bidt Bavarian Research Institute for Digital Transformation
AN INSTITUTE OF THE BAVARIAN ACADEMY OF SCIENCES AND HUMANITIES

WORKING PAPER

Regulatory Clustering of Privacy Laws

An approach to quantifying (comparative) law as an instrument for interdisciplinary research

Author:

Peer Sonnenberg

Publisher: bidt – Bayerisches Forschungsinstitut für Digitale Transformation (Bavarian Research Institute for Digital Transformation)
www.bidt.digital

Imprint

Working Paper Nr. 7

The working papers published by the
bidt represent the authors' views;
they do not represent the views of the
institute as a whole.

bidt – Bayerisches Forschungsinstitut
für Digitale Transformation
Gabelsbergerstrasse 4
80333 München
www.bidt.digital/en

Coordination
Dr Margret Hornsteiner, Leonie Liebich
Dialog bidt
dialog@bidt.digital

Design
made in – Design und Strategieberatung
www.madein.io

Release
May 2024
ISSN: 2701-2409
DOI: 10.35067/bv16-2z33

Data has become a fundamental resource in the digital economy, serving as the foundation for a variety of business models and driving innovation. Personal data, in particular, plays a crucial role in this context. However, individuals must make a conscious decision to disclose such data, which raises questions about the factors influencing their willingness to do so.

The research project "Vectors of Data Disclosure" aims to address this question by integrating perspectives from cultural studies, business informatics, and law. The project seeks to identify the cultural and regulatory factors that influence whether and how individuals disclose personal data, to investigate the decision-making process using behavioral economics, and to model the influences and interactions based on these findings.

The project team places particular emphasis on data disclosure in an international context, focusing on the cross-border nature of data disclosure between different legal and cultural spheres. The goal is to gain comparative insights into the underlying principles of data disclosure.

The project is promoted by the Bavarian Research Institute for Digital Transformation (bidt). As an institute of the Bavarian Academy of Sciences and Humanities, the Bavarian Research Institute for Digital Transformation contributes to a better understanding of the developments and challenges of the digital transformation. In doing so, it provides the foundations to shape the digital future responsibly and oriented towards the common good in dialogue with society.

The author
Peer Sonnenberg is a research assistant at the Chair of Public Law, Media and Information Law, University of Passau.
peer.sonnenberg@uni-passau.de

Abstract

English:

The issue of which regulatory concept is the best or most suitable for protecting privacy has triggered competition between more or less comparable privacy legislation. This has led to a fragmented regulatory landscape in the area of data protection and privacy. At the same time, the competition between legal systems precedes the question of how data protection law actually works in practice and how it affects the addressee of the regulation in different settings, which has not yet been conclusively clarified scientifically. Nevertheless, a comprehensive variety of legal provisions has been created, which can be subjected to closer scrutiny. However, before the different effects of various regulations can be compared, the existing legal systems and their peculiarities must first be measured in order to form the basis for an interdisciplinary consolidation. This is the most important (and perhaps the only) contribution that a legal scholar can make in this interdisciplinary field of research. However, since the legal sciences and comparative law are rather unfamiliar with interdisciplinary and empirical research, such a contribution requires a methodological starting point that simultaneously provides legally relevant findings and interoperability with the empirical research of other disciplines. In order to offer such a methodological starting point, this article proposes the concept of 'regulatory clustering' as a compromise between comparative law and interdisciplinary research. Through the comparative analysis of legal systems of very different countries and the use of a method to quantify the law, this 'regulatory clustering' attempts to offer the definition of an input variable that could also be used in the context of a research model of another discipline. It is conducted against the practical background of an interdisciplinary research project of legal studies, business informatics and cultural studies on the factors that influence individuals' decisions to disclose their personal information.

German:

Die Frage, welches Regelungskonzept das beste oder geeignetste zum Schutz von Privatsphäre ist, hat einen Wettbewerb zwischen mehr oder weniger vergleichbaren Datenschutzgesetzen ausgelöst. Dieser hat zu einer zerklüfteten Regelungslandschaft im Bereich des Datenschutzes und der Privatsphäre geführt. Gleichzeitig geht der Wettbewerb der Rechtsordnungen der wissenschaftlich noch nicht abschließend geklärten Frage voraus, wie das Datenschutzrecht in der Praxis tatsächlich funktioniert und wie es in unterschiedlichen Settings auf den Regelungsadressaten wirkt. Es wurde aber dennoch eine umfassende Vielfalt an Rechtsvorschriften geschaffen, welche einer genaueren Untersuchung unterworfen werden können. Doch bevor man die unterschiedlichen Auswirkungen verschiedener Regelungen vergleichen kann, muss man zunächst die bestehenden Rechtsordnungen und ihre Eigenheiten erfassen, um damit die Grundlage einer interdisziplinären Zusammenführung zu bilden. Dies ist der wichtigste (und vielleicht auch einzige) Beitrag, den ein Rechtswissenschaftler in diesem Forschungsfeld leisten kann. Da aber die Rechtswissenschaften und die Rechtsvergleichung mit interdisziplinärer und empirischer Forschung eher wenig vertraut sind, bedarf ein solcher Beitrag eines methodischen Ansatzpunktes, der gleichzeitig rechtlich relevante Erkenntnisse und Interoperabilität mit der empirischen Forschung anderer Disziplinen bereitstellt. Um einen solchen methodischen Ansatzpunkt zu bieten, schlägt dieser Beitrag das

Konzept eines ‘Regulatory Clusterings’ als Kompromiss zwischen Rechtsvergleichung und interdisziplinärer Forschung vor. Durch die vergleichende Analyse von Rechtsordnungen sehr unterschiedlicher Länder und die Verwendung einer Methode zur Quantifizierung des Rechts versucht dieses ‘Regulatory Clustering’ die Definition einer Input-Variablen anzubieten, die auch im Rahmen eines Forschungsmodells einer anderen Disziplin verwendet werden könnte. Es wird vor dem praktischen Hintergrund eines interdisziplinären Forschungsprojekts der Rechtswissenschaften, der Wirtschaftsinformatik und der Kulturwissenschaften zu den Faktoren durchgeführt, die die Entscheidung des Einzelnen beeinflussen, die eigenen persönlichen Informationen preiszugeben.

Content

1 Regulatory Competition and Regulatory Clustering[1]

In recent times, a hard-fought regulatory competition on data regulation has ensued throughout the world.[2] It encompasses all fields emerging from global digitalisation and datafication and, consequently, one of its main battlefields is the question of adequate privacy regulation. As a result, 143 countries have some sort of privacy legislation in place and further 18 are considering draft legislations.[3] Thus, the regulatory competition has produced quite a wide array of regulatory outcome. But how does this outcome look like and how can it be depicted? Has global regulatory competition reached international consensus on how the matter of privacy should be treated by 'regulation'[4]? Or is the result a standstill that *de lege lata* cannot be surpassed without international conflict? The endeavoring but not rarely unsuccessful search for an adequate level of protection[5] by the European Union may indicate a rather negative picture.

When conducting research on the 'right', 'adequate' or 'fitting' regulation on privacy, legal studies must, shall, and can not provide answers on its own. Whether a privacy legislation is desired and functional within one country as well as in interplay with other countries' legislations is also a question of *inter alia* cultural studies, ethics, economics, computer science, sociology, or psychology. In other words: Research on the regulatory competition of privacy laws can only be sufficiently addressed by interdisciplinary means.

The legal contribution to such question is comparative law. Comparative law can provide for a legal (normative) analysis of the existing and upcoming regulatory landscape. It can also provide for a starting point for researchers of other disciplines to dig into the actual effects this regulatory landscape imposes on individuals, societies, or global interdependencies. Therefore, this paper is going to address the fundaments of future interdisciplinary research by providing for a 'Regulatory Clustering', which depicts selected privacy jurisdictions in relation to each other in form of parameters that could supply another disciplines' research model.

---

1 This Working Paper is a shortened version of the full methodology that served as basis for further research within the underlying bidt research project 'Vectors of Data Disclosure'. The extended version of this Regulatory Clustering is accessible under Sonnenberg, 'A Regulatory Clustering of Privacy Laws – Extended Version' (2024) IRDG Research Paper Series, No. 24-01.

2 Panchenko/Reznikova/Bulatova, 'Regulatory Competition in the Digital Economy: New Forms of Protectionism' (2020) International Economic Policy 50; Hennemann, 'Wettbewerb der Datenschutzrechtsordnungen' (2020) RabelsZ 864.

3 Universität Passau, 'Global Data Law', accessible under https://datalaw.uni-passau.de/ (last accessed 11.03.2024).

4 At this point, one should note that there are different understandings of the term 'regulation'. Correctly, in this context 'regulation' must mean all circumstances and techniques, the state utilizes to affect human behavior, which is not limited to legislative law-making. In adopting this economic definition, the comparative lawyer can better grasp the concept of legal pluralism and consider extra-judicial factors. However, this Regulatory Clustering will only use the term of regulation in a narrow sense, meaning all legal norms that are generally binding and can be enforced by the state through courts. This is due to the nature and purpose of the Regulatory Clustering to depict an initial parameter of sovereign rulemaking, which inherently cannot depict extra-judicial factors. See on the different meanings of 'regulation' Dotan, 'The Common Real-Life Reference Point Methodology – or 'the Mcdonalds's Index' for Comparative Administrative Law and Regulation' in: Cane et al. (eds.), *The Oxford Handbook of Comparative Law* (2021), pp. 991, 998 et seq.

5 Art. 45 I GDPR.

2 Interdisciplinary Research and Comparative Law

The Regulatory Clustering does not constitute a method of (traditional) comparative law. It is rather a simplified method to enable interdisciplinary research on the behavioral economics perspective of data disclosure processes in conjunction with influences of cultural parameters.[6] In order to understand the underlying methodology of the Regulatory Clustering, it is necessary to understand the context of it in an interdisciplinary research project and, subsequently, the objective behind such Regulatory Clusters. The underlying project aims to identify factors at the meso level that may influence the individual decision-making process behind disclosing one's personal information. To this end, a 'Law – Behavior Gap Model'[7] has been created to investigate varying perceptions of regulation and its influences on privacy concerns, psychological comfort, or self-protective behavior – thus, ultimately, the influences on a decision-making process itself. The results should address a 'perception gap' that occurs somewhere in the transition between regulation on a macro level and the disclosure decision on a micro level.

In order to map such a 'perception gap', the regulation to be perceived needs to be defined as an input variable. Measured differences in such input variable may than be compared to the individual regulatory perception to identify co-dependencies between regulation, regulatory perception and, ultimately, the individual decision-making. To create a significant spread throughout different data sets, the model takes data of eight different jurisdictions into account, which requires eight different categories as objects of comparison. In other words, eight different jurisdictions are described and ranked (only) in relation to each other. The research objective thus moves away from classical findings of comparative law – namely the advancement and understanding of own and foreign law as well as a critical perception of legal principles and a standardization of law where possible[8] – and moves more in a rather untechnical direction of a 'quantification of law'. This is untechnical to the end, that it contradicts the fundamental assumption of comparative law, that regulation does not exist on a metrical scale and can thusly not be measured, given a certain value to, or even be deemed as 'better' or 'worse' than other legal orders on the basis of written regulation alone.[9] Rather, comparing law does not mean to place jurisdictions in competition to each other, but to see it as a pluralistic puzzle piece to fit into (possibly) competing political views, societal norms and cultural settings of the

---

6 See on the underlying interdisciplinary research project Hennemann, von Lewinski, Wawra, Widjaja (eds.), *Data Disclosure – Global Developments and Perspectives* (2023).

7 This model was already presented at the DatenTag in Berlin, cf. Stiftung Datenschutz, 'Ergebnisse des Projekts "Vektoren der Datenpreisgabe"' (19.01.2024), at 47:58, accessible under https://stiftungdatenschutz.org/veranstaltungen/unsere-veranstaltungen-detailansicht/datentag-preisgabe-von-daten-440#lg=1&slide=1 (last accessed 11.03.2024). See on the basics of the underlying research on regulatory perception Richthammer/Widjaja, 'The Effect of Regulatory Measures on Individual Data Disclosure: A Country Comparison' (2023) ECIS Research-in-Progress Papers 83.

8 Kischel, *Comparative Law* (2019), pp. 45 et seqq.; Schwartze, 'Die Rechtsvergleichung' in: Riesenhuber (ed.), *Europäische Methodenlehre* (2021), pp. 5 – 23; Sacco/Rossi, *Einführung in die Rechtsvergleichung* (third edition 2017), Erstes Kapitel, § 1, N 59, 84 et seqq.

9 Kischel, *Comparative Law* (2019), pp. 48 et seqq.; Salaymeh/Michaels, 'Decolonial Comparative Law: A Conceptual Beginning' (2022) RabelsZ 166, 172; Bennett/Raab, *The Governance of Privacy – Policy Instruments in Global Perspective* (2006), p. 24.

respective country.[10] When dealing with foreign law in relation to one's own or other foreign law, the research should be conducted without bias and should not reflect personal values of the researcher into foreign jurisdictions. The Regulatory Clustering, however, does exactly this: it ultimately places different jurisdictions in an ordinal ranking to each other, defining one as 'higher' as the other.

This Regulatory Clustering is not without precedent in theory and practice: it draws inspiration from, for example, the 'Doing Business Reports' of the world bank,[11] which were subject to comprehensive criticism from their conceptual beginning in 2004[12] to their discontinuation due to data irregularities and methodological flaws in 2021.[13] The 'Doing Business Reports', therefore, seem to be no promising source of inspiration. However, a consideration for the methodology of the Regulatory Clustering – or any other instrument for quantification of law – could be worthwhile because the 'Doing Business Reports', similar to the goal of a Regulatory Clustering, created an ordinal ranking of countries based on especially law and regulation.[14] The resulting ranking is intended to provide information on an economic variable such as the ease of starting a business, getting electricity, paying taxes, or trading across borders in a specific jurisdiction. In summary, the main criticism that lead to its discontinuation were insufficient understanding of law[15], disregard of factual circumstances and context, generalizations, manipulation of data, and the assumed premise, that a higher ranking (or the proposed reforms to achieve it) would lead to better development outcomes.[16] Against this background of criticism, the Regulatory Clustering could flourish: The variables it finds are not intended to give rise to stakeholder recommendations or to make economic statements; rather, it makes an offer – aware of its conceptual weaknesses – to provide insights for further interdisciplinary research. Such further empirical research may then address factual circumstances. The Regulatory Clustering itself does not claim to reflect legal realities. Nevertheless, legal concerns remain (and must be kept in mind) with regard to objectivity, quantification without unverifiable value

---

10 Sacco/Rossi, *Einführung in die Rechtsvergleichung* (third edition 2017) Erstes Kapitel, § 1, N 12 et seqq.

11 The World Bank, 'Doing Business Archive', accessible under https://archive.doingbusiness.org/en/doingbusiness, (last accessed 11.03.2024).

12 Salaymeh/Michaels, 'Decolonial Comparative Law: A Conceptual Beginning' (2022) RabelsZ 166, 172; Michaels, 'Comparative Law by Numbers? – Legal Origins Thesis, Doing Business Reports, and the Silence of Traditional Comparative Law' (2009) American Journal of Comparative Law 765.

13 The World Bank, 'World Bank Group to Discontinue Doing Business Report' Statement of 16 September 2021, accessible under https://www.worldbank.org/en/news/statement/2021/09/16/world-bank-group-to-discontinue-doing-business-report, (last accessed 11.03.2024).

14 See for an overview, The World Bank, 'Methodology', accessible under https://archive.doingbusiness.org/en/methodology (last accessed 11.03.2024). Note, that these reports included the wider definition of 'regulation' (note 4).

15 Michaels, 'Comparative Law by Numbers? – Legal Origins Thesis, Doing Business Reports, and the Silence of Traditional Comparative Law' (2009) American Journal of Comparative Law 765, 773.

16 Alfaro et al., 'Doing Business: External Panel Review. Final Report' (2021), accessible under https://www.worldbank.org/content/dam/doingBusiness/pdf/db-2021/Final-Report-EPR-Doing-Business.pdf (last accessed 11.03.2024).

judgement, delimitation of *de jure* and *de facto* regulation, contextualization of written law, or biases.[17]

2.1. Finding the link between comparative law and empiricism

Having outlined the shortcomings of this methodology against the background of traditional comparative law, such shortcomings can be addressed, relativized, or even justified. First of all, it should be borne in mind, that the main objective is not to compare jurisdictions in a normative sense, which would allow a deeper understanding of similar and divergent legal principles, but rather in an empirical sense, which would allow quantification and exploration of correlations with cultural variables or factors of behavioral economics. To achieve this in the most objective way possible, the variables to be studied must be precisely defined and the examined regulatory instruments must provide a comprehensive picture of the object of research. The latter leads to yet another clash with typical comparative law methodology: Comparative law research is conducted doctrinal, functional and contextual.[18] In terms of the Regulatory Clustering, this means that the comparison of legal orders should not only examine similar rules, but also address problems that could be solved by different instruments as functional equivalents, and (perhaps even more importantly) contextualize the compared instruments into context with especially societal and cultural circumstances of the regulated matter. This contextuality is in direct contrast to the aim of deriving quantifiable variables from different jurisdictions: Functional and contextual comparison would mean designing an overly complex system of legal and non-legal features and circumstances which are in constant interaction with each other. This would (a) result in a tangle of variables that would miss the point of making legal occurrences comparable with factors of other disciplines and (b) be circular, since the Regulatory Clustering aims to make legal realities tangible for cultural studies and behavioral economics, so that these disciplines can find the very (extra-judicial) co-dependencies that contextual comparative law presupposes.

The first challenge for the Regulatory Clustering is to select the right regulatory instruments to be studied in the different jurisdictions as objects of comparison. On the one hand, the factors must be narrow and precise enough to provide for comparable and significant variables for useful quantitative research from other disciplines' perspectives. On the other hand, the choice of instruments examined must reflect the diversity and uniqueness of the respective legal system and not impose a biased view on foreign regulation, which may be closer to the basic legal understanding of the conducting researcher. As the overall research topic in this scenario is the influence of regulation on the decision to disclose personal data, the main regulatory instruments will be found in data protection and data privacy legislation. Such legislation will be the main source for the Regulatory Clustering. If one would instruct solemnly legal scholars with this choice, it is likely that the choice falls on a rather broad mixture of instruments, which is understandable given the aforementioned background that contextual comparative law should be conducted in a holistic manner, taking into account as many

---

[17] For an overview of legal criticism, see Kern, *Justice between Simplification and Formalism* (2007); less critical Siems, 'Numerical Comparative Law: Do We Need Statistical Evidence in Law in Order to Reduce Complexity' (2005) Cardonzo Journal of International and Comparative Law 521.

[18] Salaymeh/Michaels, 'Decolonial Comparative Law: A Conceptual Beginning' (2022) RabelsZ 166, 170; Kischel, *Rechtsvergleichung* (2015), pp 164 et seqq.

contextually relevant legislations as possible. This, in turn, would undermine the utility of the Regulatory Clustering as a tool for interdisciplinary research on law as a quantifiable factor.

