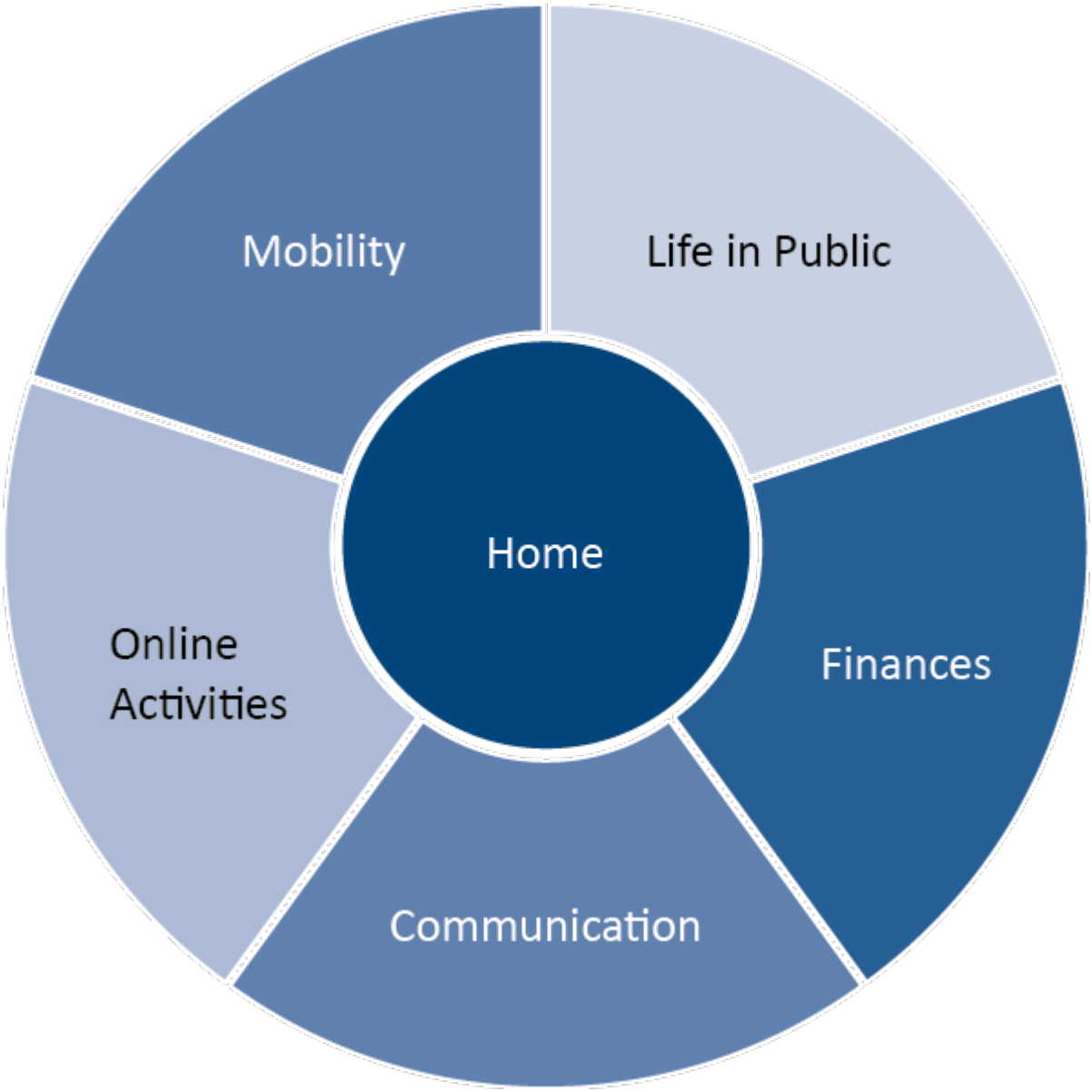
III. Six-Step Methodology

1. Identification of surveillance powers

The first step is to identify the relevant surveillance scenarios to be covered by the Surveillance Barometer. These include both the targeted production of data about individuals by state agencies through physical methods (e.g., covert observation) or technical methods (e.g., telephone tapping), as well as the retrieval of data generated and owned by third parties (service providers or the private individuals themselves). The latter is mainly carried out through production orders that concern existing data, realtime data, and data that will be generated in a future period of time. From the perspective of the basic rights holders, the most appropriate approach emerged as a systematisation according to sensitive spheres of private life where extensive personal data is continuously generated – knowingly and unknowingly – which could potentially be tapped via the various types and methods of surveillance. *Figure 1* illustrates the sensitive spheres of daily life in which citizens are particularly vulnerable as regards infringements of their privacy.

Above all, one's private home is of explicit sensitivity in this regard, as it is at the core of one's private life. Audio and video surveillance of private premises are only two of many methods of covert surveillance. In addition, any physical objects and data repositories including computers, electronic devices, and smart home gadgets can become targets of standard search and seizure operations in this private sphere. Besides the immediate seizure of portable home devices, data can also be gathered remotely from commercial service providers. Alongside the private home, communication, the usage of social media and other online activities are accordingly relevant spheres as they generate numerous types of digital traces, including inventory data, traffic data or metadata, passwords, activity data, and not least the very contents of the communications, whether oral or written. Similar vulnerabilities exist in relation to people's finances. This goes far beyond the traditional registration of property and income ownership. The globalisation and digitalisation of financial services, together with the trend towards cashless payments, have paved the way for a fundamental expansion and intensification of surveillance powers, enabling a greater number of agencies to gather and distill detailed insight into how individual citizens conduct their lives. Lastly, people's presence in public has traditionally provided many opportunities for exposure to observation. Today, mobility has become a target point for a variety of new surveillance powers. In addition to the afore-mentioned record of PNR data (see above, II.1.), automobility is a key producer of sensitive data: personal data about car owners and their driving behaviour, technical data automatically generated by the car itself, data recorded by the manufacturer, etc. These data can be generated by state agents through speed control, digital parking control, automated section control based on automated licence plate recognition, GPS tracking, etc. or through the seizure of existing data, e.g., records from the navigation systems, technical information, data generated by connectivity services, dashcam content, and, most controversially, image and video records from Tesla's Sentry Mode.

