On Measuring Fundamental Rights Protection: Can and Should Data Protection Law Learn From Environmental Law?

JÖRG POHLE

Data protection, understood as the protection from the negative consequences of the increasing 'datafication' of the world[1] and 'industrialization' of information processing[2] for individuals, groups and the society, and environmental protection share three structural characteristics.[3]

The first common feature is the universality of the problems. Both data protection and environmental protection are responses to an ever increasing scope and permeation of today's technology that has made the whole earth the prerequisite, the object and the result of technical processes, the natural world as well as the social world. Data protection is the response to the fact that information technologies make information universally available and computable, fundamentally change forms, situations and contents of individual and societal communication, and allow for those who control these technologies to amass power and to amplify, consolidate and perpetuate control over their environment.[4]

The second common feature of the two problem areas is that they both touch on the very identity of modern Western societies, they are what in the past has been called "existential". They are both downsides of progress – or: "progress" –, which for a very long time was perceived along the lines of: progress in enlightenment, progress in technology, progress in living conditions. Both regarding the industrialisation of material production and of information processing, the limits to growth, the limits to (technological) progress are becoming ever more visible.

At least in Germany, and maybe more generally in the European Union as well, there is a third common feature: political demands are mainly directed towards the state, touching on a particular understanding of the (constitutional) state. Both data

[1] Fiedler, Herbert (1975), Datenschutz und Gesellschaft. In: Siefkes, D. (ed.), *GI – 4. Jahrestagung*. Berlin: Springer, pp. 68–84.

[2] Steinmüller, Wilhelm (1981), Die Zweite industrielle Revolution hat eben begonnen – Über die Technisierung der geistigen Arbeit. In: *Kursbuch* 66, pp. 152-188.

[3] Podlech, Adalbert (1987), Der Datenschutz und die Akzeptabilität unserer Gesellschaftsordnung. In: Hohmann, H. (ed.), *Freiheitssicherung durch Datenschutz*. Frankfurt am Main: Suhrkamp, pp. 19–24.

[4] For an introduction to this broad understanding of data protection see Pohle, Jörg (2016), Transparenz und Berechenbarkeit vs. Autonomie- und Kontrollverlust: Die Industrialisierung der gesellschaftlichen Informationsverarbeitung und ihre Folgen. In: *Mediale Kontrolle unter Beobachtung* 5(1), Article 5.

protection and environmental protection are thus eminently political issues, which at the same time defy the oversimplified dichotomy of "an affirmation of the strong state and the subordination of data protection to state necessities vs. an emphasis on the freedom of the citizen and a preference of data protection over the effectiveness of government action".[5]

ENVIRONMENTAL LAW'S INCREASING DRIVE TOWARDS QUANTIFICATION

Against this background, it is rather surprising that the overlap between data protection and environmental protection has not extensively been covered in the scholarly literature. This contribution to the *liber amicorum* for Ingolf Pernice will shed some light on a peculiar aspect of the last decades' development in both the environmental protection discourse and law that may provide a possible starting point for investigating how today's data protection law might be further developed in order to strengthen its application as well as its enforcement in practice: the drive towards quantification.

At the very same time, this idea taps well into Ingolf Pernice's extensive experience in shaping environmental protection law and institutions: as a member of the European Commission's Legal Service from 1987 to 1993, Ingolf Pernice not only encouraged the founding of the European Environment Agency (EEA), but also participated as a legal advisor of the European negotiating delegation at the United Nations Conference on Environment and Development (UNCED), better known as the Rio Summit, in 1992. Both the EEA and the Rio Summit are deeply linked to environmental law's increasing reliance on quantification.[6]

The EEA's mission is to provide independent information on the environment for policy-makers. This information is based on the DPSIR framework – Drivers, Pressures, State, Impact and Response model of intervention –, a causal framework describing the interdependent interactions between society and the environment,[7] which is an extension of the PSR model – Pressure, State, Response – developed by OECD in the 1980s.[8]

The most important achievement of the Rio Summit, held in June 1992, was an agreement on the United Nations Framework Convention on Climate Change (UNFCCC) which in turn led to the Kyoto Protocol, adopted in 1997, and the Paris Agreement, adopted in 2015. Whether the UNFCCC's objective of stabilising

[5] Podlech (1987), op. cit., pp. 22–23. The German text refers to "Bürger", it most probably means "subjects of fundamental rights" though.