The basis for the selection of the regulatory instruments to be studied is therefore a taxonomy for categorizing data protection legislation, which was developed for this sole purpose in collaboration with legal scholars and behavioral economists.[19] This taxonomy is based on the assumption that regulatory perception can be modelled by mainly[20] two categories of (data protection and privacy) law: The first category is the set of regulations that promise an objective standard of protection to which all entities must adhere to. The mere existence of such regulation may assure the individual that their personal information is already sufficiently protected *de jure*. They do not need to get involved in adjusting the level of protection of their personal information. This category is called 'assured level of privacy'.[21] The other category includes such regulation that allow individuals to adjust and co-determine the level of protection of their personal information. This category is called 'self-determined level of privacy'.[22] The distinguishing criterion between the two is, whether the regulation requires user-involvement. This categorization allows for a comprehensive choice of instruments of data protection and privacy regulation, which nonetheless also fits into an interdisciplinary research model. The resulting clusters consist of a group of sixteen[23] instruments, that ensure privacy without user involvement and a group of eight[24] instruments that involve the individual's choice of the level of privacy granted. One regulatory instrument is defined throughout all examined jurisdiction by the problems it addresses and the objectives it seeks to achieve, thus implementing a functional approach.

However, such definition poses major epistemological difficulties. It may depend – inadvertently – on the origin and affiliation of the conducting researcher. Already prior to epistemology, there is an undeniable informational gap in any field of comparative law[25]: Naturally, technical burdens such as language, including the correct translation of legal terms, and the accessibility of legal sources and

---

[19] See on the underlying categorization of law Richthammer/Widjaja, 'Vectors of Data Disclosure – The Information Systems Perspective' in: Hennemann, von Lewinski, Wawra, Widjaja (eds.), *Data Disclosure – Global Developments and Perspectives* (2023) 37, 45 et seq., and *Richthammer/Widjaja,* 'The Effect of Regulatory Measures on Individual Data Disclosure: A Country Comparison' (2023) ECIS Research-in-Progress Papers 83. Note that in these early texts, the delimiting terminology had been 'measures demanding user action' and 'measures that assure privacy' or with/without user action.

[20] The taxonomy further subdivides legal measures according to the time at which they take effect and the nature of such effect. However, such delimitation is not relevant for the proposed regulatory perception model and thusly not relevant for the goal of the Regulatory Clustering of quantifying relevant legal variables. It can be relevant, however, in the context of other clustering purposes, see chapter 6.

[21] Richthammer/Widjaja, 'Vectors of Data Disclosure – The Information Systems Perspective' in: Hennemann, von Lewinski, Wawra, Widjaja (eds.), *Data Disclosure – Global Developments and Perspectives* (2023) 37.

[22] Ibid.

[23] The instruments concerning assured level of privacy are: prerequisites of information handling, sensitive information, purpose limitation, subsequent information handling, domestic transmission to third parties, transmission to third parties abroad, data minimization, deletion obligations, data quality, data security, internal documentation, registries, internal responsibility management, certification and self-regulation, regulation on public information, and cyber surveillance authority.

[24] The instruments concerning a self-determined level of privacy are: consent, right to object / opt-out, right to deletion, right to rectification, right to access, right to data portability, information obligations, and data breach notification.

[25] Dotan, 'The Common Real-Life Reference Point Methodology – or 'the Mcdonalds's Index' for Comparative Administrative Law and Regulation' in: Cane et al. (eds.), *The Oxford Handbook of Comparative Law* (2021) 991, 994.

secondary literature, as well as factual burdens, such as a deep understanding of the functioning of foreign law or contexts of regulatory choices, automatically affect any comparative research. And in terms of epistemology itself, the assessment of critical factors and objectives of research will be determined by the researcher's decision. They and their research may therefore be particularly vulnerable to cognitive distortions.[26] Most dangerously, the categorization under the umbrella terms 'assured level of privacy' and 'self-determined level of privacy' may be distorted by a confirmation bias of the author: As the author has been trained and has conducted research in European data protection law, the categorization may follow the unjustified assumption that the structure and main elements of data privacy legislation around the world are roughly similar to the GDPR. Nevertheless, to anticipate the result, research on this Regulatory Clustering has confirmed the existence of a *de jure* Brussels Effect[27] at least in the sense that fundamental concepts are often similar – it does not address nor answer the question whether such similarities were in fact influenced by EU legislation. However, the combination of aforementioned informational gap and the risk of confirmation bias may negatively influence the interpretation of different regulation, concepts, and functions in favor of a GDPR-bias. Therefore, a further optimization of the methodology could include the consultation of legally competent locals.

2.2. Definition of researched variables

Once the regulatory instruments to be compared by the Regulatory Clustering have been identified, the next step is to define the target variable by which the instruments will be compared and to create a scale for the resulting ranking. This question poses three fundamental dogmatic problems: (a) it is virtually impossible to quantify law and measure it as an absolute value that can then be compared with other law; (b) even if a ranking can be found within a variable, the question remains of how to scale the ranking so that differences between legal orders can be classified; and (c) how to ensure an objective assessment, given that different legal approaches may be based on different concepts, values and policy objectives.

All three problems stem from the fundamental recognition that law is a value-based concept and that such concepts can only be described and depicted to a very limited extent by empirical data and figures.[28] There are many possible variables and even more definitions for them. The impossibility of quantification of law can only be adequately addressed if the methodology of the Regulatory Clustering is consistent in itself. The Regulatory Clustering can therefore only serve its purpose if a precise definition is provided, and its internal logic are strictly adhered to.

---

[26] The most prominent confirmation bias refers to the phenomenon that when confronted with a foreign belief or concept that diverges from the own, one tends to deviate from it and apply more familiar rules, cf. Linarelli, ´Behavioural Comparative Law: Its Relevance to Global Commercial Law-Making' in: Akseli/Linarelli (eds.), *The Future of Commercial Law: Ways Forward for Change and Reform* (2019) 69, 102 et seqq.

[27] Bradford, The Brussels Effect (2020).

[28] Von Aswege, *Quantifizierung von Verfassungsrecht* (2016), p. 475. See on such methodological shortcoming of the discipline of legal studies itself Dotan, 'The Common Real-Life Reference Point Methodology – or 'the Mcdonalds's Index' for Comparative Administrative Law and Regulation' in: Cane et al. (eds.), *The Oxford Handbook of Comparative Law* (2021) 991, 997.

Having in mind the interdisciplinary research question the Regulatory Clustering is embedded in,[29] the variables have to take into account that the existence and the design of the respective regulatory instrument may have influence on their perception and thus their behavior, because they (perceive that they) can rely on either assured or self-determined privacy regulation. Accordingly, the question is to what extent the regulatory instruments examined promise an efficient protection of individual privacy. The term 'efficiency' is loaded with value judgements about what constitutes 'efficient protection of privacy'. While some may argue that efficiency is associated with the restriction of processing methods, others may argue that efficient privacy protection regulation means balancing individual privacy interests with the economic and societal utility of personal information.[30] Also, it would presuppose a definition of a universal standard of privacy. But privacy is a good that cannot be the same for every individual; different social actors in different scenarios may be in need of different 'levels' or 'means' of protection.[31] Thus, 'efficiency' allows for too much subjectivity and cannot precisely define a coherent variable. It would be more objective – without siding with one or the other approach – to assess a 'standard' of regulatory instruments (detached from the individual case) on an on the basis of how much it restricts processing activities: While this may yet again constitute a certain GDPR-bias (which follows precisely this approach)[32], it does and shall not pass judgement on whether it is the 'right' approach to privacy regulation. Given that the individual's privacy – regardless of other beneficial factors (for the self and for society) – is most dominantly protected when no handling of personal information is allowed at all,[33] it seems plausible to measure the level of privacy protection to be (potentially) perceived by the degree of restrictions imposed on the information handling entity[34]. This degree could be broadly defined as the scope of information handling activities that are legally possible after the application of the regulatory instrument. More precisely, this must also include those regulatory instruments that do not directly restrict the handling activity itself but require the controller to fulfil certain criteria in connection to the information handling. In these situations, the cost of compliance[35] can serve as a benchmark for the degree of restriction.

---

29 The Regulatory Clustering shall provide a variable for regulation that can fit into a regulatory perception model, see above.

30 Such opposed views of the goals and means of privacy protection can, for example, be found in the trans-atlantic discussion of the right to privacy as a fundamental right or a fundamental freedom, cf. Whitman, 'The Two Western Cultures of Privacy: Dignity versus Liberty' (2003) Yale Law Journal 1151.

31 Bennett/Raab, *The Governance of Privacy – Policy Instruments in Global Perspectives* (2006), pp. 31 et seqq.

32 Using the approach which the GDPR follows as benchmark, imposes a heavy risk for a stringent methodology. It may appear that the Regulatory Clustering – even without intending to do so – leans to the presumption of superiority of western (European) law before other legal concepts. Such presumptions are suitable to undermine an objective assessment of legal concepts that might follow completely different ideas and paradigms, cf. Salaymeh/Michaels, 'Decolonial Comparative Law: A Conceptual Beginning' (2022) RabelsZ 166, 172; Michaels, 'Comparative Law by Numbers? – Legal Origins Thesis, Doing Business Reports, and the Silence of Traditional Comparative Law' (2009) American Journal of Comparative Law 765. The Regulatory Clustering must bear this weakness in mind whenever possible and suitable.

33 However, this positivist assumption can only be true within the frame of this Regulatory Clustering: As it does not look normatively at the law in action, it disregards other potentially relevant factors of the degree of protection. The positive law alone remains. To this extent, notions of legal pluralism are not (yet) relevant in this context.

34 Such entity shall forthwith be named 'controller' or if they handle the information on behalf of another person and this differentiation becomes necessary 'processor'.

35 It is inherently difficult to pinpoint a certain 'cost of compliance', as many factors may influence the amount of money spent within one entity. A brief overview of what can be interpreted as 'cost of privacy compliance' can be found in Chander et al., 'Achieving Privacy: Costs of Compliance and Enforcement of Data Protection Regulation' (2021) Policy Research Working Paper 9594, pp. 9 et seqq.

Altogether, this would constitute the variable of 'regulatory intensity'. This variable will be the main connecting point for the Regulatory Clustering forthwith.

2.3. An ordinal ranking system

Whilst these definitions open up the possibility for a ranking on a micro level (by defining one regulatory instrument as more or less intensive than another comparable instrument from another jurisdiction), other problems remain unaddressed. This becomes particularly clear when attempting to construct an overall ranking by combining the various individual rankings. Comparing two jurisdictions as such must take into account all the factual and legal circumstances and subsequently provide a holistic view on the two jurisdictions being compared:[36] For example, some jurisdictions may rely on restrictions on data collection, while others may rely on restrictions on subsequent information handling; while some might rely on criminal law and prosecution, others may rely on private law and litigation; while some may rely on a variety of objective obligations, others may rely on a strong system of oversight and enforcement. It is not the purpose of the Regulatory Clustering to judge, which of these and other regulatory choices are overall the most 'intensive' or 'best'. Consequently, an 'overall ranking' of the examined jurisdictions must be interpreted as the sum of restrictions and expected compliance costs imposed (or expected to be imposed) on the information handling entity.

However, this does not address the problem of comparability of individual regulatory instruments both within their category and in their entirety with other categories: It is difficult to draw a consistent line between two regulatory instruments within the same category and declare one as more intensive than the other. While this may be easy, for example, when both follow the same basic approach, but one is more comprehensive or the other provides for more exceptions, other situations are much more difficult to assess, for example, when two very different approaches address the same problem and achieve regulatory objectives with comparable intensity by using very different means.

Usually, at this point, quantification and delimitation require either empirical or mathematical data. The law, with its aspects of a heuristic[37], and to this end hermeneutically inclined[38], discipline, cannot provide either. To conduct empirical research on this topic would require defining the perception of legal norms, which is the epistemic goal that inevitably precedes this Regulatory Clustering. Using empirical data for this Regulatory Clustering would be circular. The Regulatory Clustering must therefore find a solution to describe regulatory instruments as mathematical values. It must provide the basis which can confer meaning to empirical data. To take up the above problem of describing a

---

[36] Von Lewinski, 'Collision of Data Protection Law Regimes', in: Hennemann, von Lewinski, Wawra, Widjaja (eds.), *Data Disclosure – Global Perspectives and Developments* (2023) 197, 211; in D'Alberti, 'Units and Methods of Comparison', in: Cane et al. (eds.), *The Oxford Handbook of Comparative Administrative Law* (2020) 118, 130 et seq.

[37] Law touches a variety of complex realities and arising factual problems. It therefore relies on its own, very specific, methodology of moral judgements and systemization, in the realization that otherwise the legal scholar would be helpless in solving the encountered problems, cf. as a comprehensive overview, Gigerenzer/Engel (eds.), *Heuristics and the Law* (2006).

[38] The interpretation of texts, in this context dominantly present in the 'pure' law in the books, is a key method of accumulating legal insights, cf. also Röhl, *Rechtssoziologie* (1987), p. 88; Baldus, 'Gesetzesbindung, Auslegung und Analogie: Grundlagen und Bedeutung des 19. Jahrhunderts', in: Riesenhuber (ed.), *Europäische Methodenlehre – Handbuch für Ausbildung und Praxis* (2015) 23, 39 et seqq.; Ricoeur, 'Zu einer Hermeneutik des Rechts: Argumentation und Interpretation' (1994) Deutsche Zeitschrift für Philosophie 375.

value-based concept with quantifiable numbers, it seems impossible to assign a value to a single instrument that can then be aligned with other values of the other jurisdictions to form a cardinal scale.[39] To avoid assigning a mathematical value to a moral value, the use of an ordinal scale[40] is most promising. It allows the legal scholar to place jurisdictions and their regulatory instruments in proportion to each other without assigning a concrete mathematical value to it. Nevertheless (and there is no way around this), some specific cases will have to rely on individual (normative) analysis to make a delimitation.

The biggest problem with an ordinal scale remains the combination of single rankings to an overall ranking: Throughout all jurisdictions, the individual regulatory instruments are not exactly equally important within the logic of the respective overall approach. Some instruments would have relative relevance depending on their practical importance or their intensity in relation to other instruments or aspects of the same jurisdiction. Thus, calculating an overall rating by averaging an individual rating runs the risk of giving a picture of the law that is correct in detail but wrong from a general, holistic perspective. Creating an overall ranking means carefully considering the individual relevance for the respective jurisdiction. An overall rating could therefore be based roughly on a Regulatory Clustering, but still requires attentive legal (normative) analysis.

In line with the objective of contributing to interdisciplinary research, the overall ranking of the Regulatory Clustering can be simplified[41] by sorting the examined legal orders into three or four categories of regulatory intensity, relative to each other and not to a natural zero: ('limited')[42], 'moderate', 'robust' and 'heavy'.[43] Classification in clusters can be achieved by assigning a value between 0 and 8 to each individual ordinal ranking.[44] Assigning a value can also help to absorb distortions in an average ordinal ranking. Such distortions may arise from significant normative gaps between two ordinal rankings. This categorization would at least allow cardinal differences within one category of regulatory instruments to be compared with differences within other, equally generalized

---

39 A cardinal scale in this regard constitutes a ranking of values and in addition to that depicts the distance in value between the different properties.

40 An ordinal scale in this regard provides for a ranking which depicts one regulatory instrument as higher or lower than the other but makes no statement about how large the difference in the target variable (here regulatory intensity) is in between two properties.

41 For all the aforementioned reasons of the impossibility to quantify law, the only goal of such methodologies can be simplification for the purpose of further research in the form of overcoming informational gaps or enabling legal understanding for empirically driven disciplines. See on this goal of simplification Dotan, 'The Common Real-Life Reference Point Methodology – or 'the Mcdonalds's Index' for Comparative Administrative Law and Regulation' in: Cane et al. (eds.), *The Oxford Handbook of Comparative Law* (2021) 991, 1005 et seq.

42 This category is only relevant on the level of individual regulatory instruments. On an overall scale, none of the examined jurisdictions fall in the category 'limited'.

43 This scale is adopted from DLA Piper, 'Data Protection Laws of the World' (2023), accessible under https://www.dlapiperdataprotection.com/index.html, (last accessed 11.03.2024), even though the author refrains from any definition of these terms or the used methodology to create such categorization. This categorization also seems to consider material law and enforcement as one combined aspect which is not the goal of the Regulatory Clustering.

44 This means, the value 0 means non-existent regulation, 1-2 is limited, 3-4 is moderate, 5-6 is robust, and 7-8 Is heavy regulation.

variables from other disciplines such as cultural studies (e.g. cultural dimensions[45]), or behavioral economics (e.g. regulatory perception[46]). The auxiliary implementation of a cardinal value score would provide more context to an overall average ranking and raise awareness of relevant misrepresentations of the ordinal rankings.

2.4. Law in the books vs. law in action

The variable 'regulatory intensity' as defined above includes only those restrictions and compliance costs that are possible and as such enforceable under the law at question. The Regulatory Clustering of regulatory intensity in the described extent does not take into account the actual enforcement of the investigated regulation. If this were the case, it would have to define 'regulatory intensity' as restrictions and compliance costs, that are actually adhered to by the information handling entity. This definition would only be congruent with the definition used above[47] in a utopian vision of society where abstract law is automatically applied and complied with by individual at the micro level (*homo juridicus*). In reality, legislative power can only extend as far as the addressees are willing to limit themselves (for sociological, cultural, economic, or other reasons whatsoever) and as far as the executive can give practical effect to the law. This divergence between what the legislator originally intended and what is actually practiced can be described best as the conflict between law in the books and law in action.[48]

The consequence of this conflict for a Regulatory Clustering is that it can only depict the first step of regulatory perception by building a foundation of law in the books which then has to be implemented in practice as 'law in action'. Only and only then, regulatory perception can be measured as relevant factor influencing individual behavior (Fig. 1). Demonstrating differences between law in the books (what should be), law in action (what is) and regulatory perception (how the addressee perceives the law in action) can help to outline the efficacy of different regulatory and factual approaches to the object of research – which in this particular case is the influence of privacy regulation on individual decision-making.

---

45 Hofstede, 'Dimensionalizing Cultures: The Hofstede Model in Context' (2011) Online Readings in Psychology and Culture; Hofstede, 'The Dimensions of National Culture' (2022), accessible under https://hi.hofstede-insights.com/national-culture, (last accessed 11.03.2024); Globe, 'An Overview of the 2004 Study: Understanding the Relationship Between National Culture, Societal Effectiveness and Desirable Leadership Attributes' (2020); Globe, 'Country Map' (2020), accessible under https://globeproject.com/results/#country.https://globeproject.com/study_2004_2007#theory, (last accessed 11.03.2024).

46 Richthammer/Widjaja, 'The Effect of Regulatory Measures on Individual Data Disclosure: A Country Comparison' (2023) ECIS Research-in-Progress Papers 83.

47 Regulatory intensity means the degree to which it is possible to handle personal information in combination with the required costs to comply with the law, see above → 2.2.

48 See fundamentally Pound, 'Law in books and law in action' (1910) American Law Review 12; Sacco/Rossi, *Einführung in die Rechtsvergleichung* (third edition 2017) Erstes Kapitel, § 1, N 67; for a more modern understanding Halperin, 'Law in Books and Law in Action: The Problem of Legal Change' (2011-2012) Maine Law Review 45; under the name of 'law on the ground' but virtually meaning the same, see also Bamberger/Mulligan, *Privacy on the Ground* (2015), pp. 3 et seqq.

