IRDG Institut für das Recht der digitalen Gesellschaft

UNIVERSITY OF PASSAU Faculty of Law

UNIVERSITY OF PASSAU IRDG RESEARCH PAPER SERIES NO. 24-1

A REGULATORY CLUSTERING OF PRIVACY LAWS

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

Peer Sonnenberg

March 2024

Place of Publication

Institute for Law of the Digital Society, University of Passau

c/o Chair of German and European Private Law, Civil Procedure, and Legal Theory

Innstraße 39, 94032 Passau

https://www.jura.uni-passau.de/irdg/

Author

Peer Sonnenberg s a research assistant and doctoral candidate in law at the University of Passau, Chair of Public Law, Media Law and Information Law (Prof. Dr. Kai von Lewinski). His research interests include international and European data protection law with a focus on international data protection law, cross-border data transfer as well as European methodology. He graduated from the University of Passau with a degree in law in 2022.

Abstract

The question of which regulatory concept is the best or most suiting for protecting privacy has initiated regulatory competition between privacy laws around the world that are comparable to a greater or lesser extent. This resulted in a ragged regulatory landscape of privacy and data protection legislation. At the same time, this regulatory competition precedes the scientifically not yet conclusively clarified question of how privacy legislation actually works in practice. What it did provide for, though, is a comprehensive arsenal on legislation that can be made subject to practical research on exactly this question. But before one can compare different effects of different regulation, one must first measure the existing jurisdictions and their peculiarities. Such is the foremost (and maybe only) contribution, a legal scholar can make to this field of research. But as legal studies and comparative law are not very familiar to interdisciplinary and empirical research, such contribution is in need of a methodological starting point that can provide for legally relevant insights and interoperability with other disciplines' empirical research at the same time. To offer such methodological starting point, this paper proposes the concept of a "Regulatory Clustering" as compromise between comparative law and interdisciplinary research. By comparatively analyzing jurisdictions of very dissimilar countries and using a method of quantification of law, this "Regulatory Clustering" tries to offer the definition of an input variable that could also be used in the context of a research model of another discipline. This paper is conducted against the practical background of an interdisciplinary research project of law, behavioral economics, and cultural studies on factors influencing the individual's decision to disclose the own personal information.

Cite as

Sonnenberg, P. (2021). A Regulatory Clustering of Privacy Laws – Extended Version. *University of Passau Institute for Law of the Digital Society Research Paper Series No. 21-01*. https://www.jura.uni-passau.de/irdg/publikationen/research-paper-series.

Keywords

Data protection, privacy, data disclosure, comparative law, comparative law methodology, international law, Brazil, California, China, Germany, Ghana, Switzerland, USA, interdisciplinary research, studies of legal custom and practice.

Contents

A. Regulatory Competition and Regulatory Clustering

In recent times, a hard-fought regulatory competition on data regulation has ensued throughout the world.[1] It encompasses all fields emerging from global digitalization 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.[2] 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"[3]? 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[4] 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.

B. 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

---

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

[2] Universität Passau, Global Data Law, accessible under https://datalaw.uni-passau.de/ (last accessed 04.03.2024).

[3] 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 behaviour, 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.

[4] Art. 45 I GDPR.

of data disclosure processes in conjunction with influences of cultural parameters.[5] To understand the methodology behind the Regulatory Clustering, one must understand the context of it in an interdisciplinary research project and, subsequently, the goal behind such Regulatory Clusters. The underlying project aims to identify – on a meso level – factors that might influence the individual decision-making process behind disclosing one's personal information. To this extent, a "Law – Behavior Gap Model"[6] was 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 depict such a "perception gap", the regulation to be perceived must 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 sets of data, the model takes data of eight different jurisdictions into account, which requires eight different categories as objects of comparison. In other words, eight different legal orders shall be described and ranked in relation to (only) each other. Thus, the research objective moves away from classic findings of comparative law – namely being 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[7] – and moves more in a rather untechnical direction of "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 just by looking at written regulation.[8] Rather, comparing law does not mean to place legal orders 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 respective country.[9] Whenever addressing foreign law in relation to the own or other foreign law, the research should be conducted without biases or should not reflect personal values of the researcher into foreign jurisdictions. The Regulatory Clustering, however, does exactly this: it ultimately puts different legal orders in an ordinal ranking to each other, defining one as "higher" as the other.

---

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

[6] This model, which currently goes by a working title, was already presented at the DatenTag in Berlin, cf. *Stiftung Datenschutz*, Ergebnisse des Projekts „Vektoren der Datenpreisgabe" (19.01.2024), accessible under https://stiftung-datenschutz.org/veranstaltungen/unsere-veranstaltungen-detailansicht/datentag-preisgabe-von-daten-440#lg=1&slide=1 (last accessed 04.03.2024). See on the basics of the underlying regulatory perception research *Richthammer/Widjaja*, The Effect of Regulatory Measures on Individual Data Disclosure: A Country Comparison, ECIS Research-in-Progress Papers (2023) 83.

[7] *Kischel*, Comparative Law (2019), pp. 45 et seqq.; Schwartze, in: Riesenhuber (ed.), Europäische Methodenlehre, Die Rechtsvergleichung (2021), pp. 73 – 96, N 3; *Sacco/Rossi*, Einführung in die Rechtsvergleichung (third edition 2001), Erstes Kapitel, § 1, N 59, 84 et seqq.

[8] *Kischel*, Comparative Law (2019), pp. 48 et seqq.; *Salaymeh/Michaels*, Decolonial Comparative Law: A Conceptual Beginning, RabelsZ (2020), p. 166, 172.

[9] *Sacco/Rossi*, Einführung in die Rechtsvergleichung (third edition 2001) Erstes Kapitel, § 1, N 12 et seqq.

This Regulatory Clustering is not unmatched in theory and practice: it draws inspiration from the "Doing Business Reports" of the world bank,[10] which were subject to comprehensive criticism from its conceptual beginning in 2004[11] until they discontinued due to data irregularities and methodological flaws.[12] 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", similarly to the goal of a Regulatory Clustering, created an ordinal ranking of countries based on especially law and regulation.[13] The found ranking shall 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 leading to its discontinuation were insufficient understanding of law[14], 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) leads to better development outcomes.[15] Against this background of criticism, the Regulatory Clustering might prosper: Its found variables shall not give raise to stakeholder recommendations or make economic statements; it, rather, makes an offer – in knowledge of its conceptional 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. Still, legal concerns remain (and must be kept in mind) in regards of objectivity, quantification without unverifiable value judgement, delimitation of *de jure* and *de facto* regulation, contextualization of written law, or biases.[16]

I. 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, one must bear in mind, that the main goal is not the comparison of legal orders in a normative sense, that allows deeper understanding of corresponding and diverging legal principles, but rather in an empirical sense, that allows quantification and research on correlation with cultural variables or factors of behavioral economics. To achieve this in the most objective way possible, the sought after variables must be precisely defined and the examined regulatory instruments must present a comprehensive picture of the research subject. The latter leads to yet another clash with typical comparative law

---

[10] *The World Bank*, 'Doing Business Archive', accessible under https://archive.doingbusiness.org/en/doingbusiness, (last accessed 04.03.2024).

[11] *Salaymeh/Michaels*, Decolonial Comparative Law: A Conceptual Beginning, RabelsZ (2020), p. 166, 172; *Michaels*, Comparative Law by Numbers? – Legal Origins Thesis, Doing Business Reports, and the Silence of Traditional Comparative Law, 57 American Journal of Comparative Law, 765–795 (2009).

[12] *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 04.03.2024).

[13] See for an overview, *The World Bank*, Methodology, accessible under https://archive.doingbusiness.org/en/methodology (last accessed 04.03.2024). Note, that these reports included the wider definition of "regulation" (N 3).

[14] *Michaels*, Comparative Law by Numbers? – Legal Origins Thesis, Doing Business Reports, and the Silence of Traditional Comparative Law, 57 American Journal of Comparative Law, 765–795 (2009), p. 773.

[15] *Alfaro et al.,* Doing Business: External Panel Review. Final Report (2021).

[16] 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, 13 Cardonzo Journal of International and Comparative Law 521 (2005).

methodology: Comparative law research is conducted doctrinal, functional and contextual.[17] In regards to the Regulatory Clustering, this means that the comparison of legal orders should not only examine similar rules, but also address problems which could be solved by various instruments as functional equivalent, and maybe even more relevant, put the compared instruments into context with especially societal and cultural circumstances of the regulated matter. This contextuality stands in direct contrast to the goal of deducting quantifiable variables from different legal orders: Functional and contextual comparison would mean to draft an overly complex system of legal and non-legal peculiarities 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, because the Regulatory Clustering aims to make legal realities tangible for cultural studies and behavioral economics, so that these disciplines can find the very co-dependencies that contextual comparative law presupposes.

The choice of the right regulatory instruments to be examined in the different legal orders as object for comparison imposes the first challenge for the Regulatory Clustering. The factors shall be on one hand 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 examined instruments must reflect the diversity and uniqueness of the respective legal order and not impose a biased view on foreign regulation, which can be rather akin to the basic legal understanding of the conducting researcher. Because in this scenario, the overall research subject 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 a Regulatory Clustering. If one would instruct solemnly legal scholars with this choice, it would be likely that the choice falls on a rather broad mixture of instruments, which is understandable before the aforementioned background that contextual comparative law should be conducted in a holistic manner, taking as many contextually relevant legislations as possible into account. This again, would undermine the utility of the Regulatory Clustering as instrument of interdisciplinary research on law as a quantifiable factor.

Therefore, the basis of the choice of regulatory instruments to be examined lies in a taxonomy to categorize data protection legislation developed for this sole purpose in cooperation of legal and behavioral economics researchers.[18] This taxonomy builds on the assumption that regulatory perception can be modeled by mainly[19] two categories of (data protection and privacy) law: The first category is the set of regulation that promise an objective standard of protection, which all entities must adhere to. The mere existence of such regulation might ensure the data subject, that their personal data is *de jure* already sufficiently protected. They do not need to involve themselves in adjusting the level of protection of his personal information. This category is called "assured level

---

[17] *Salaymeh/Michaels,* Decolonial Comparative Law: A Conceptual Beginning, RabelsZ (2020), p. 166, 170; *Kischel,* Rechtsvergleichung (2015), pp 164 et seqq.

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

[19] 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 below → F.

of privacy".[20] The other category includes such regulation that empowers the individual to adjust and co-determine the level of protection of their personal information. This category is called "self-determined level of privacy".[21] The differentiation criterium 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[22] instruments, that ensure privacy without user involvement and a group of eight[23] instruments involving the individual's decision in the level of granted privacy. One regulatory instrument is defined throughout all examined jurisdiction by the problems it addresses and the purposes it aims to achieve, thus implementing a functional approach.

However, such definition imposes great epistemological difficulties. It may be – involuntarily – dependent on the origin and affiliations of the conducting researcher. Preceding epistemology, there is an undeniable informational gap in any area of comparative law[24]: Naturally, technical burdens such as language, including correct translation of legal terms, and accessibility of legal sources and secondary literature, as well as factual burdens, such as a deep understanding of the functioning of foreign law or contexts of regulatory choices, automatically affects any comparative research. And as far as epistemology itself is concerned, the assessment of critical factors and objectives of research will be determined by the researcher's decision. They and their research may therefore be in particular danger of cognitive distortions.[25] 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 was educated 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[26] at least in this regard 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 danger of confirmation bias may negatively influence the interpretation of different regulation,

---

[20] *Richthammer/Widjaja,* ´The Behavioural Economics Perspective´, in: Hennemann, von Lewinski, Wawra, Widjaja (eds.), Data Disclosure, Vectors of Data Disclosure (2023).

[21] Ibid.

[22] 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.

[23] 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.

[24] *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), p. 991, 994.

[25] 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), pp. 69, 102 et seqq.

[26] *Bradford,* The Brussels Effect (2019).

concepts and functions in favor of a GDPR-bias. Further optimization of the methodology may therefore include the consultation of legally competent locals.

II. 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 under which the instruments will be compared and to create a scale for the resulting ranking. This question imposes three fundamental dogmatical problems: (a) it is quasi an impossibility to quantify law and measure it as an absolute value which can then be compared to other law; (b) even if a ranking can be found within a variable, the question remains how the ranking can be scaled so that differences between legal orders can be classified; and (c) how can an objective assessment be guaranteed, although different legal approaches can be based on different concepts, values and policy goals?

All three problems arise from the fundamental recognition that law is a value-based concept and such concepts can to a very limited extent only be described and depicted with empirical data and figures.[27] There are many possible variables and even more definitions for them. The impossibility of quantification of law can only be sufficiently addressed when the methodology of the Regulatory Clustering is consistent in itself. The Regulatory Clustering can therefore only reach its purpose if a precise definition is put forward and there is strict adherence to this definition and its inner logics.

Having in mind the interdisciplinary research question the Regulatory Clustering is embedded in,[28] the variables have to take into account that the existence and the design of the respective regulatory instrument might have influence on their perception and, therefore, might raise the individuals psychological comfort or might lower privacy concerns because they (perceive that they) can rely on either assured or self-determined privacy regulation. According to this, the question at hand is, to what extent the examined regulatory instruments promise an efficient protection of individual privacy. The term "efficiency" is loaded with the value judgement of what is deemed "efficient protection of privacy". While some may argue that efficiency comes with the restriction of processing methods, others may argue that efficient privacy protection regulation means to balance individual protection interests with economic and societal utility of personal information.[29] Thusly, "efficiency" allows for too much subjectivity and cannot precisely define a coherent variable. It would be more objective – without taking side with one or the other approach – to assess regulatory instruments on the basis of how much it restricts processing activities: Even though this may yet again constitute a certain GDPR-bias (which follows precisely this approach) [30], it does and shall

---

[27] *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), p. 991, 997.

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

[29] 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, Yale Law Journal (2003) p. 1151.

[30] 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, RabelsZ (2020), p. 166, 172; *Michaels*, Comparative Law by Numbers? – Legal Origins Thesis, Doing Business Reports, and the Silence of Traditional Comparative Law, 57

not pass judgement on whether it is the "right" approach to privacy regulation. Given that individual privacy – without regard to other beneficial factors (for the self and the society) – is most dominantly protected, if handling personal information is not allowed at all,[31] 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[32]. This degree could be broadly defined as the quantity of legally possible handling activities after applying the regulatory instrument. More precisely, this must also include such regulatory instruments that do not directly restrict the handling activity itself but oblige the controller to fulfill certain criteria in connection to the information handling. In these situations, the cost of compliance[33] can serve as a benchmark for the degree of restriction. Altogether, this would constitute the variable of "regulatory intensity". This variable shall be the main connecting point for the Regulatory Clustering forthwith.

The Regulatory Clustering is also useful for identifying other potential variables for further research. In this regard, it could be interesting – having the assumed "Brussels Effect"[34] in mind – to look at the "proximity to the GDPR". Proximity can mean for example the number of regulatory instruments which are similar to the GDPR, provided that the GDPR (or Data Protection Directive) predates them and the degree of such similarities. This particular quantification might address the question, whether the existence of legal transplants (which are per definition akin to the legal order and might collide with preexistent legal concepts and values)[35] has a negative impact on the perception of the transplant. For the purpose of this particular "Privacy Regulatory Clustering", the "regulatory density" can also be an interesting variable to be quantified. This could be the number of factual situations which the regulation not only addresses via general clauses or similar stipulations, but also specifically by implementing rules according to the peculiarity of the individual case. Of course, these are not the only variables a Regulatory Clustering could help research with. Rather, it can – once conducted – quantify jurisdictions in many other regards, not limited to the categories and variables identified here, nor to the discipline of privacy law or the research goal of interdisciplinary behavioral analysis.

III. An ordinal ranking system

Whilst these definitions open the possibility for a ranking on a micro level (by defining one regulatory instrument as more or less intensive than another comparable instrument from a different jurisdiction), other problems remain unaddressed. This becomes especially clear when trying to generate an overall ranking via combination of the various individual rankings. Comparing two legal orders as such shall take all factual and legal circumstances into account and subsequently

American Journal of Comparative Law, 765–795 (2009). The Regulatory Clustering must bear this weakness in mind whenever possible and suitable.

[31] 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.

[32] Such entity shall forthwith be named "controller" or, if they handle the information on behalf of another person and this differentiation becomes necessary "processor".

[33] 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, Policy Research Working Paper 9594 (2021), pp. 9 et seqq.

[34] *Bradford,* The Brussels Effect (2019).