Figure 1: Sensitive spheres of private life subject to surveillance



2. Normative analysis of regulations

Based on this analytical structure along the five most sensitive spheres of private life, the MPI-CSL's research team collated a full record of all relevant legal provisions under which police, prosecution, customs and intelligence agencies[42] are permitted to collect data or other forms of personal information.[43] In total, the research team identified some *3,500 statutory provisions and sub-provisions*[44] under which the competent security agencies in Germany are permitted to initiate surveillance operations.[45] Such provisions quite often include several statutory alternatives of the same type of measure to which diverging legal and/or situational conditions apply. These conditions include specified catalogue crimes, different degrees of suspicion, and different threat categories, etc. The measures must be organised and operated in different ways – for example, differing in scope or threshold, or governed by either more lenient or more restrictive procedural rules. As a first key product, the Surveillance Barometer enables comprehensive surveillance maps to be designed. These maps offer people the opportunity to trace the different areas in which they are effectively at risk of being subject to an infringement of their privacy. It also allows them to retrieve detailed information about which agency can tap into which sphere of life, according to which regulation, and under which rules. In the near future, dynamic surveillance maps will be made accessible to the general public in an online database.[46]

3. Normative intensity assessment

Another core element of the MPI-CSL's further analyses is the assessment of the normative intensity of the fundamental rights infringements that go with state surveillance, based on a set of standardised criteria. To this end, a complex category system was developed that takes into account all characteristics that can be assigned in an abstract manner and quantifies them according to their relative constitutional weight. From the voluminous body of the FCC's case law, a total of 18 abstract parameters[47] were extracted in order to assess normative intensity in detail. Functionally, two types of criteria must be distinguished.

The first group consists of factors which constitute the basic severity of infringement. These include the privacy grade of information acquired, the aim and duration of an operation, and the potential impact on third parties (see *Table 1a*). Next to these constituting factors, the second group comprises potential mitigating circumstances. These features, which aim to alleviate the potential impact of fundamental rights infringements, are an essential part of security legislation in the form of, e.g., regulations on legal and operational thresholds, procedural safeguards, and mechanisms of internal or external control, either *ex ante* or *ex post* (see *Table 1b*). Both groups of factors consist of nine variables, each subdivided into several sub-categories (items) and rated on a scale from 1 and to 10. However, the various factors do not all carry the same constitutional weight. These differences have been taken into account by assigning individual weighting factors, which also range between 1 and 10 (see *Tables 1a and 1b* again). The values of the constituting and the mitigating factors have been inversely scaled according to their distinct function. Altogether, intensity can be determined according to 118 items. [48]

Table 1a: Factors constituting basic severity

Constituting Factors

	Criteria	Weighting factor	Relative weight (%)
1.	Privacy grade of information acquired	10	32
2.	Spread width (potential impact on third parties)	4	13
3.	Recourse on retained data	4	13
4.	Maximum duration	3	9.5
5.	Temporal direction	3	9.5
6.	Degree of covertness	3	9.5
7.	Role of person(s) targeted	2	6.5
8.	Method/technique used	1	3
9.	Aim of surveillance measure	1	3
	Total	31	99

Table 1b: Mitigating factors

Mitigating Factors

	Criteria	Weighting factor	Relative weight (%)
1.	Legal threshold: protected legal interest/reference crime	10	25
2.	Operational threshold: type of (potential) threat/degree of suspicion	10	25
3.	Requirements for authorisation	5	12.5
4.	Additional formal safeguards	5	12.5
5.	Protection of those entitled to refuse to testify	3	7.5
6.	Duty to erase collected data after use	3	7.5
7.	Duty to notify those affected	2	5
8.	Duty to keep track records	1	2.5
9.	External control mechanism	1	2.5
	Total	40	100

The next step is to calculate the refined normative intensity scores, which are composed of the respective severity and mitigation scores of each statutory variant. Rather than simply multiplying the two scores, a mitigation formula[49] was developed to reflect the relative weight of the mitigating factors. This implies that statutory safeguards cannot counterbalance the true impact of a fundamental rights infringement, neither to a major nor even to a full extent. Otherwise, it might so happen that a measure of high severity, which regularly goes hand in hand with high protection standards (e.g., a covert remote search of a private computer), and a measure of low severity, to which no or only minor procedural constraints apply (e.g., an automated inventory data request), score similarly. As a result of intensive preliminary testing, the maximum possible reduction effect of mitigation was set at 15 per cent of the severity score, decreasing with lower severity.[50]