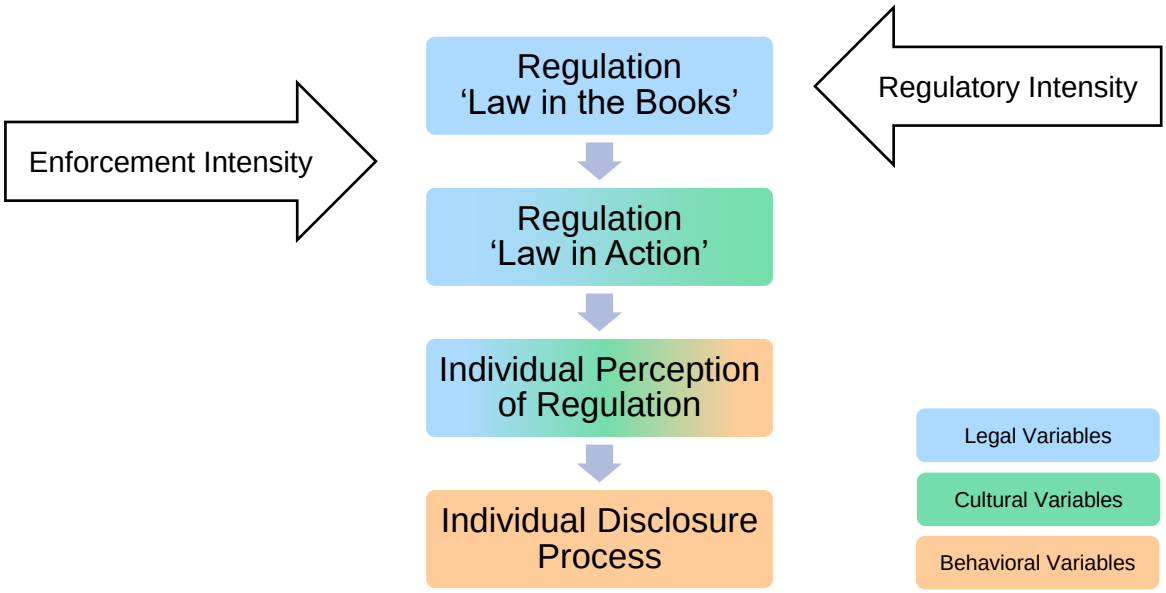

Figure 1: Classification of the Regulatory Clustering within a Law – Behavior Gap Model[49]

However, this methodology requires a definition and a method of measurement of law in action which from a legal point of view is one, if not the, main hurdle in research on regulatory perception. All the same, traditional methods of (comparative) law cannot sufficiently address this problem: Some scholars of comparative law deem 'law in the books' as no law at all, because it is only fictional and does not reflect reality.[50] According to this interpretation, comparative law must never take into account the law in the books. Consequently, comparative law is the comparison of law in action. Not to be mistaken, this should be the primary goal of comparative law, because only law in action grants insights into different legal realities. Nonetheless, law in action remains a complex concept that cannot be adequately described by legal studies alone. The actual impact of law is the result of a multitude of interactions between a wide range of factors, both within and outside the law.[51] 'Pure' comparative legal analysis can subsequently only be one of many cooperating instruments to measure law in action. Most likely, measurement would require empirical research.

However, this Regulatory Clustering is not based on such empirical research, but rather on descriptive comparative law and its quantification. It follows a different line of reasoning, that law in the books is in fact law from an objective point of view; it constitutes one necessary variable which in combination with other non-legal variables, is ultimately integrated into law in action. The representation of the impact of legislation in the sense of this Regulatory Clustering is also important because it is the only variable that can be directly and precisely influenced by government institutions and therefore the only level at which sovereign adjustments can be made.

---

[49] This model was already presented at the DatenTag in Berlin, cf. Stiftung Datenschutz, 'Ergebnisse des Projekts "Vektoren der Datenpreisgabe"' (19.01.2024), accessible under https://stiftungdatenschutz.org/veranstaltungen/unsere-veranstaltungen-detailansicht/datentag-preisgabe-von-daten-440#lg=1&slide=1 (last accessed 11.03.2024).

[50] Fundamentally Gorla, *Diritto comparator e diritto commune europeo* (1981), pp. 303 – 306, 361; see also Sacco/Rossi, *Einführung in die Rechtsvergleichung* (third edition 2017), Erstes Kapitel, § 1, N 67.

[51] Dotan, 'The Common Real-Life Reference Point Methodology – or 'the Mcdonalds's Index' for Comparative Administrative Law and Regulation' in: Cane et al. (eds.), *The Oxford Handbook of Comparative Law* (2021) 991, 996.

To this end, the Regulatory Clustering could also try to approximate a law in action variable. The most important regulatory instruments that can be used to ensure congruence between law in the books and law in action are such (legal and factual) instruments linked to enforcement or consequences of non-compliance. If there is no threat that law can be implemented by force or that there will be other negative consequences, it cannot be expected that the individual voluntarily complies with abstract rules.[52] The Regulatory Clustering can those introduce a third[53] category of regulatory instruments: measures of enforcement. However, the variable 'regulatory intensity' as defined above does not seem suitable to quantify such enforcement measures: Enforcement itself does not require the information handling entity to restrict its activities or increase its compliance costs. Rather, it seeks to compel compliance, regardless of the content or nature of the rules enforced. Given that such enforcement measures could bridge the Gap between law in the books and law in action, a benchmark should focus on the question, whether the measures are likely to translate law in the books to law in action. This definition comes close to the already rejected variable of 'efficiency', which makes the quantification of enforcement a very complex matter.

An approach for the Regulatory Clustering could be to look at the quantity and quality of legally possible measures that help translate law in the books to law in action. This would mean that enforcement measures would include instruments relating to administrative monetary and non-monetary sanctions, relevance of criminal prosecution, possibilities of civil litigation, powers of supervisory authorities or the procedural system of enforcement. However, this approach would still solemnly consist of aspects of law in the books (as they would describe possibilities of enforcement, not actual enforcement). A truly meaningful approach to law in action requires research into the frequency and intensity with which legally possible enforcement measures are used in practice and how such enforcement practices are perceived by the addressees of the substantive law being enforced.[54] This would establish a link between law in action and the regulatory perception and could provide for the variable of 'intensity of enforcement' – even though there is a certain circularity between methodology (definition of variables) and research objective (regulatory perception).

---

[52] Tamanaha, 'The Rule of Law and Legal Pluralism in Development' (2011) Hague Journal on the Rule of Law 2; Swenson, 'Legal Pluralism in Theory and Practice' (2018) International Studies Review 438, 445.

[53] Besides self-determined and assured level of privacy.

[54] See for a brief attempt to narrow such approach down below → 5.2.

2.5. Jurisdictions subject to research

Having outlined the methodology, objectives, categories and definitions of the Regulatory Clustering, the only missing aspect is the concrete jurisdictions to be compared. The examined jurisdictions are the ones of Germany (EU)[55], Switzerland[56], USA[57], California[58], Brazil[59], Ghana[60], Japan[61], and China[62]. These countries represent a great diversity in economic relevance, legal concepts, social and cultural structures, and governmental organisation. They are spread throughout the 'global north' as well as the 'global south' in a political understanding,[63] but also in a mere geographical sense throughout the whole globe. This spread allows for not only the comparison of diverse jurisdictions, but also the analysis of embedment in different cultural settings.

A detailed introduction of the examined jurisdictions can be found in the full version of the Regulatory Clustering.[64]

---

55 The main legal source is the General Data Protection Regulation (EU) 2016/679 of 2018 (GDPR) and the German Federal Data Protection Act of 1978 (BDSG). One should bear in mind that that an overall standard of European law cannot be directly induced from German law. Rather, there can be substantial differences in the national interpretation of European law (even after the implementation of the GDPR), cf. Bamberger/Mulligan, Privacy on the Ground (2015), p. 9.

56 The main legal source is the Federal Act on Data Protection of 2023 (FADP). The Regulatory Clustering does only focus on this current legislation. However, one must bear in mind that this new FADP partly greatly deviates from the old FADP and that those very recent changes might distort the regulatory perception of laypersons.

57 Legal sources can be found in various sector-specific statutory law, as well as in common law practices, which makes the USA very difficult to assess. The Regulatory Clustering does especially take into account the case law of the FTC as well as central regulatory pieces like the HIPAA, COPPA, FCRA, and Privacy Act.

58 The main legal source is the California Consumer Privacy Act of 2020 (CCPA) as amended by the California Privacy Rights Act of 2023 (CPRA). Similar to Switzerland, the recent (but not as significant) changes could cause distorted regulatory perceptions.

59 The main legal source is the Brazilian Data Protection Law No. 13,709/2018 of 2020 (LGPD).

60 The main legal source is the Data Protection Act (Act 843) of 2012 (DPA).

61 The main legal source is the Act No. 57 on the Protection of Personal Information of 2003 (APPI).

62 Legal sources can be found in various statutory laws. The most important legislation is the Personal Information Protection Law of the People's Republic of China of 2021 (PIPL), and the Cybersecurity Law of the People's Republic of China of 2017 (CSL). When assessing legal realities in China, one should always bear in mind, that the Chinese system utilizes a rule by law rather than a rule of law approach, which means that legal restrictions might not apply to public authorities and can be case aside rather arbitrarily, cf. on the rule by law and its consequences Ng, 'Is China a 'Rule-by-Law' Regime?' 67 Buffalo Law Review 793 (2019); Chio, Rule of Law or Law by Rule: A Brief Analysis of Chinas Legal System, 33 The International Relations Journal San Francisco State University 29 (2014); Czarnocki et al., 'Government access to data in third countries – Final Report' EDPS/2019/02-13 (2021), p. 12.

63 Cf. comprehensively Salaymeh/Michael, 'Decolonial Comparative Law: A Conceptual Beginning' (2022) RabelsZ 166; in another context but with the same conception Chander/Schwartz, 'Privacy and/or Trade' (2023) The University of Chicago Law Review 49, 105 et seqq.

64 Sonnenberg, 'A Regulatory Clustering of Privacy Laws – Extended Version' (2024) IRDG Research Paper Series, No. 24-01, pp. 11 et seqq.

2.6. Conclusions for the methodology

The preceding observations show that the idea of a Regulatory Clustering encounters many methodological weaknesses. Some might even call it 'the crudest and most unscientific way of legal comparison'[65]. Nevertheless, it can still be used as an interdisciplinary research tool that approaches a middle ground between two (or more) completely different disciplines. By attempting to quantify regulatory instruments and jurisdictions, the Regulatory Clustering can contribute to an interdisciplinary analysis of the co-dependences and interactions of research variables from different disciplines.

Still, the shortcomings in terms of traditional legal methodology that this approach entails must be addressed somehow. The best way to do so is to precisely define the researched categories (regulatory instruments divided into those that provide for an assured and a self-determined level of privacy) and the target variable to be applied to the categories (regulatory intensity). Regulatory intensity in this context is the degree to which the regulatory instrument imposes restrictions on information handling activities. Such restrictions can be imposed by directly regulating the handling activities or by imposing objective obligations that raise compliance costs if an entity wants to handle personal information.

Legal criticism that the Regulatory Clustering does not take into account circumstances outside its parameters and thus exhausts itself in the knowledge of foreign law can be dismissed to the extent that the Regulatory Clustering offers only an excerpt of a higher, interdisciplinary research goal. In particular, it opens up the possibility of an even more contextual understanding of law if it is combined with (empirical) findings from other disciplines.

Finally, the expectations of the method must be clear: The Regulatory Clustering is not intended to be a holistic representation of legal or factual circumstances, nor shall it pass judgement on the efficiency of privacy regulations. Rather, its sole purpose is to depict an ordinal scale of regulatory intensity as an approximation rather than an absolute value, so that this scale can be used to quantify law to some extent and to utilize it as a variable for further interdisciplinary research.

3 Clustering Regulatory Intensities

Conducting the Regulatory Clustering along the rules laid out above is a difficult and especially protracted task. It requires to look into the relevant laws and its respective interpretation by courts and executive organs of each jurisdiction, as well as an analytical comparison of the findings. As it would surpass the scope of this paper, the concrete conduction can be found in another, lengthier version of this paper.[66] Here, the Regulatory Clustering will content itself with naming the relevant norms and reproduce the respective ranking.[67] Readers are kindly invited to consult the

---

[65] Sacco/Rossi, *Einführung in die Rechtsvergleichung*, (third edition 2017) Erstes Kapitel, § 1, N 77.

[66] Sonnenberg, 'A Regulatory Clustering of Privacy Laws – Extended Version' (2024) IRDG Research Paper Series, No. 24-01, pp. 18 et seqq.

[67] Wherever feasible, the concrete ranking is represented in the order in which the different jurisdictions are named.

aforementioned version of this paper, to gain further insights. The same applies for enforcement intensities in chapter 4.

Having outlined different rankings of regulatory and enforcement intensities, it is possible to create different country profiles in chapter 5, which is a brief overview of this paper's contribution to comparative data privacy law. Chapters 6 and 7 then completes the circle by outlining the resulting (possible) contribution to interdisciplinary (legal) research.

3.1. Assured Level of Privacy

The presumably[68] most important aspect of data privacy law are such regulations, that impose objective behavioral and organizational obligations on the information handling entity. Such rules compose the assured level of privacy within the meaning of this Regulatory Clustering. As this chapter shows, the assured level of privacy is – at least in terms of quantity and regulatory density – the focus of privacy legislation around the world.

3.1.1. Prerequisites of Information Handling

The prerequisites under which it is allowed to handle personal information can be categorized in three different groups which are further graded within themselves: Prohibition of information handling subject to permission[69], permission subject to prohibition[70], and general free flow of data[71]. The resulting restrictiveness usually sets the tone for the regulatory intensity of the respective approach to regulating privacy.

3.1.2. Sensitive Information

Usually, handling sensitive information requires higher prerequisites and triggers stricter obligations. This is especially the case in those countries that are already restricting 'normal' information

---

[68] There is some discussion, as to whether the core of privacy protection law should be the individual empowerment of the user, or the implementation of an objective layer of protection, which is indifferent to user action or even knowledge, cf. regarding the GDPR: Engeler, 'Der Konflikt zwischen Datenmarkt und Datenschutz – eine ökonomische Kritik an der Einwilligung' (2022) NJW 3398, N 23 et seqq.; or regarding the US approach Rothschild, 'Against Notice and Choice: The Manifest Failure of the Proceduralist Paradigm to Protect Privacy Online (or Anywhere Else)' (2018) Cleveland State Law Review 558; Reidenberg et al., 'Privacy Harms and the Effectiveness of the Notice and Choice Framework' (2015) A Journal of Law and Policy for the Information Society 485.

[69] Such is the case in China (Art. 13 PIPL), Ghana (Art. 20 DPA), Brazil (Art. 7 LGPD). Germany (Art. 6 GDPR).

[70] Such is the case in Switzerland (Art. 30 et seq. FADP).

[71] Such is the case in California, Japan, and the USA. However, these countries set a certain minimum threshold by prohibiting for example 'unfair or deceptive acts' in the USA (15 USC § 45 (a)) or 'improper acquisition' and 'inappropriate use' in Japan (Art. 19, 20 I APPI).

handling[72] and in Japan, where a prohibition subject to permission does apply to handling sensitive information[73]. Only few additional safeguards are implemented in Californian, US, and Swiss law.[74]

Sensitive information is usually considered to be such relating to religious, political, and union beliefs and practices, health, race and ethnicity, sexual orientation, and activity, genetic or biometric identification, criminal records, or minors. Only California significantly surpasses this global standard.[75]

3.1.3. Purpose Limitation

The requirement to handle information only in accordance with a specific and legitimate purpose does appear in every of the examined jurisdiction and, respectively, takes central relevance.[76] The purpose limitation principle is deeply intertwined with further data privacy principles, such as data minimization or storage limitation.

3.1.4. Subsequent Information Handling

Closely related to the purpose limitation principle are rules that restrict information handling activities that are not in accordance with the originally specified purpose. Such secondary purposes must always show some form of direct connection to the primary purpose.[77]

3.1.5. Domestic Transmission to Third Parties

One possibility of subsequent information handling is the third-party transfer of personal information. Consequently, many jurisdictions apply the same prerequisites.[78] The rest of the examined jurisdictions prescribe a special regime on third-party transfers based around consent/opt-out, thus incentivizing direct collection.[79] Of these, Ghana deserves to be singled out: Art. 88, 89 DPA prohibit

---

72 Especially in China (Art. 28 II, 29 PIPL), but also in Brazil (Art. 11 LGPD), Germany (Art. 9 GDPR), and Ghana (Art. 27 DPA).

73 Cf. Art. 20 II APPI.

74 Cf. in California § 1798.121 CCPA, in the USA the various sector specific laws such as the HIPAA or the COPPA, and in Switzerland Art. 6 VII lit. a); 22 II lit. a); 30 II lit. c) FADP.

75 Cf. § 1798.140 (ae) CCPA.

76 The purpose limitation principle is most pronounced in Brazil (Art. 6 I LGPD), China (Art. 6 PIPL), Germany (Art. 5 I lit. b) GDPR), and Ghana (Art. 22 DPA), but does also exist in Japan (Art. 17 et seq. APPI), Switzerland (Art. 6 III FADP), California (§ 1798.100 (b),(c)), and the USA (so called 'broken promise').

77 The nature of such connection can vary: In China, Art. 6 I PIPL requires a 'direct relation'. Art. 17 II APPI in Japan is very similar. California (§ 1798.100 (c) CCPA), Ghana (Art. 17 lit. d) DPA), Switzerland (Art. 6 III FADP), Germany (Art. 5 I lit. b) GDPR), and Brazil (Art. 6 I LGPD) require compatibility.

78 Such jurisdictions are Switzerland (the only notable restriction results from Art. 30 II lit. c) FADP), Germany, and Brazil (with the specification of Art. 7 § 5 LGPD).

79 For China, cf. Art. 25 PIPL, for Ghana Art. 21 II DPA, for Japan Art. 27 APPI, and for California, which is in this regard similar (but more restrictive) to the US § 1798.100 (d); § 1798.115 CCPA.

selling and purchasing personal data, i.e. prohibiting commercial third-party transfers, and Art. 21 DPA generally prescribes collection directly from the individual.

Another, less regulated variant of data transfers is the outsourcing of information handling activities by entrusting a contractor (processor) with the information. Throughout all jurisdictions such outsourcing is subject to sufficient contractual safeguards.[80]

3.1.6. Transmission Abroad

When it comes to transfers abroad, most jurisdictions decided to implement partial data localization legislation: Transmission abroad are only possible if there are sufficient guarantees that the third country provides for a comparable/adequate level of (privacy) protection.[81] Only some countries deviate – in one of two extremes – from this middle-ground approach: China has implemented a 'digital border wall' around its territorial borders[82], while Ghana and the USA, including California, rely on international free flow of data by not creating specific restrictions to third country transfers.[83]

3.1.7. Data Minimization

The data minimization principle flanks the purpose limitation principle, so that the information handling shall not only be in accordance with the purpose, but also limited to the proportionate scope necessary for the achieving the purpose. This or a similar principle can be observed in all of the examined jurisdictions.[84]

3.1.8. Deletion Obligations

When the lifecycle of the personal information has ended, for example when it is no longer necessary for achieving the purpose, the information must be deleted. Such objective deletion obligations exist in all examined jurisdictions.[85] Other potential triggers for objective (i.e. proactive) deletion obligations can be expiry of a retention period, internal discovery of non-compliance, or missing accuracy.

---

[80] Cf. for China Art. 21 PIPL, for Ghana Art. 29 et seq. DPA, for Japan Art. 25 APPI, for California § 1798.100 (d), for Brazil Art. 39 I LGPD, for Germany Art. 28 GDPR, and for Switzerland Art. 9 FADP.

[81] Such countries are Germany (Art. 44 et seqq. GDPR), Switzerland (Art. 16 et seq. FADP), Brazil (Art. 33 et seqq. LGPD), and Japan (Art. 28 APPI). Note, that the latter two place more significance in consent as exception to sufficient guarantees.