[6] Moldan, Bedrich; Janoušková, Svatava & Hák, Tomáš (2012), How to understand and measure environmental sustainability: Indicators and targets. In: *Ecological Indicators* 17, pp. 4–13.

[7] Smeets, Edith & Weterings, Rob (1999), *Environmental indicators: Typology and overview.* European Environment Agency, Technical report No. 25.

[8] Lehtonen, Markku (2008), Mainstreaming sustainable development in the OECD through indicators and peer reviews. In: *Sustainable Development* 16, pp. 241–250.

greenhouse gas concentrations in the atmosphere, the Kyoto Protocol's objective of reducing greenhouse gas emissions or the Paris Agreement's objective of decreasing global warming – they all demand for and depend on quantifying properties of the environment to create indicators that guide the implementation of policies, the selection of specific measures as well as the monitoring of achievements.

QUANTIFICATION'S JANUS-FACEDNESS

The greatest challenge with regards to quantification is that it's not just a new or different description of the social and the natural world, but a means of reconfiguring them. The very process of quantification imposes new meanings on the world and makes old ones disappear.[9] At the same time, it is a *social* process of assigning numbers to the natural and the social environment.[10] Quantification has been identified as a potential driver towards a (further) depoliticization of inherently political issues,[11] which fundamental rights certainly are, and merely attempting to quantify fundamental rights like human dignity or personal freedom might result in a loss of legitimacy.[12] It has advantages as well, though, and that's the very reason for exploring its applicability. The main advantage is that it simplifies comparison between different approaches and means of protection, and at the same time goes beyond subjective views and individual interests. For example, quantification, or more broadly: formalization, would prevent (supreme or constitutional) courts from simply generating cloudy outpourings, as they do now, that in the end must lead to arbitrary results, which not only structurally undermines fundamental rights, but also the courts' legitimacy.[13] The very process of making things auditable[14] would demand greater clarity, though it would also introduce more contingency, regarding the object of protection and the conditions under which they are or may be threatened in order to develop suitable as well as societally acceptable indicators for their protection. It would thus prevent scholars, legislators and engineers from hiding behind the smoke screens that are produced by mingling arbitrary, one-sided understandings of essentially

9 Porter, Theodore M. (1994), Making Things Quantitative. In: *Science in Context* 7(3), pp. 389–407.

10 "It is *we* who assign numbers to nature." Carnap, Rudolf (1966), *Philosophical Foundations of Physics: An Introduction to the Philosophy of Science*. New York: Basic Books, p. 100.

11 Harbordt, Steffen (1975), Die Gefahr computerunterstützter administrativer Entscheidungsprozesse: Technokratisierung statt Demokratisierung. In: Hoffmann, G. E.; Tietze, B. & Podlech, A. (eds.), *Numerierte Bürger*. Wuppertal: Peter Hammer Verlag, pp. 71–77; Lischka, Konrad & Stöcker, Christian (2017), *Digitale Öffentlichkeit: Wie algorithmische Prozesse den gesellschaftlichen Diskurs beeinflussen*. Working paper, ed. by Bertelsmann Stiftung.

12 Grechenig, Kristoffel & Lachmayer, Konrad (2011), Zur Abwägung von Menschenleben – Gedanken zur Leistungsfähigkeit der Verfassung. In: *Journal für Rechtspolitik* 19, pp. 35–45.

13 For an early critique on this development see Schlink, Bernhard (1974), *Abwägung im Verfassungsrecht*. Berlin: Duncker & Humblot.

14 Power, Michael (1996), Making Things Auditable. Accounting. In: *Organizations and Society* 21(2/3), pp. 289–315.

contested concepts[15] with terminological coincidence, such as "privacy", "anonymity" or "dignity", as it is common practice nowadays.

FORMALIZATION AND QUANTIFICATION IN PRIVACY AND DATA PROTECTION LAW (DISCOURSE)

The field of privacy and data protection law has a long, but thin and severely lopsided history of discourses on measuring both risks, or threats, and protection from these risks and threats.

ON MEASURING PRIVACY AND ANONYMITY

The first proposal of a measurable indicator for protecting the privacy of people was made in the 1960s in the Senate Hearings on Computer Privacy. In what has much later been called *k*-anonymity, a computer system would be built to allow "output data only in aggregates that contain a sufficient number of individual respondents to make identification of individuals difficult"[16], with the *k*, i.e. the number of people among which an individual would be indistinguishable, hence *k*-anonymity, chosen according to the risks, threats or possible damages caused by an attacker being able to identify an individual. This kind of "statistical disclosure control"[17] thus obviously builds upon the assumption that identifiability of the individual is a causal condition for the kind of consequences that this understanding of privacy aims to prevent or mitigate.