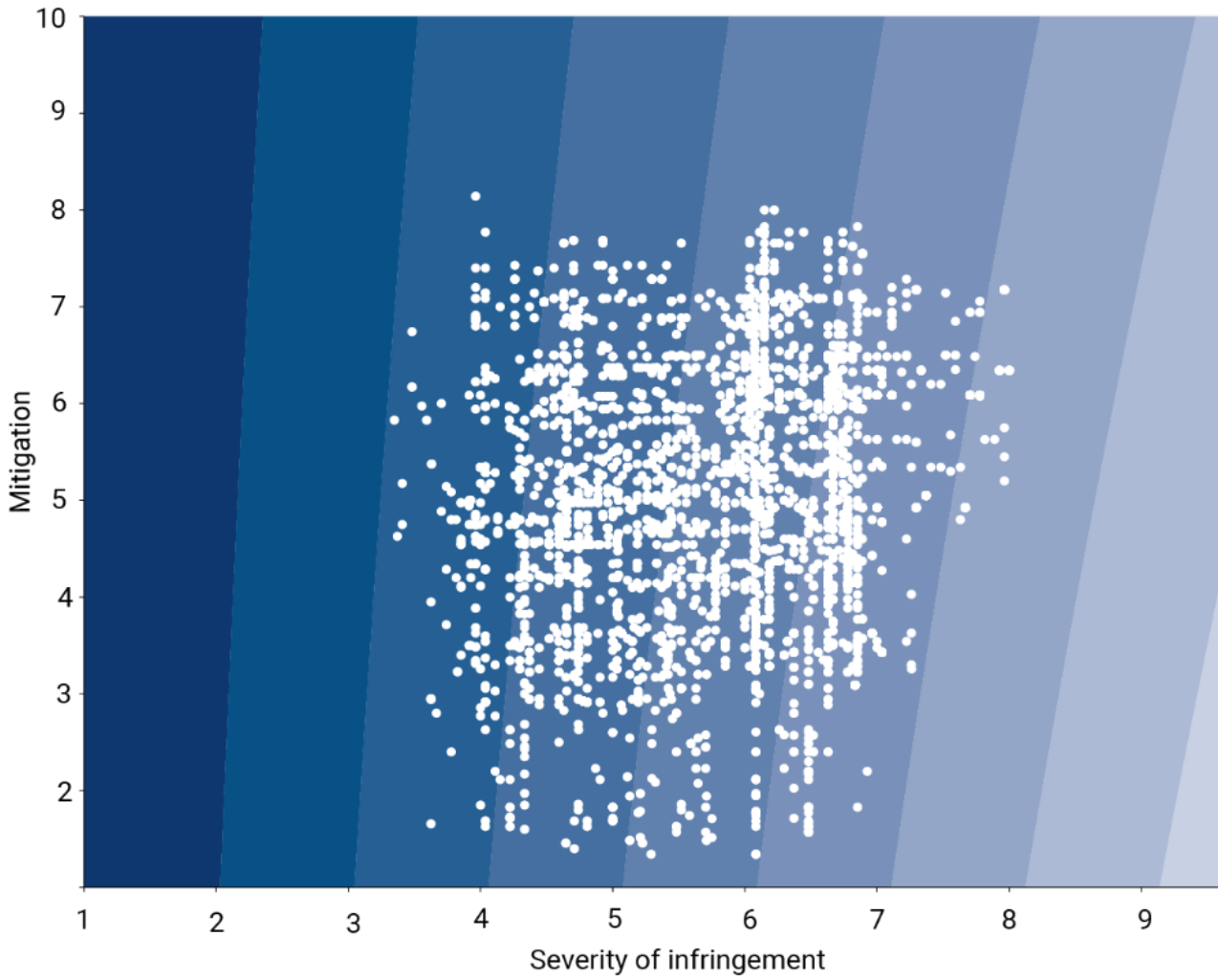
Having completed the normative intensity assessment for all the relevant statutory provisions and their variants in force in 2022,[51] the research team's findings provide detailed insight into the intensities of the fundamental rights infringements. *Table 2* provides an overview of the variance in the three normative scores. While the basic severity of statutory surveillance powers varies between 3.348 and 8.0, refined intensity scores that take into consideration the mitigating factors are moderately lower, ranging between 3.055 and 7.342. The variance is significantly broader when looking at the configuration of the statutory safeguards, as reflected in the mitigation score. The minimum is 1.343 and the maximum is 8.143. This indicates, firstly, that there is a broad range of legislative options for achieving a (more) protective configuration of surveillance powers, and, secondly, that legislatures do in fact make use of such moderating techniques in different ways and to varying degrees. It follows that the same powers are often regulated in different ways in the respective laws, with mitigation scores varying by more than 30 per cent.[52] These findings underline the fact that legislatures in fact have considerable – political – leeway in shaping surveillance powers and, in doing so, determine the concrete levels of basic rights protection.

Table 2: Key scores of all relevant provisions under review (Germany, 2022)

	Severity score (S)	Mitigation score (M)	Refined normative intensity score (NI)
Minimum	3.348	1.343	3.055
Maximum	8.0	8.143	7.342
Mean	5.756	5.111	5.312
Median	6.0	5.175	5.448

Overall, intensities score above average. This is also confirmed by the fact that the median intensity is higher than the corresponding arithmetic mean. *Figure 2* illustrates the three-dimensional dispersion of the scores for all variants. It provides interesting insights into the general shape of surveillance powers in Germany. The pattern depicts a phenomenon that has been theoretically discussed in the literature as the unitising effect of the Federal Constitutional Court's rulings on the general standards of statutory basic rights protection. This supports the premise that key rulings by the FCC on a particular aspect of a single piece of legislation shape the margin of legislative autonomy to the effect that relevant laws tend to approximate, in particular, new or amending laws on the same subject matter that are subsequently passed.[53] In addition, extreme statutory configurations are prevented; there are no outliers at the far end of the scale. Across all provisions, however, the variance in mitigation (y-axis) is considerably high for most of the severity grades identified. The protective regulations governing surveillance powers scoring at around grade 4, for example, are as diverse as those for most of the powers scoring at grade 6 or even 6.9. Consequently, surveillance powers of the same severity grade that come with very high protection standards (between grades 7 or 8) in one case may be mitigated to a significantly lower degree in another, sometimes even lower than grade 2. This implies that the various legislatures pursue different policy priorities, which are realised through their distinct employment of mitigating factors. Only surveillance powers at the highest severity levels (i.e., higher than grade 7 on the x-axis) are subject to significantly high(er) protection standards such as, e.g., strict judicial ex ante control.

*Figure 2: Refined normative intensity scores (Germany, 2022)**



*) Contour Plot for NI = S – S (0.15 * M / 10) and NI >=1.

As illustrated, the normative data provided by the Barometer reflects the potential and limits for the statutory regulation of surveillance in Germany. The scores describe the normative level of surveillance in terms of the assessment of existing surveillance powers. The frequency with which these powers are used is not yet included in this analytic step.

4. Quantitative dimension of surveillance

In addition to the normative intensity of the relevant basic rights infringements, their frequency is of equal importance when assessing the general level of surveillance in a society. The reason for this is because the statutory potentialities identified and evaluated in the previous step only materialise via their operational implementation (see also above, II.3.). It should also be borne in mind that the greater the number of surveillance operations carried out, the more vulnerable a society becomes as a whole. This is why the number of surveillance measures conducted is an additional element of the Surveillance Barometer concept. In a subsequent work package, the relevant statistical data must be collected for each surveillance provision identified. These data will be aggregated into frequency scores that carry equal weight in the final formula. In

addition to the absolute frequency the density, i.e. the relative frequency in relation to the resident population, is taken into account.