[35] *Watson,* Legal Transplants (1993); see also on legal transplants in data protection law *Hennemann,* Wettbewerb der Rechtsordnungen, RabelsZ (2020), p. 864, 890.

create a holistic view on the two compared legal orders:[36] For example, while some legal orders might rely on restrictions of data collection, others might rely on restrictions of subsequent information handling; while some might rely on criminal law and prosecution, others might rely on private law and litigation; while some might rely on a variety of objective obligations, others might rely on a strong oversight and enforcement system. 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 legal orders must be interpreted as sum of restrictions and expected compliance-costs imposed (or expectedly imposed) on the controller.

However, this leaves the problem of comparability of individual regulatory instruments both within their category and in their entirety with other categories unaddressed: It is hard to draw a consistent line between two regulatory instruments within the same category, declaring one as more intensive than the other. Whilst this can 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 a lot more difficult to assess, for example, when two very different approaches address the same problem and reach regulatory goals with comparable intensity by use of very different means.

Usually, at this point, quantification and delimitation requires either empirical or mathematical data. The law cannot provide either with its aspects of a heuristic[37], and to this end hermeneutically inclined[38], discipline. To conduct empirical research on this topic would require to define the perception of legal norms, which is the epistemic goal that this Regulatory Clustering inevitably precedes. Using empirical data for this Regulatory Clustering would be circular. The Regulatory Clustering must therefore find a solution to describe regulatory instruments as mathematical value. It must constitute the basis which can confer meaning to empirical data. To pick up the aforementioned problem to describe a value-based concept with quantifiable numbers, it seems impossible to assign a value to a single instrument which can then line up with other values of the other jurisdictions to form a cardinal scale.[39] To prevent an assignment of mathematical value to moral value, the use of an ordinal scale[40] is most promising. It enables the legal scholar to put jurisdictions and their regulatory instruments in proportion to each other without assigning a concrete mathematical value to it. Still (and there is no way around this), some specific cases must rely on individual (normative) analysis for delimitation.

---

[36] *Von Lewinski,* 'Data Disclosure, Collision of Data Protection Law Regimes ', in: Hennemann, von Lewinski, Wawra, Widjaja (eds.), pp. 197 – 214 (2023), p. 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, The MIT Press (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.; *Ricoer,* Zu einer Hermeneutik des Rechts: Argumentation und Interpretation, Deutsche Zeitschrift für Philosophie 42 (1994), pp. 3, 375 – 384.

[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.

The biggest problem with an ordinal scale remains the combination 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 prominence or their intensity in relation to other instruments or aspects of the same jurisdiction. Thus, calculating an overall rating through the average of an individual rating runs the risk that this ranking provides a picture of the law that is correct in its details but wrong from a general, holistic perspective. To create an overall ranking means to carefully consider the individual relevancy for the respective jurisdiction. Therefore, an overall rating could roughly rely on the basis of a Regulatory Clustering, but still requires attentive legal (normative) analysis.

Following the goal of contributing to interdisciplinary research, the overall ranking of the Regulatory Clustering can be simplified[41] by sorting the examined legal orders in 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 within 0 and 8 to the individual ordinal ranking.[44] The assignment of a value can also help to absorb distortions in an average ordinal ranking. Such distortions can arise from significant normative gaps between two ordinal rankings. This categorization would achieve – to the least – that cardinal differences within one category of regulatory instruments can be put into relation to differences within other, equally generalized variables of other disciplines such as cultural studies (for example cultural dimensions[45]), or behavioral economics (for example regulatory perception[46]). The auxiliary implementation of a cardinal value score would put more context to an overall average ranking and raise awareness for relevant misrepresentations of the ordinal rankings.

IV. Law in the books vs. law in action

The variable "regulatory intensity" as defined above only includes the restrictions and compliance costs that are possible and as such enforceable under the given law. The Regulatory Clustering of regulatory intensity in the described extent does not look at the actual enforcement of the investigated regulation. If that was the case, it has to define "regulatory intensity" as restrictions and

---

[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), pp. 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?t=world-map&c=AL, (last accessed 04.03.2024), 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.

[45] *Hofstede*, 'Dimensionalizing Cultures: The Hofstede Model in Context' (2011) 2(1) Online Readings in Psychology and Culture; *Hofstede*, 'The Dimensions of National Culture' (2022), accessible under https://hi.hofstede-insights.com/national-culture, (last accessed 04.03.2024); *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 04.03.2024).

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

compliance costs, that the information handling entity actually adheres to. This definition would only be congruent with the definition applied above[47] in a utopian idea of society where abstract law is automatically applied and adhered to by the individual on a micro level (*homo juridicus*). Under actual circumstances 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 create a practical effect to law. This divergence of 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 fundament of law in the books which then must be implemented in practice as law in action. Only and only then, one can measure regulatory perception. Demonstrating differences between law in the books (what shall be), law in action (what is) and regulatory perception (how does the addressee perceive law) can help to outline efficiencies of different regulatory and factual approaches to the matter subject to research – which in this particular case is the influence of privacy regulation on individual decision-making.

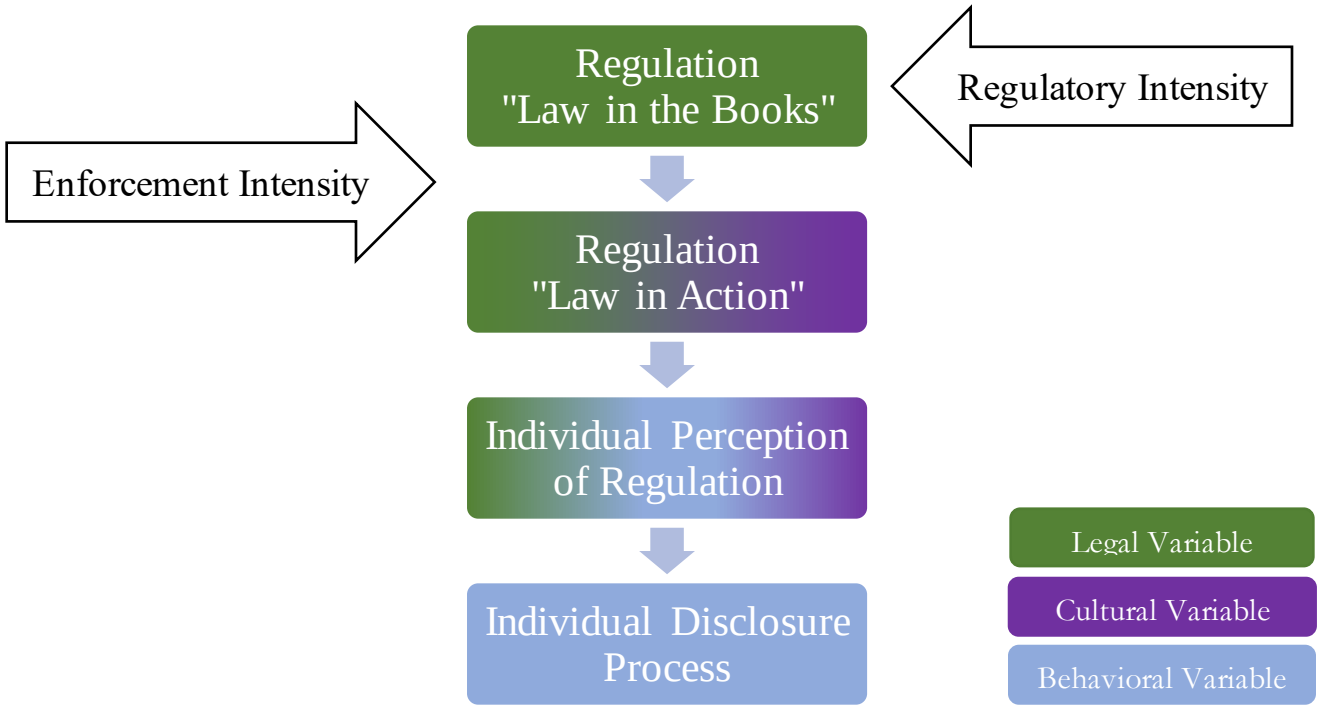

Figure 1: Classification of the Regulatory Clustering within a Law - Behavior Gap Model

However, this would require a definition and a method of measurement for law in action which constitutes one, if not the, main hurdle of regulatory perception research from a legal point of view. All the same, traditional methods of (comparative) law cannot sufficiently address this problem:

---

[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 → II.

[48] See fundamentally *Pound,* Law in books and law in action, 44 American Law Review (1910), pp. 12 – 36; *Sacco/Rossi,* Einführung in die Rechtsvergleichung (third edition 2001) Erstes Kapitel, § 1, N 67; for a more modern understanding *Halperin,* Law in Books and Law in Action: The Problem of Legal Change, 64 Maine Law Review (2011-2012), pp. 45 – 76; 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.

Fundamental scholars of comparative law deem "law in the books" as no law at all, because it is only fictional and does not depict reality.[49] According to this interpretation, comparative law shall never take into account the law in the books. Consequently, comparative law means comparison of law in action. Not to be mistaken, this shall be the foremost goal of comparative law, because only law in action grants insights in different legal realities. Nonetheless, law in action remains a complex concept which legal studies on its own cannot sufficiently describe. The actual impact of law arises from a multitude of interactions of a wide range of factors, both within and outside the law.[50] "Pure" comparative legal analysis can subsequently only be one of many cooperating instruments to measure law in action. Most probably, measurement would require empirical research.

Nonetheless, this Regulatory Clustering is not based on such empirical research, but rather on descriptive comparative law and its quantification. It follows another reasoning, that law in the books is in fact law from an objective point of view; it forms one necessary variable which ultimately integrates in combination with other non-legal variables into law in action.

To this end, it could also try to approach a law in action variable. The main regulatory instruments, which can be implemented to ensure congruence between law in the books and law in action are such (legal and factual) instruments connected 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 adheres to abstract rules.[51] Thus, the Regulatory Clustering can introduce a third[52] category of regulatory instruments: measures of enforcement. The variable "regulatory intensity" as defined above, however, appears not suitable to quantify such enforcement measures: Enforcement itself does not require the information handling entity to restrict its handling activities or to raise its compliance costs. Rather, it aims to force compliance upon the addressee, notwithstanding the content or nature of the enforced rules. Having in mind, that such enforcement measures could build a bridge between law in the books and law in action, a benchmark should be centered around 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 into the quantity and quality of legally possible measures helping with the translation from 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 significant approach to law in action requires research on how often and how intense the legally possible enforcement measures are used in practice and how such enforcement practices are perceived by the addressees of the enforced material law.[53]

---

[49] Fundamentally *Gorla,* Diritto comparator e diritto commune europeo (1981), pp. 303 – 306, 361; see also *Sacco/Rossi,* Einführung in die Rechtsvergleichung (third edition 2001) Erstes Kapitel, § 1, N 67.

[50] *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), p. 991, 996.

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

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

[53] See for a brief attempt to narrow such approach down below → D.II.

This would draw a connection between law in action and regulatory perception and might 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).

V. Jurisdictions subject to research

Having outlined the methodology, goals, categories and definitions of the Regulatory Clustering, the only aspect missing are the concrete jurisdictions to be compared. The examined jurisdictions are the ones of Germany (EU)[54], Switzerland[55], USA[56], California[57], Brazil[58], Ghana[59], Japan[60], and China[61]. These countries represent a great diversity in economic relevance, legal concepts, social and cultural structures and governmental organization. They spread throughout the "global north" as well as the "global south" in a political understanding,[62] 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. The examined jurisdictions as well as the reason of their inclusion shall now be briefly introduced.

1. Germany

Often referred to as the "Gold Standard of Data Protection"[63], the GDPR must be a relevant factor in the discussion of any data protection or privacy regulation. Its extraterritorial reach and overall influence on international politics[64] makes it inevitable to consider compatibility and frictions with the GDPR. Germany – together with the USA and Japan – represents the Global North and global economic superpowers in this Regulatory Clustering.

As the GDPR is a regulation of the European Union, it is applicable for all its member states. However, the member states are granted leeway to specify on the GDPR in certain aspects with own legislation. As this Regulatory Clustering is embedded in *inter alia* cross-cultural research, it refrains from addressing the European Union as one jurisdiction, but rather focuses on German law, which is mostly synonymous to the GDPR with the addition of the federal Data Protection

---

[54] 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).

[55] The main legal source is the Federal Act on Data Protection of 2023 (FADP).

[56] Legal sources can be found in various sector-specific statutory law, as well as in common law practices, see on this again below.

[57] The main legal source is the California Consumer Privacy Act of 2020 (CCPA) as amended by the California Privacy Rights Act of 2023 (CPRA).

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

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

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

[61] 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).

[62] Cf. comprehensively *Salaymeh/Michael,* Decolonial Comparative Law: A Conceptual Beginning, RabelsZ (2020), p. 166; in another context but with the same conception *Chander/Schwartz,* Privacy and/or Trade, 90 The University of Chicago Law Review 1 (2023) 49 – 135, pp. 105 et seqq.

[63] *Mantelero,* The Future of Data Protection: Gold Standard vs. Global Standard (2020); *Buttarelli,* The EU GDPR as a clarion call for a new global digital gold standard, 1 April 2016, accessible under https://edps.europa.eu/press-publications/press-news/blog/eu-gdpr-clarion-call-new-global-digital-gold-standard_en (last accessed 04.03.2024).

[64] Often described as the "Brussels Effect", *Bradford,* The Brussels Effect (2019).

Act and various other specific federal legislation. However, the concrete interpretation and implementation of the GDPR within different member states can vary[65], which is why one cannot directly induce an overall European GDPR practice from a German GDPR practice. While the implementation of the GDPR has achieved a lot of convergence in the law in the books of the member states, this is not true for the respective law in action.

2. Switzerland

In this analysis, Switzerland represents the only continental European jurisdiction, which is not part of the European Union and therefore not subject to EU law. With entering into force in 1992, Switzerland provides for one of the oldest comprehensive privacy legislations around the world with the Federal Act on Data Protection. However, provisions of this legislation were considered rather lax, and, eventually, Switzerland gave in to the economic and political pressure from the EU border to completely revise the FADP which entered into force in 2023.[66] That is only one of many examples of "autonomous implementation" – the process of adjusting the own legislation according to developments in the European single market and its legislation.

Naturally, comparative law would focus on depicting and analyzing the new and current law of a country. However, the Regulatory Clustering is embedded in interdisciplinary research of regulatory perception. An overhauled legislative act imposes a problem for empiric research, because one cannot expect from an average respondent, that his perception of law is always up to date. For this reason, the original Regulatory Clustering takes both – the old and the new FADP – into account. However, it would be counterproductive for the purpose of this paper (constructing a methodological and material basis for further research) to take the old law into account, as it will not be relevant for future research. Therefore, this paper does only address the new FADP which entered into force in 2023.

3. Brazil

Brazil is one of two analyzed BRICS countries and therefore represents the privacy law of an emerging economy. It is also one of the most prospering economies in Latin America and its legislation may be influential to neighboring economies seeking access to the US as well as the European market. Unlike other examined countries, Brazil is also a country of great social and economic injustice and shaken by a history of corruption and abuse of power.[67]

In recent years, Brazil began to address regulation on matters of the Internet with the *Marco Civil da Internet* in 2014 and in 2018, under the impression of the Cambridge Analytica scandal and inspired by the GDPR, enacted the LGPD, which came into force in 2020.[68]

4. USA

The United States of America are, at least in this regard, the most federally structured of the examined jurisdiction: The federal government has legislative competencies only where the constitution

---

[65] *Bamberger/Mulligan,* Privacy on the Ground (2015), p. 9.

[66] *Sonnenberg/Hoffmann,* Data Protection Revisited – Report on the Law of Data Disclosure in Switzerland, in IRDG Research Paper Series, No. 22-17, pp. 1 et seq.

[67] *Hoffmann,* LGPD Et Al. – Report on the Law of Data Disclosure in Brazil, in IRDG Research Paper Series, No. 22-06, p. 1.