This assumption of causality between the individuals' identifiability and the impact on their fundamental rights and freedoms has been the leitmotif of both the research and the public discussion regarding suitable indicators for privacy protection ever since. It is thus no surprise that anonymity is generally seen as a guarantee for the protection of the data subjects' rights and freedoms, and thus perceived as a meaningful goal for both regulation and systems design.[18] Unfortunately, this assumption of causality between identifiability and impact is not only hardly ever made explicit, but also never proven.[19]

At the same time, this common reference to anonymity does not imply a shared understanding of the very concept of anonymity across disciplines, such as between

[15] Gallie, Walter Bryce (1956), Essentially Contested Concepts. In: *Proceedings of the Aristotelian Society* 56, pp. 167–198.

[16] Miller, Arthur Raphael (1969), Personal Privacy in the Computer Age: The Challenge of a New Technology in an Information-Oriented Society. In: *Michigan Law Review* 67(6), pp 1089–1246, 1217.

[17] Dalenius, Tore (1977), Towards a methodology for statistical disclosure control. In: *Statistik Tidskrift* 15, pp. 429–444.

[18] Van Rossum, H. et al. (1995), *Privacy-Enhancing Technologies: The Path to Anonymity*. Information and Privacy Commissioner / Ontario, Canada & Registratiekamer, The Netherlands.

[19] Pohle, Jörg (to appear), Technisch abgesicherter Freiheitsschutz jenseits von Privatheit. Folgerungen aus der produktivsten Phase der Datenschutzdebatte für die Digitalmobilität. In: Klumpp, D. (ed.), *Datengovernance für Digitalmobilität*.

law and computer science,[20] as terminological coincidence does not imply conceptual similarity. It thus seems rather counterproductive for the protection of fundamental rights and freedoms that developments such as *k*-anonymity and its derivatives like *l*-diversity[21] or *t*-closeness[22], or differential privacy[23], but also secure multi-party computation[24] or federated machine learning[25], which are currently very in vogue, are uniformly acclaimed and the companies that use such methods are widely praised.

Even more questionable is that the applicable data protection law, such as the EU General Data Protection Regulation, is built upon and strongly depends on this false assumption of causality. It is thus the only legal implementation of a protection of fundamental rights in which this protection is made dependent on the fact that those who infringe on the fundamental rights – more precisely: the actors who create or operate sources of risk for such rights – have positively identified or are able to identify the particular fundamental rights' holders beforehand.[26]

There are other privacy metrics beyond those that are based on the equation of privacy with anonymity.[27] Unfortunately, they all refer to understandings of privacy where privacy equals either secrecy or confidentiality, and always – at least implicitly – confined to "sensitive" information.[28] This problem is aggravated by increasingly placing hopes in technical privacy solutions, which are oftentimes collectively called Privacy-Enhancing Technologies (PETs): the very way these technical solutions are

[20] Hölzel, Julian (2019), Differential Privacy and the GDPR. In: *European Data Protection Law Review* 5(2), pp. 184–196.

[21] Machanavajjhala, A. (2007), *l*-Diversity: Privacy Beyond *k*-Anonymity. In: *ACM Transactions on Knowledge Discovery from Data (TKDD)* 1(1), article no. 3.

[22] Li, Ninghui; Li, Tiancheng & Venkatasubramanian, Suresh (2007), *t*-Closeness: Privacy Beyond *k*-Anonymity and *l*-Diversity. In: Chirkova, R. et al. (eds.), *Proceedings of the 23rd International Conference on Data Engineering (ICDE 2007)*. Washington, DC: IEEE Computer Society, pp. 106–115.

[23] Dwork, Cynthia (2006), Differential Privacy. In: *Automata, languages and programming (ICALP 2006)*. Part II. Berlin: Springer, pp. 1–12.

[24] Chaum, David; Damgård, Ivan B. & van de Graaf, Jeroen (1988), Multiparty Computations Ensuring Privacy of Each Party's Input and Correctness of the Result. In: Pomerance, C. et al. (eds.), *Advances in Cryptology — CRYPTO '87*. Berlin: Springer, pp. 87–119.

[25] Bonawitz, Keith et al. (2017), Practical Secure Aggregation for Privacy-Preserving Machine Learning. In: Thuraisingham, B. et al. (eds.), In: *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS '17)*. New York: ACM, pp. 1175–1191.