Methodologically, two challenges need to be solved. First, the calculation model must balance out extreme quantitative imbalances that arise between surveillance measures that are extremely rare (such as dragnet investigations or remote computer searches with no more than a handful of cases per year) and cases of mass surveillance involving hundreds of thousands or even millions of applications per year (such as banking data queries or automated retrievals of telecommunications inventory data). To keep quantifications manageable, absolute numbers will be converted into indexed frequency coefficients with values between 1 and 10. Assuming that low numbers are much more prevalent than high ones, and that rare applications correlate with high and very high intensity, indexing will be carried out on the basis of a logarithmic scale to allow for a more detailed count in the lower intervals.[54]

Secondly, imbalances arising from differences in citizens' actual exposure to surveillance, caused by the fragmentation of legislative and operational competences in the Federal Republic of Germany, need to be taken into account. For example, there are the surveillance measures imposed by federal agencies acting under federal law, e.g., involving the Federal Criminal Police Office of Germany (BKA). These federal measures have a different overall impact than those carried out under state laws, which only capture subjects under the respective state jurisdictions. Consequently, calculations must also reflect differences in the regional populations. One way to address this impact disparity, is to aggregate frequency as incidence rates per 100,000 inhabitants – a well-accepted standard epidemiological method established in other areas of security policy, e.g., to portray crime rates and incarceration rates. At the same time, incidence rates can serve as an easily comprehensible reference frame for the general public, a concept which also gained popularity during the COVID-19 pandemic.

5. Surveillance scores

Both parameters – the intensity and the frequency of all the different surveillance measures – are the core elements of the MPI-CSL's Surveillance Barometer. Representing the *normative (constitutional) intensity and empirical frequency* of interventions, these elements must be combined in the fifth step. The respective surveillance scores can be generated by multiplying the intensity and the incidence scores, each ranging from 1 to 10. These scores then vary between 1 and 100 on a closed scale. This step is only possible if data on the frequency of the various surveillance measures is available. Ideally, in the future, surveillance scores should be provided for all surveillance measures effectively carried out in a calendar year – categorised by the specific statutory surveillance powers under which they are authorised. Currently, most agencies in Germany are not yet prepared to produce and deliver the necessary data for various reasons (see below, IV.).

6. General surveillance indices

The final step of the concept is the aggregation of the various scores into general surveillance indices to provide a comprehensive overview of the state of surveillance in the country and the relevant areas in which citizens' right to privacy is more or less vulnerable to state surveillance activities. These indices can be aggregated according to several parameters distinguishing between national and regional levels, between different sectors (e.g., policing, prosecution, and intelligence), and between the types and techniques of surveillance (e.g., telephone tapping, acoustic surveillance of private premises, retrieval of financial data, remote computer searches, and GPS tracking[55]).

At the moment, the Surveillance Barometer is fully operational for the delivery of normative intensity values only. *Figure 3a* shows the averaged normative indices for German surveillance powers under federal law and

under state law. It shows that the general level of surveillance intensity associated with the respective statutory powers is lowest in the state of Saxony and highest in Saarland. The average intensity of federal powers is also moderate, with an overall score that remains below the average of all of them.

The overall picture, however, changes significantly when viewing the accumulated impact (*Figure 3b*). When all surveillance powers are added up, the total number of statutory powers under federal law far exceeds that of the federal states, by more than 100 per cent. This is due to the existence of specialised federal agencies that have no state-level counterparts[56] and the sheer multitude of their powers, some of which are even exclusive, such as the collection and analysis of PNR data by the BKA. Their number alone also contributes to the level of surveillance, as it naturally increases the likelihood of individuals being targeted by a federal agency rather than a state agency.

*Figure 3a: Normative surveillance scores – averaged: Federal level and federal states (Germany, 2022)***

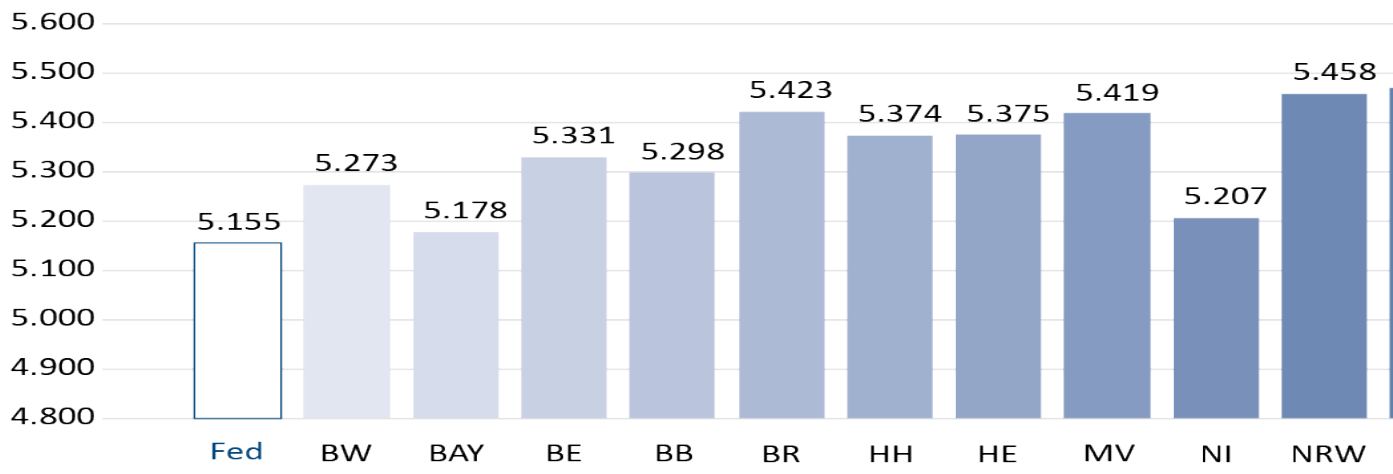
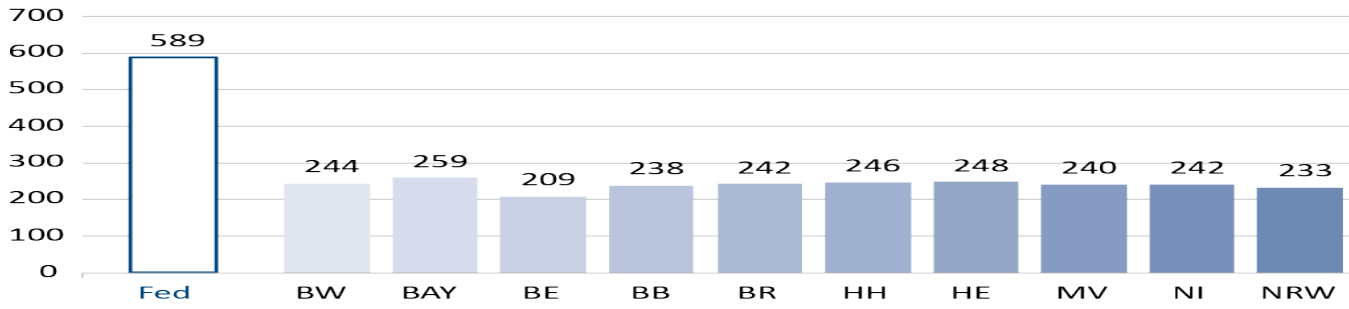