[68] Ibid.

grants them.[69] The US-Constitution, however, does not explicitly assign privacy legislation to the federal legislator,[70] which results in a multitude of privacy legislation on individual state level.[71] These different privacy acts diverge from and sometimes contradict each other so that is impossible to summarize them as one coherent legal order. However, splintering the Regulatory Clustering according to the US privacy legislation would go beyond its scope. Therefore, the Clustering looks only at the federal level and – as the most prominent and influential[72] example of state privacy legislation – the CCPA of California. This might change in the future, as there is yet another proposal for a federal and comprehensive act on privacy (the American Data Privacy and Protection Act[73]) brought before congress, based on the federal competence of the "interstate commerce rule".[74]

In addition to that, the USA represents (alongside Ghana) the only country with a partial common law system. The countries legislation and applied law is divided in statutory and case law, making it difficult to precisely identify and analyze the relevant sources of law. Even more so, the US approach to privacy regulation is a sector specific one, that implements statutory rules only for certain areas which are deemed especially worthy of protection/regulation.[75] Some of the most prominent federal acts are the Fair Credit Reporting Act (FCRA), protecting financial secrecy and accuracy, the Children's Online Privacy Protection Act (COPPA), protecting the rights of minors, and the Health Insurance Portability and Accountability Act (HIPPA), regulating the use of health information. The Regulatory Clustering will therefore show fundamental principles that span over such sector specific regulation and address factors that emerged from the common law (especially the FTC practice of settlement agreements[76]).

A privacy legislation, that is not only sector-specific, but also federally splintered, shows the limitations of the proposed methodology of a Regulatory Clustering. Such legislation can only be quantified with remarkably more effort and even then, the legislation would not be defined as "US-legislation" but rather "federal USA", "California", "Virginia" and so forth. This is the reason why the Regulatory Clustering will separately include an example of state legislation.

5. California

Naturally, California is no independent jurisdiction, but rather subject to federal US law. Nonetheless, California is in a way special when talking about US legislation, as it is often the state of California that comes forward with new legislation starting a race to the top within the USA and

---

[69] Art. I Sec. 8 in conjunction with the tenth amendment to the US Constitution.

[70] *Genz,* Datenschutz in Europa und den USA (2004), p. 57 et seqq.

[71] There are already eleven states who have signed comprehensive privacy protection laws, cf. *Desai,* US State Privacy Legislation Tracker, accessible under https://iapp.org/resources/article/us-state-privacy-legislation-tracker/ (last accessed 04.03.2024).

[72] Cf. the *de jure* "California Effect" which already demonstrated the impact of Californian privacy legislation with its data breach notification. See on this concrete example *Solove/Schwartz,* Information Privacy Law, (7th edition 2021) p. 39; more generally *Chander/Kaminsky/McGeveran,* Catalyzing Privacy Law, 105 Minnesota Law Review 1733 (2021), pp. 1742 et seqq., 1781 et seqq., 1802.

[73] H.R.8152 – 117th Congress (2021-2022).

[74] *Genz,* Datenschutz in Europa und den USA (2004) pp. 58 et seq.

[75] Cf. for an overview *Solove/Schwartz,* Information Privacy Law (7th edition, 2021), pp. 38 et seq.

[76] *Solove/Hartzog,* The FTC and the New Common Law of Privacy, Columbia Law Review (2014), p. 583.

the whole world.[77] As California yet again takes a forerunner position within the USA in the context of privacy legislation, it seems justified to acknowledge the special legal situation in California separate from the federal level.

The CCPA entered into force in 2020 and has seen significant amendments by ballot initiative (the CPRA), which entered into force in 2023. With the CPRA, California faces a similar problem of novel legislation as Switzerland. However, in contrast to Switzerland, the main body of legislation remained untouched and only certain additions were made. Consequently, the CPRA does not interfere with the research goal of this Regulatory Clustering.

The parallel application of federal law imposes a much more complex problem in grasping state privacy laws: In general, federal law preempts any state law if not stated otherwise and (a) when the federal law leaves no regulatory room for state law, (b) it comes into conflict with state law (i.e. physical impossibility of compliance with both laws), or (c) if state law impedes the achievement of a federal objective (supremacy clause).[78] As there is no comprehensive federal statute dealing with privacy protection, it is likely that the CCPA is not preempted by federal law.[79] One should note, that the CCPA explicitly exempts its applicability in cases related to DPPA, GLBA, FCRA, or HIPAA and it is possible to comply with both CCPA and COPPA at the same time.[80] However, assuming parallel applicability of state and federal law will enable the possibility that a practice unlawful under the CCPA could also constitute an "unfair and deceptive" practice under the FTCA, which will trigger two parallel sanctions (by the FTC under the FTCA and the Californian Attorney General / CPPA under the CCPA).[81] Ultimately that would mean that on substantive level as well as on enforcement level, California is a plus in relation to federal US law and must therefore categorically rank higher.

6. Ghana

Ghana is the least developed of the examined countries. It represents African privacy legislation which is a part of the world often overlooked in comparative law and on a geo-political level often used as playball of other global powers. Nonetheless, as one of the more developed countries of the African Union, Ghana is a perfect example of "frontier markets" that might gain relevance in the future.

Even though Ghana is part of the Commonwealth and therefore a common law country, it provides for one statutory omnibus law on data privacy – the Data Protection Act of 2012. However, as is common in post-colonial African countries, the DPA is treated more like a legal transplant from the EU rather than a legislation which has organically risen from Ghanaian society.[82] It is also interesting to include an African country in this regard: Since the colonial era, there has been a

---

[77] Thusly, California has been name-giving to concept of regulatory competition, cf. *Vogel,* Trading Up: Consumer and Environmental Regulation in a Global Economy (1997), pp. 5 – 8.

[78] *Saquella,* Personal Data Vulnerability: Constitutional Issues with the California Consumer Privacy Act, Jurimetrics (2020) 215, pp. 226 et seq.

[79] Ibid, p. 233.

[80] Ibid; § 1798.145 (c) – (f) CCPA.

[81] The existence of the FTCA itself can also not preempt the CCPA, Ibid, p. 234.

[82] *Hoffmann,* Data Protection Act(ion) – Report on the Law of Data Disclosure in Ghana, in IRDG Research Paper Series, No. 22-01, p. 1.

pronounced legal pluralism in African countries, which combines civil law and common law, but also allows traditional laws to be applied even with priority in some cases.[83]

7. Japan

Alongside China, Japan represents privacy legislation in the Asian room. However, Japan represents an entirely different socio-economic and political system. It can be categorized as a modern post-industrialized economy with far-reaching (especially constitutional) ties to the USA.

The Japanese APPI was originally enacted in 2003, flanked by the Act on the Protection of Personal Information Held by Administrative Organs (APPIHAO) and Held by Incorporated Administrative Agencies (APPIHIAA). The APPI was later, in 2015, completely overhauled and strengthened again in 2021, in order to reach an adequacy agreement with the European Union, which was achieved in 2019. In 2023, the three aforementioned Acts were consolidated in one comprehensive APPI.

8. China

China is the only authoritarian country in this analysis – a techno-authoritarian to be more precise. The country does also provide a completely different setting to start with: On one side, the country suffers from great inequalities especially regarding more rural communities, and on the other side it thrives to take the global lead as technological superpower.

Including a country like China in the Regulatory Clustering leads to two central problems: Firstly, there is an overlapping and partly converging, partly contradicting regulatory thicket of different privacy related laws and administrative guidelines and recommendations.[84] While this thicket makes it harder to grasp Chinese privacy legislation, this is not the main problem with quantifying Chinese privacy law. Rather, it is the authoritarian concept of state – a rule by law, rather than a rule of law.[85] From this rule by law concept follows – for the purpose of addressing privacy regulation – that there is no principle of legality of proportionality to which the government must adhere to. Rather, the law is solemnly understood as policy instrument of the government to which it is no subject. Consequently, privacy regulation cannot limit the collection of personal data by the government and the individual has no rights or means of protection before the government.[86] The lack of these fundamental (western) concepts leads in practice to a massive disregard of internationally recognized human rights in relation to mass surveillance,[87] and consequently a disregard of an adequate level of privacy whatsoever. This surveillance apparatus in conjunction with comprehensive

---

[83] *Hennemann/Boshe/von Meding,* Datenschutzrechtsordnungen in Afrika, ZfDR (2021), pp. 193, 197 with further proof.

[84] See only *Hünting,* Endeavour to Contain Chinas' Tech Giants – Country Report on China, IRDG Research Paper Series (22/15), pp. 9 et seqq.

[85] See in summary of the two conflicting concepts in China *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).

[86] *Czarnocki et al.,* Government access to data in third countries – Final Report, EDPS/2019/02-13(2021) p. 12.

[87] *Human Rights Watch,* China's Algorithms of Repression Reverse Engineering a Xinjiang Police Mass Surveillance App (2019), accessible under https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering- xinjiang-police-mass (last accessed 04.03.2024); *Amnesty International*, Everything you need to know about human rights in China, accessible under https://www.amnesty.org/en/location/asia-and-the-pacific/east-asia/china/report-china/ (last accessed 04.03.2024); *Lilkov,* Made in China: Tackling Digital Authoritarianism, WMCES (2020).

horizontal and vertical information sharing obligations in context of the Social Credit System[88] reduces the level of privacy for Chinese citizens in the public sector virtually to zero. But all the same, the Regulatory Clustering will find that the regulation on assured level of privacy and self-determined level of privacy (under exclusion of any public authority and its powers) is the most intensive of the examined legal orders. These contrasting findings have their root in the fact that the Regulatory Clustering only provides insight into certain instruments regulating privacy, which are predominantly implemented as a general rule, applying both to public and private entities. It does not differentiate between obligations for public and private actors. Here, the shortcomings of the Regulatory Clustering, such as that it can only look at a particular frame of regulation and does not follow a holistic analysis, become most evident. But even in such supposed flaws of the method, there is the possibility of gaining knowledge: Even if a legal and political analysis of the Chinese data protection laws comes to the conclusion, that there is an insufficient level of privacy protection, this can be different from a cultural or behavioral economics point of view. The horizontal regulation of private entities in relation to each other is an intensive one which casts a lot of obligations on the controller which they must adhere to in order to protect the personal information from misuse by them or other information handling entities. This very partial recognition of high privacy standards can be informative when looking at cultural understandings of privacy (which are not necessarily influenced by governmental organization) or perception of privacy regulation vis-à-vis other private actors.

To this end and always under the caveat that the Regulatory Clustering cannot depict all legal and factual circumstances of the regulation, it can still help to understand genuine privacy legislation in the framing of self-determined and assured level of privacy towards other private actors and to quantify the regulation as such.

VI. 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"[89]. However, it can still be used as an interdisciplinary research tool that approaches a middle ground of two (or more) disciplines that are completely dissimilar to each other. By trying to quantify regulatory instruments and jurisdictions, the Regulatory Clustering can contribute to an interdisciplinary analysis of the codependences and interactions of research variables from different disciplines.

Still, the shortcomings in traditional legal methodology coming along with this approach must be addressed somehow. This is done best by precisely defining the researched categories (regulatory instruments divided into those providing 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 regard is the degree of restriction of information handling activities put forward by the respective regulatory instrument. Such restrictions can be imposed by directly regulating handling activities or by implementing 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

---

[88] *Hünting,* Endeavour to Contain Chinas' Tech Giants – Country Report on China, IRDG Research Paper Series (22/15), p. 20.

[89] *Sacco/Rossi,* Einführung in die Rechtsvergleichung, (third edition 2001) Erstes Kapitel, § 1, N 77.

that the Regulatory Clustering only offers an excerpt of a higher, interdisciplinary research goal. Especially, it opens the possibility of an even more contextual understanding of law if it is combined with (empirical) insights of other disciplines.

Finally, the expectations of the method must be clear: Neither shall the Regulatory Clustering depict 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 and not as an absolute value, so that this scale can be used to quantify law to a certain extent and to utilize it as a variable for further interdisciplinary research.

C. Clustering Regulatory Intensities

A proposal on how a Regulatory Clustering can be conducted and how it could help with insights on the matter follows now in sections C. and D. The resulting insights also with regard to comparative law can be found in the individual country profiles in section E.

I. Assured Level of Privacy

The following chapters will address such regulation that grants an objective standard of protection without user involvement. They address behavioral obligations on modalities of information handling activities.

1. Prerequisites of Information Handling

One of the central decisions – if not the most central – is the legal circumstances under which personal information may be handled at all. Essentially, a jurisdiction takes one of two paths: Either prohibiting information handling subject to permission or – in a differentiated manner – allowing information handling entirely and connecting regulation to the means of handling and not its prerequisites.

Naturally, a prohibition subject to permission restricts more information handling and is therefore more "intensive" in the meaning of this Regulatory Clustering. In this regard, China took the most intensive path in enumerating various elements of authorization in Art. 13 PIPL, but not including the otherwise common justification of overriding private interest. Most other jurisdictions implementing a prohibition subject to permission[90] added such "legitimate" or "overriding" interest alongside other common elements like consent, performance of contract or legal obligation. Nuances, such as research purposes in Brazil[91] or vital interest in Germany[92] may diverge in individual cases but do not have an impact on the ranking of intensity. Even though Ghana does also implement a prohibition subject to permission, it also establishes remarkably the principle that information should only be collected directly from the individual.[93] However, indirect collection is allowed under circumstances that only slightly deviate from the bases for authorization in Art. 20 DPA (by being more specific). Nonetheless, this specification does rank Ghana (only very slightly) higher than Brazil and Germany but not as high as China.

---

[90] These being Brazil, Germany and Ghana.

[91] Art. 7 IV LGPD.

[92] Art. 5 I lit. d) GDPR.

[93] Art. 21 DPA.

Other countries are (to different extents) less restrictive: Switzerland only forbids certain "personality violations"[94], which in return can be justified similarly to the aforementioned grounds of authorization, thus constituting a permission subject to prohibition. Japan and the US are even less restrictive only requiring any[95] utilization purpose. There are only very certain prohibitions of information handling, mostly connecting to deception or other improper use.[96]

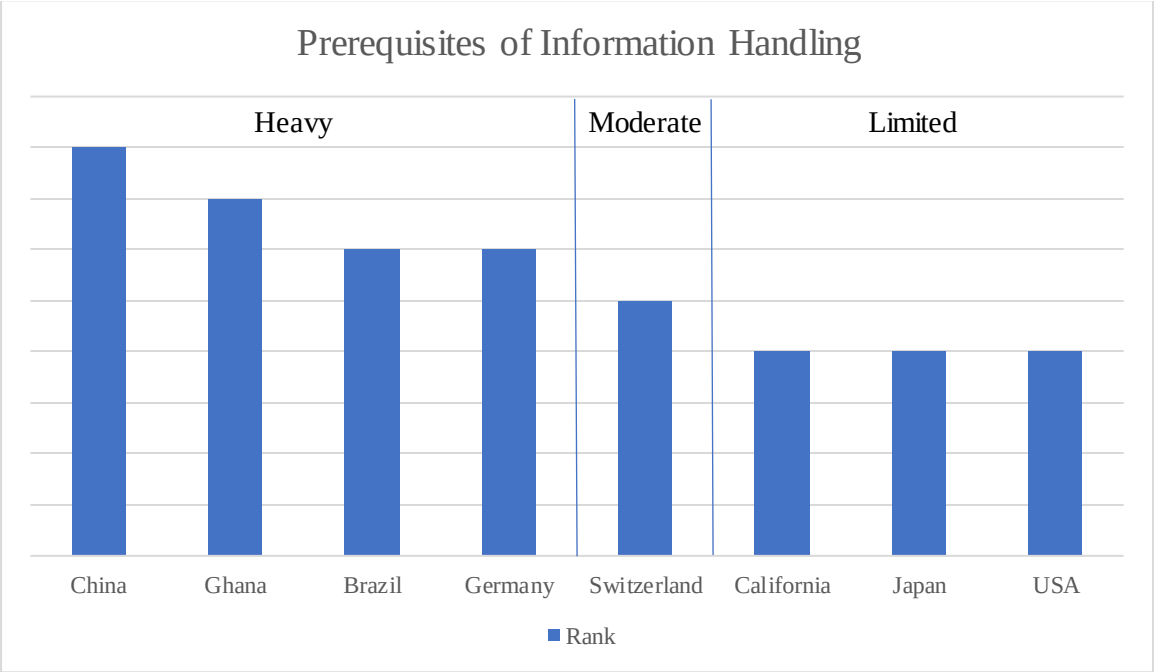

Figure 2: Ranking of regulation on prerequisites of information handling

2. Sensitive Information

The assessment of how intensive the regulation for handling sensitive information is, is twofold: First, the restriction of handling activity is larger when a lot of categories of information are deemed "sensitive" and therefore especially worthy of protection. Second, the intensity greatly relies on the concrete restrictions imposed on handling sensitive information.