[26] For an early critique on this self-limitation see Brinckmann, Hans (1982), Vom Datenschutzrecht zum Recht des Verbraucher-, Arbeits- und Umweltschutzes. In: *Datenschutz und Datensicherung* 6(3), pp. 157–164, 158. See also the contribution of Julian Hölzel in this volume.

[27] For an exhaustive overview see Wagner, Isabel & Eckhoff, David (2018), Technical Privacy Metrics: A Systematic Survey. In: *ACM Computing Surveys (CSUR)* 51(3), article 57.

[28] It has been long established that all sensitivity classification is arbitrary, especially in the field of law, see Simitis, Spiros (1990), „Sensitive Daten" – Zur Geschichte und Wirkung einer Fiktion. In: Brem, E. et al. (eds.), *Festschrift zum 65. Geburtstag von Mario M. Pedrazzini*. Berne: Stämpfli & Cie, pp. 469–493. It has also been shown early in the debate that sensitivity is not a property of information, see Steinmüller, Wilhelm et al. (1971), *Grundfragen des Datenschutzes*. Expertise on behalf of the German Ministry of the Interior, German Bundestag Record No. VI/3826, Appendix 1, p. 73.

constructed, i.e. as computable representations of the world, both drives and is driven by the apparent straightforwardness of these metrics and the illusive ease of their application.

ON (NOT) MEASURING DATA PROTECTION

The data protection debate always had a focus on anonymity as strong as the privacy debate[29], but much less so on secrecy or confidentiality. It has, however, also looked beyond anonymity, secrecy and confidentiality in its search for formalization and measurability of fundamental rights protection – though with mixed results.

Against the backdrop of extensive research in the field of legal informatics, which had a particular focus on how to formulate legal provisions in order to ensure their suitability for automation,[30] for some time the debate strongly engaged with the formalization of legal requirements for fundamental rights protection, including the "descriptiveness of the necessity relation", "model adequacy", or "sufficient validity".[31] Within this research field, particular attention has been paid to the formalization of purpose(s), the relations between purposes as well as purposes and sub-purposes, and purpose-binding[32] – though without any long-term effects on the broader data protection research or practice.

Explicit attempts to employ quantifiable indicators for both risks to and protection of fundamental rights have long been limited to references to the quantity of data about individuals to be processed.[33] The very construction of this indicator is based on the assumption that the less personal data about an individual is collected, stored and processed, the smaller the risks are for the individual's fundamental rights.[34]

The main strand of the debate has instead focused on procedural measures, such as codes of conduct, data protection authorities' decisions or sanctions imposed on non-compliant data controllers.[35] A key argument was that attempting to establish per-

[29] Starting as early as 1970, cf. Steinmüller, Wilhelm (1970), *EDV und Recht – Einführung in die Rechtsinformatik*. Berlin: J. Schweitzer Verlag, p. 88.

[30] Cf. von Berg, Malte (1968), *Automationsgerechte Rechts- und Verwaltungsvorschriften*. Cologne: G. Grote'sche Verlagsbuchhandlung.

[31] Podlech, Adalbert (1982), Individualdatenschutz – Systemdatenschutz. Brückner, K. & Dalichau, G. (eds.), *Beiträge zum Sozialrecht – Festgabe für Grüner.* Percha: Verlag R. S. Schulz, pp. 451–462.

[32] Hoffmann, Bernhard (1991), *Zweckbindung als Kernpunkt eines prozeduralen Datenschutzansatzes.* Baden-Baden: Nomos Verlagsgesellschaft.

[33] Starting as early as 40 years ago, e.g. Burkert, Herbert (1985), *Datenschutz und Informations- und Kommunikationstechnik. Eine Problemskizze.* Workshop report no. 6. Ministry for Labour, Health and Welfare North Rhine-Westphalia, pp. 14ff.

[34] Pohle, Jörg (2014) Kausalitäten, Korrelationen und Datenschutzrecht. In: Pohle, J.; Knaut, A. (eds.), *Fundationes I: Geschichte und Theorie des Datenschutzes.* Münster: Monsenstein und Vannerdat, pp. 85–105 (paragraph 28).