*Figure 3b: Normative surveillance scores – accumulated: Federal level and federal states (Germany, 2022)**



** Fed. = Germany Federation, BWE = Baden-Württemberg, BAY = Bavaria, BE = Berlin, BB = Brandenburg, BR = Bremen, HH = Hamburg, HE = Hesse, MV = Mecklenburg-Western Pomerania, NI = Lower Saxony, NRW = North Rhine-Westfalia, RP = Rhineland-Palatinate, SL = Saarland, SN = Saxony, SA = Saxony-Anhalt, SH = Schleswig-Holstein, TH = Thuringia.

The category system, with its detailed set of variables, enables all types of surveillance to be compared with one another. Presenting the data in the form of specified indices reveals both the total, cumulative burden of surveillance and its composition. In particular, this enables key areas of surveillance and potential critical levels of surveillance within individual sectors to be identified and pinpointed. The model is not static but can be flexibly adapted to the current legal status quo within the relevant reference period. This makes it well suited for responding to rapid regulatory developments, which are characteristic of security law.

IV. Outlook

The MPI-CSL's Surveillance Barometer is a valuable instrument for mapping and measuring both the extent and impact of surveillance actions on individuals and the resident population. Moreover, it highlights the potential for enhancing fundamental rights protection through the systematic identification of opportunities for regulatory adjustment. This is the first time that a thorough assessment model based on a uniform set of criteria has been tested in the field of state surveillance. Once established as a scientifically based transparency project for Germany, it can easily be modified and adapted for application in other jurisdictions.

However, the path towards reinforcing transparency in the use of surveillance powers is not merely a matter of political expediency; it also has a clear constitutional dimension. In the FCC's case law, transparency in the operations of public agencies has gained increasing importance as a fundamental prerequisite for proportionality. Among other things, the Court established a constitutionally grounded duty to implement effective record-keeping practices for all measures involving a fundamental rights infringement.[57] In the context of government surveillance measures, in particular, transparency has two dimensions: (1) an individual dimension focusing on those directly affected, and (2) a societal dimension. Regarding the latter, further internal and external aspects can be distinguished. These include the function of transparency as a prerequisite for effective professional oversight and judicial control, for democratic control in the political arena and society, and for internal organisational control and resource management.[58] In Germany, the most urgent practical challenge to date is to remedy the lack of reliable statistical data on the application of statutory powers, including surveillance operations. This sparse availability of data leaves the public in the

dark about their use. In this regard, the grim picture of a surveillance society – often expressed by human rights activists[59] – could be seen as a *symptom of a lack of transparency*.

In Germany, the unavailability of data is also the result of structural deficits in digitalisation. It is not uncommon still for annual counting lists to be compiled by manually browsing paper files. At the same time, digital case management systems used in the police force and in other public sectors have been configured to disable automated record functions deliberately, in order to prevent unlawful performance monitoring and to dispel eventual data protection concerns.

Yet, a promising policy tool, which has received increasing attention in recent years as an instrument to generate better availability of statistical data, involves statutory duties to produce and publish statistical records about the use of specific measures considered to have the potential to seriously infringe fundamental rights. Telecommunications surveillance and remote online searches of private computers are exemplary areas in which the FCC's calls for greater transparency have led to the introduction of transparency provisions. Such regulations can currently be found in the German Code of Criminal Procedure,[60] the Federal Criminal Police Office Act,[61] and many state police laws,[62] for example. In most cases, however, these provisions cover only a very limited number of surveillance powers, primarily those that have been the subject of public controversy and political resistance in parliamentary proceedings. They have also been used as an incentive to get the relevant bills passed. These provisions differ significantly from one another in terms of both form and content. So far, the statistics have sometimes only been provided to the respective parliamentary bodies and are not always publicly accessible. In direct comparison, Sec. 101b of the Code of Criminal Procedure[63] appears to be the current gold standard as the Federal Office of Justice (*Bundesamt für Justiz*) publishes the data online.[64] With an advanced judicial and political pressure, the volume of data provided by other agencies should also increase in the coming years. Subsequently, these statistics will become an important resource for the Barometer.