In regards of the first point of assessment, California has the most comprehensive catalogue of sensitive information including more generic categories such as genetic data or ethnic origin but also one's geolocation, social security number, or account log-in.[97] Also, due to the sector-specific approach of the federal US law, certain categories of information are specially protected by federal law.[98] A more common catalogue of sensitive information in other jurisdictions comprise of

---

[94] Art. 30 et seq. FADP.

[95] This chapter does only address the prerequisites of information handling which do not include the regulation on how to handle the information once allowed to handle it. Accordingly, the question of which requirements are to be placed on a utilization purpose is not a question of prerequisites but of purpose limitation (→ 3.). The fact that said jurisdiction always requires a certain purpose makes the mere existence of a utilization purpose the only relevant factor in this category.

[96] For Japan, cf. Art. 19, 20 I APPI. In the US, there is the threshold of not conducting a "unfair or deceptive act" enforceable by the FTC as main privacy regulator via 15 USC § 45 (FTC Act).

[97] Cf. §

[98] These include e.g. financial information (Fair Credit Reporting Act of 1970, FCRA), health information (Health Insurance Portability and Accountability Act of 1996, HIPAA), information relating to minors (Children's Online

information relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic and biometric data, minors and intimate information.[99]

As to the regulation on handling sensitive information, restrictions diverge and also depend on the overall approach to handling personal information outlined above. Therefore, intensity must carefully be assessed having in mind the standard regulation applying to "normal" personal information. In this regard, Switzerland adds the least amount of restrictions.[100] California only adds additional provisions (the possibility to restriction and heightened information obligation)[101]. The most restrictive jurisdictions impose a completely new regime on handling sensitive information,[102] and are led by China, shortly followed by Japan, requiring consent without allowing for alternatives.[103]

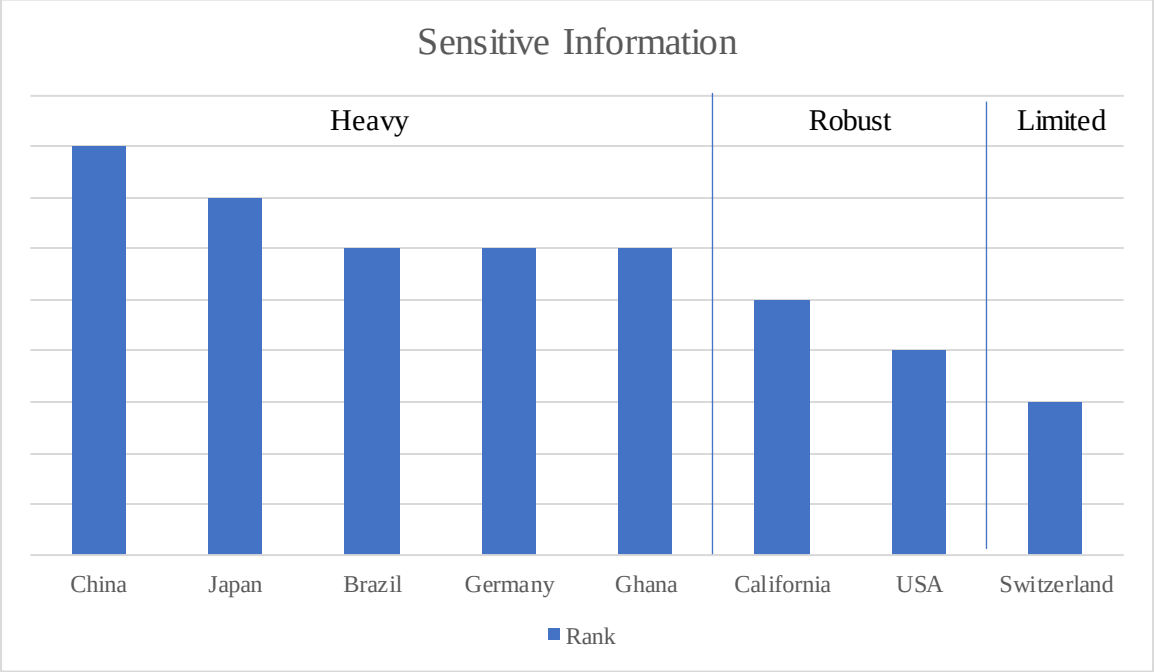

Figure 3: Ranking of regulation on handling sensitive information

Privacy Protection Act of 1998, COPPA), or telecommunication (Cable Communications Policy Act of 1986, Cable Act).

[99] For an overview, cf. *Wawra,* in: Hennemann, von Lewinski, Wawra, Widjaja (eds.), Data Disclosure, Data Sensitivity and Data Protection Literacy in Cross-Cultural Comparison (2023), pp. 169, 172 et seqq.

[100] Especially, there are heightened consent requirements (Art. 6 VII lit. a) FADP) and a prohibition of third-party transfers (Art. 30 II lit. c) FADP).

[101] § 1798.121 CCPA.

[102] Most interestingly, Japan primarily requires consent and allows for exceptions to this, such as vital interest, legal obligation, public hygiene, or public information, but not overriding private interest (Art. 20 II APPI), making Japan second to most restrictive. One must bear in mind that Japan follows one of the least restrictive approaches to information handling otherwise. Countries which follow a general prohibition subject to permission crafted more restrictive bases for authorization, cf. for Brazil Art. 11 LGPD, for Germany Art. 9 GDPR, and for Ghana which provides for the most nuanced approach, Art. 37 DPA.

[103] Art. 29 PIPL. In Art. 28 II PIPL, there is also the requirement that there is a specific purpose and a "need to fulfil".

3. Purpose Limitation

Having outlined the prerequisite of handling personal information, the most common and vital principle legislators impose on controllers in privacy concepts, is the principle of purpose limitation. This principle is – in its general outline – basically the same in all analyzed jurisdictions: Personal information can only be handled in accordance with a specific purpose. However, the concrete design and scope of such purpose limitation may vary.

Fundamentally, this principle comprises in its widest extent of a direct connection between purpose and handling activity, a definition and communication of a precise purpose the information is handled for, and legitimacy of the purpose. These four elements can be found in Brazil, Germany, Ghana, and China.[104] Japan and Switzerland do not require "legitimate" purpose[105], but measure the nature of the purpose against general principles such as lawfulness or appropriateness. The least restrictions prevail in the US: Purpose limitation does especially surface in FTC case law where it is only allowed to handle personal information in the accordance with the purposes which the controller communicated to the individual.[106] This was codified in California in § 1798.100 (b) and (c) CCPA. But both, FTC case law and CCPA require preciseness or legitimacy in a broad manner as compared to the other jurisdictions. Very similar to Japan and Switzerland, such regulation exhaust in the prohibition of "unfair and deceptive acts". Nonetheless, one must bear in mind the central function of purpose limitation in the "notice and choice"[107] approach of US privacy regulation. This "notice and choice model" embodies the idea that any information handling activity should be permissible as long as the respective individual has been sufficiently informed so that they can make an informed and autonomous choice on whether they are in agreement with the processing or not.

---

[104] Cf. for Brazil Art. 6 I LGPD, for Germany Art. 5 I lit. b) GDPR, for Ghana Art. 22 DPA, and for China Art. 6 PIPL.

[105] Cf. for Japan Art. 17 et seq. APPI; and for Switzerland Art. 6 III FADP.

[106] This is widely regarded as the prosecution of "broken promises", cf. only *Solove/Hartzog,* The FTC and the New Common Law of Privacy, Columbia Law Review (2014), pp. 583, 628 et seqq.

[107] *Reidenberg et al.,* Privacy Harms and the Effectiveness of the Notice and Choice Framework, A Journal of Law and Policy for the Information Society (2015), pp. 485, 489 et seqq.; *Solove/Hartzog,* The FTC and the New Common Law of Privacy, Columbia Law Review (2014), pp. 583, 592 et seq.

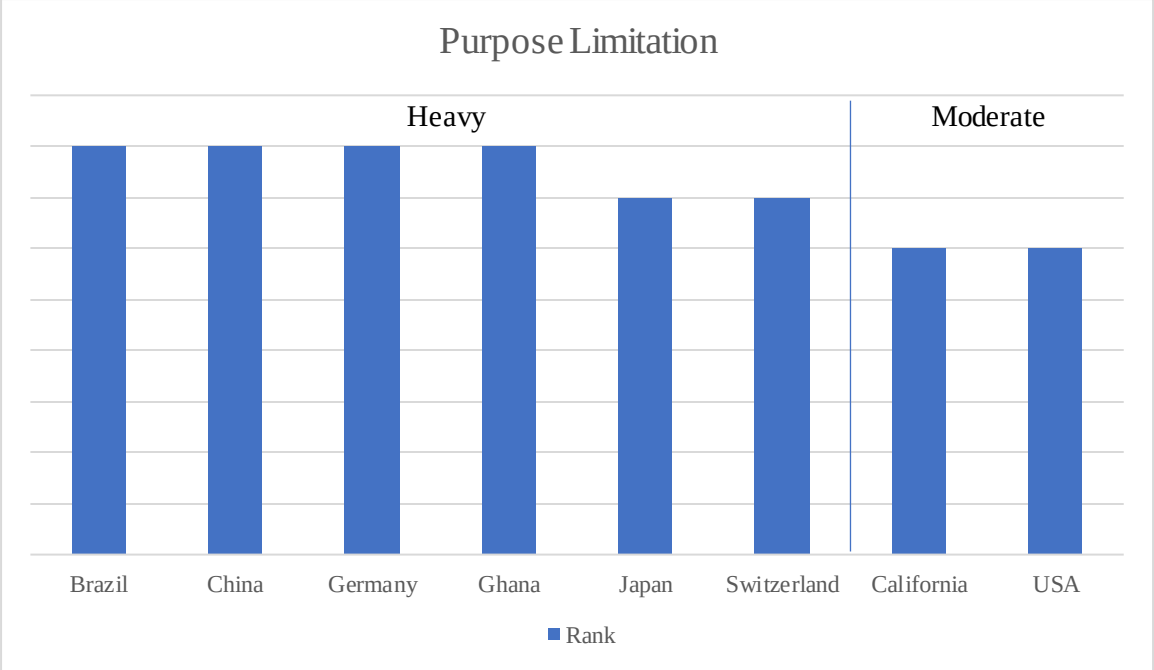

Figure 4: Ranking of regulation on purpose limitation

4. Subsequent Information Handling

Another term for subsequent information handling is secondary purpose limitation: it concerns the scenarios where obtained information is processed for another purpose than the original and is thus also strongly connected to purpose limitation. Most jurisdictions prescribe a certain connection to the secondary purpose, very similar to primary purpose limitation. An exception to this is US privacy law, which limits its regulation to notice of change of purpose and which is not bound to any special requirements of such secondary purpose.

In other jurisdictions, the extent of the required connection varies: Brazil and Germany require that the secondary purpose is not incompatible with the primary purpose.[108] In contrast, Ghana, California and Switzerland require positive compatibility[109] which may exclude such purposes that are not incompatible but entirely unrelated. Constituting a slightly higher degree of restriction, Japan prohibits alteration of purpose that is "beyond the extent that can be appreciably linked to what is was before alteration"[110] and China requires a direct relation between primary and secondary purpose[111], both creating a more intensive link between original and subsequent processing. Note, that the APPI (in Art. 18) provides for a possibility to override subsequent information handling restrictions.

---

[108] See for Germany Art. 5 I lit. b), 6 III GDPR, for Brazil Art. 6 I LGPD. However, one must consider for Brazil Art. 9 § 2 LGPD, which by *argumentum e contrario* lowers the prerequisites for subsequent information handling when the original handling was based on consent.

[109] See for Ghana Art. 17 lit. d) DPA, for California § 1798.100 (c) CCPA, and for Switzerland Art. 6 III FADP.

[110] Cf. Art. 17 II APPI (English translation by the official Japanese Law Translation website of the Japanese Ministry of Justice, accessible under https://www.japaneselawtranslation.go.jp/en/laws/view/4241/en (last accessed 04.03.2024).

[111] Cf. Art. 6 I PIPL; Nr. 7.3 lit. a) of the Information security technology – Personal information security specification of 2020, GB/T 35273-2020(2020) (hereinafter "2020 Specifications").

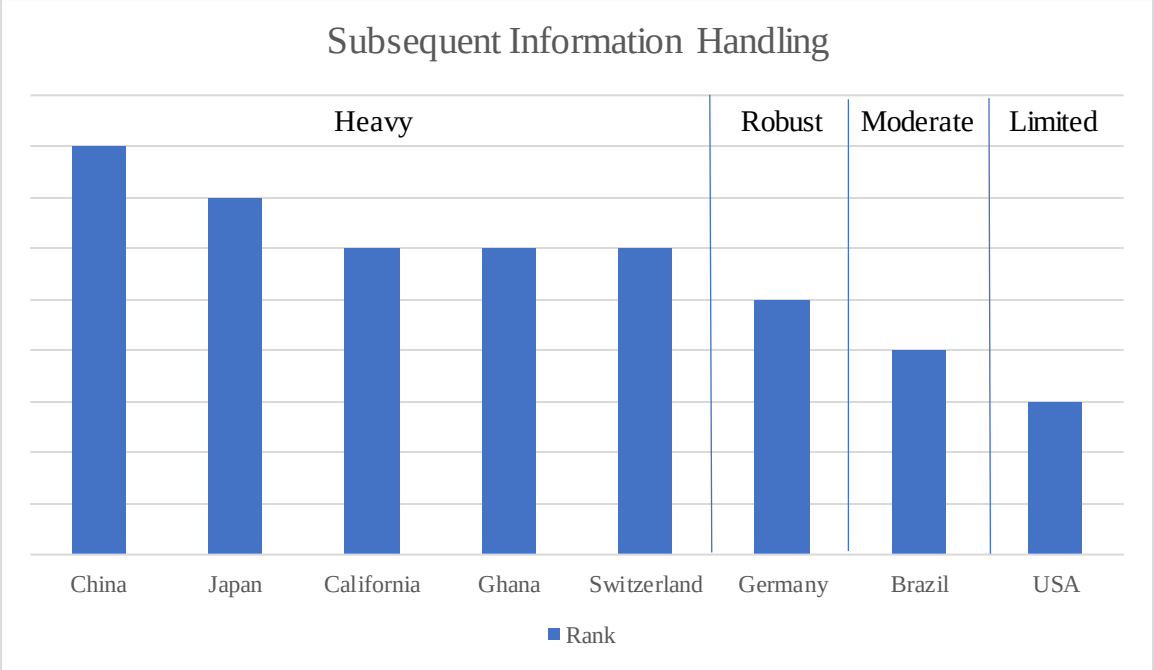

Figure 5: Ranking of the regulation on subsequent information handling

5. Domestic Transmission to Third Parties

Domestic transmission of personal information to third parties is often directly connected to subsequent information handling. This is because many jurisdictions define a third-party transfer merely as alteration of purpose (if the transfer was no primary purpose). Examples include Brazil, Germany and Switzerland with no specific regulation on third party transfers.[112] In other jurisdictions third party transfers take a much more vital place: China and Japan require prior consent before every transfer which is subject to only few exemptions.[113] The CCPA requires any transfer to be based on a contract, connects special information obligation to the sharing (notice and choice model[114]).[115] Ghana does prescribe (similar to Japan) a special regime for the legitimacy of third party transfers.[116] Very interestingly, Ghana does also stipulate specific prohibitions of third party transfers, especially the selling and purchasing of personal information of another person (Art. 88, 89 DPA). While this does not target third party transfers in general, it limits to a wide extent the practice of using personal information as an economic good – a practice that can often be observed in the USA and the so-called "data broker model".

The federal US constitute a problem in identifying regulation of third-party transfers: On the one side the US concept relies – just like California – on an opt-out notice and choice approach. However, there is no concrete ruling for handling such transfers. There is FTC case law practice, as to which the unauthorized sharing of personal information can constitute a deceptive act if the

[112] However, Brazil does include the specific requirement of obtaining prior consent when transferring personal information if the original information handling was also based on consent, Art. 7 § 5 LGPD.

[113] Cf. for China Art. 25 PIPL, and for Japan Art. 27 APPI which includes a little more exemptions than China.

[114] See on this model already above, → C.I.3.

[115] Cf. § 1798.100 (d) CCPA for the contract requirement and § 1798.115 CCPA for the notification obligation which especially prescribes to give the opportunity to opt-out from any third-party transfers.

[116] Cf. Art. 21 II DPA.

consumer could have reasonably expected that his information will not be shared.[117] This is a lower restriction than the subsequent information handling regulation in other jurisdictions which is why the federal US does rank last.