[82] Cf. Art. 38 PIPL.

[83] In Ghana, however, there exists something like an incorporation principle in Art. 18 II DPA, which may allow foreign data localization laws to directly take effect in Ghanaian law.

[84] The principle can be found in Brazil in Art. 6 III LGPD, China in Art. 6 PIPL, Germany in Art. 5 I lit. c) GDPR, California in § 1798.100 (c) CCPA, Ghana in Art. 19 DPA, Japan in Art. 18 I APPI, and in Switzerland in Art. 6 II and III FADP. The principle, that information shall only be kept where it is necessary for the stated purpose is also widely accepted in US case law.

[85] Cf. for China Art. 47 PIPL, for Switzerland Art. 6 IV and V FADP, for California § 1798.100 CCPA, for Japan Art. 22 APPI, for Brazil Art. 15 LGPD, for Germany Art. 5 I lit. d) and e) GDPR, and for Ghana Art. 24 DPA.

3.1.9. Data Quality

The latter is part of the data quality principle, which obliges the information handling entity to keep personal information correct and up to date. This principle can be observed in two different categories: Either, handled information must always be correct if its correctness is relevant for the respective purpose[86], or the inaccuracy of the information must also constitute a violation of the rights of the individual[87].

3.1.10. Data Security

When handling personal information, the handling entity shall adopt sufficient technical and organizational measures to prevent security incidents such as the unauthorized access, use, or disclosure and the accidental loss or alteration of the personal information. It is universally accepted that such data security does – in accordance with the risk of security incidents – such measures may include internal best practices and training, encryption, or physical access restrictions.[88] The only anomaly is Ghana, where the supervisory authority has still not issued any concrete guidelines after 12 years.

3.1.11. Internal Documentation

Shifting away from information handling prerequisites and basic principles, all jurisdictions have come to the conclusion that such objective standards do not sufficiently protect individual privacy, as it would be very difficult to assess the compliance with these obligations. Therefore, modern data privacy laws do also include accountability mechanisms.

One aspect of accountability is a recordkeeping obligation that would require all information handling entities to keep track of their activities.[89] Another way of requiring the information handling entity to produce internal documentation is the risk assessment of certain practices (often called (data protection) impact assessment or similar). Such assessments, however, are mostly only required in certain situations.[90] China is an exemption, as Art. 54 and 55 PIPL require regular impact assessments (for example when entrusting a processor) and even more so ‘PI Audits’ regardless of risk.

---

[86] This form of the data quality principle can be found in Brazil (Art. 6 V LGPD), Germany (Art. 5 I lit. d) GDPR), Ghana (Art. 26 DPA), Japan (Art. 22 APPI), and Switzerland (Art. 6 V FADP).

[87] Regularly, this requires a direct negative effect on the individual, which is often apparent in credit registers. Examples can be found in China (Art. 8 PIPL), California, and the USA (both within tort law and sector specific regulation such as § 611 FCRA).

[88] Cf. for Germany Art. 32 GDPR, for China Art. 9 and 51 et seqq. PIPL, for Switzerland Art. 8 FADP, for California § 1798.100 (e) CCPA, for Japan Art. 23 APPI, for Brazil, Art. 46 et seqq. LGPD, and for Ghana Art. 28 DPA. Data security is also a vital part of US case law.

[89] Such obligation is in place in Germany (Art. 40 GDPR), Switzerland (Art. 12 FADP), and in Brazil (Art. 37 LGPD). In Japan, Art. 29 APPI requires a record only of third-party transfers.

[90] Impact assessments shall be conducted when there is an expectedly high risk for the individual. This obligation exists in California (§ 1798.185 (a)(15)(A) CCPA), Germany (Art. 35 GDPR), and Switzerland (Art. 22 FADP).

3.1.12. Registries

Data protection registries originated from the old Swiss data protection law, which required all information handling entity to publicly register with the supervisory authority. Meanwhile, it has abandoned this concept as it was deemed impractical. Now, such register can only be found in Ghana (Art. 27 DPA). The idea of having to publicly announce certain facts echoes only faintly in public information obligations[91] and the obligation to announce a domestic representative[92].

3.1.13. Internal Responsibility Management

Many jurisdictions (in this sample six out of eight jurisdictions) know the concept of a data protection officer (or similar), who is responsible for overseeing internal compliance, offering advice on information handling activities and communicating with the individual or supervisory authority. However, it is not always mandatory to appoint such internal supervisor: They become necessary when there is an expectedly high risk for the individual which could arise from the nature and/or quantity of the handled information, or the size of the company.[93] In other jurisdictions, appointing an internal supervisor is not mandatory but either brings regulatory benefits or is merely advised as organizational security measure.[94]

3.1.14. Certification and Self-Regulation

It is also common to allow private organizations to craft their own self-regulatory framework, which mostly takes the form of a certification mechanism or the subjection to a private supervision organization.[95] Regularly, the legal consequences of adhering to a self-regulation are marginal and mostly of factual nature. However, in California and the USA, self-regulation plays a significant role, as one of the main focuses of FTC enforcement is the persecution of ‘broken promises’ and the binding character of self-declarations.[96]

---

91 Such possibility exists in Japan (Art. 21 I APPI) and California (§ 1798.130 (a)(5) CCPA).

92 Such obligation exists in China (Art. 53 PIPL), Germany (Art. 27 GDPR), and Switzerland (Art. 14 et seq. FADP). However, in both scenarios, the obligations serve inherently other purposes than a registry obligation: The information obligation addresses modalities of information, and the domestic representative eases communication abroad, while a data protection registry shall generally raise transparency before the public.

93 Such regulation can be found in Brazil (Art. 41 LGPD), Germany (Art. 37 et seqq. GDPR), and China (Art. 52 PIPL).

94 In Switzerland, Art. 23 IV FADP allows to consult the data security advisor (Art. 10 FADP) instead of the FDPIC. In Ghana, according to Art. 58 DPA, an information handling entity only may appoint a data protection supervisor. In Japan, there is only a recommendation by the PPC, cf. Personal Information Protection Commission Japan, ‘Guidelines on the Act on the Protection of Personal Information’ (2023), p. 165, accessible under https://www.ppc.go.jp/personalinfo/legal/guidelines_tsusoku/ (last accessed 11.03.2024).

95 Such allowances exist in Japan (Art. 47 et seqq. APPI), Switzerland (Art. 13 FADP), Brazil (Art. 50; 52 § 1 IX LGPD), and Germany (Art. 40 et seqq. GDPR). In China and Ghana, concepts of self-regulation do only vaguely surface and take a subordinate role (for example certified codes of conducts appear in Ghana in Art. 24 IV and 64 III DPA. The same goes for China and Art. 62 No. 4 PIPL).

96 Solove/Hartzog, ‘The FTC and the New Common Law of Privacy’ (2014) Columbia Law Review 628 et seqq. The binding effect of self-declarations in the USA can be exemplified by § 1798.140 (d)(4) CCPA, which broadens the scope of application of the CCPA to those who declare themselves as CCPA-compliant.

3.1.15. Regulation on Public Information

Social media and the internet as medium for global interconnectivity produce scenarios where personal information were made publicly available by the individual themselves, i.e. they have already disclosed their personal information to the public. Consequently, all of the examined jurisdictions have implemented at least some privileges for handling publicly accessible information.[97] Such privileges can range from easement of prerequisites of processing to advance opt-out mechanisms to the complete exclusion from the scope of application of the respective privacy legislation.

To dim the negative consequences of personal information once publicized (the internet does not forget), many jurisdictions have developed a 'right to be forgotten' of some sorts.[98]

3.1.16. Cyber Surveillance Authority

Lastly in terms of assured level of privacy, one cannot discuss the state of privacy in one country without acknowledging the power authorities have to surveil their citizen especially by means of communication interception or mass data retention. Such measures for the purpose of (serious) criminal prosecution and national security exist in every country which (mostly) follow a similar basic scheme: The purpose of surveillance must be a serious one, the measure must be *ultima ratio* and at least necessary for the purpose, and such measure are subject to judicial reservation, which can be postponed only in certain scenarios (mostly of urgency). Of course, details may vary, and such deviations may have significant influence on the level of protection in the respective country. However, this is not the place for a detailed analysis of the various security relevant legislations in the examined countries.[99] Nonetheless it is worth mentioning that the both extremes within this category are neighboring countries: While China can be classified as techno-authoritarian regime which utilizes surveillance powers to an unproportionate extent, Art. 35 of the Japanese constitution does only allow an infringement of the secrecy of communication for criminal prosecution purposes – but not for national security.

---

[97] Such privileges can be found in Brazil (Art. 7 § 3 LGPD), Germany (Art. 9 II lit. e) GDPR), Japan (Art. 20 II (vii) APPI), China (Art. 13 Nr. 6, 27 PIPL), Switzerland (Art. 30 III FADP) and to the widest extent in California (§ 1798.140 (v)(2) CCPA. Publicly accessible information does also enjoy protection under the first Amendment in the US in general).

[98] As such, this right is only acknowledged by the GDPR as standalone individual right (Art. 17 I, II GDPR) that obliges the information handling entity to ensure that it is possible to delete public information from publicly accessible sources (i.e. 'make the internet forget'). However, various courts for example in Japan, Switzerland, and the USA have interpreted their right to deletion in a similar way.

[99] For more details, see Sonnenberg, 'A Regulatory Clustering of Privacy Laws – Extended Version' IRDG Research Paper Series, No. 24-01, pp. 36 et seqq.

3.2. Self-determined Level of Privacy

Other than objective obligations imposed on information handling entities, privacy legislation around the world grant a variety of individual rights to the data subject, which enables them to enact a certain control on the handling of their personal information. The assessment of the intensity of most user rights is twofold: first, one must look at the extent to which the right exists, and then at the applicable exemption to adherence of an invoked user right. These exemptions are broadly similar across most jurisdictions and user rights and are therefore only subject to discussion in the long version of this Regulatory Clustering.[100]

3.2.1. Consent

The most prominent concept of self-determined level of privacy is consent prior to the collection of personal information. In most jurisdictions, consent is a freely given, specific, informed, unambiguous and often express declaration, which – to a greater or lesser extent – justifies the handling of personal information.[101]

3.2.2. Right to Object / Opt-Out

Opt-out or objection is the post-disclosure counterpart to consent: According to it, the individual does always have the right to interrupt and forbid (future) information handling activities. Such right does – at least in the form of revocation of consent – exist in every of the examined jurisdictions.[102] Commonly, opt-out or objection is only possible when there is a violation of other privacy laws or there is no other basis of authorization besides consent. This is, however, notably not the case in California and the USA, where opt-out is a central and often definite tool for individual control over one's personal information.

3.2.3. Right to Deletion

Similar to objection, invoking a right to deletion ends the lifecycle of the handled information and it must be deleted. Such right can be invoked in all examined jurisdictions, when there is no authorization to handle the information, there is an objection, the information is inaccurate or unnecessary for the purpose or there is another violation of privacy laws.[103]

---

[100] Ibid, pp. 40 et seqq.

[101] This is most dominant in those jurisdictions that have implemented a prohibition subject to permission, i.e. China (Art. 13 Nr. 1; 14; 16 PIPL), Germany (Art. 4 I Nr. 11; 7 IV; 6 I lit. a) GDPR), Brazil (Art. 5 XII; 7 I LGPD), and Ghana (Art. 20 I DPA). Even though Japan does not rely on a general prohibition subject to permission, it does restrict certain handling activities with consent as main element of authorization (Art. 18 I and II; 20 II; 27 I APPI). Similarly, Switzerland uses consent as element of justification for a violation of personality (Art. 31 I FADP). Even Californian and US legislation rarely relies on advance consent (e.g. 15 USC § 6502 (b)(1)(ii) COPPA or § 1798.120 (d) CCPA).

[102] Cf. for Ghana Art. 20 II DPA, for California § 1798.120 and .121 CCPA as well as the US overall approach of 'notice and choice', for Switzerland Art. 30 II lit. b) and 31 II FADP, for Germany Art. 21 GDPR, for Brazil Art. 8 § 5 and 9 § 2 LGPD, for China Art. 15 PIPL, and for Japan, Art. 35 I, V.

[103] Cf. for California § 1798.105 (a) CCPA which mirrors the respective intensity on federal level, for Switzerland Art. 32 II FADP, for Brazil Art. 16 IV; 18 IV and VI LGPD, for Ghana Art. 33 DPA, for China Art. 47 PIPL, for Japan Art. 35 APPI, and for Germany Art. 17 GDPR.

3.2.4. Right to Rectification

As self-determined counterpart of the data quality principle, a right to rectification allows the individual to oblige the information handling entity to correct or update factually or relatively inaccurate, incomplete, or outdated information.[104]

3.2.5. Right to Access

In every examined jurisdiction the individual has a right to request information on the information handling activity such as the handling purposes, contacts of the handling entity, third-party transfers, and other handling modalities.[105] This catalogue does regularly also include the 'raw' information handled by the entity.[106]

3.2.6. Right to Data Portability

As an effort against network- and resulting lock in-effects, many jurisdictions try to empower the individual to make the personal information handled by another entity tangible, so that a relocation to another service provider is as easy as possible. This is most efficiently achieved by directly requiring the information handling entity to transfer held information to another service provider[107], but can also be achieved with the 'raw' information access of the individual in a readily readable and tangible format.[108]

3.2.7. Information Obligations

Information obligations are the objective counterpart of the right to access. Nonetheless, they are part of the self-determined level of privacy because it is their sole purpose to empower the individual so that they can invoke the instruments that grant them a self-determined level of protection. Such obligations exist in every examined jurisdiction to a rather high extent and require the information handling entity to provide various information (which are the same as under the right to access with the addition to more extensive information such as applicable retention periods, existence of user

---

[104] Consequently, the right to rectification can be found in all jurisdictions with a data quality principle: Cf. for Ghana Art. 33 I lit. a) DPA, for Brazil Art. 18 III LGPD, for China Art. 46 PIPL, for Germany Art. 16 GDPR, for Japan Art. 34 APPI, for California § 1798.106 (a) CCPA, and for Switzerland Art. 32 I FADP. Only the federal US does not provide for effective rectification rights. They can only vaguely be found in sector specific legislation such as 15 USC § 1681i FCRA.

[105] Cf. for Germany Art. 15 GDPR, California § 1798.110 (a) CCPA, Brazil Art. 18 LGPD, Switzerland Art. 25 II FADP, Ghana Art. 35 I DPA, and (in a more generalist form) China Art. 45, 48 PIPL.

[106] In Japan, the scope is even limited to only this 'raw' access, cf. 33 I APPI.

[107] Jurisdictions following this approach are China (Art. 45 III PIPL), Brazil (Art. 18 V LGPD), Germany (Art. 20 GDPR), and Switzerland (Art. 28 FADP).

[108] Jurisdictions following this approach are California (§ 1798.130 (a)(3)(B)(iii) CCPA), and in a lot less feasible extent Ghana (Art. 35 XII DPA) and Japan (Art. 33 II APPI).

rights, where applicable invoked legitimate interest, or adopted security measures) to the individual at the latest at the time of collection.[109]

3.2.8. Data Breach Notification

Similar to general information obligation is the data breach notification an objective obligation which predominantly serves the purpose of empowering the individual decision and is therefore part of the self-determined level of privacy. It requires the information handling entity to report any relevant security incidents to the supervisory authority and/or the affected individual and exists in all of the examined jurisdictions.[110] Core aspect of ranking the extents of single data breach notification obligations is the question whether and under what circumstances the individual besides the supervisory authority is to be directly informed.

3.3. Further Specifics

With that, all relevant instruments (in relation to the research purpose) of assured and self-determined level of privacy have been examined and put in comparison to other privacy legislations. Still, it should be noted that there is a variety of further regulation that was not included in this quantification. These regulations were omitted because their relevance is rather insignificant in comparison to other examined jurisdictions and would therefore distort the weighting of the ranking, which in principle assesses all categories as equally relevant. Other reasons for leaving out certain instruments can be their relative insignificance in comparison to the own regulatory approach and that individual instruments are so unique that they cannot reasonably be weighed against other jurisdictions. Nonetheless, some of such specific instruments should be very briefly mentioned here, even though they do not contribute to the Regulatory Clustering.

Corresponding factors can be, for example prerequisites and consequence of anonymization and pseudonymization[111], regulation on personal information as economic good[112], privacy by design and

---

[109] Cf. for California §§ 1798.110, 1798.130 (a)(5) CCPA, for Germany Art. 12 et seqq. GDPR, for Brazil Art. 9 LGPD, for China Art. 17 PIPL, for Japan Art. 21; 27 II; 32 APPI, for the federal USA the general 'notice-and-choice' approach, for Switzerland Art. 19 et seqq. FADP, and for Ghana Art. 27 II DPA.

[110] Cf. for Ghana Art. 31 DPA, for China Art. 57 PIPL, for Germany Art. 33 et seq. GDPR, for Brazil Art. 48 LGPD, for Japan Art. 26 APPI, for Switzerland Art. 24 FADP, and for California § 1798.82 Civil Code of California, which mirrors the US overall approach of 'notice-and-choice'.

[111] Often, such information is (supposedly that there is a universal threshold up to which an information is sufficiently de-identified across every jurisdiction) excluded from regulation because they either do not count as personal information (Art. 12 LGPD in Brazil or recital 26 of the GDPR in Germany) or are specifically excluded (§ 1798.145 (a)(6) CCPA). Japan has even introduced a complete separate regime on handling pseudonymized and anonymized information (Art. 41 et seqq. APPI).

[112] Regulation on the commercialization of information can be manifold: Popular examples are a prohibition of coupling (for example Art. 16 PIPL in China, Art. 7 IV GDPR in Germany, or Art. 7 XI MCI in Brazil) and competition oversight (as can be best seen in the activities of the FTC as competition supervision in the USA or recent activities of the Germany competition supervision against Meta, cf. CJEU, 4.7.2023, C-252/21, NZKart (2023) p. 430 – *Meta Platforms*) to tackle power imbalance in cases of digital monopolies. However, legislators can also regulate the value of personal information as can be seen in the Californian financial incentives program (§ 1798.125 (b) CCPA) and the Swiss competition privilege (Art. 31 II lit. b) FADP) on one extreme, and the Ghanaian prohibition of trade with personal information (Art. 88, 89 DPA) on the other end.

privacy be default[113], multi-referential information[114], the corporate privilege in Switzerland[115], automated decision-making (especially scoring)[116], or restrictions of direct marketing[117]. These instruments all have in common, that they may have very different extents and relevance, and might even be completely contradictory to approaches from other jurisdictions, as can be seen best in the example of the commercialization of personal information.

Ultimately, the clustering does not depict the laws regulating privacy in its entirety – nor does it intend to do so. Other not mentioned factors of privacy law could be laws regarding intellectual property and trade secrets, disclosure obligations or even constitutional foundations as well as many more regulatory (and extra-judicial[118]) pieces. It is not within the capabilities of this Regulatory Clustering to weigh such holistic regimes against each other, but rather to give an approximation of the central privacy rules of the jurisdictions in relation to each other.