Ultimately, the Surveillance Barometer concept could be used as a blueprint for developing a Europe-wide transparency monitor.[65] From an EU perspective, it could be applied as an analytical tool to help the European Commission and/or the European Parliament and its committees conduct comparative evaluations of how EU laws have been implemented in national legislation across Member States. Experience gained from the German pilot project could be a useful incentive for this purpose. At the European level as well, the availability of necessary statistical materials is expected to improve steadily, as EU legislation increasingly mandates statistical data collection from Member States. The requirements for the quality and validity of data provided have been enhanced over time. Whereas older acts such as, for example, the 2012 Victims' Rights Directive[66] or the 2013 Cybercrime Directive[67] oblige Member States only to provide "data and statistics" (in the latter example only in three-year cycles), more recent pieces such the 2024 Asset Recovery and Confiscation Directive[68] have been setting forth significantly higher standards, requiring the production and maintenance of comprehensive statistics on a variety of concretely specified types of data,[69] to be delivered on an annual basis. Even more extensive are the requirements for the statistical recording of more or less all relevant activities carried out in the field of money laundering control.[70] Consideration should also be given at EU level to establishing a more systematic framework for the provision of meaningful statistic records. In the end, European statistical requirements may have a positive impact, as they can also help increase the availability of national data, which did not previously exist or were not publicly accessible at the domestic level.

---

1. This includes both data owned by citizens and data generated and administered by public agencies or commercial service providers.↩
2. P. Schaar, *Das Ende der Privatsphäre: Der Weg in die Überwachungsgesellschaft*, 2007.↩
3. In absence of an explicit competence in pre-Lisbon times, the initiative was inappropriately promoted as a subject of market regulation. Cf., e.g., H.-J. Albrecht, A. Grafe & M. Kilchling, *Rechtswirklichkeit der Auskunftserteilung über Telekommunikationsverbindungsdaten nach §§ 100g, 100h der*

Strafprozessordnung, BT-Drucksache 16/8434 of 28.02.2008, pp. 41 et seq., <https://dserver.bundestag.de/btd/16/084/1608434.pdf>; A. Adensamer, *Handbuch Überwachung*, 2020, pp. 34 et seq. Note: All hyperlinks in this article were last accessed on 28 April 2026.↩

4. Directive 2006/24/EC of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks, OJ L 105, 13.4.2006, 54.↩
5. ECJ, 8 April 2014, Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland, Seitlinger & Others*, EU:C:2014:238.↩
6. Cf., e.g., Fennelly's notion of the "life, death and afterlife" of that directive: D. Fennelly, "Data retention: The life, death and afterlife of a directive", (2019) 19(4), *ERA-Forum*, 673-692. For the debate on data retention at the EU level, see also T. Wahl, "Council: The Way Forward in Data Retention", (2019) *eucrim*, 106 with further news references; A. Juszczak and E. Sason, "Recalibrating Data Retention in the EU", (2021) *eucrim*, 238-266.↩
7. Cf., e.g., R. Sarre, "The Surveillance Society: A Criminological Perspective", in: E.C. Viano (ed.), *Cybercrime, Organized Crime, and Societal Responses*, 1985, pp. 291-300.↩
8. Cf., e.g., P. Schaar, *op. cit.* (n. 2); T. Singelnstein & P. Stolle, *Die Sicherheitsgesellschaft. Soziale Kontrolle im 21. Jahrhundert*, 2008; N. Zurawski (ed.), *Surveillance Studies. Perspektiven eines Forschungsfeldes*, 2008.↩
9. BVerfG, 2.3.2010, 1 BvR 256, 263, 586/08 = BVerfG Official Case Reports E 125, 260. Abbreviated English version available at <www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2010/03/rs20100302_1bvr025608en.html>.↩
10. BVerfG, *op. cit*. (n. 9), annot. 218 (English version).↩
11. BVerfG, *op. cit*. (n. 9), annot. 218 (original German version). This sentence was not translated in the abbreviated English version of the ruling.↩
12. A. Roßnagel, "Die ‚Überwachungs-Gesamtrechnung' – Das BVerfG und die Vorratsdatenspeicherung", (2010) 63(18), *Neue Juristische Wochenschrift (NJW)*, 1238-1242; A. Roßnagel et al., "On the Introduction of a Surveillance Calculus in Germany", Policy Paper, *Forum Privacy and Self-determined Life in the Digital World*, April 2022, <https://publica-rest.fraunhofer.de/server/api/core/bitstreams/47c4f3a8-73d4-405b-806f-072f4aa9c1bb/content>.↩
13. Originally, this approach leaned on the doctrine of "chilling" effects of state surveillance powers which are presumed to deter ("chill") citizens from exercising their rights and freedoms for fear of legal repercussions. The various aspects of that doctrine, including its weaknesses, are discussed, e.g., by J.W. Penney, "Understanding Chilling Effects", (2022) 106(3), *Minnesota Law Review*, 1451-1530.↩
14. The extremely low number of remote computer searches in police practice has been documented, for example, in an evaluation of these statutory powers carried out by the Federal Criminal Police Office of Germany (BKA) in the years 2009-2014; for more details, see H.-J. Albrecht & R. Poscher, *Evaluationsbericht zu den §§ 4a, 20j, 20k des Bundeskriminalamtgesetzes*, BT-Drucksache 18/13031 of 23.06.2017, <https://dserver.bundestag.de/btd/18/130/1813031.pdf>.↩
15. Cf., e.g., J.-B. Maillard, "European Union", in: B. Vogel & J.-B. Maillard (eds.), *National and International Anti-Money laundering Law. Developing the Architecture of Criminal Justice, Regulation and Data Protection*, 2000, pp. 71-155.↩
16. These include, *inter alia*, information on citizens' bank and credit card accounts (inventory data) as well as detailed records of bank and credit card transactions, smart payments, cash transactions (above a certain limit), content data, etc. For a comprehensive analysis of all the various powers public agencies have to access and process the retained data, see C. Kaiser, *Privacy and Identity Issues in Financial Transactions: The proportionality of the European anti-money laundering legislation*, dissertation University of Groningen, 2018, <https://research.rug.nl/en/publications/privacy-and-identity-issues-in-financial-transactions-the-proport/2018>; L.M. Landerer, *Massenüberwachung von Finanzdaten. Die Geldwäschebekämpfung unter der Sicherheitsverfassung*, 2025.↩
17. Cf., e.g., E. Orrù, "The European PNR framework and the changing landscape of EU-security", *Verfassungsblog – On Matters Constitutional*, 21 December 2021, https://verfassungsblog.de/os3-pnr/.↩
18. With Regulation (EU) 2024/1624 of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, OJ L 2024/1624, new and further tightened elements of money laundering control will enter into force in July 2027, referred to by Tosza as silent expansion of the administrative AML control regime; S. Tosza, Enforcement of international sanctions as the third pillar of the anti-money laundering framework. An unannounced effect of the AML reform and the Sanctions Directive, 2024, *New Journal of European Criminal Law*, 15(3), pp. 336-356.↩
19. In German terminology and doctrine, 'basic rights' (*Grundrechte*) is used as a synonym for fundamental/human rights.↩
20. For more details, see, e.g., G. Letsas, "Proportionality as Fittingness: The Moral Dimension of Proportionality", (2018) 71(1) *Current Legal Problems*, 53-86; E. Orrù & R. Poscher, *Conceptions of Data Protection and Privacy. Legal and philosophical perspectives*, 2025.↩
21. Cf. M. Löffelmann, *Überwachungsgesamtrechnung und Verhältnismäßigkeitsgrundsatz*, 2022; *id*., "Eingriffsintensität und Eingriffsschwelle. Eine Formel für den Gesetzgeber", (2023) *Zeitschrift für das gesamte Sicherheitsrecht (GSZ)*, 92-96; *id*., "Die Überwachungsgesamtrechnung", (2024) *Zeitschrift für das gesamte Sicherheitsrecht (GSZ)*, 18-22.↩
22. Suggested readings include, e.g., D. Lyon, *Surveillance Studies: An Overview*, 2012; *id*., *Surveillance Studies: A Very Short Introduction*, 2024, and the contributions provided in D. Wright & R. Kreissl, *Surveillance in Europe*, 2015.↩
23. Cf., e.g., S. Altwicker-Hármori et al., "Measuring Violations of Human Rights – An Empirical Analysis of Awards in Respect of Non-Pecuniary Damage under the European Convention for Human Rights", 2016, 76(1) *Zeitschrift für ausländisches öffentliches Recht und Völkerrecht (ZaöRV)*, 1-51, <www.zaoerv.de/76_2016/76_2016_1_a_1_52.pdf>.↩
24. Cf., e.g., D. Wright & P. de Hert, *Privacy Impact Assessment*, 2012.↩
25. Cf., e.g., P. de Hert, "A Human Rights Perspective on Privacy and Data Protection Impact Assessment", in: D. Wright & P. de Hert (eds.), *Privacy Impact Assessment*, 2012, pp. 33-76; J. Milaj, "Privacy, surveillance, and the proportionality principle: The need for a method of assessing privacy implications of technologies used for surveillance", (2016) 30(3) *International Review of Law, Computers & Technology*, 115-130; G. Malgieri & C. Santos, "Assessing the (severity of) impacts on fundamental rights", (2025) 56 *Computer Law & Society Review: The International Journal of Technology Law and Practice*, 106113, <https://www.sciencedirect.com/science/article/pii/S0267364925000081>.↩
26. Cf., e.g., J. Milaj, *op. cit.* (n. 25).↩
27. Cf., e.g., M.-H. Maras, "The economic costs and consequences of mass communications data retention: Is the data retention directive a proportionate measure?", 2012, 33(2) *European Journal of Law and Economics*, 447-472.↩
28. D. Wright & C.D. Raab, "Constructing a surveillance impact assessment", 2012, 28(6) *Computer Law and Security Review*, 613-626.↩