Concerning transmission to third parties, most jurisdictions provide rules for using a processor as subcontractor or other means of outsourcing information handling activities.[118] Such rules are essentially similar, requiring (contractual) safeguards between controller and processor.[119]

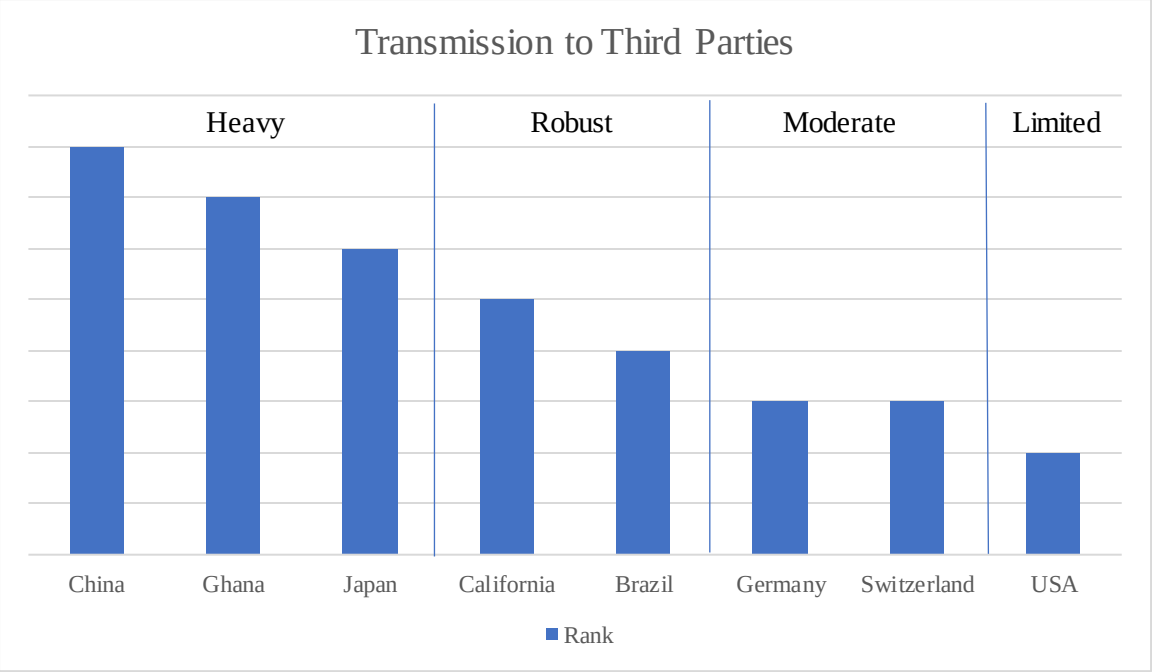

Figure 6: Ranking of regulation on inland data transfers

6. Transmission Abroad

The rules for third party transfers across nation borders are often not similar to the general rules of third-party transfers. Jurisdictions seek to protect "their" information against migration abroad which would deprive a country of its access to information and legal as well as technical protection of such emigrated information.[120]

In international comparison there are two poles of such regulation of international data flows: On the one side, there is complete localization of information, only very selectively allowing for

[117] On this and the resulting privacy harms of unauthorized sale of personal information *Keegan/Schroeder,* Unpacking Unfairness: The FTC's Evolving Measures of Privacy Harms, Journal of Law, Economics & Policy (2019) pp. 19, 32 et seqq.

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

[119] Besides the US which does not know specific regulation for third parties in general, Japan stands out because its privacy legislation does not provide for the concept of "processor" or similar. Instead, it requires the supervision of all persons entrusted with handling personal information for the controller, Art. 25 APPI. Such supervision is (realistically speaking) only very restrictively possible via contract.

[120] See in general for the global trend of data sovereignty via regulation transnational data flows *Chander/Le,* Data Nationalism, Emory Law Journal (2015) p. 677; *Arner/Castellano/Selga,* The Transnational Data Governance Problem, University of Hong Kong Faculty of Law Research Paper No. 2021/039.

authorized transmissions abroad.[121] On the other side, there is the concept of free flow of data which does not impose any specific obligation to adhere to when transmitting personal information abroad.[122] A special case of the latter concept is Ghana: it does not prescribe any further restrictions on third party transfers abroad. However, the DPA requires the compliance with foreign law if the information of foreigners originating from a foreign country or being processed there.[123] Thus, the incorporation of foreign law leads to a *de facto* increase of regulation to adhere to when frequenting international transfer modalities.[124]

Between the two aforementioned poles lay the jurisdictions that impose a conditional data localization regime and therefore connect cross-border data flows to certain requirements. These countries prescribe either a certified adequate level of protection in the third country, equivalent guarantees or separate justification via especially consent. The most restrictive of these jurisdictions are the ones primarily requiring authorized safeguarding frameworks like adequacy decisions or standard contractual clauses and only provide single case exceptions.[125] Of lesser intensity are such jurisdictions that place institutional authorization and individual grounds for authorization (i.e. consent) on an equal footing.[126]

---

[121] This most restrictive regulation can be found in China, Art. 38 PIPL.

[122] This is the case for federal US and California. Due to the contractual requirement for third party transfers of the latter there is a factual restriction of transmissions (i.e. conclusion of contracts) abroad.

[123] See for a basic incorporation principle Art. 18 II DPA and for the specific requirement for foreign processors Art. 30 IV DPA.

[124] Even though this does only directly affect the import of information, it could also have adverse effects on the export, as international partnerships may raise the risk that foreign law becomes applicable.

[125] Such countries are Germany (Art. 44 et seqq. GDPR) and Switzerland (Art. 16 et seq. FADP) where the latter provides for wider exceptions.

[126] Such countries are Brazil (Art. 33 et seqq. LGPD) and Japan (Art. 28 APPI) where the latter focuses on advance consent and not primarily on safeguarding guarantees apart from taking "necessary measures to ensure continuous implementation of the equivalent measures by the third party". Also, Japan applies the same exemptions to the consent requirement as to "normal" third party transfers.

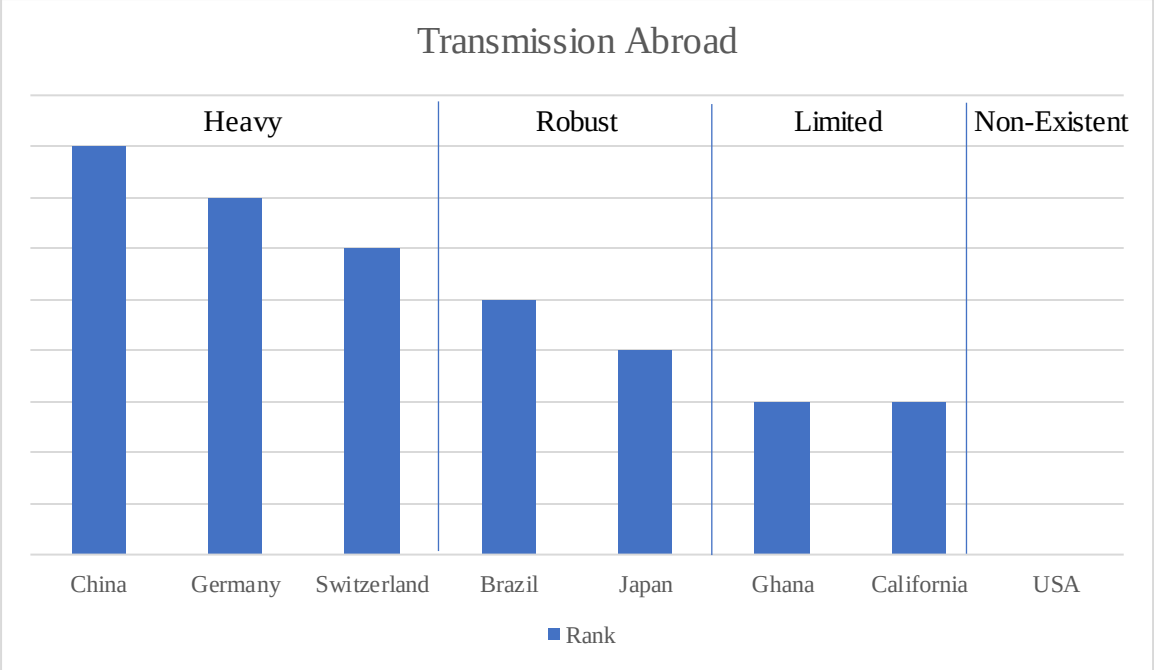

Figure 7: Ranking of regulation on data transfers abroad

7. Data Minimization

Closely linked to purpose limitation is the principle of data minimization. It prescribes the limitation of handling personal information in relative comparison to the purpose it is handled for.

In its most restrictive form (namely in Brazil, California, China, and Germany[127]), the data minimization principle requires the controller to only use the personal information in a way that is limited to what is strictly necessary to achieve said purpose. All four of these jurisdictions require the information handling to be relevant and necessary for the purpose and also in an appropriate scope, weighing individual rights and interests of the controller. A little less restrictive are Ghana which requires relevance, necessity and appropriateness only for the purpose itself but not in relation to the information handling[128], followed by Japan, which does not prescribe appropriateness of the information handling in relation to the purpose[129] and Switzerland, which does prescribe general proportionality but not concrete necessity in relation to the purpose.[130] The US data minimization principle is least restrictive: It mostly appears in few sector-specific laws and in case law to that extent that information shall not be kept where it is not necessary for a stated purpose.[131]

---

[127] Cf. for California § 1798.100 (c), for China Art. 6 PIPL, for Brazil Art. 6 III LGPD and for Germany Art. 5 I lit. c) GDPR.

[128] Cf. Art. 19 DPA. Connecting minimization only to the purpose but not the actual information handling activity allows the risk of in itself excessive means of information handling under the caveat of non-excessive purpose. However, this will most likely be covered interpretation of Art. 19 DPA.

[129] In this sense, Art. 18 I APPI allows for information handling that is necessary for achieving a purpose but might be the more intensive alternative of two options or may be entirely unproportionate to the degree of privacy infringements. Such scenarios are only covered by the general prohibition of improper means.

[130] Cf. Art. 6 II and III FADP.

[131] *Solove/Hartzog,* The FTC and the New Common Law of Privacy, Columbia Law Review (2014), p. 583, 653; *Glocker,* Der California Consumer Privacy Act (2022), p. 169.

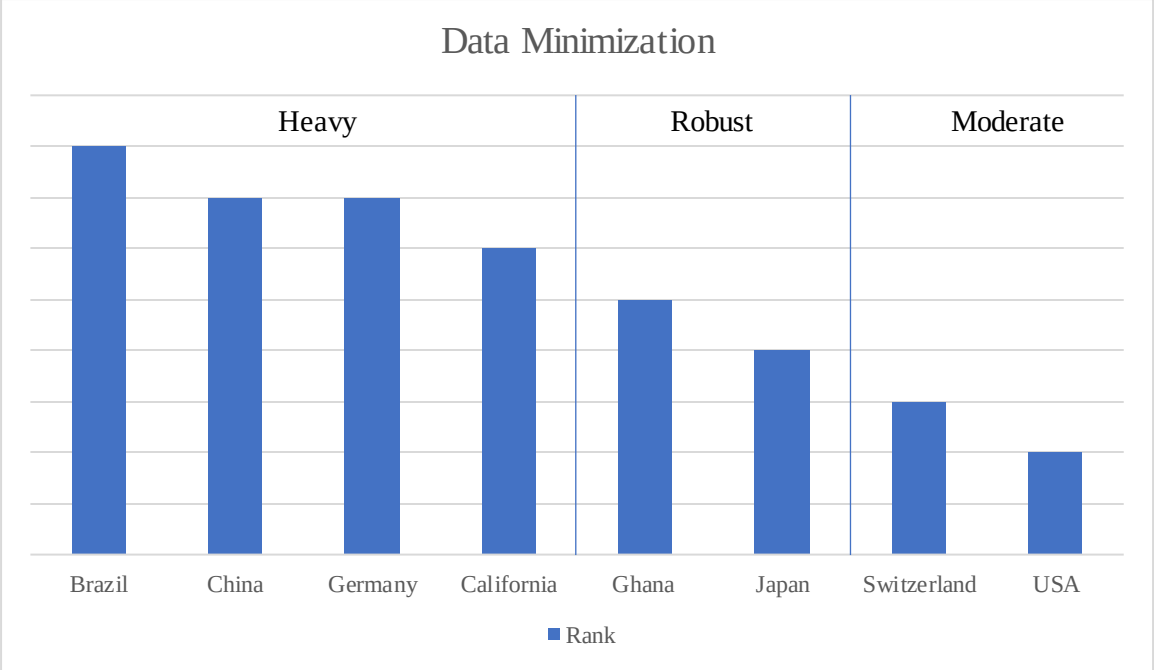

Figure 8: Ranking of regulation on data minimization

8. Deletion Obligations

Rules on how long entities are allowed to keep personal information and on when they are required to delete such information are closely linked to the principle of data minimization: Most jurisdictions measure retention periods strictly against the background of necessity in relation to the purpose.[132] Other possible triggers for deletion obligations (other than the later discussed right to deletion) are missing accuracy[133], expiry of self-proclaimed or legally required retention periods[134], or the internal discovery of non-compliance[135]. Common exemptions are statistical or research purposes[136], the anonymization of personal information[137], legal obligation[138], and – most restrictively – overriding necessity[139]. Therefore, the benchmark for the assessment is how comprehensive the combination of the two factors of the prerequisites of deletion obligations and their exceptions are.

---

[132] Cf. for Brazil Art. 15 I LGPD, for China Art. 47 I no. 1 PIPL, for Germany Art. 5 I lit e) GDPR, for Ghana Art. 24 DPA and for Switzerland Art. 6 IV FADP.

[133] Cf. for Japan Art. 22 APPI, for Germany Art. 5 I lit. d) GDPR and for Switzerland Art. 6 V FADP.

[134] This is of primary importance in the US and especially California (§ 1798.100). However, such possibilities can also be found in Brazil (Art. 15 II LGPD) and China (Art. 47 I no. 2 PIPL).

[135] Only in China, Art. 47 I no. 4 PIPL.

[136] Found in Brazil (Art. 16 II LGPD), Germany (Art. 5 I lit. e) GDPR) and Ghana (Art. 24 II DPA).

[137] In Germany, it is only prohibited to allow identification beyond the retention periods. In Brazil, there is the possibility to keep anonymized data for exclusive internal use.

[138] Found in Brazil (Art. 16 I LGPD) and Ghana (Art. 24 I lit. a) DPA).

[139] This rather comprehensive exemption can only be found in Ghana (Art. 24 I lit. b) and c) DPA).

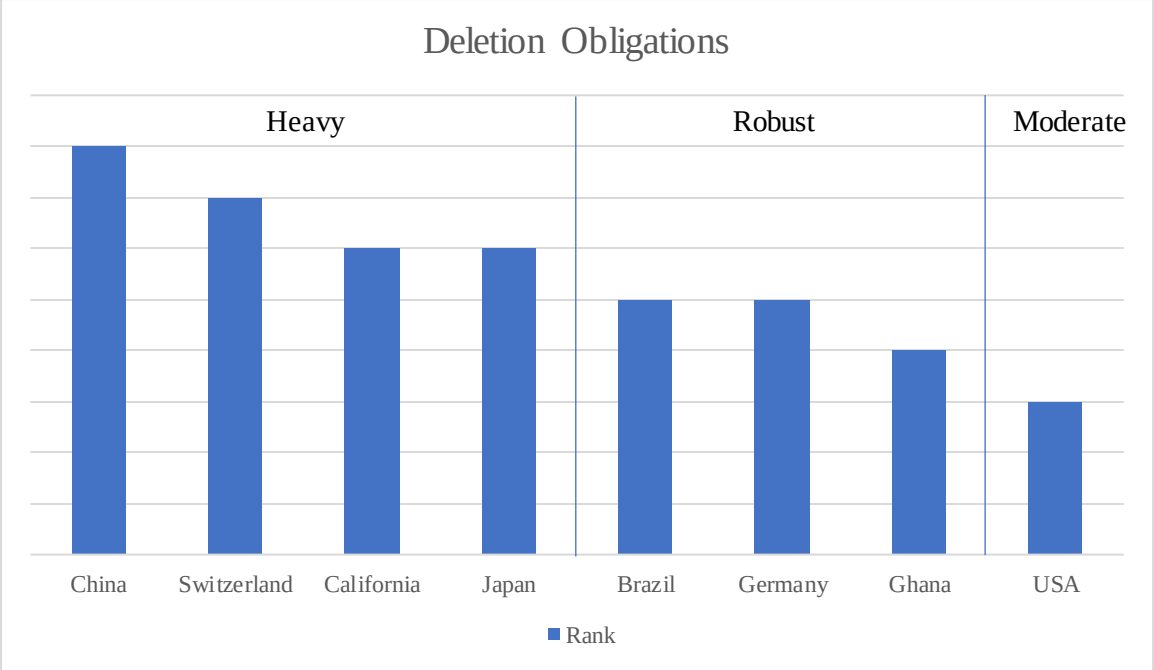

Figure 9: Ranking of regulation on deletion obligations

9. Data Quality

Another fundamental principle of different privacy laws is the data quality principle. In its furthest extent it comprises of a pro-active obligation to keep information correct and up to date in relation to the necessity for achieving its purpose.[140] Most remarkably in this regard are Germany (requiring necessity only for the actuality) and Brazil (requiring the information to be "clear"). The less intensive approach of China in Art. 8 PIPL is connecting the data quality directly to the rights and interests of the individual. Thus, the purpose is no longer decisive but rather the question, whether inaccurate or outdated information impose an actual risk for legitimate interests of the individual. Lastly, US and Californian regulation remain largely silent on data quality. Only very rarely US statutory law determines a specific requirement for actuality or accuracy.[141] Also, the common law body provides for the possibility of e.g. the false light invasion of privacy tort[142], which is a category of self-determined level of privacy and thus only creates a factual incentive for data quality.