3.4. Conclusion for Regulatory Intensities

3.4.1. Overall Assured Level of Privacy

Assessing the rank of each privacy-related instrument in one jurisdiction in relation to the same instrument in other jurisdictions does only provide for a very micro perspective, which cannot contribute to the research question, how law can constitute a quantifiable, comparable parameter in an interdisciplinary research model. It is therefore crucial to now combine the examined instruments into one average ranking. Even though this cannot constitute a holistic and therefore true statement on the effects of a certain legislation, it does provide a suggestion as to how different legislation can be clustered into relation to each other. Accordingly, a clustering of a combined assured level of privacy as examined in this paper looks like this:

---

[113] Originally introduced in Art. 25 GDPR, this concept begins to set foot in other jurisdictions such as Switzerland (Art. 7 FADP) and Brazil (such requirements are interpreted to be in the scope of Art. 46, 49 LGPD, cf. Hoffmann, 'LGPD Et Al. – Report on the Law of Data Disclosure in Brazil' (2022) IRDG Research Paper Series, No. 22-06, p. 45)

[114] While multi-referential information is often discussed as opposing third party interest, Ghana is the only of the examined countries that has explicitly introduced this important concept to their legislation, cf. Art. 35 IV DPA.

[115] Cf. Art. 20 IV, 26 III and most importantly 31 II lit. b) FADP.

[116] Examples can be found in Art. 20 LGPD (Brazil), Art. 24 PIPL (China), § 1798.185 (a)(16) CCPA (California), Art. Art. 41 DPA (Ghana), and Art. 21 II FADP (Switzerland).

[117] Corresponding to the commercialization of personal information, different jurisdictions handle marketing purposes differently: While some jurisdictions restrict related handling activities (for example Art. 40 DPA (Ghana) or a little less restrictive Art. 21 II GDPR (Germany)), others may even incentivize it (for example § 1798.140 (e)(6) and § 1798.140 (ah)(1) CCPA (California)).

[118] See on the notion of legal pluralism and privacy protection Greenleaf, *Asian Data Privacy Laws* (2014), p. 8; Bennett/Raab, *The Governance of Privacy: Policy Instruments in Global Perspective* (2006), chapters 6 and 7. It delves from the assumption that abstract norms influencing behavior do not always come from legal texts or other sovereign acts, see on this already above, note 4 as well as chapter 2.4.

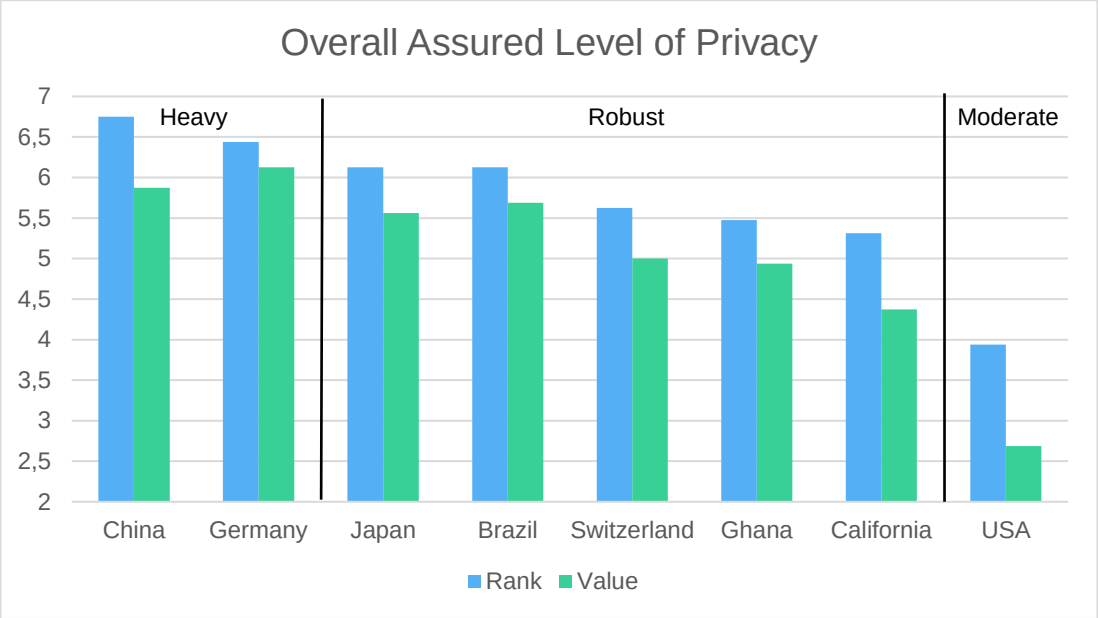

Figure 2: Overall ranking of the assured level of privacy across different jurisdictions

This ranking is led by China, although is has a lower average value score than Germany, in second place. This is because the main instance that causes China to lose average value being the point of cyber surveillance, which is more of a structural deficit of the Chinese system in terms of privacy vis-à-vis the government. On the other hand, Chinese privacy regulation leads in central aspects such as prerequisites of information handling, sensitive information, and transmission of information inlands as well as abroad. Therefore, this ranking stays true to the average ranking being higher than Germany's average ranking.

Similarly, Japan and Brazil score nearly the same ranking: Japan, having the same average ranking, struggles to reach the same average value score as Brazil, which outperforms the Japanese regulation in terms of prerequisites of information handling and internal responsibility management. However, this would not take into account the peculiarity of the Japanese system, which focuses on regulation of subsequent information handling, third party transmissions, and sensitive information. In these categories, the Japanese ranking scores significantly higher than Brazil. As a result, despite the same ranking, Japan ranks slightly higher than Brazil in the overall ranking.

The second half of the ranking poses no such problems: Switzerland is in fifth place at some distance, followed by Ghana and California, and the USA, which is by far in last place.

3.4.2. Overall Self-Determined Level of Privacy

While regulation on assured level of privacy can create a wide range of quantities, the self-determined level of privacy in the examined jurisdiction is rather homogeneous:

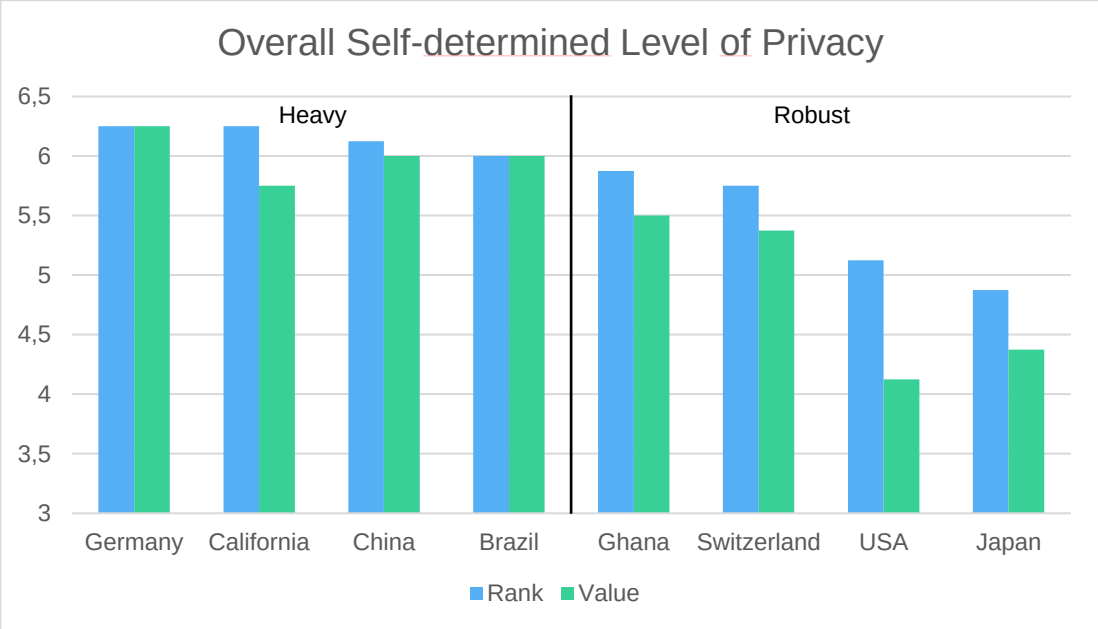

Figure 3: Overall ranking of the self-determined level of privacy across different jurisdictions

This time, Germany unambiguously takes the first place. California is a little off, as it ranks as high as Germany, but scores a significantly lower value than Germany, China, and Brazil. However, one must consider the relative importance of user involvement in the Californian regulation. The categories in which California ranks (and scores) the highest (right to access, deletion, and objection, as well as individual information) are crucial for the Californian notice-and-choice approach[119]. Having this in mind, it seems reasonable to maintain the high overall ranking and place California second, ahead of China and Brazil.

Ghana and Switzerland follow at a relatively short distance, while the USA and Japan are far behind, which comes surprising for Japan, as Japan – unlike their forerunner USA – provides for a dedicated omnibus privacy legislation with their APPI.

[119] The 'notice-and-choice approach' is fundamental for the US as well as Californian privacy law. In its essence it provides for the general rule, that the individual must always be informed of all relevant information handling activities regarding their personal information. With this information, the individual shall also have the possibility to terminate the concerned information handling activity at any times in order to maximize user autonomy. This principle is reflected not only in legislation but also in common law casuistry, and enforcement of competition law. Cf. on the basics of this concept Reidenberg et al., 'Privacy Harms and the Effectiveness of the Notice and Choice Framework' (2015) A Journal of Law and Policy for the Information Society 485, 489 et seqq.; Solove/Hartzog, 'The FTC and the New Common Law of Privacy' (2014) Columbia Law Review 583, 592 et seq.

3.4.3. Overall Ranking of Regulatory Intensities

If combining the average rank and the average value of all examined legal instruments, the Regulatory Clustering produces the following (final) ranking on regulatory intensity:[120]

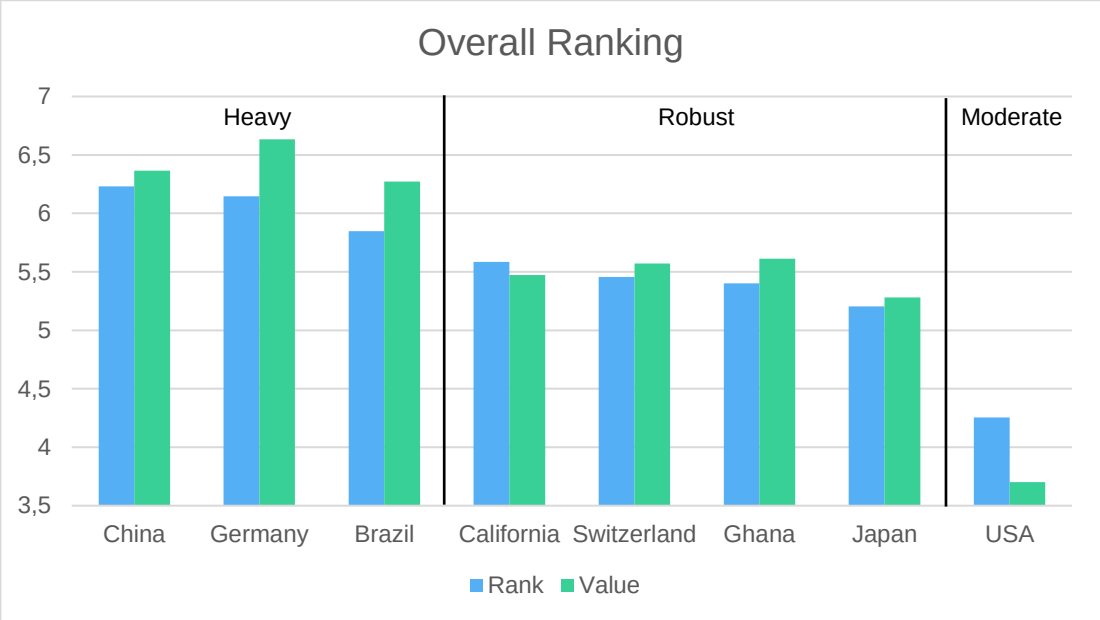

Figure 4: Overall ranking of the examined jurisdictions of privacy

For the same reasons as already above, China ranks very closely ahead of Germany, followed closely by Brazil. The order of California, Switzerland and Ghana is rather difficult to assess, as they all have different rankings and value scores. It has to be judged whether the relative significance of the factor mainly contributing to their respective value score justifies a rearrangement contrary to the ordinal ranking. On this basis, Ghana must be ranked behind the other two, as its critical factor is the registry obligation. While this is a unique method of transparency, similar goals can also be reached by a combination of internal responsibility management and information obligations – both of which are ranked higher in the other two jurisdictions. As for the head-to-head comparison between California and Switzerland, it comes down to the discrepancy between assured level of privacy and self-determined level of privacy: As Swiss regulation is principle-based, it outperforms California in many instruments that implement a level of protection regardless of user involvement. As a result, the autonomy-based approach in California grants the individual greater autonomy than in Switzerland. It is not the intent of the Regulatory Clustering to take a normative stance in favor of either of these approaches, which is why California and Switzerland overall rank the same.

Another big discrepancy between assured level of privacy and self-determined level of privacy exists in Japan, which results in their low placement, only surpassed (again by a lot) by the USA.

---

[120] In calculating the average, the sum of the results of self-determined level of privacy is doubled, since it contains only half as many categories as assured level of privacy in order to give self-determined and assured level of privacy equal significance.

4 Clustering Enforcement Intensities

Having outlined and experimented how the Regulatory Clustering can apply to different regulatory intensities, in the next step an attempt will be made to cluster enforcement intensities. This is of importance because – as already mentioned (→ 2.4.) – regulatory intensities as analyzed above, do only describe the law in the books. Closing the gap between law in action requires further factors.[121] One of them can be the 'efficiency' of enforcement.

This Regulatory Clustering must therefore find a variable that can describe the enforcement intensity to as objectively as possible. This excludes the subjective notion of 'good' or 'effective' enforcement. Nor is it sufficient to assess the degree of behavioral restrictions as has been done with the regulatory intensity: enforcement does not restrict the individual *per se* but is merely a means of ensuring that actual restrictions imposed by substantive law are adhered to. Nevertheless, enforcement activities are in this sense restrictive, as they can 'hurt' the perpetrator.[122] Therefore, enforcement intensity can best be described as the ability of a jurisdiction to act on the perpetrator in a way that is intrusive and thus has negative effects for him. However, since the mere possibilities of enforcement are closer to the theoretical law in the books than to the actual law in action, empirical evidence on the examined possibilities needs to be gathered. Due to the incomparable nature of empirical evidence and possibilities of enforcement, the two sub-categories cannot be accumulated, resulting in a rather fragmented picture which can only vaguely identify the most and least intensive enforcement regimes. However, this picture can still help to understand, how law in the books might be transferred into law in action.

In conclusion to these preliminary remarks, enforcement intensity is even more difficult to assess than regulatory intensity. It can best be done by empirical research.[123] However, this Regulatory Clustering is not based on empirical data (as this is not the goal of it, see above → 2.3/2.4.), which is why this section must remain a vague approximation of an objective standard of theoretical protection.

---

[121] Dotan, 'The Common Real-Life Reference Point Methodology – or 'the Mcdonalds's Index' for Comparative Administrative Law and Regulation', in: Cane et al. (eds.), *The Oxford Handbook of Comparative Law* (2021) 991, 996.

[122] The problem with this definition is, that it cannot be pinpointed, what sanction is 'hurtful' in which situations. A good example of this is the EU, whose enforcement record may indicate that high fines alone may not be sufficient to effectively influence international big tech companies, cf. Bradford, *Digital Empires: The Global Battle to Regulate Technology* (2023), p. 140.

[123] Cf. Greenleaf, *Asian Data Privacy Laws* (2014) p. 66, referencing a foundational work for the European adequacy standard (Bennett/Raab, The Governance of Privacy – Policy Instruments in Global Perspectives (2006)).

4.1. Instruments of Enforcement

4.1.1. Powers of the Supervisory Authority

All of the examined jurisdictions have introduced a supervisory authority alongside their privacy legislation.[124] The USA is the exception because there, the Federal Trade Commission (FTC) which is the general competition supervision is also responsible for privacy protection. Otherwise, privacy supervisory authorities are often also equipped with the responsibility for freedom of information. In terms of duties all of those supervisory authorities are responsible for investigating and remedying violations as well as public information and consultation activities. The respective role of the supervisory authority diverges insofar as there is a more or less tiered procedure before binding orders and sanctions are issued: Regularly, the supervisory authority issues a warning of some sorts before it obliges the information handling entity to take certain organizational steps or refrain from certain activities and issues financial sanctions.[125] Sometimes, such orders do only have binding effect when they are affirmed by court.

4.1.2. Administrative Fines

Financial sanctions can only be imposed on the information handling entity by means of either binding penalty notices of administrative bodies (the supervisory authority) or by judgement of a criminal court (see below). Jurisdictions can often be categorized of following one of these two enforcement approaches. Five of the eight examined jurisdiction follow mainly the approach of imposing administrative fines upon the perpetrator.[126] Such (hypothetical) fines can range from $2.500 per violation in California up to ca. $22.000.000 USD in Germany or 5% of the annual revenue in China.

4.1.3. Penal Sanctions

If a jurisdiction does not rely on their supervisory authority to impose monetary fines, the criminal courts carry the main burden of effectively enforcing privacy legislation. This category is led by such

---

[124] § 1798.199.10 CCPA created the California Privacy Protection Agency (CPPA); Art. 51 GDPR created numerous national supervisory authorities in the EU and Germany; Art. 55-A LGPD created the National Data Protection Authority (ANPD) in Brazil; Art. 1 DPA created the Data Protection Commission (DPC) in Ghana; Art. 130 APPI created the Personal Information Protection Commission (PPC) in Japan, and Art. 43 FADP created the Federal Data Protection and Information Commissioner (FDPIC) in Switzerland. Only China does not have assigned one single supervisory authority, but rather relies on a vast patchwork of governmental supervisory bodies. However, the PIPL speaks of 'departments fulfilling personal information protection duties and responsibilities' and therefore empowers all the relevant authorities.

[125] Such remedial powers can be found in China (Art. 66 PIPL), California (§ 1798.199.55 (a)(1) CCPA, which mirrors the power of the FTC to issue wide ranging cease and desist orders), Germany (Art. 58 II GDPR), and to a lesser extent, following a more cooperative approach Brazil (Art. 52 (§ 6) LGPD), Ghana (Art. 75 DPA), Japan (Art. 148 APPI), and Switzerland (Art. 51 FADP).

[126] Basis for authorization to impose monetary administrative sanctions can be found in California (§ 1798.155 (a), the federal USA (15 USC § 45 (l) and § 56 (a) FTCA), Germany (Art. 83 V and VI GDPR), Brazil (Art. 52 II LGPD), and China (Art. 66 II PIPL). There also is the possibility of imposing a 'civil fine' (which can be interpreted as an administrative sanction by the supervisory authority) of up to (merely) ca. $650 USD, cf. Art. 185 APPI.

countries that declare it a criminal offence to not comply with an order of the supervisory authority.[127] However, every jurisdiction provide for a criminalization of especially malicious privacy violations, which exists as sanctioning regime besides the actual system of enforcing privacy law.

4.1.4. Private Enforcement

Last, but not least, (privacy) legislation can be enforced via private enforcement. This means either via original basis of claims resulting from the privacy legislation[128], general private/tort law[129], and/or collective redress mechanisms[130]. Such mechanisms are more or less equally pronounced in the examined jurisdictions.

4.1.5. Extent of Liability

It is finally of great relevance for the utility of sanctions of whatever nature, to whom they apply. In this regard, there are three categories of jurisdictions: those who directly hold the person behind an information handling entity liable[131], those who hold the information handling entity as corporate body liable[132], and finally those who implement a dual system where either the individual or the entity or both at the same time can be held liable for violations[133].