[35] This has been quite harshly criticised by many scholars, cf. e.g. De Hert, Paul & Gutwirth, Serge (2006), Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power. In: Claes, E.; Duff, A. & Gutwirth, S. (eds.), *Privacy and the Criminal Law.* Antwerpen: Intersentia, pp. 61–104 (71, 77f., 87ff.).

formance indicators is fraught with the central difficulty of data protection law's goals being vague and contested.[36] While this argument is based on an understanding of data protection laws' goal being the protection of privacy, with privacy itself being essentially contested,[37] it hasn't yet been re-evaluated against the backdrop of the EU General Data Protection Regulation's clear and unambiguous formulation of the law's goal in Article 1(2), i.e. to protect "fundamental rights and freedoms of natural persons".

Where the General Data Protection Regulation refers to measurable indicators, most of them are constructed from the perspective of the controller and the controller's information processing, not from the perspective of the data subject. For example, Articles 24, 25 and 32 GDPR refer to the scope of the processing, while Recitals 62, 75 and 91 refer to the number of data subjects. Thus, in essence these indicators don't indicate risks to fundamental rights. Instead, they seem to be used for the simple reason that they are measurable.[38] The only exception is the Regulation's reference to the likelihood and severity of risks for fundamental rights and freedoms in Articles 24, 25 and 32, though both the scholarly literature and the commentaries then fail to operationalise fundamental rights and freedoms. They all simply refer to the list in Recital 75, which includes references to the amount and other properties of the personal data, the number of data subjects affected, but also the unauthorised reversal of pseudonymisation. Explicit references to fundamental rights and freedoms are both scarce and superficial: "discrimination" and "where data subjects might be deprived of their rights and freedoms". A similar superficiality can be observed in the scholarly literature, which conflicts with the extensive coverage of other harms, such as distress, anxiety or to the individual's reputation.[39]

Last but not least, there is a small strand of research that focuses on using formal models to translate data protection requirements into technical requirements which are then to be implemented into ICT systems.[40]

[36] Raab, Charles D. & Bennett, Colin J. (1996), Taking the measure of privacy: can data protection be evaluated? In: *International Review of Administrative Sciences* 62, pp. 535–556.

[37] Mulligan, Deirdre K.; Koopman, Colin & Doty, Nick (2016), Privacy is an essentially contested concept: a multi-dimensional analytic for mapping privacy. In: *Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences* 374(2083), p. 20160118.

[38] Such shift has long been observed in organisational studies, see Kling, Rob (1980), Social analyses of computing: Theoretical perspectives in recent empirical research. In: *ACM Computing Surveys (CSUR)* 12(1), pp. 61–110 (81–83).

[39] Cf. e.g. Wagner, Isabel & Boiten, Eerke (2018), Privacy Risk Assessment: From Art to Science, by Metrics. In: Garcia-Alfaro, J. et al. (eds.), *Data Privacy Management, Cryptocurrencies and Blockchain Technology. ESORICS 2018 International Workshops, DPM 2018 and CBT 2018, Proceedings*. Cham : Springer, pp. 225–241.

[40] See e.g. Bräutigam, Lothar; Höller, Heinzpeter & Scholz, Renate (1990), *Datenschutz als Anforderung an die Systemgestaltung*. Opladen: Westdeutscher Verlag; or Fischer-Hübner, Simone (1994), Ein formales Datenschutz-Modell. In: Bauknecht, K. & Teufel, S. (eds.), *Sicherheit in Informationssystemen*. Zurich: vdf Hochschulverlag AG, pp. 107–119.

TOWARDS MEASURABLE INDICATORS FOR FUNDAMENTAL RIGHTS PROTECTION

The debate has yet to produce meaningful indicators for both risks to and protection of fundamental rights and freedoms, let alone measurable indicators, that takes into account what these rights and freedoms actually guarantee.[41]

The simplest approach would be to count the number of rights and freedoms affected, whether because there is data collected on the exercise of these rights and freedoms, the processing or use of data impinges on their exercise, or their exercise is affected, e.g. inhibited, restricted or controlled, by the information and communication technology imposed upon or used by the fundamental rights' holder. The impact on fundamental rights could either be direct or indirect, e.g. by chilling effects[42], with the latter being much harder to assess than the former.[43] A sociological equivalent to the fundamental rights coverage might be the number of societal subsystems (Talcott Parsons, Niklas Luhmann), subfields (Pierre Bourdieu) or spheres of life (Ferdinand Schoeman) covered or affected by the data, the data processing and use, or the technology.[44] Another alternative indicator might be the number of covered or affected social roles, i.e. sets of rights, duties, expectations, norms and behaviors that an individual has to face and fulfill.[45] The most well-known societal roles include citizens, family members, employees, customers, or patients, with data protection then understood as protecting the functional differentiation of these social roles with their associated promises of freedom vis-à-vis powerful organisations.[46]