[140] This is the case 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).

[141] An example would be § 611 FCRA. In such cases it is apparent that an inaccurate credit score may have directly adverse effects on the individual.

[142] Restatement (Second) of Torts, § 652E.

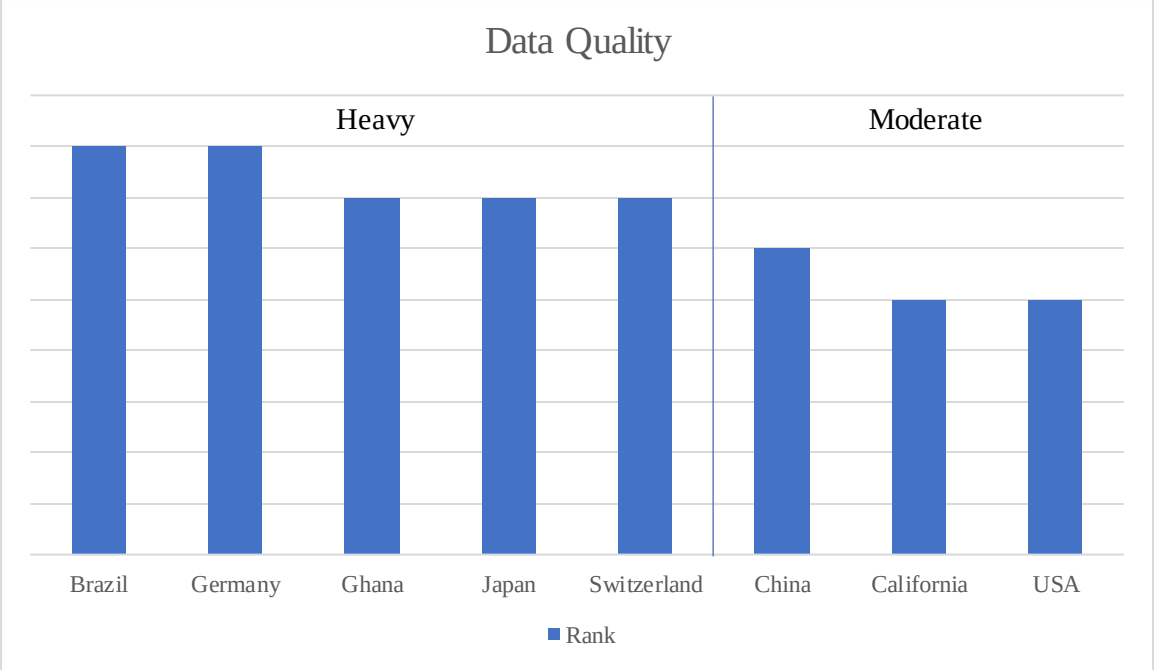

Figure 10: Ranking of regulation on data quality

10. Data Security

Turning to such regulation that prescribe objective obligation on how to organize information handling activities, rules requiring a certain threshold are probably the most relevant for assessing compliance costs. Therefore, all examined jurisdictions require the controller to implement reasonable measures (or similar) to prevent violations of privacy rights which are commonly defined as unauthorized access to or the loss of information.[143] Having the same base prerequisites, it is difficult to differentiate intensity rankings between different regulation on data security.

Even when looking at administrative specifications and secondary sources, these similarities largely remain.[144] The most prominent security measures can be divided into four subcategories: personnel, physical, systematic and technical. On a personnel level, the individuals handling information must be sufficiently qualified and regularly trained and supervised. On a physical level, information must be stored in a way that is not physically accessible for any unauthorized person. On a systematic level, the internal structures of a controller shall optimize secure information handling, for example by implementing best practices or self-monitoring and -assessment systems. Lastly, on a technical level, information shall be stored in a way that negates the possibility of unintended loss or damage, as well as the unauthorized technical access by third parties. Related measures include encryption, cybersecurity software or certificate-based access. Requirements on all four levels can be found in administrative specifications in nearly all examined jurisdictions.

[143] See for Brazil Art. 46 et seqq. LGPD, for California § 1798.100 (e) CCPA, for China Art. 9 and 51 et seqq. PIPL, for Germany Art. 32 GDPR, for Ghana Art. 28 DPA, for Japan Art. 23 APPI and for Switzerland Art. 8 FADP.

[144] As for administrative specifications and other soft law guidelines in the different jurisdictions, see for California *Harris,* California Data Breach Report of the Attorney General (2016), pp. 27 et seqq.; for China Art. 6.2, 7.2, 11.7 of the 2020 Specifications as well as the MLPS 2.0; for Germany see e.g. *BSI,* IT-Grundschutz-Kompendium (2023); for Japan Art. 20 of the Enforcement Rules for the Act on Personal Information (2017); and for Switzerland *FDPIC,* Leitfaden zu den technischen und organisatorischen Massnahmen des Datenschutzes (2015).

Even in US-case law[145] and statutory regulation[146], data security is a central aspect of privacy. But corresponding requirements – as always on federal US level, unlike to other jurisdictions – do not apply to all situations where information is handled. Still, abovementioned standards do often find a way into US regulation and privacy practices in the form of international standards (such as ISO 27001) which are often part of self-regulation commitments or even administrative guidelines.[147] Apart from that, only Brazil and Ghana stand out negatively because they do not have any specifications on their statutory requirements of appropriate security measures. While in Brazil it can be expected that the ANPD which was only recently founded will adopt guidelines very similar to internationally agreed on standards[148], the Ghanaian DPC has failed to adopt any guidelines throughout the last 12 years of its existence and is not likely to adopt any in the near future.

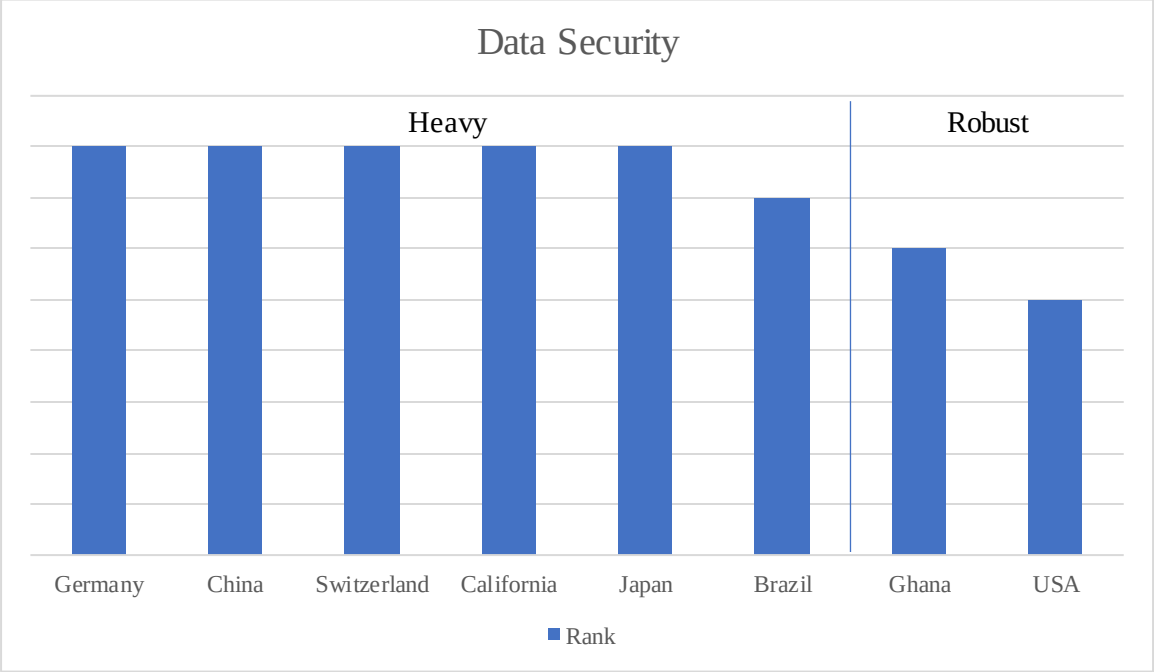

Figure 11: Ranking of Regulation on data security

11. Internal Documentation

It is quite frequent to impose internal documentation obligations on the controller to use it as a subject of supervision and self-control. Such internal documentation often includes the tracking of own information handling activities, the analysis of such activities and its potential influences on rights and interests of the individual (often referred to as "impact assessments").

Only two jurisdictions – Germany and Switzerland – require a precisely defined "register of processing activities" which includes information on processors, purposes, retention periods or data

[145] *Solove/Hartzog,* The FTC and the New Common Law of Privacy, Columbia Law Review (2014), pp. 642 et seq., 650 et seqq.

[146] Examples of statutory data security requirements may be found in 45 CFR §164.306 (HIPPA), 15 USC § 6801 (GLBA), or 16 CFR §312.8 (COPPA).

[147] As is the case in California, which Attorney General recommends to comply with the "20 Center of Internet Security Controls", cf. *Harris,* California Data Breach Report of the Attorney General (2016), p. 30.

[148] Thusly, the ANPD, on October 4, 2021, has already adopted corresponding guidelines for small businesses. Accordingly, the general guidelines on data security can be expected to be even more restrictive.

security measures.[149] Brazil follows a slightly less intensive and more generalist approach by ordering controller and processor to keep records of only personal data processing operations carried out by them.[150] Even less restrictive are sectoral obligations, such as the one imposed in Japan, requiring to prepare a record of the circumstances of only third party transfers.[151] Recordkeeping obligations can also factually arise from the necessity to comply with other legal obligations.[152]

Crucial for the intensity of internal documentation is when and to which extent an impact assessment (or alike) must be conducted. Most restrictive in this regard is China[153], always requiring an impact assessment when there is a major influence on individuals, e.g. the handling, international transfer or sharing of sensitive information. There shall also be a regular "PI Audit" of information handling activities in general. Other jurisdictions settle for requiring impact assessments whenever there is a "high risk" for individual rights.[154] Where existent, the content of the assessment is roughly the same, with the (to be expected[155]) exception of California which only requires an audit in relation to cybersecurity. Brazil, Ghana, Japan and federal US do not know any impact assessments. However, such impact assessments can be required by the supervisory authority within the scope of their remedial powers.[156]

[149] See for Germany Art. 40 GDPR and for Switzerland Art. 12 FADP.

[150] Art. 37 LGPD. By only referring to the processing activity *per se*, it becomes evident that this shall not include the wide array of circumstances like data security measures referred to in Germany and Switzerland.

[151] Art. 29 APPI.

[152] Most relevant is the compliance with access requests or the conducting of an impact assessment which by default require the controller to keep track of their activities and could later be subject to regulation.

[153] Cf. Art. 54 et seqq. PIPL.

[154] This is the case in California (§ 1798.185 (a)(15)(A) CCPA), Germany (Art. 35 GDPR) and Switzerland (Art. 22 FADP).

[155] The CPPA has yet to draft regulation on cybersecurity audits, cf. *CPPA,* Preliminary Rulemaking Activities on Cybersecurity Audits, Risk Assessments, and Automated Decisionmaking, accessible under https://cppa.ca.gov/regulations/pre_rulemaking_activities_pr_02-2023.html (last accessed 04.03.2024).

[156] This is most apparent in Brazil, Art. 38 LGPD.

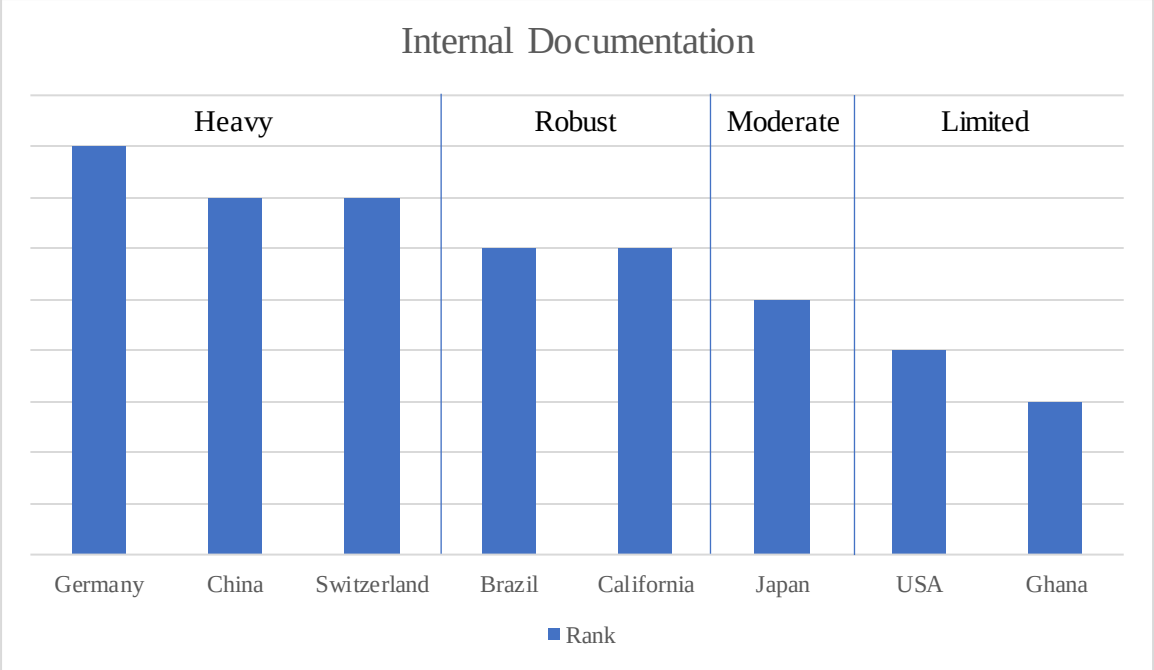

Figure 12: Ranking of regulation on internal documentation

12. Registries

A kind of counterpart to internal documentation is a register of information handling activities that is publicly accessible and holds information on all entities handling personal information within the scope of the law.

Most examined jurisdictions do not have such publicly accessible registers. Closest to a publicly available register comes the obligation in some countries to publicly name a domestic representative if the controller has no branch inlands.[157] Instead of public registers, jurisdictions rely on internal documentation, individual information and data breach notification. This is best shown by the revised Swiss FADP that held a comprehensive registry obligation in Art. 11a FADP of 1992 in its old version. This was later replaced with aforementioned instruments that were new to the old FADP. It was argued that a register was not frequented often enough to be efficient.

However, Ghana stands out with a comprehensive obligation without exceptions to publicly register with the supervisory authority[158], thus allowing for public oversight of information handling entities. The only other country requiring registry information is Japan, granting the possibility to make certain information publicly available to fulfill information obligations,[159] and California, requiring the controller to make a privacy policy public on its website every 12 months in addition to individual information to the consumer.[160] While this is no centralized register as in Ghana, it does provide for more publicity of information handling entities which goes beyond the requirement of public availability in other jurisdictions.