4.1.6. Further Specifics

While the above-mentioned aspects can be assumed to constitute the core of any enforcement regime, it cannot precisely depict all aspects of enforcement capabilities. Other rather specific and across different legal cultures diverse factors can be accessibility of justice , means of dispute settlements , collective redress mechanisms , or cost shifting . Such factors may have great influence on the actual transition into law in the books but are impossible to quantify properly due to the diversity of potential interactions with non-legal factors.

---

127 Such countries are Japan (Art. 178 APPI), Switzerland (Art. 63 FADP), and Ghana (Art. 80 DPA). Of these countries, Japan provides for the costliest sanction with up to ca. $680.000 USD, cf. Art. 184 I (i) APPI.

128 As is the case in Brazil, cf. Art. 42 LGPD; California, cf. § 1798.150 (a)(1) CCPA (only in cases of data breaches); China, cf. Art. 69 PIPL; Germany, cf. Art. 82 GDPR; Ghana, cf. Art. 43 DPA, and Switzerland, cf. Art. 32 II-IV FADP.

129 As is the case in Japan, cf. Art. 709 of the Japanese Civil Code; and the USA, cf. § 652 Restatement (Second) of Torts.

130 Collective redress mechanisms can be manifold. They can take the appearance of class actions, like in California and the USA, of consumer organizations like in Art. 80 GDPR in Germany, or of collective interest lawsuits (or similar) such as Art. 42 § 3 LGPD in Brazil or public interest litigation in China.

131 An example of such countries that solely rely on personal liability are naturally those who rely on criminal liability only and do not know corporate criminal liability, i.e. Ghana.

132 An example of such countries that hold the legal entity liable are those who mainly rely on administrative sanctions and do not cast separate liability on the individual (i.e. Brazil, California (US), and Germany). Nonetheless individual liability can occur in the rarer cases of criminal prosecution following a privacy violation

133 Such dual systems can be observed in China (implementing dual liability of the corporation and selected individuals behind it, Art. 66 PIPL) and to a lesser extent Japan (exceptionally allowing to additionally fine the organization the perpetrator was acting for in Art. 184 APPI), as well as Switzerland where a criminal corporate liability allows for an alternate liability of the corporation, cf. Art. 102 of the Swiss Penal Code.

4.2. Empirical Evidence

As already mentioned, this should only be a brief classification of the examined jurisdictions as to whether the above outlined possibilities of enforcement are actually practiced, and whether these enforcement practices seem efficient. One should also bear in mind that findings of a 'low' level of intensity could either be the result of high compliance (resulting in no need of excessive enforcement activities) or low popularity/efficiency of enforcement instruments (resulting in a limited use of them) and *vice versa*. This section shall only very briefly look into the question, what aspects could provide for parameters on the basis of which actual enforcement can be further researched.

When it comes to likelihood that privacy legislation is actually adhered to, one should especially look at the activities of the supervisory authority – both in terms of quantity and quality. For example, European supervisory authorities have already amassed around 500 final orders for administrative fines[134], while the Japanese PPC has only engaged in one of such procedures[135] and the Ghanaian DPC has not picked up significant enforcement activities at all[136]. On the other hand, the Japanese PPC is very active when it comes to its consultative function, having issued 217 advice/guidance notices in one year.[137] Activities of supervisory authorities also differ in their value of the dispute: While the highest sanction yet in Brazil has only reached ca. $3.000 USD,[138] authorities in the USA, China and Germany have respectively enacted fines which reach the billions[139]; and in Germany the average fine amounts to ca. §1.900 USD[140]. It should also be considered, how established the different supervisory authorities are within their respective system: While the Ghanaian DPC struggles to set foot on any enforcement activity, the Brazilian ANPD is only slowly developing after being introduced in 2020, and the US FTC does mainly enforce competition law not privacy law, authorities like the European DPCs or the Swiss FDIPC look back on experience of 25 years of activity.

---

134 For an overview of GDPR enforcement activities, cf. CMS, 'GDPR Enforcement Tracker', accessible under https://www.enforcementtracker.com/ (last accessed 11.03.2024).

135 Personal Information Protection Commission Japan, Annual Report 2022 (2023), accessible under https://www.ppc.go.jp/files/pdf/050609_annual_report.pdf (last accessed 11.03.2024).

136 Data Protection Commission Ghana, Public Announcement of July 21, 2023 (2023) accessible under https://www.dataprotection.org.gh/media/attachments/2023/07/24/bnft-publication.pdf (last accessed 11.03.2024).

137 Personal Information Protection Commission Japan, Annual Report 2022 (2023), accessible under https://www.ppc.go.jp/files/pdf/050609_annual_report.pdf (last accessed 11.03.2024).

138 ANPD, Administrative Process No. 00261.000489/2022-62.

139 Cf. for the USA ($5 billion USD) FTC, Facebook, Inc., In the Matter of, accessible under https://www.ftc.gov/legal-library/browse/cases-proceedings/092-3184-182-3109-c-4365-facebook-inc-matter (last accessed 11.03.2024); cf. for China (ca. $1,2 billion USD) BakerMcKenzie, 'Global Data Privacy & Security Handbook: China – Regulators and Enforcement Priorities', accessible under https://resourcehub.bakermckenzie.com/en/resources/data-privacy-security/asia-pacific/china/topics/regulators-and-enforcement-priorities (last accessed 05.12.2023); and cf. for Germany (ca. $1,3 billion USD) DPC Ireland, 'Decision of the Data Protection Commission made pursuant to Section 111 of the Data Protection Act, 2018 and Articles 60 and 65 of the General Data Protection Regulation' March 12, 2023, DPC Inquiry Reference: IN-20-8-1, accessible under https://edpb.europa.eu/system/files/2023-05/final_for_issue_ov_transfers_decision_12-05-23.pdf (last accessed 11.03.2024).

140 Schmid/Esser, 'Numbers and Figures: 5 years of GDPR – what has happened so far, expressed in numbers' accessible under https://cms.law/en/deu/publication/gdpr-enforcement-tracker-report/numbers-and-figures (last accessed 11.03.2024).

Another factor which could indicate how well privacy legislation is known and acted upon are numbers on private enforcement activities and invocation of user rights. For example, Brazil has an exceptionally high quota on litigation that rely on violations of the LGPD.[141] On the contrary, Japanese people are often regarded as less litigious and private enforcement does consequently not play a big role in Japan.[142] For the same reasons, Japanese courts grant only marginal sums as compensation[143], while the practice of class actions and punitive damages in the USA and California result in settlements worth billions[144].

At last, as (privacy) law is a matter that is not exclusively decided by legislation and other sovereign acts, one can consider factors outside immediate privacy legislation.[145] However, as such often extra-judicial factors and their effects are difficult to pinpoint and prove without empirical research and especially impossible to quantify, such factors must remain hypothetical assumptions. Another such factor to be considered could be the rule of law situation, which strengthens the enforcement in China, because a rule by law regime is not bound to the limitations of law, but also weakens the system in Brazil, at it is shaken by corruption. In this category of not quantifiable factors do also fall extra-judicial (alternative) dispute resolution mechanisms, which is most pronounced in Japan, where the enforcement system is strengthened in this regard, that public actors tend to voluntarily admit mistakes and compensate damages.[146]

---

141 Opice Blum, 'LGPD_Lookout: Annual Jurimetrics Report 2022' (2022) accessible under https://opiceblum.com.br/wp-content/uploads/2019/07/09-relatorio-jurimetria-2022.pdf (last accessed 11.03.2024).

142 Hoffmann, 'Data Protection by Definition – Report on the Law of Data Disclosure in Japan' (2022) IRDG Research Paper Series, No. 22-03, pp. 8 and 24. Note, however, that this assumption is a highly disputed one, see for example Yoshida, 'The Reluctant Japanese Litigant – A 'New' Assessment' (2003) Electronic Journal of Contemporary Japanese Studies, no. 5.

143 The highest compensation rewarded has apparently yet reached only ca. $310 USD, cf. Greenleaf/Shimpo, 'The puzzle of Japanese data privacy enforcement' (2014) International Data Privacy Law 139, 145.

144 Very recently, Google has settled a class action worth more than $5 billion USD, cf. Stempel, 'Google settles $5 billion consumer privacy lawsuit' (2023) accessible under https://www.reuters.com/legal/google-settles-5-billion-consumer-privacy-lawsuit-2023-12-28/ (last accessed 11.03.2024).

145 See on the notion of legal pluralism and privacy protection Greenleaf, *Asian Data Privacy Laws* (2014), p. 8; Bennett/Raab, *The Governance of Privacy: Policy Instruments in Global Perspective* (2006), chapters 6 and 7. It delves from the assumption that abstract norms influencing behavior do not always come from legal texts or other sovereign acts, see on this already above, note 4 as well as chapter 2.4.

146 Wang, 'Cooperative Data Privacy: The Japanese Model of Data Privacy and the EU-Japan GDPR Adequacy Agreement' (2020) Harvard Journal of Law & Technology 661, 679.

4.3. Conclusion for Enforcement Intensities

The resulting landscape of privacy enforcement in the analyzed jurisdictions does look something like this:

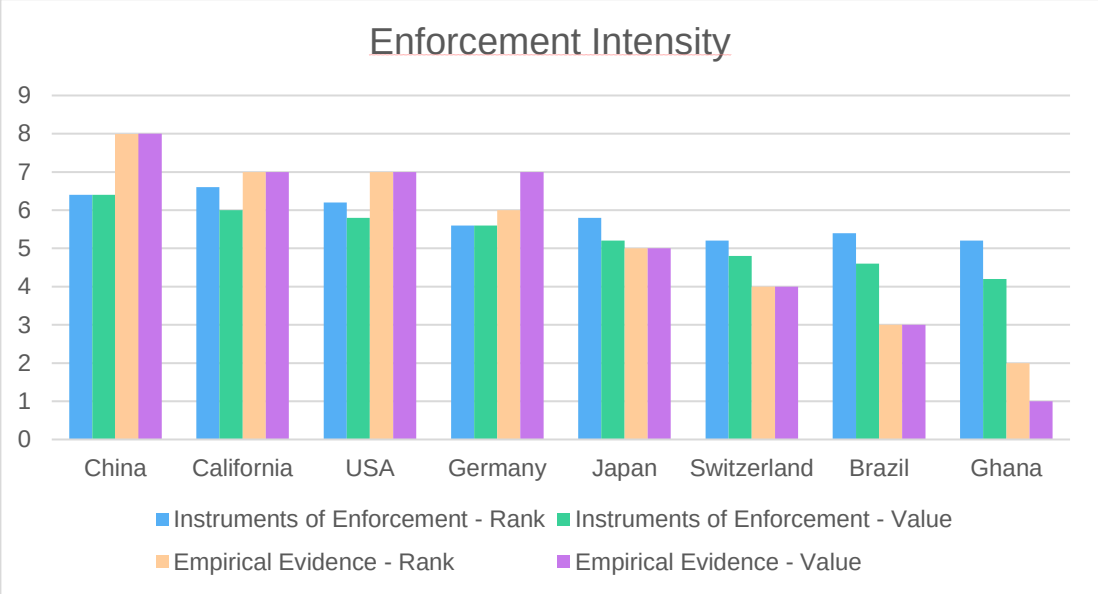

Figure 5: Overall ranking of enforcement intensities

California, the USA, and, above all, China have the most intensive/intrusive enforcement systems, both in terms of theoretical possibilities and actual activities of enforcement. The same is true for Germany, even though it is overall slightly less intensive. Although the Japanese system is slightly better equipped with enforcement instruments than the German system, it lacks actual practical implementation. The remaining jurisdictions, led by Brazil and especially Ghana, show a large discrepancy between what the jurisdiction allows regulators to enforce and what they actually enforce. While the Swiss and Brazilian rankings may be subject to change due to the novelty of both, the ANPD and the revisited FDPIC, Ghana has no so such ‘puppy license’.

5 Country Profiles

After this paper focused on quantification of law, rather than on portrayal of the examined privacy laws, the following chapter shall briefly summarize the key findings for the individual privacy jurisdictions. As such, this chapter will be the main contribution to comparative data privacy law.

5.1. China

China is a cluster in its own right. It is a techno-authoritarian regime that operates a rule by law rather than a rule of law. Therefore, one cannot reasonably expect any certain standard of privacy protection within China, especially vis-à-vis the Chinese government. Nevertheless, the Chinese law provides for extensive protections in the private sector. In fact, China provides for the highest assured and overall level of privacy protection in this ranking: The PIPL imposes severe restrictions

on information handling activities such as collection and sharing of information and alteration of the handling purpose. In many cases, the Chinese law requires the individual's prior consent above all else.[147] This unquestioned primacy of consent tipped the scales in favor of China being ranked first in this Regulatory Clustering. The Chinese system is also very capable of enforcing its strict regulation, as evidenced by its high ranking in both, enforcement possibilities and actual enforcement. Art. 13 PIPL is a good representation of the Chinese system as a whole: It implements a prohibition of information handling subject to permission and specifies on bases for authorization. Interestingly, it includes a variety of descriptions of certain public interests (such as statutory duties and responsibilities, public health, news reporting, or public opinion supervision), but does not include any private interests. Consequently, there is a rather great scope for information handling in favor of the state, but rather limited scope for private purpose information handling. Eventually, it is not clear, whether big tech companies associated with the Chinese state have to abide by such the private sector restrictions, which is why China – in practice – cannot be reasonably put on first place, even though the data in this paper imply so.

5.2. Germany

Unsurprisingly, Germany and the GDPR lead the democratic regimes in this Regulatory Clustering. The main point of criticism on the GDPR has always been that it imposes too much and too uncertain restrictions on the utility of personal data and that it unduly increases the compliance expenses of the controller to an unreasonable extent.[148] This criticism has manifested itself here, as Germany does score a high value rating in nearly every category. It is especially restrictive due to its strict prohibition subject to permission, empowerment of individual information and transparency, and the variety of objective (legal, technical, and organizational) obligations on how to handle collected information. The only notable anomaly is the regulation on third-party transmissions inlands: While other jurisdictions implement specific regulation on third party transfers, seeing them as one of the main privacy concerns, the GDPR does not explicitly differentiate between internal information handling and information sharing. Third party transfers are nonetheless subject to the same (intensive) general regulation on information handling, which can restrict such third-party transfers. Another problem of the German (and in particular European) system is its enforcement dimension: Even though having the most intensive substantial regulation, its enforcement system does not reach the same capabilities as China or the USA (including California) in terms of enforcement instruments and actual enforcement activities. Reasons for this can be found in the complexity of coherence mechanism between the variety of different national supervisory authorities, the uncertainty about

---

147 In Art. 13 PIPL, there is no basis for authorization because of overriding private interest, which gives consent even greater relative relevance than in other GDPR-like jurisdictions. But there are even more explicit scenarios that underline the relevance of prior consent in China: Art. 21 III (a processor entrusting another processor), Art. 23 and 39 (third party transfers), Art. 25 (public disclosure of personal information), Art. 29 (handling sensitive information), and Art. 31 PIPL (handling information of a minor) all require prior consent and all do not provide for exemptions or alternatives to consent.

148 Amongst many Veil, 'Die Datenschutz-Grundverordnung: des Kaisers neue Kleider' (2019) NVwZ 686; Roßnagel, 'Die Evaluation der Datenschutz-Grundverordnung' (2020) MMR 657; Determann, 'California Privacy Law Vectors for Data Disclosures' in Hennemann, von Lewinski, Wawra, Widjaja (eds.), *Data Disclosure – Global Developments and Perspectives* (2023) 121, 141. The other point of criticism is potentially adverse effects on digital competition and innovation, cf. only Gal/Aviv, 'The Competitive Effects of the GDPR' (2020) Journal of Law and Economics 349.

the interpretation of the GDPR, high demand of resources to enforce the regulatory thicket that is the GDPR, and the failure to effectively reach Big Tech companies beyond EU borders.[149]

5.3. Brazil

The LGPD has been heavily inspired and influenced by the GDPR. This is also reflected in its regulatory intensity ranking, which is just below that of Germany. Its substantive regulation, in terms of its intensity, often does not deviate significantly from that of the GDPR. Where the Brazilian legislator deviates negatively from the GDPR standard, it is only a small change in the design of the corresponding GDPR provisions. In many aspects, the LGPD can be described as the 'little brother of the GDPR'. It transplants a regulatory concept from the post-industrial West (the Global North) to a less developed country in the Global South. As a result, such regulation is supposedly inappropriate to the needs and regulatory goals of a developing economy like Brazil's, and it is this uncritical transplantation that is the main point of criticism of the LGPD.[150]

The most apparent manifestation of this unsuccessful transplantation is the incapability to properly enforce the heavy restrictions that Brazil has implemented on a substantive level. While there is potential especially with the comprehensive private enforcement practice[151], this might also hinder proper access to justice, as the Brazilian judiciary struggles to deal with the vast amount of civil actions.[152] The ANPD is unlikely to improve significantly in the immediate future because (a) is has only recently been established and will time to take its place as proper supervisory authority, and (b) there are concerns about its independency as it is part of the federal administration, which itself has been criticized for recurrent corruption and other rule of law issues.[153]

Ultimately, Brazil must first overcome structural problems in terms of rule of law, judicial infrastructure, and confrontation with its own culture on privacy. Until then, the theoretically intensive LGPD loses a lot of its practicability and impact.

5.4. Switzerland

Until very recently, Switzerland followed a very liberal approach to privacy regulation with a regulatory intensity comparable to that of the USA. In an effort to uphold the EU adequacy decision, this rather lax legislation was completely revised in 2023, which has also boosted the regulatory

---

149 Gentile/Lynskey, 'Deficient by Design? The Transnational Enforcement of the GDPR' (2022) International and Comparative Law Quarterly 799; Lancieri, 'Narrowing Data Protection's Enforcement Gap' (2022) Maine Law Review 17.

150 Gadoni Canaan, 'Stimulating Innovation through Personal Data Protection Regulation: Assessing the Replication of GDPR into LGPD' (2022) accessible under https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4154500 (last accessed 11.03.2024).

151 This is especially due to the existence of frequent collective redress mechanisms and a high litigiousness resulting in many civil actions on privacy matters.

152 Zimmermann, 'How Brazilian Judges Undermine the Rule of Law: A Critical Appraisal' (2008) International Trade and Business Law Review 179.

153 Hoffmann, 'LGPD Et Al. – Report on the Law of Data Disclosure in Brazil' (2022) IRDG Research Paper Series, No. 22-06, pp. 1, 3; Erickson, 'Comparative Analysis of the EU's GDPR and Brazil's LGPD: Enforcement Challenges with the LGPD' (2019) Brooklyn Journal of International Law 869, 884 et seqq.

intensity ranking of Switzerland. The main approach to privacy regulation remains a different one than the one of the GDPR: The Swiss abuse legislation[154] generally allows information handling but requires compliance with certain fundamental principles.[155] A violation of such principles would constitute a violation of personality and requires justification. Thus, Swiss privacy law is more rights- than risk-based and allows for a lot more information handling activities than GDPR-like regulation. It should also be noted, that Switzerland tends to implement regulatory easements in favor of free competition on a data driven market, which can be observed in various concern privileges and in particular the justification of personality violations, when the controller handles information for the purpose of their competitiveness.[156] Nonetheless, the new FADP has introduced some comprehensive objective obligations such as internal documentation or individual information along with strong fundamental principles, which places Switzerland's regulatory intensity well in the middle of this ranking.