29. According to Sajfert, their quality sometimes amounts to little more than "lip service"; J. Sajfert, *Resolving Legal Conflicts Between Data Access Investigative Measures and Data Protection Law in the EU. The case for quantitative data and balancing*, dissertation Université du Luxembourg, Faculty of Law, Economics and Finance, and Vrije Universiteit Brussel, Faculty of Law and Criminology, p.4, <https://orbilu.uni.lu/handle/10993/60157>.↩
30. For more details, see, e.g., R. Poscher & M. Kilchling, "Wie lässt sich die Überwachung der Bürgerinnen und Bürger messen? Pilotprojekt zur Messung der Überwachung in Deutschland", (2022) *Deutsche Richterzeitung* (*DRiZ*), 98-101; J. Milaj, *op. cit*. (n. 25); G. Malgieri & C. Santos, *op. cit*. (n. 25).↩
31. For more details, see Malgieri & Santos, *op. cit*. (n. 25).↩
32. For theoretical analyses of system-inherent problems of measurement in the context of the proportionality concept, see R. Poscher, "§ 3 – The Basic law as a constitution of proportionality balance", in: M. Herdegen et al. (eds.), *Constitutional Law in Germany. A Handbook in Transnational Perspective*, 2025; *id*., "What would it take? The potential and limits of proportionality analysis in law", (2025) 16(3) *Jurisprudence*, 443-476.↩
33. Bäcker collates all of them into four basic levels of intensity: low, medium, high, and highest: M. Bäcker, "§ 28 – The security constitution", in: M. Herdegen et al. (eds.), *Constitutional Law in Germany. A Handbook in Transnational Perspective*, 2025, annot. 25.↩
34. Judge Schluckebier, BVerfG, *op. cit*. (n. 9), annot. 311-314.↩
35. Judge Eichberger, BVerfG, *op. cit*. (n. 9), annot. 343.↩
36. Judge Schluckebier, BVerfG, *op. cit*. (n. 9), annot. 314.↩
37. Löffelmann therefore speaks of "*Begriffssynkretismus* [terminological syncretism]"; M. Löffelmann, "Datenerhebung aus dem „Smart Home" im Sicherheitsrecht", (2020) *Zeitschrift für das gesamte Sicherheitsrecht (GSZ)*, 244-250.↩
38. It is likely that additional descriptive categories will have to be created for future cases.↩
39. Based on similar considerations, Roßnagel, (2010) NJW, *op. cit*. (n. 12), 1242 launched the idea of a "double proportionality test".↩
40. See above, II.1.↩
41. For a list of relevant projects, see Max-Planck-Institut zur Erforschung von Kriminalität, Sicherheit und Recht (MPI-CSL), *Überwachungsgesamtrechnung für Deutschland. Pilotstudie basierend auf der wissenschaftlichen Evaluation ausgewählter Überwachungsbefugnisse der Sicherheits- und Strafverfolgungsbehörden – Band 1*, 2025, p. 10; <https://pure.mpg.de/rest/items/item_3649030_9/component/file_3649042/content>.↩
42. Germany's architecture of security agencies is rather diverse. Responsibilities are distributed among 18 police agencies (2 federal and 16 state police forces), 25 prosecution divisions (organised alongside the jurisdiction of the 24 higher state courts, plus the Federal Attorney General who has primary jurisdiction in selected types of cases), 19 intelligence services (3 federal and 16 state agencies), and 4 customs agencies (Customs Criminal Office, Customs Investigations Bureau, Financial Intelligence Unit – FIU, Central Office for Sanctions Enforcement). With the exception of the prosecution sector, to which the German Code of Criminal Procedure applies, all other agencies act under their own sectoral laws, which are formally and substantively quite diverse.↩
43. <https://csl.mpg.de/815178/what-is-the-current-state-of-germany-s-security-laws>.↩
44. As of 2024.↩
45. Domestic surveillance powers exclusively. (Trans-)national operations carried out by foreign agencies as well as data generated abroad and later shared with German agencies are not included. For conclusions drawn from the EncroChat, SkyECC and ANOM cases, see M. Lassalle and S. Lannier, "EncroChat – A Judicial Chronology"; and T. Wahl, "What Remains of the ordre public in Transnational Surveillance?" (both contributions are in this issue); as well as S. Gless, "Heiligt der Zweck die Mittel 2.0?" (2026), 144 *Schweizerische Zeitschrift für Strafrecht (ZStrR),* 80–107.↩
46. The urls will be: <https://surveillance-barometer.de> and <https://surveillance-barometer.eu>.↩
47. This exclusive focus on abstract parameters follows from the methodological limitation that the circumstances of individual surveillance operations could be collected by means of a case-by-case (file) analysis only.↩
48. For a complete inventory of the 18 variables and their composition, see MPI-CSL, *loc. cit*. (n. 41); *id*., *Überwachungsgesamtrechnung für Deutschland. Pilotstudie basierend auf der wissenschaftlichen Evaluation ausgewählter Überwachungsbefugnisse der Sicherheits- und Strafverfolgungsbehörden – Band 2: Manual,* 2025, https://pure.mpg.de/rest/items/item_3649032_9/component/file_3649041/content.↩
49. NI = S – S (0.15 * M / 10) and NI >=1 (see below, Figure 2).↩
50. For more details, see MPI-CSL, *op. cit.* (n. 41), *id*., *op. cit.* (n. 48).↩
51. Updates and amendments for 2023 and 2024 have almost been completed, too.↩
52. For more details, see MPI-CSL, *op. cit*. (n. 41), pp. 52 et seq.↩
53. K. Hesse, *Der unitarische Bundesstaat*, 1962, p. 9; K. Graulich, "Das Handeln der Polizei- und Ordnungsbehörden zur Gefahrenabwehr", in: M. Bäcker et al. (eds.), *Handbuch des Polizeirechts*, 7th ed. 2021, pp. 341-823 (p. 372).↩
54. For the purpose of the Barometer, it matters whether a high- or very high-intensity measure is carried out 10 or 20 times; however, it is irrelevant whether a standard measure of (very) low intensity has 100,001, 100,010, or 100,500 counts.↩
55. In total, more than 50 different types and techniques of surveillance were identified; for more details, see MPI-CSL, *loc. cit.* (n. 41), pp. 25 et seq. (table 2).↩
56. See above, footnote 42.↩
57. BVerfGE 125, 260, 344; *op. cit.* (n. 9).↩
58. For further details, see MPI-CSL, *op. cit*. (n. 41), pp. 16 et seq.↩
59. See above, I.↩
60. Sec. 101b StPO.↩
61. Sec. 88 BKAG.↩
62. E.g., Sec. 90 Police Act for Baden Württemberg, Art. 52 Bavarian Police Act, etc. For a comprehensive list, see MPI-CSL, *op. cit*. (n. 41), pp. 18 et seq. (table 1).↩
63. This provision obliges all prosecution offices (state and federal) to provide detailed annual statistics on the following covert measures of surveillance ordered and carried out, together with some further statutorily specified details about the circumstances of their execution: surveillance of telecommunication, remote computer search, capture of telecommunication traffic data (meta data), capture of usage data in