---

[157] See for China Art. 53 PIPL, for Germany Art. 27 GDPR and for Switzerland Art. 14 et seq. FADP.

[158] Cf. Art. 27 DPA.

[159] Cf. Art. 21 I APPI. Because this would exclude individual information, it is the only possibility to gain information from the controller. Therefore, there is a high registry-like relevance of such information in Japan.

[160] § 1798.130 (a)(5) CCPA. Cf. on this two-prong requirement *Glocker,* Der California Consumer Privacy Act (2022), pp 150 et seqq.

Figure 13: Ranking of the regulation on registries

13. Internal Responsibility Management

Six out of eight examined jurisdictions (Brazil, China, Germany, Ghana, Japan and Switzerland) contain regulation of a person responsible for the company's handling of personal information.[161] Where required, this responsibility includes advising and supervising the controller, as well as communication with the individual and the supervisory authority.[162] As far as these responsibilities are concerned, said jurisdictions provide roughly the same level of intensity. Nonetheless, there is great diversity on the prerequisite of an obligation to appoint a responsible person:

The most intensive regulations are those which always require an information handling entity to appoint such person. However, no jurisdiction contains such regulation. Brazil comes close with a general obligation that exempts only small businesses, self-employed and startups[163], followed by China after Germany, implementing risk-based approaches.[164] Other jurisdictions – such as Switzerland and Ghana – do know the concept of a responsible person, but – in the case of Ghana – do only regulate the qualifications of such person, or – in the case of Switzerland – only incentivize instead of requiring the appointment.[165] California as well as the US in general and Japan do not

[161] This person is often referred to as data protection officer/advisor/supervisor or similar.

[162] See for Brazil Art. 41 LGPD, China Art. 52 PIPL, for Germany Art. 37 et seqq. GDPR, for Ghana, Art. 58 DPA and for Switzerland Art. 10 FADP.

[163] Cf. Art. 41 § 3 LGPD and ANPD Resolution CD/ANPD No. 02.

[164] While the GDPR sees the regulation triggering risk where the controller is a public body, the information handling is comprehensive and on a regular basis or where sensitive information is handled, the PIPL sees the risk in the quantity of handled information.

[165] According to Art. 23 IV FADP, a controller can refrain from consulting the FDPIC after a data protection impact assessment resulted in the finding of a high risk, if they have consulted their internal data security advisor according to Art. 10 FADP.

know the concept as legal term, even though there is a common practice to appoint a "Chief Privacy Officer" (CPO).[166]

Internal responsibility management is not only addressed by appointing a data protection officer of some sorts, but also concerns regulation on organizational structures and supervision of employees handling personal information. Such regulation can be found in the provisions on data security, but is most apparent in Japan, in Art. 24 APPI.

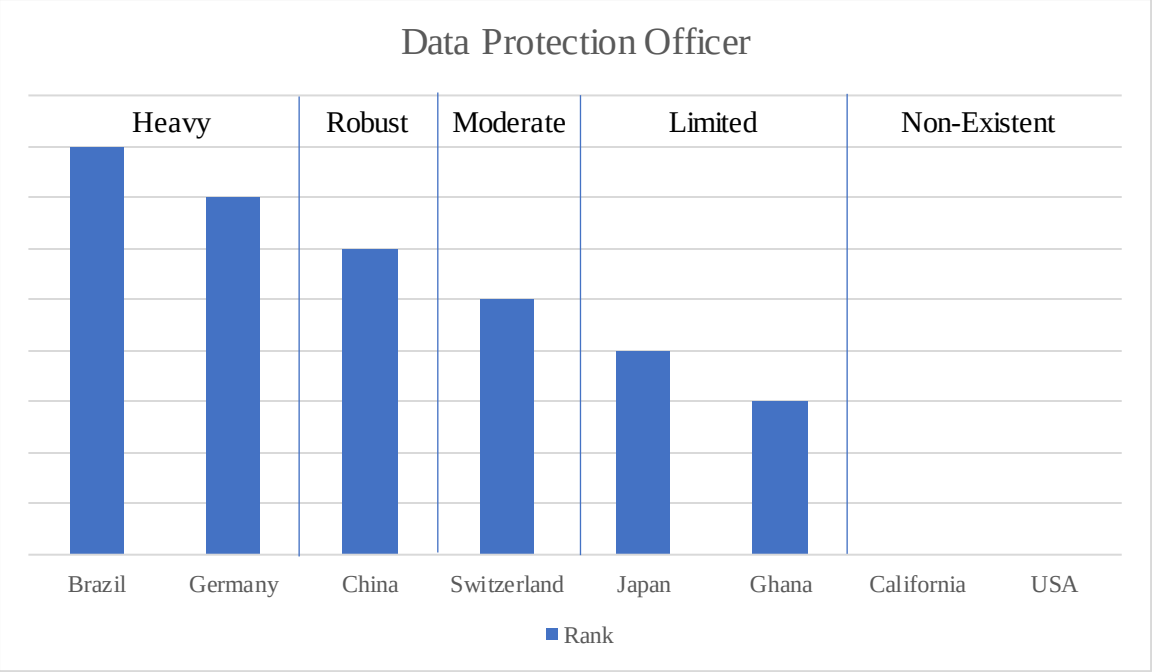

Figure 14: Ranking of regulation on internal responsibility management

14. Certification and Self-Regulation

As a general regulatory concept, regulated self-regulation is a popular alternative from direct state regulation.[167] In privacy protection laws the concept appears especially in the form of certification mechanisms, codes of conduct, and industry standards. However, in most jurisdictions such practices are not mandatory and do not have any legally binding effects but only ease compliance or offer other incentives.[168] Especially comprehensive regulation of such voluntary self-regulation can

[166] In this regard, Japan is a little more restrictive than the US, because the PPC recommends appointing a CPO as organizational security measure, cf. *PPC,* 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 04.03.2024). This could give raise to a factual obligation following chilling effects of looming PPC enforcement. However, this is a great example of the weaknesses of this methodology: Not legally defining a CPO ranks the US law lower than the Ghanaian one, even though the concept of a "data protection supervisor" in Ghanaian privacy practices is a lot less common than in the US. Nonetheless, as far as law in the books is concerned, the Ghanaian law imposes a higher restrictions on the controller because if he wants to appoint a responsible person, he must do so in accordance with the DPA.

[167] See on privacy regulation concepts beyond government regulation *Hirsch,* The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation, Seattle University Law Review (2011) pp. 455 et seqq. See on the term of "regulated self-regulation" coined by EU law, *Cafaggi,* Self-Regulation in European Contract Law, European Journal of Legal Studies (2007), p.163, 174.

[168] The designs of such regulation are manifold: In Switzerland successful certification may release from the obligation to conduct an impact assessment (Art. 22 V; 13 FADP). Slightly less incentivized, in Germany, successful certification or codes of conduct can ease the requirements for data security and impact assessments and can lower the sanctions (Art. 83 II lit. j); 35 VIII; 32 III GDPR). Also, in Brazil, sanctions can be lower, if the controller crafted

be found in Japan in the appearance of the "certified personal information protection organization" (Art. 47 et seqq. APPI).

The US and consequently California place a much more significant role in binding self-regulation. As FTC case law is one of the most dominant factors of federal privacy regulation[169], its enforcement of "broken promises" gives great relevance to the rules that companies impose on themselves.[170] A good codified example of this prominence and relevance is § 1798.140 (d)(4) CCPA, allowing entities which usually would not fall within the scope of the CCPA to declare themselves compliant with the CCPA and with that fall within its scope of application.

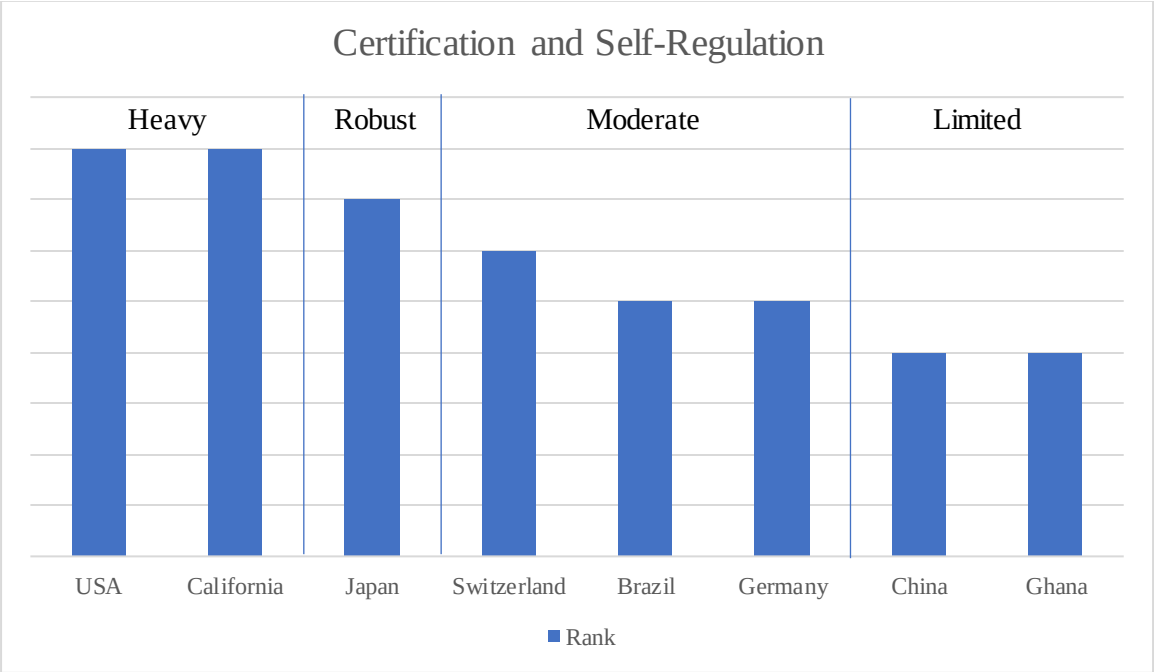

Figure 15: Ranking of the Regulation on Certification and Self-Regulation

15. Regulation on Public Information

This category on public information is in opposition to the other categories not a restrictive category but rather an enabling one. This is because most jurisdictions privilege the handling of information that have been made publicly accessible by either public authorities or the individual himself. Therefore, the most restrictive jurisdiction is the one that has implemented the least privileges for public information.

California has implemented the most privileges by entirely excluding information that the controller has reason to believe were made public by the individual.[171] In granting publicly accessible information protection under the First Amendment, the US in general allows most handling of such

internal compliance practices (Art. 52 § 1 IX LGPD). Ghana and China only allow for best practices and similar to ease factual compliance, but do not connect any hard legal consequence to such self-regulatory systems.

[169] See in general on the role of the FTC as regulator *Solove/Hartzog,* The FTC and the New Common Law of Privacy, Columbia Law Review (2014), p. 583.

[170] Ibid, pp. 628 et seqq.

[171] Cf. § 1798.140 (v)(2) CCPA.

information.[172] The only other jurisdiction that does not require the information to be made public by the individual themselves or a public authority is Ghana, allowing for subsequent processing of publicly accessible information in general.[173] Other wide-reaching privileges are found in China and Switzerland which allow handling public information as long as there is no opposing will.[174] Germany and Japan allow such privileges only when handling sensitive information (which allows for the interpretation that there is also a privilege for "normal" information)[175] while Brazil still requires a weighing of interests.[176]

One should note that a "right to be forgotten" or similar obliges to delete information made public by the controller after a certain time period and therefore also falls within the scope of this category. Such stricter regulation exists in Germany, Switzerland, Japan, and the US to (very) different extents.[177]

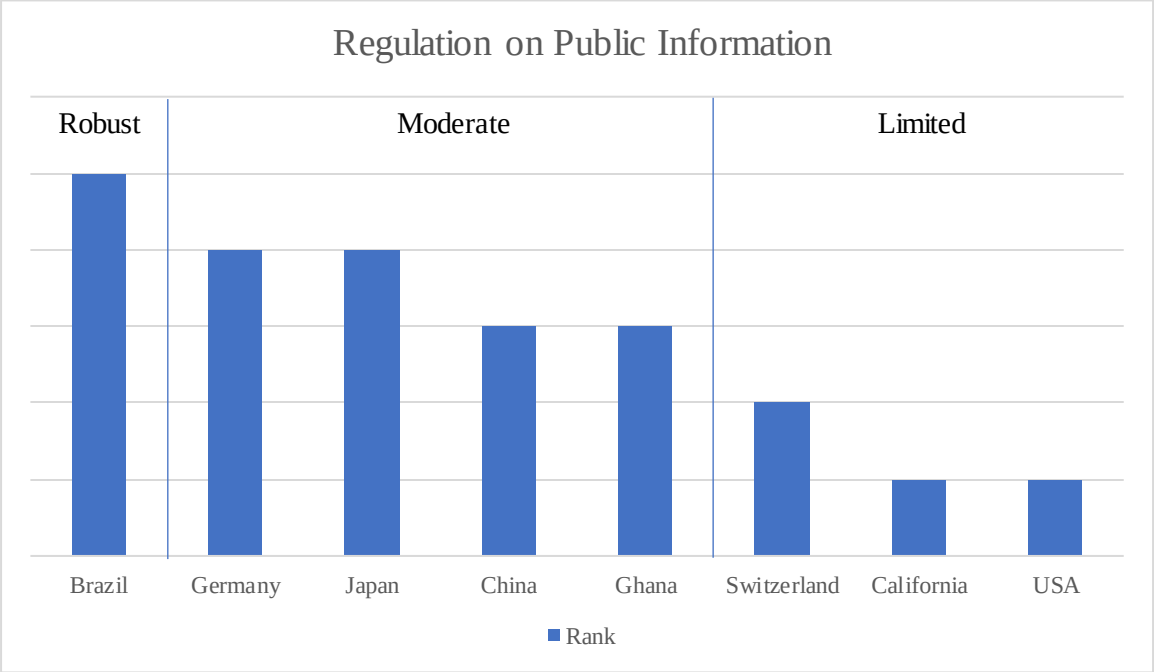

Figure 16: Ranking of regulation on publicly available information

[172] In making information public they are viewed as part of the public discourse which shall not be altered. This is best described by Restatement (Second) of Torts, § 652D comment b, which states that "there is no liability when the defendant merely gives further publicity to information about the plaintiff that is already public". See on public information and the First Amendment *Bambauer,* Is Data Speech?, Stanford Law Review (2014), pp. 57 et seqq. See on cases of privileged handling of personal information *Glocker,* Der California Consumer Privacy Act (2022), p. 51.

[173] Cf. Art. 25 III lit. b) DPA.

[174] See for China Art. 13 Nr. 6, 27 PIPL, and for Switzerland Art. 30 III FADP. Between the two, China is notably more restrictive as Art. 27 PIPL requires prior consent anyway, if there is a major influence on individual rights and interests.

[175] See for Germany Art. 9 II lit. e) GDPR and for Japan Art. 20 II (vii) APPI.

[176] Cf. Art. 7 § 3 LGPD.

[177] See for Germany Art. 17 II GDPR, for Switzerland *Rosenthal,* Das neue Datenschutzgesetz, Jusletter 16 (Dezember 2020) p. 52; for Japan *Zufall,* Challenging the EU's 'Right to be Forgotten'? Society's 'Right to Know' in Japan, European Data Protection Law Review (2019=, pp. 17 et seqq.; and for the US *Büyüksagis,* Towards a Transatlantic Concept of Data Privacy, Fordham Intellectual Property, Media & Entertainment Law Journal (2019), pp. 139 et seqq. with reference to the FCRA as US pendant to the fundamental *Google Spain* judgement of the CJEU.

16. Cyber Surveillance Authority

Especially having in mind the recent dispute of powers of security authorities to comprehensively collect information by monitoring telecommunication in context of the EU-US adequacy decision and the general debate on information prerogative or restriction of the state, regulation concerning cyber surveillance and investigative powers of public authorities in the context of signal intelligence play a vital role in modern privacy understandings.[178] The Regulatory Clustering has no intend to normatively contribute to this debate, but it must acknowledge that cyber surveillance is an important factor to determine the level of protection of personal information against public authorities (be their access lawful or unlawful). Therefore, the higher the hurdles for public authorities to gain access to personal information, the higher the assured level of privacy provided for by the respective jurisdiction. This does also fit within the frame of the underlying research question of disclosure behavior towards private actors, because many surveillance legislations do connect their surveillance measures to service providers the personal information were disclosed to (e.g. mass data retention and access requests).