Interestingly, Switzerland is the only country of the global north that has a notable deficit enforcing its privacy laws. Swiss legal scholars observe that this struggle mainly stems from the practice of refraining from administrative sanctions and relying solemnly on criminal prosecution.[157] This practice refers technically and legally challenging questions on privacy to cantonal criminal prosecution authorities, rather than to the FDPIC which was created precisely to deal with such issues. One can argue that this shortcoming can be compensated by the FDPIC aiding cantonal authorities with such proceedings. But the FDPIC, who is also responsible for freedom of information matters, is under-equipped and does only rarely engage in criminal prosecution matters. This cannot be compensated by private enforcement due to its respective lack of prominence.

5.5. Ghana

At least on a textual level, Ghana has sought inspiration from the EU Data Protection Directive and also partly of the US approach[158]. While the general direction is similar to the GDPR (prohibition subject to permission, great relevance of prior consent, purpose limitation and data minimization as well as some objective requirements post collection), there are some very unique features: As only country to do so, Ghana requires all information handling entities to publicly register with the DPC which can greatly enhance public transparency. That this approach may not be the most functional, however, can be observed in (a) the low compliance rate to this register in Ghana, which has only

---

154 Cf. on this terminology Stark, ''Der Gesetzgeber hat mehr Bürokratie geschaffen'. Interview mit David Rosenthal' (2021) 2, accessible under https://www.computerworld.ch/social/interview/gesetzgeber-buerokratie-geschaffen-2713114.html (last accessed 11.03.2024).

155 These are: Legality, proportionality, purpose limitation, data minimization, correctness, and accuracy, informed and voluntary consent in the individual case, and data security.

156 See Art. 31 II lit. b) FADP, which also includes a concern privilege.

157 Rosenthal, 'Das neue Datenschutzgesetz' (2020) Jusletter 16, p. 70; Sonnenberg/Hoffmann, 'Data Protection Revisited – Report on the Law of Data Disclosure in Switzerland' (2022) IRDG Research Paper Series, No. 22-17, p. 57.

158 At least when it comes to cross-border data transfers and a prominent right to objection which is – unlike to the GDPR – not connected to the legitimacy of information handling.

very recently begun to grow, and (b) the example of Switzerland which has abandoned the very same instrument, because it thought the practical implementation as inefficient.

Other examples for unique regulation approaches are the prohibition to buy and sell information of other individuals, which has great implications for the Ghanaian position on business orientated models like the 'data broker model' and makes Ghana exceptionally restrictive on the commercial aspects of personal information. The DPA does interestingly not differentiate between third party transfers inlands and abroad. It does not rely on data localization, but rather disincentivizes data transfers into Ghana by incorporating foreign law into the own.[159] In the end, Ghana negatively deviates often and at times greatly from the regulatory intensity of the GDPR, which makes it the least intensive of those jurisdictions that are (partly) inspired by European legislation.

This low ranking does only intensify when combined with Ghana's enforcement intensity: Ghana is one of three jurisdictions relying on criminal prosecution instead of administrative sanctions. While a criminal law approach is often considered less effective than the administrative law approach[160], it still has some good arguments on its side (such as particularly tangible sanctions or reliance on more efficient criminal prosecution mechanisms as well as higher standards of justice). Nonetheless, to be able to savor from these advantages, one needs a functional prosecution system. This, in turn, requires extensive activities of a proficient supervisory authority or other entity that brings infringements to the court. The DPC that would be responsible for this, however, has been very inactive in recent times. Until end of 2023, when the DPC announced enforcement activities[161], one could have thought that a supervisory authority and therefore privacy protection law itself, did not exist in Ghana.

5.6. Japan

The Japanese regulation stands out from the rest of the jurisdictions as it provides for a middle ground between liberal free flow of information and preventive risk-based restrictions. While this could also be said about Switzerland, the FADP – in contrast to the APPI – shows a lot of similarities to the GDPR.

Most strikingly, Japan is the only of the examined jurisdiction that scores lower in self-determined level of privacy than in assured level of privacy. Having no special prerequisites of information handling besides purpose limitation, the Japanese system mainly focuses on post-collection regulation. It comprises of three central elements subject to restrictions: change of the original purpose (subsequent information handling), third-party transfers, and handling sensitive information. In all three categories, the APPI stipulates 'heavy' restrictions.[162] The same is true for basic

---

159 Art. 18 II DPA.

160 See above → note 157.

161 Data Protection Commission Ghana, 'Public Announcement of July 21, 2023' (2023) accessible under https://www.dataprotection.org.gh/media/attachments/2023/07/24/bnft-publication.pdf (last accessed 11.03.2024).

162 It is interesting, that the basic regulation in these categories (prior consent which can be refrained from in cases of e.g. statutory obligation, protection of life and property, public wellbeing, or research) are virtually the same throughout all three

principles on information handling (purpose limitation, data minimization, data quality, data security), which all must be adhered to post-collection. While this would provide for a decent level of protection, that would leave out the low degree of user involvement in the APPI: The only notable relevant factor empowering the individual user is the relative importance of consent, which cannot – unlike in most other jurisdictions – be replaced by legitimate private interest. Except the right to rectification, user rights are either narrow or subject to a lot of exemptions. Overall, the APPI reaches a high level of assured and self-determined level of protection (only) in the three categories of subsequent information handling, third party transfers, and sensitive information. This very sectoral protection cannot (in terms of restrictiveness) keep up with the scope of other omnibus privacy laws. Alongside this rather low level of material protection, there also is a rather special system of enforcement. The Japanese system relies on criminal prosecution, which was so far only acted upon once. But this is by no means the central part of the system: Litigation in Japan is not as popular as it is in other examined jurisdictions. Instead, there is a lot of extra-judicial settlement, for example in the form of publicity, voluntary compensation, and cooperative remediation. Such trends can also be observed in privacy contexts: Data Breach Notifications are quite popular, and the PPC is very active in terms of guidance, consultation, and public information. Therefore, even if privacy is not often enforced before a court, it can be expected that voluntary and cooperative non-legal enforcement in Japan can be quite sufficient to implement the APPIs rules into practice.

5.7. USA

One of the most striking observations when looking at the US ranking is probably that it ranks significantly last on a substantive level, but – besides China – first on the enforcement dimension. Indeed, the USA commands great and intrusive authority for law enforcement purposes. The FTC as well as the courts settling class actions do not shy away from imposing tangible, well enforceable sanctions for privacy violations. It even is to be expected that this trend is likely to propel in the future, putting privacy as one of the main tasks for significant US law enforcement activities.[163]

Despite this upward trend on enforcement level, substantive US law on privacy paints a different picture: The US law does only deem certain areas as especially worthy of protection; other areas completely lack any statutory regulation and are left for occasional, insufficient common law practices.[164] The existing statutory law does often target sector-specific problems (such as user control of correctness of credit records in the FCRA, or parental control in the COPPA) and apart from that establishes only minimal privacy principles and a 'notice-and-choice model'[165]. The latter is the only reason, why the USA is not ranked as low concerning self-determined level of privacy. The 'notice-and-choice model' is also manifested in the FTC case law practice of preventing 'unfair and deceptive acts'. It puts user autonomy in the foreground and seeks to enable the users free and informed decision if he does not want his information being handled. Therefore, the main objective of

---

categories, cf. Art. 18 III, 20 II, and 27 APPI. One can argue that the Japanese legislator sees all three of these information handling activities as equally threatening to privacy.

163 Norton Rose Fulbright, 2023 Annual Litigation Trends Survey – Perspectives from Corporate Counsel, pp. 6, 17.

164 At the moment, the US common law body is severely underdeveloped to tackle the challenges of the technically and legally complex matter that is privacy, cf. Citron/Solove, 'Privacy Harms' (2022) Boston University Law Review 793, 862.

165 See on this model already above, → note 120.

the US regulation is to create a rather high self-determined level of privacy by granting post-collection deletion and objection rights, combined with sufficient individual information. However, the high relevance of self-regulatory certification bodies and the common practice of enforcing broken promises might be an indication that the US industry is often not satisfied with the scope of state legislation and intends to apply its own standards. This assessment might change, if the federal legislator is able to pass a federal omnibus privacy law (currently labeled as the Federal Consumer Online Privacy Rights Act (COPRA)[166]). Similar proposed legislation, however, has so far never been successful.

5.8. California

California cannot stand alone besides the federal USA and must be assessed as part of its jurisdiction.[167] As such, California can profit from all the benefits of the US legislation (especially its high enforcement capabilities and sector specific specifications). Even more so, it can add to already pre-existing features, making the Californian system maybe even more intensive/intrusive.[168]

Nonetheless, the true factor of differentiation between federal and state law is the substantive law and the abandonment of sector-specific regulation in favor of omnibus legislation. This should be no normative statement on which of the two approaches is the better one, but the Regulatory Clustering shows, how the two vary in terms of restrictiveness and compliance costs. The CCPA, in its basic approach, pursues the same regulatory objective as the federal law: it seeks to empower individual autonomy over its personal information. Consequently, California ranks (besides Germany) the highest of all examined jurisdictions in terms of self-determined level of privacy. Unlike Germany, the CCPA does not focus on prior consent, but rather on post-collection opt-out. It places a particular prominent role on user involvement, such as providing for easy opt-out modalities and giving the consumer comprehensive information on the individual activity of the controller, as well as on its general business. Virtually, the CCPA does allow a lot of information handling activities as long as the consumer does exactly know of such activities and is always offered the opportunity to opt-out (which is once again the notice-and-choice approach). *Vice versa*, and only consequential, publicly accessible information is subject to the lowest level of protection of all analyzed jurisdictions – especially when the information was disclosed by the individual. Apart from that, the CCPA does only reluctantly implement additional objective obligations on the controller: It now provides for more regulation on data minimization and in general the end of an information's life cycle, but completely lacks provisions, on internal documentation and responsibility, registries, or third-party transfers abroad, which is the reason, why California does still rank low in terms of assured level of privacy.

---

166 Legislative initiative of the 117th Congress (2021 – 2022) – S.3195, accessible under https://www.congress.gov/bill/117th-congress/senate-bill/3195 (last accessed 11.03.2024).

167 Cf. on the parallel system of federal and state privacy laws in the USA Saquella, 'Personal Data Vulnerability: Constitutional Issues with the California Consumer Privacy Act' (2020) Jurimetrics 215, 226 et seq.; Sonnenberg, 'A Regulatory Clustering of Privacy Laws – Extended Version' (2024) IRDG Research Paper Series, No. 24-01, p. 15.

168 A good example would be the fact, that regularly Californian citizens are entitled to a larger compensation in federal class action settlements. It remains to be seen, whether sanctions imposed by the Californian Attorney General and the CPPA do also add intensity to the Californian system.

6 Approximating an Overall Rating

The findings of this paper potentially allow for different clusters to be construed: the originally intended clustering of regulatory intensities puts Germany together with China first, and Brazil only slightly behind them. California, Switzerland, and Ghana provide for very similar intensities, even though they all follow different approaches to privacy regulation. Finally, Japan does not provide for an intensive and comprehensive self-determined level of privacy, thus giving the APPI its low ranking, which is only surpassed by the sector-specific approach of the USA.

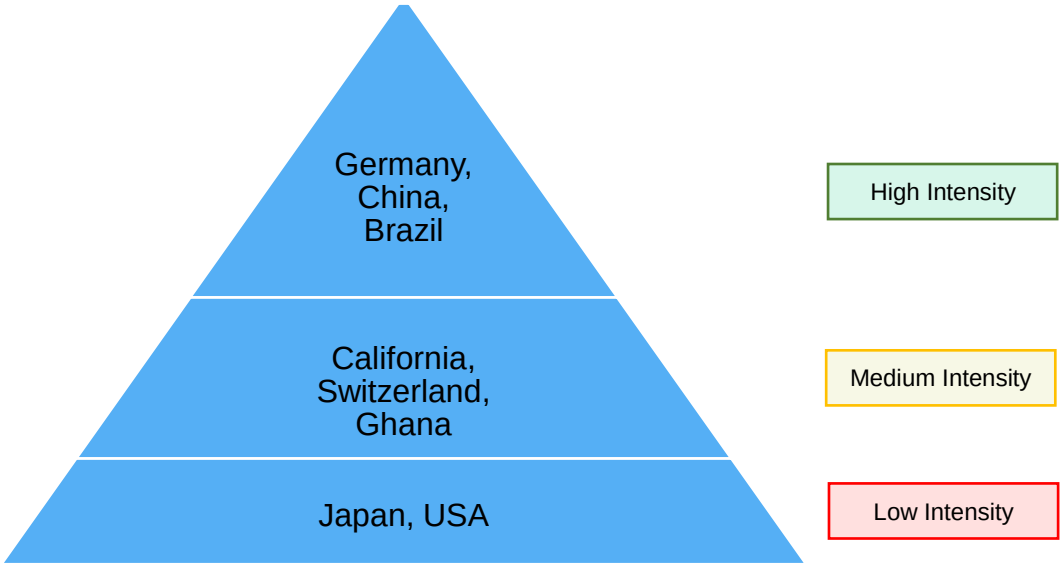

Figure 6: Final clustering of regulatory intensities

However, the additional remarks on enforcement intensities might change this picture: The USA and in particular California seem very capable of enforcing their rather lax substantive law, which might suggest that they are the countries where law in the books and law in action are closest together. On the contrary, Brazil (and to some extent Ghana) with its GDPR-like regulation appears to have very intensive regulation that is, however, implemented in a system of weak or unfitting enforcement. Therefore, the law in action is likely to fall far short of the standard provided for by law in the books. Such 'Enforcement Gap'[169] is also evident in more developed countries such as Germany, Switzerland and even the US.[170] Only China with its techno-authoritarian system, and Japan with its extra-judicial settlement culture might be a little less prone to such systematic enforcement deficiencies (whether judicial or extra-judicial). However, assessing the capabilities and activities of a country's enforcement mechanism in combination with regulatory intensities may offer a more realistic view of the privacy laws of the jurisdictions under review:

[169] Lancieri, 'Narrowing Data Protection's Enforcement Gap' (2022) Maine Law Review 16.

[170] Ibid, pp. 25 et seqq.

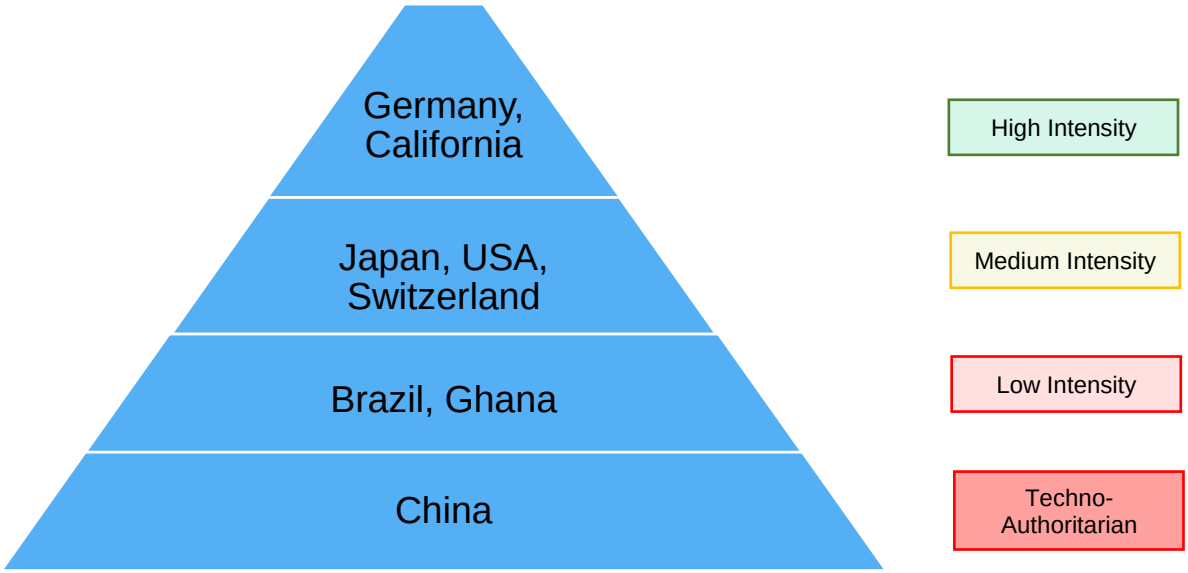

Figure 7: Final clustering of jurisdictions after consideration of the material and enforcement dimension

A Regulatory Clustering may not be limited to a ranking of any sorts. It could also (perhaps more appropriately) describe a set of categories to which different jurisdictions can be assigned. An example would be the clustering of basic approaches to privacy regulation. This would create five distinct clusters, as most jurisdictions have a different, unique touch. China would form a cluster of strict control of information handling activities, enabling such activities for the purpose of greater social good or – if one would put it in maybe more suiting words – state interest. Germany, Brazil, and Ghana would all fall within the same category of intensive risk-based regulation. These jurisdictions minimize threats to privacy through preventive restrictions. Switzerland only partially falls into this category: It has a lot of preventive mechanisms in place, but its main approach to privacy is the principle-based abuse legislation, that does only prohibit the unlawful violation of personality rights by e.g. violating fundamental privacy principles without justification. Another category of its own is Japan, which allows relatively broad collection of information, but restricts post-collection handling activities. The last cluster – let's call it 'autonomy-based' approach – includes the USA and California and describes the basic concept of allowing all handling activities on the one hand but giving the individual comprehensive information and rights to control such information handling activities.

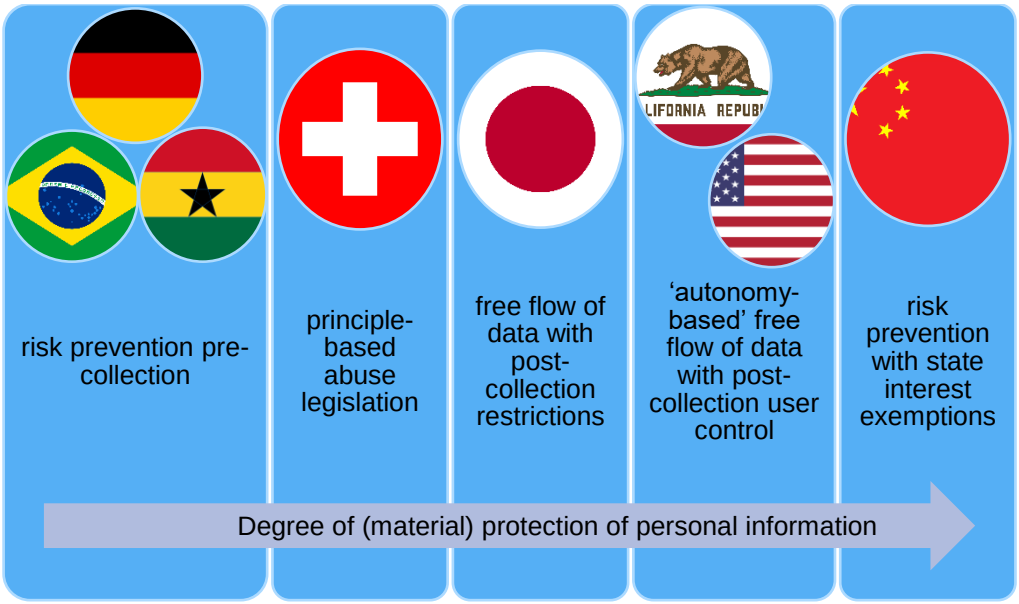

Figure 8: Regulatory approaches to privacy protection

Other clustered variables for which the Regulatory Clustering could be made fruitful might be the proximity of jurisdictions/regulatory approaches to each other[171], economic reference[172], the time at which regulation takes effect[173], or the role of governmental information handling[174].