respect of digital services, and acoustic surveillance of private premises. Meanwhile, data about telephone tapping are available for a long time period since 2000; the collection of others started later, in particular those relating to measures which were introduced only a few years ago.↩

64. Cf. <www.bundesjustizamt.de/DE/Service/Justizstatistiken/Justizstatistiken_node.html>.↩
65. According to Sajfert, *op. cit.* (n. 29), ensuring transparency is the one of the most challenging fundamental principles for the EU as a whole.↩
66. Art. 28 of Directive 2012/29/EU of 25 October 2012 on minimum standards on the rights, support and protection of victims of crime, OJ L 315, 14.11.2012, 57.↩
67. Art. 14 of Directive 2013/40/EU of 12 August 2013 on attacks against information systems, OJ L 218, 14.8.2013, 8.↩
68. Art. 28 of Directive (EU) 2024/1260 of 24 April 2024 on asset recovery and confiscation, OJ L. 2024/1260.↩
69. Specified in Art. 28 lit. a-k.↩
70. Art. 9 of Directive (EU) 2024/1640 of 31 May 2024 on the mechanisms to be put in place by Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, OJ L 2024/1640.↩

* Authors statement

The authors would like to thank Indira Tie, Dr. Anna Pingen, and Thomas Wahl from the eucrim team for their careful review of the manuscript and their valuable comments. The authors would also like to extend their sincere thanks to Ines Hofmann for designing and formatting the charts and tables.

About eucrim

The project is co-financed by the Union Anti-Fraud Programme (UAFP), managed by the European Anti-Fraud Office (OLAF).

Co-funded by
the European Union