This reference to powerful organisations might lead to a second indicator that could be made quantifiable: the power imbalance between such organisations and those that depend on them, e.g. their audiences, or are affected by their informational activities or the technology they design, develop and operate. This approach would tap into the long history of understanding data protection as a means for condition-

[41] On this understanding of fundamental rights and freedoms see Rusteberg, Benjamin (2009), *Der grundrechtliche Gewährleistungsgehalt : Eine veränderte Perspektive auf die Grundrechtsdogmatik durch eine präzise Schutzbereichsbestimmung*. Tübingen: Mohr Siebeck.

[42] White, Gregory L. & Zimbardo, Philip G. (1975), *The Chilling Effects of Surveillance: Deindividuation and Reactance*. ONR Technical Report Z-15, Los Angeles: Office of Naval Research.

[43] Cf. Staben, Julian (2016), *Der Abschreckungseffekt auf die Grundrechtsausübung – Strukturen eines verfassungsrechtlichen Arguments*. Tübingen: Mohr Siebeck.

[44] Cf. Pohle, Jörg (2012), Social Networks, Functional Differentiation of Society, and Data Protection. *arXiv:1206.3027* [cs.CY]. Retrieved from https://arxiv.org/abs/1206.3027.

[45] The concept of (social) role was originally introduced by Linton, Ralph (1936), *The Study of Man : An Introduction*. New York: Appleton-Century-Crofts, pp. 113–131; and strongly shaped by Parsons, Talcott (1951), *The Social System*. Glencoe: Free Press.

[46] Müller, Paul J. (1975), Funktionen des Datenschutzes aus soziologischer Sicht. In: *Datenverarbeitung im Recht* 4, pp. 107–118.

ing of power asymmetries.[47] One the one hand, this indicator would be somewhat related to the size of a data controller, which is used in Section 38(1) German Federal Data Protection Act to define whether a data protection officer must be appointed. On the other hand, the size of a data controller itself has been shown to be a bad indicator for the risks posed by an organisation in the digital era.[48]

Regarding the individual rights and freedoms, societal subsystems or social roles, a sensitive indicator could be how extensive is the coverage or how much meaningful freedom is left unsurveilled, unrecorded or uncontrolled.[49] Unfortunately, this indicator does not seem to allow for easy quantification, though it is already used indirectly to assess the "additive encroachment on fundamental rights".[50]

Thus, the situation seems quite daunting: most attempts to quantification and measurement in the privacy and data protection field have ended up in a blind alley, either by producing indicators that do not indicate risks to or protection of fundamental rights and freedoms, or by getting forgotten in the meandering discourse of the past fifty years in this field. It is time to go beyond the oversimplified quantifications that characterise today's debate, the almost sole focus on the data subjects' identifiability or the number of affected people. It is time to restart the quest for suitable measurable indicators that directly address the fundamental rights and freedoms at stake, with the promises they entail and the spheres of freedom they create.

[47] Cf. Scheuch, Erwin K. (1974), Datenschutz als Machtkontrolle. In: Dammann, U. et al. (eds.), *Datenbanken und Datenschutz*. Frankfurt am Main: Herder & Herder, pp. 171–176; Rost, Martin (2014), Neun Thesen zum Datenschutz. In: Pohle, J. & Knaut, A. (eds.), *Fundationes I: Geschichte und Theorie des Datenschutzes*. Münster: Monsenstein und Vannerdat, pp. 37–44.

[48] Pohle, Jörg (2018), *Datenschutz und Technikgestaltung: Geschichte und Theorie des Datenschutzes aus informatischer Sicht und Folgerungen für die Technikgestaltung*. Doctoral dissertation, Humboldt-Universität zu Berlin, Germany, p. 241. Retrieved from https://edoc.hu-berlin.de/handle/18452/19886.

[49] See for an approach to construct an analysis of the remaining freedoms Pohle, Jörg (2019), Freiheitsbestandsanalyse statt Überwachungs-Gesamtrechnung – Ein Alternativvorschlag. In: *FIfF-Kommunikation* 36(4), pp. 37–42.

[50] Starnecker, Tobias (2017), *Videoüberwachung zur Risikovorsorge. Body-Cam zur Eigensicherung und Dashcam zur Beweissicherung – Eine verfassungs- und datenschutzrechtliche Analyse*. Berlin: Duncker & Humblot, pp. 365–366.