Ultimately, this Regulatory Clustering shows that different jurisdictions all have their own advantages, disadvantages, approaches, and problems when it comes to privacy. Depending on the variable to be studied, as well as the purpose of the research, the Regulatory Clustering could be a good

---

171 This cluster would be very similar to the aforementioned one: it would target the comparability of the examined jurisdictions and their basic approaches to privacy regulation. Such clustering can be relevant in context of examining the de jure Brussels Effect as Brazil, China, Ghana and naturally Germany all show a very close proximity to the GDPR. To a lesser extent, this is also true for Switzerland. Japan, however, is a little more orientated towards the US/Californian approach: Both rely on generally free flow of information and post-collection regulation. The difference between the two (which would ultimately put them in different clusters) is that in the US the user has the possibility to opt-out at any time, while in Japan, prior consent must be obtained if there is a change in the information handling activity.

172 The definition of such variable could be the degree to which the economic relevance of the information handling activity is taken into account and enables (or restricts) such activities. It therefore would be a high economic reference if commercial handling of information gets incentivized. This is the case in the USA and in particular California with its financial incentive regulation and Switzerland with its competition privileges. The contrary side of this cluster would consist of such jurisdictions that restricts information handling for commercial purposes. Such jurisdictions are China, not providing for a legitimate private interest as basis of authorization (which to some extent would also include Japan), and Ghana prohibiting the sale of someone else's personal information.

173 The definition of such variable could be the main amount of obligations to be adhered to either before the information is collected (this would be e.g. prior consent or security measures, which must be in place by the time, information is collected), and after they would be collected (e.g. subsequent information handling or purpose limitation). Part of the pre-collection cluster would be Brazil, China, Germany, and Ghana, while the post-collection cluster would consist of Japan (due to their focus on subsequent information handling), California and USA (due to their opt-out approach), and somewhat in-between both Switzerland (due to their principle-based approach).

174 The definition of such variable could be the same as the one for regulatory intensity with the difference that it focuses on the restrictions imposed on information handling by public organs. Most of the examined jurisdictions have specific regulation in place for such cases. These regulations were not aspect of this Regulatory Clustering and would need more attentive research.

starting point for interdisciplinary research in the field of legal studies: Despite its frictions with conventional comparative law, building clusters of different jurisdictions may allow for a better cross-cultural comparison of different legal effects. The reader may also see the results of this paper as a starting point, to conduct research on how law in the books is translated into law in action. Perhaps this is also the only contribution a legal scholar can and shall make in answering the question of cultural, social, or behavioral effects of law without crossing the boundaries to other research areas.

7 Embedment in further Interdisciplinary Research

With respect to the underlying research project 'Vectors of Data Disclosure', this Regulatory Clustering *in concreto* helps to assess, classify, and understand the ratings that polled professionals and laypersons have given to their respective jurisdiction.

For example, the relatively low regulatory intensity (and overall ranking) of the federal USA is not reflected in the views of privacy professionals interviewed in the USA, who by majority deem their privacy legislation framework as providing for a sufficient level of protection regarding consumers' data autonomy and fundamental rights and to prevent corporate misuse of consumer data.[175] This contrasts with Japan and Switzerland with a comparable (but nonetheless higher) degree of regulatory intensity, both of which are at the 'low satisfaction' end of the respective scale.[176] Such discrepancies appear across a wide range of items: There is no significant difference between US and German respondents on whether the data protection / privacy regulation is deemed sufficient to protect fundamental right[177], despite being on opposite sides of regulatory intensity scale. Rather, German professionals are significantly less likely than their US counterparts to agree with the statement that data protection/privacy regulation enables consumers to easily manage their privacy settings, despite Germany's higher ranking in the category of self-determined privacy.[178] This suggests, that there are influences on regulatory perceptions outside of the Regulatory Clustering. These influences may stem from cultural parameters or specific behavioral patterns. So to speak, the 'vector' as measured by the Regulatory Clustering does not arrive at the expected destination because another, non-legal parameter has changed in a direction opposite to the one predicted by the Regulatory Clustering. However, there are also some matches between the Regulatory Clustering and other data: For example, Ghanaian and Japanese professionals perceive the privacy enforcement in their country as low, while, with significant difference, Chinese professionals perceive their governmental enforcement to be significantly higher than in more than half of the other countries, which is consistent with the results of this Regulatory Clustering in terms of enforcement

---

175 Wawra/Thir, 'Data Protection and Informational Privacy: Perceptions of Regulations and Practices in Cross-Cultural Comparison' (DeGruyter, in preparation).

176 Ibid.

177 Ibid.

178 Ibid. One could argue that the higher agreement in the USA may solely result from over-regulation in Germany (because the respondents may perceive the German legislation as too restrictive). But this assumption as internationally generalizable finding is *prima facie* disproven by Switzerland and Japan, which both provide for a rather low regulatory intensity ratings (comparable to the USA) and also significantly lower agreement to the positive impact of the regulations' impact on consumers' ability to manage their privacy needs.

intensity.[179] As shown by these examples, the Regulatory Clustering has outlined legal factors on the first level of the 'Law – Behavior Gap Modell'[180] and can now be used in combination with empirical data of the cultural studies and behavioral economics section of the project. Such combination is currently in preparation and will ultimately reflect the overall interdisciplinary outcome of the 'Vectors of Data Disclosure' project.

[179] Ibid.

[180] Cf. on this model above → 2.4.

List of references

Alfaro, L. et al. (2021) Doing Business: External Panel Review. Final Report. https://www.worldbank.org/content/dam/doingBusiness/pdf/db-2021/Final-Report-EPR-Doing-Business.pdf [11.03.2024].

Baker McKenzie. Global Data Privacy and Security Handbook. https://resourcehub.bakermckenzie.com/en/resources/global-data-privacy-and-cybersecurity-handbook [11.03.2024].

Baldus, C. (2015). Gesetzesbindung, Auslegung und Analogie: Grundlagen und Bedeutung des 19. Jahrhunderts. In: Riesenhuber, K. (ed.). Europäische Methodenlehre – Handbuch für Ausbildung und Praxis. Berlin, 22-52.

Bamberger, K.A./Mulligan, D.K. (2015). Privacy on the Ground: Driving Corporate Behavior in the United States and Europe. Cambridge/London.

Bennett, C.J./Raab, C.D. (2006) The Governance of Provacy: Policy Instruments in Global Perspective. Cambridge/London.

Bradford, A. (2020). The Brussels Effect: How the European Union Rules the World. Oxford/New York.

Bradford, A. (2023). Digital Empires: The Global Battle to Regulate Technology. Oxford/New York.

Canaan, R.G. (2022). Stimulating Innovation through Personal Data Protection Regulations: Assessing the Replication of GDPR into LGPD. English Translation. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4154500 [11.03.2024].

Chander, A. et al. (2021). Achieving Privacy: Costs of Compliance and Enforcement of Data Protection Regulation. In: Policy Research Working Paper 9594. https://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=3392&context=facpub [11.03.2024].

Chander, A./Schwartz, P.M. (2023). Privacy and/or Trade. In: The University of Chicago Law Review 90 (1), 49-135.

Chio, K. (2014). Rule of Law or Law by Rule: A Brief Analysis of China's Legal System. In: The International Relations Journal San Francisco State University 33 (Spring), 29-45.

Citron, D.K./Solove, D.J. (2022). Privacy Harms. In: Boston University Law Review 102, 793-863.

CMS. GDPR Enforcement Tracker. https://www.enforcementtracker.com/ [11.03.2024].

Czarnocki, J. et al. (2019). Government access to data in third countries. Final Report. EDPS/2019/02-13. https://www.edpb.europa.eu/system/files/2022-01/legalstudy_on_government_access_0.pdf [11.03.2024].

D'Alberti, M. (2020). Units and Methods of Comparison. In: Cane, P. et al. (eds.). The Oxford Handbook of Comparative Administrative Law. Oxford/New York, 118-136.

Data Protection Commission Ghana (2023). Public Announcement of July 21, 2023. https://www.dataprotection.org.gh/media/attachments/2023/07/24/bnft-publication.pdf [11.03.2024].

Determann, L. (2023). California Privacy Law Vectors of Data Disclosures. In: In: Hennemann, M. et al. (eds.). (2023). Data Disclosure – Global Developments and Perspectives. Berlin, 121-145.

DLA Piper. (2023). Data Protection Laws of the World. https://www.dlapiperdataprotection.com/index.html [11.03.2024].

Dotan Y. (2021). The Common Real-Life Reference Point Methodology – or: 'the Mcdonald's Index' for Comparative Administrative Law and Regulation. In: Cane, P. et al. (eds.). The Oxford Handbook of Comparative Administrative Law. Oxford/New York, 990-1007.

Engeler, M. (2022). Der Konflikt zwischen Datenmarkt und Datenschutz – eine ökonomische Kritik an der Einiwlligung. In: Neue Juristische Woche 74 (47), 3398-3405.

Erickson, A. (2019). Comparative Analysis of the EU's GDPR and Brazil's LGPD: Enforcement Challenges with the LGPD, In: Brooklyn Journal of International Law 44 (2), 859-888.

Gal, M.S./Aviv, O. (2020). The Competitive Effects of the GDPR. In: Journal of Competition Law & Economics 16 (3), 349-391.

Gentile, G./Lynskey, O. (2022). Deficient by Design? The Transnational Enforcement of the GDPR. In: International & Comparative Law Quarterlly 71 (4), 799-830.

Gigerenzer, G./Engel, C. (eds.). (2006). Heuristics and the law. Cambridge/London.

Globe. (2020a). An Overview of the 2004 Study: Understanding the Relationship Between National Culture, Societal Effectiveness and Desirable Leadership Attributes. https://globeproject.com/study_2004_2007%3Fpage_id=data.html#data [11.03.2024].

Globe. (2020b). Country Map. https://globeproject.com/results/#country.https://globeproject.com/study_2004_2007#theory [11.03.2024].

Gorla, G. (1981). Diritto comparator e diritto commune europeo. Milan.

Greenleaf, G. (2014). Asian Data Privacy Laws: Trade and Human Rights Perspectives. Oxford/New York.

Greenleaf, G./Shimpo, F. (2014). The Puzzle of Japanese Data Privacy Enforcement. In: International Data Privacy Law 4 (2), 139-154.

Halperin, J.L. (2011). Law in Books and Law in Action: The Problem of Legal Change. In: Marine Law Review 64 (1), 45-76.

Hennemann, M. (2020). Wettbewerb der Datenschutzrechtsordnungen. In: RabelsZ 84 (4), 864-895.

Hennemann, M. et al. (eds.). (2023). Data Disclosure – Global Developments and Perspectives. Berlin.

Hoffmann, T. (2022a). Data Protection by Definition – Report on the Law of Data Disclosure in Japan. In: IRDG Research Paper Series 22-03. https://www.jura.uni-passau.de/fileadmin/dokumente/fakultaeten/jura/institute/irdg/Research_Paper_Series/Hoffmann_Data_Disclosure_Japan_Data_Protection_by_Definition.pdf [11.03.2024].

Hoffmann, T. (2022b). LGPD Et Al. – Report on the Law of Data Disclosure in Brazil. In: IRDG Research Paper Series 22-06. https://www.jura.uni-passau.de/fileadmin/dokumente/fakultaeten/jura/institute/irdg/Research_Paper_Series/22-06.pdf [11.03.2024].

Hofstede, G. (2011). Dimensionalizing Cultures: The Hofstede Model in Context. In: Online Readings in Psychology and Culture 2 (1).

Hofstede, G. (2022). The Dimensions of National Culture. https://hi.hofstede-insights.com/national-culture [11.03.2024].

Kern, C. (2007). Justice between Simplification and Formalism: A Discussion and Critique of the World Bank sponsored Lex Mundi Project on Efficiency of Civil Procedure. Tübingen.

Kischel, U. (2019). Comparative Law. English ed. Oxford/New York.

Lancieri, F. (2022). Narrowing Data Protection's Enforcement Gap. In: Maine Law Review 74 (1), 16-72.

Linarelli, J. (2019). Behavioural Comparative Law: Its Relevance to Global Commercial Law-Making. In: Akseli. O./Linarelli, J. (eds.). The Future of Commercial Law: Ways Forward for Change and Reform. Oxford/New York. 69-106.

Michaels, R. (2009). Comparative Law by Numbers? – Legal Origins Thesis, Doing Business Reports, and the Silence of Traditional Comparative Law. In: American Journal of Comparative Law 57 (4), 765-796.

Ng, K.H. (2019). Is China a "Rule by Law" Regime?. In: Buffalo Law Review 67 (3), 793-821.

Norton Rose Fulbright (2023). 2023 Annual Litigation Trends Survey – Perspectives from Corporate Counsel. https://www.nortonrosefulbright.com/-/media/files/nrf/nrfweb/knowledge-pdfs/2023-litigation-trends-survey.pdf [11.03.2024].

Opice Blum. (2022). LGPD_Lookout: Annual Jurimetrics Report 2022. https://opiceblum.com.br/wp-content/uploads/2019/07/09-relatorio-jurimetria-2022.pdf [11.03.2024].

Panchenko, V./Beznikova, N./Bulatova, O. (2020). Regulatory Competition in the Digital Economy: New Forms of Protectionism. In: International Economic Policy 32-33 (01-02), 49-78.

Personal Information Protection Commission Japan – PPC (2023b). Annual Report 2022. https://www.ppc.go.jp/files/pdf/050609_annual_report.pdf [11.03.2024].

Personal Information Protection Commission Japan – PPC. (2023a). Guidelines on the Act on the Protection of Personal Information. https://www.ppc.go.jp/personalinfo/legal/guidelines_tsusoku/ [11.03.2024].

Pound, R. (1912). Law in Boos and Law in Action. In: American Law Review 44 (1), 12-36.

Reidenberg, J.R. et al. (2015). Privacy Harms and the Effectiveness of the Notice and Choice Framework. In: I/S: A Journal of Law and Policy 11 (2), 485-524.

Richthammer, M./Widjaja, T. (2023a). Vectors of Data Disclosure – The Information Systems Perspective. In: Hennemann, M. et al. (eds.). (2023). Data Disclosure – Global Developments and Perspectives. Berlin, 35-49.

Richthammer, M./Widjaja, T. (2023b). The Effect of Regulatory Measures on Individual Data Disclosure: A Country Comparison. In: ICIS Research-in-Progress Papers 83.

Ricoeur, P. (1994). Zu einer Hermeneutik des Rechts: Argumentation und Interpretation. In: Deutsche Zeitschrift für Philosophie 42 (3), 375-384.

Röhl, K.F. (2013 [1987]). Rechtssoziologie. Köln.

Rosenthal, D. (2020). Das neue Datenschutzgesetz. In: Jusletter 16. November 2020.

Roßnagel, A. (2020). Die Evaluation der Datenschutz-Grundverordnung: Eine vertane Chance zur Verbesserung der Verordnung. In: Multimedia und Recht 22 (10), 657-661.

Rothschild, J.A. Against Notice and Choice: The Manifest Failure of the Proceduralist Paradigm to Protect Privacy Online (or Anywhere Else). In: Cleveland State Law Review 66 (3), 558-648.

Sacco, R./Rossi, P. (2017). Einführung in die Rechtsvergleichung. 3rd edition. Baden-Baden.

Salaymeh, L./Michaels, R. (2022). Decolonial Comparative Law: A Conceptual Beginning. In: RabelsZ 86 (1), 166-188.

Saquella, A.J. (2020). Personal Data Vulnerability – Constitutional Issues with the California Consumer Privacy Act. In: Jurimetrics 60, 215-245.

Schmid, A./Esser, L. (2023). Numbers and Figures: 5 years of GDPR – what has happened so far, expressed in numbers. https://cms.law/en/deu/publication/gdpr-enforcement-tracker-report/numbers-and-figures [11.03.2024].

Schwartze, A. (2021). Die Rechtsvergleichung. In: Riesenhuber, K. (ed.). Europäische Methodenlehre. 4th edition. Berlin, 73-96.

Siems, M. (2005). Numerical Comparative Law: Do We Need Statistical Evidence in Law in Order to Reduce Complexity. In: Cardonzo Journal of International and Comparative Law 13, 521-540.

Solove, D.J./Hartzog, W. (2014). The FTC and the New Common Law of Privacy. Columbia Law Review 114, 583-676.

Sonnenberg, P. (2024). A Regulatory Clustering of Privacy Laws – Extended Version. IRDG Research Paper Series No. 24-01. https://www.jura.uni-passau.de/fileadmin/dokumente/fakultaeten/jura/institute/irdg/Research_Paper_Series/24_01.pdf [11.03.2024].

Sonnenberg, P./Hoffmann, T. (2022). Data Protection Revisited – Report on the Law of Data Disclosure in Switzerland. In: IRDG Research Paper Series 22-17. https://www.jura.uni-passau.de/fileadmin/dokumente/fakultaeten/jura/institute/irdg/Research_Paper_Series/22_17.pdf [11.03.2024].

Stiftung Datenschutz. (2024). Ergebnisse des Projekts "Vektoren der Datenpreisgabe". Video vom 19.01.2024. https://stiftungdatenschutz.org/veranstaltungen/unsere-veranstaltungen-detailansicht/datentag-preisgabe-von-daten-440#lg=1&slide=1 [11.03.2024].

Swenson, G. (2018). Legal Pluralism in Theory and Practice. In: International Studies Review 20 (3), 438-462.

Tamanaha, B.Z. (2011). The Rule of Law and Legal Pluralism in Development. In: Hague Journal on the Rule of Law 3 (1), 1-17.

The World Bank (2021). World Bank Group to Discontinue Doing Business Report. Statement of 16 September 2021. https://www.worldbank.org/en/news/statement/2021/09/16/world-bank-group-to-discontinue-doing-business-report [11.03.2024].

The World Bank. Doing Business Archive. https://archive.doingbusiness.org/en/doingbusiness [11.03.2024].

The World Bank. Methodology. https://archive.doingbusiness.org/en/methodology [11.03.2024].

Universität Passau (2024). Global Data Law. https://datalaw.uni-passau.de/ [11.03.2024].

Veil, W. (2019). Die Datenschutz-Grundverordnung: des Kaisers neue Kleider. In: Neue Zeitschrift für Verwaltungsrecht 36 (10), 686-696.

von Aswege, H. (2016). Quantifizierung von Verfassungsrecht. Zahlenverwendung im Verfassungsrecht und Zahlengenerierung durch das Bundesverfassungsgericht im Spannungsfeld natur- und geisteswissenschaftlicher Rationalität. Berlin.

von Lewinski, K. (2023). Collision of Data Protection Law Regimes. In: Hennemann, M. et al. (eds.). (2023). Data Disclosure – Global Developments and Perspectives. Berlin, 195-215.

Wang, F.Y. (2020). Cooperative Data Privacy: The Japanese Model of Data Privacy and the EU-Japan GDPR Adequacy Agreement. In: Harvard Journal of Law & Technology 33 (2), 661-691.

Wawra, D./Thir, V. (in preparation). Data Protection and Informational Privacy: Perceptions of Regulations and Practices in Cross-Cultural Comparison. De Gruyter (Berlin).

Whitman, J.Q. (2004). The Two Western Cultures of Privacy: Dignity vs. Liberty. In: The Yale Law Journal 113 (6), 1151-1221.

Yoshida, M. (2003). The Reluctant Japanese Litigant: A 'New' Assessment. In: Electronic Journal of Contemporary Japanese Studies (Discussion Paper 5).

Zimmermann, A. (2008) How Brazilian Judges Undermine the Rule of Law: A Critical Appraisal. In: International Trade and Business Law Review 11, 179-217.