As this clustering is conducted in the context of individual disclosure decisions, the most important factor will be the surveillance of telecommunication services (which were used for said disclosure). Such bodies of law can diverge heavily in its structure and may have very individualistic nuances depending on the analyzed jurisdiction. Therefore, this particular clustering shall only deliver a brief overview of possible telecommunication surveillance.

For a start, the two (geographically neighboring) extremes shall be pointed out: Japan and China. As previously mentioned, China classifies as "rule by law" country. Therefore, state authority surveillance must not necessarily abide to statutory law, even though the Chinese statutory law provides for commonly used safeguards.[179] In fact, it seems as though the Chinese legislator purposefully tries to cloud the hypothetical as well as factual surveillance powers of Chinese authorities.[180] It is well documented that the Chinese authoritarian system relies on comprehensive cyber surveillance tools, which is only underlined by statutory provisions such as the use of personal identity recognition to safeguard public security in Art. 26 PIPL or various disclosure obligations to the state in the context of its social credit system.[181] Therefore, it does not need detailed description of statutory law to rank China last.

On the very contrary, the Japanese legislation provides for very few authorities for cyber surveillance: As the constitution prescribes, the secrecy of communication can only be infringed for

---

[178] This debate does mainly take place in the context of international human rights law, *cf. Watt,* The Role of International Human Rights Law in the Protection of Online Privacy in the Age of Surveillance, 9th International Conference on Cyber Conflict (CyCon) (2017) but is also a political one, as can be seen in the EU-US conflict on the newly introduced Transatlantic Data Privacy Framework.

[179] Such safeguards are, for example, rule of law, proportionality, or purpose limitation, cf. *Cai,* Enforcing a New National Security? China's National Security Law and International Law, Journal of East Asia and International Law (2017), p. 81.

[180] *Qian et al.,* Four Takeaways From a Times Investigation Into China's Expanding Surveillance State, June 21, 2022, accessible under https://www.nytimes.com/2022/06/21/world/asia/china-surveillance-investigation.html (last accessed 04.03.2024).

[181] *Hünting,* Endeavour to contain Chinas' Tech Giants – Country Report on China, University of Passau IRDG Research Paper Series No. 22-15, pp. 19 et seq.

purposes of criminal prosecution.[182] In addition to the resulting refrain from national security signal intelligence, there is also no possibility to require access to information held by internet service/access provider – Art. 197 II of the Japanese Code of Criminal Procedure is only of voluntary nature, and (the common) non-compliance with the request of an official is not sanctioned.[183] The only relevant law for cyber surveillance is Art. 3 I of the Wiretapping Act[184], allowing public prosecutors and judicial police officers to intercept communication with a judicial warrant, if there are sufficient grounds to suspect that the subject has committed one of certain serious crimes and where the interception is necessary for the prosecution and it is extremely difficult to achieve the same purpose otherwise. The resulting lack of surveillance powers of Japanese authorities not only entails criticism of the functionality of Japanese cyber security law,[185] but also constitutes the highest level of protection for communication data in this clustering.

With that, the core elements of international cyber surveillance can be lined out as follows: Intercepting communication for criminal prosecution purposes, (national) security purposes and strategic intelligence purposes, which can be differentiated between foreign and domestic signal intelligence. Such interception is flanked by the possibility to request access to information stored by telecommunication companies. To provide efficient access, this regulation is often accompanied by a mass data retention obligation. Common ground for justification of surveillance measures is the reasonable cause to suspect that a certain serious crime (such as terrorism, drug and human trafficking, money laundering or organized crime) was committed or planned, subsidiarity of communication surveillance to other fact-finding measures, and (strict) necessity for the specific purpose. Another very central aspect is the judicial reservation and a "judicial-like"[186] surveillance of the intelligence community.

Within this general framework, there are more and less distinguishable nuances between the remaining jurisdictions: The most restrictive designs can be found in Germany and Switzerland, which have quite similar legislation on cyber surveillance: both have most of the above-mentioned measures and safeguards in place but allow for exemptions to judicial reservation when requesting inventory data from telecommunication companies.[187] While Swiss law provides for more

---

[182] Art. 35 of the Japanese Constitution. See on this interpretation the self-declaration of the Japanese ministry of justice in the adequacy decision between Japan and the EU from 14 September, 2018 (OJ L 2019/76, 19.3.2019), p. 54.

[183] Ibid, p. 48.

[184] Act No. 137 of August 18, 1999 on Communications Interception for Criminal Investigation.

[185] *Tsuchiya,* Japan's Response to Cyber Threats in the Surveillance Age, Seton Hall Journal of Diplomacy and International Relations (2015), pp. 7, 18.

[186] This terminology originates from the German Federal Constitutional Court (BVerfG, judgement of 19.5.2020 – 1 BvR 2835/17, NJW 2020, p. 2235), but can be seen in various other concepts such as the US Foreign Intelligence Surveillance Court (FISC).

[187] Cf. for interception of communication for criminal prosecution purposes § 100a of the German Code of Criminal Procedure and §§ 269 et seqq. of the Swiss Code of Criminal Procedure. Additionally, there are some different provisions in the respective intelligence law, which boil down to a very similar framework, cf. for Germany §§ 172 et seqq. of the Telecommunications Act (TKG); §§ 5, 49 et seqq. of the Act on the Federal Criminal Police Office (BKAG); the Article 10 Act (G-10); or §§ 3 et seqq., 19 et seqq. of the Act on the Federal Intelligence Service (BNDG). Cf. for Switzerland the entire Federal Act on the Surveillance of Post and Telecommunication (BÜPF) of 2016, as well as Art. 27 et seqq. of the Federal Act on the Intelligence Service (NDBG) of 2015.

protection in cases of foreign intelligence,[188] it is less restrictive when it comes to especially mass data retention.[189]

The now remaining jurisdictions rank below Germany and Switzerland, because especially they do allow for a much more rigorous scope of surveillance: While this is true for Brazil to the extent that the requirements are less intensive,[190] that in practice, procedural requirements are less intensive,[191] that there is a stricter mass data retention obligation,[192] and that ANATEL[193] uses a program to directly and sweepingly require access to stored traffic data,[194] the Brazilian law employs a similar constitutional restriction as Japan, so that Art. 5 XII of the Brazil constitution does only allow interception of communication for the purposes of criminal investigation and prosecution.[195] Thusly, Brazil ranks slightly higher than the US, and – given the subsidiary nature of state law – also California. Main point of criticism in the US is the possibility of indiscriminate bulk collection of information either from communication interception or access requests ("National Security Letters") by surveillance authorities (mainly the National Security Agency (NSA) and Federal Bureau of Investigation (FBI)).[196] Most strikingly, there are situations, where judicial reservation can be replaced by a simple administrative subpoena[197] or by decisions of the president through the

---

[188] While Art. 26 III NDBG prescribes the same requirements as for domestic intelligence to foreign intelligence, with the exemption of infiltration of foreign IT systems, Germany provides for a special regime for foreign intelligence, with § 19 and § 23 BNDG not requiring judicial reservation and potentially allowing for mass collection.

[189] Art. 21 II and 26 V BÜPF requires telecommunication providers to store all inventory and traffic data for 6 months. However, this mass data retention is currently pending before the ECtHR, cf. *Kire,* Vorratsdatenspeicherung am Europäischen Gerichtshof für Menschenrechte, 05.07.2023, accessible under: https://www.digitale-gesellschaft.ch/2023/07/05/vorratsdatenspeicherung-am-europaeischen-gerichtshof-fuer-menschenrechte-digitale-gesellschaft-vs-schweiz/ (last accessed 04.03.2024). In Germany, the CJEU has declared the similar § 176 TKG as unlawful, because the risk of indiscriminate mass collection without specific connection to the individual case violates the right to data protection and secrecy of communication, cf. CJEU, judgement of 20.9.2022 – C-794/19, NJW 2022, p. 3135.

[190] Especially, surveillance can apply to any crimes that are not sanctioned with "mere" retention, and the judicial reservation is abandoned (and not replaced with other "judicial-like" supervision) for certain data such as e-mail address, telephone number, or the national identity number, *Dahlmann et al.,* Privacy and Surveillance in the Digital Age: a comparative study of the Brazilian and German legal framework (November 2015), p. 16.

[191] For example, even though the Wiretapping Act of 1998 (Law 9.296), in Art. 5, stipulates that in general, the maximum period of interception is 15 days, in practice, the Brazilian Supreme Court has stretched this duration to up to 7 months, cf. ibid, pp. 7 et seq.

[192] According to Art. 13 et seqq. of the Marco Civil of 2013 (Law 12.850), certain traffic data must be stored for up to 12 months.

[193] The Brazilian Communications Agency.

[194] *Magrani,* Systematic Government Access to Private-Sector Data in Brazil, International Data Privacy Law (2014). pp. 30, 33. Note that this only imposes a risk of surveillance, as the ANATEL has declared that they do not use such data for surveillance purposes.

[195] *Santoro,* Epistemic Problems of Telephone Interception in Brazil, Journal of Law and Criminal Justice (June 2023), pp. 13, 15.

[196] The critics of such authorizations (mainly the Federal Wiretap Act of 1986 (18 USC §§ 2510 – 2523), the Stored Communications Act of 1986 (18 USC §§ 2701 – 2713), and the Foreign Intelligence Surveillance Act of 1978 (50 USC §§ 1801 – 1885c) can be found in the CJEU judgement invalidating the EU-US Privacy Shield (CJEU, judgement of 16.7.2020 – C-311/18, NJW 2020, p. 2613) as well as in the accompanying literature (for example *Wittmann,* Nobody Watches the Watchmen – Rechtliche Rahmenbedingungen und zunehmende Ausweitung der öffentlichen Videoüberwachung in den USA, ZaöRV (2013) 371). See on a more favorable view on the US practice of surveillance *Posner,* Privacy, Surveillance, and Law, The University of Chicago Law Review (2008), p. 245; and *Yoo,* The Legality of the National Security Agency's Bulk Data Surveillance Programs, Harvard Journal of Law & Public Policy (2014), p. 901.

[197] For example, 18 USC § 2703 (b)(1)(B).

Attorney General[198], which may circumvent effective and transparent[199] judicial control as to whether the surveillance activity was necessary for the concrete minimal[200] purpose. Finally, while other countries' intelligence communities can profit from the benefit of the doubt that they have not overly stretched or abused their surveillance powers, the Snowden revelations in 2013 have cast a shadow on the actual scope to which the US intelligence community does still conduct mass surveillance measures.

Finally, there is the rather rudimentary framework of Ghana. Its core[201] consists of the so called "Spy Bill"[202], which allows the National Security Supervisor in cases of urgency to authorize to intercept communication for 48 hours (Art. 4 III). This was argued to be a gateway for abuse and not suitable to protect the Ghanaian citizens' privacy.[203] While such criticisms follow a similar line like in the case of the US, it must also be pointed out that the scope of application of Ghanaian cybersurveillance law is rather vague and broad,[204] and mass data retention in Art. 77 of the Cybersecurity Act is quite significant.[205] It ultimately ranks Ghana below the US, which has no history of mandatory mass data retention.[206]

---

198 For example, 50 USC § 1802.

199 Even though activities of the intelligence community are supervised by the Foreign Intelligence Surveillance Court, this courts' hearings are held in secret, cf. *in re Motion for Release of Court Records*, 526 F. Supp. 2d 484, 487-90 (FISC 2007).

200 A minimization principle can be found in various provisions of the US surveillance law statutes. The most popular example for such restriction is the Presidential Policy Directive - Signal Intelligence Activities of 2014 (PPD-28) that states in § 1 (d), that all signal intelligence activities shall be "as tailored as feasible". Such minimization is vital part of the constitutional level of protection granted (only to US citizens) by the Fourth Amendment, see *Rubinstein,* Minimization and the Fourth Amendment, New York Law Forum (1974), p. 861.

201 See for other relevant laws concerning intelligence and especially criminal prosecution *Apau/Koranteng,* An overview of the digital forensic investigation infrastructure of Ghana, Forensic Science International: Synergy (2020), pp. 299, 301 et seq.

202 Interception of Postal Packets and Telecommunication Messages Bill of 2016.

203 *Adarkwah,* Counter-Terrorism Framework and Individual Liberties in Ghana, African Journal of International and Comparative Law (2020), pp. 50, 60 et seqq.

204 For example, Art. 2 I of the Spy Bill allows for interception for the purposes of *inter alia* "fighting crime in general", or "other serious crimes", or Art. 69 of the Cybersecurity Law of 2020 (Act 1038) only requires a specific criminal investigation regardless of the nature of the crime.

205 Traffic and content (!) data must be stored for at least twelve months, which can be extended by the high court, and inventory data must even be stored for six years.

206 *Determann,* Datenschutz in den USA – Dichtung und Wahrheit, NVwZ (2016), pp. 561, 566.

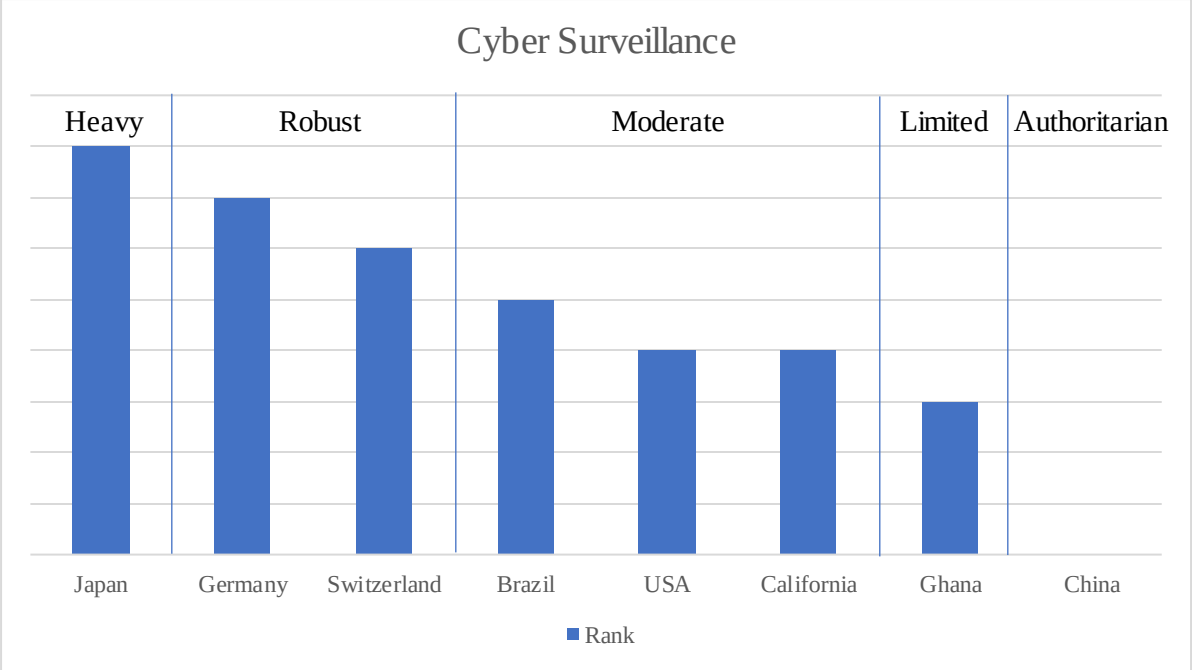

Figure 17: Ranking of regulation on cyber surveillance activities

II. 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.

1. Consent

Predominant throughout most jurisdiction is the concept of individual consent. The assessment of restrictions due to a consent requirement is twofold: First and foremost, it looks into the relative relevance of consent in the respective jurisdiction. Then, it takes prerequisites of valid consent into account.

Regarding the relevance, there is a great overlap with the general prerequisites (→ I.1.): The countries implementing a prohibition subject to permission use consent as main (but not only/exclusive) element of authorization[207]. Even in such jurisdictions where there is no prohibition subject to permission, consent is often needed for certain justification. This is the case in Switzerland, excluding a violation of personality[208], and for Japan, requiring consent for subsequent information handling, third party transfers, and sensitive information[209]. What all these jurisdictions have in common is the fact that consent is either factually or legally primary ground of authorization for handling personal information[210]. In this regard, Japan holds a rather special position, as the APPI (in

[207] See for Brazil Art. 7 I LGPD, for China Art. 13 Nr. 1 PIPL, for Germany Art. 6 I lit. a) GDPR, and for Ghana Art. 20 I DPA.

[208] Cf. Art. 31 I FADP.

[209] Cf. Art. Art. 18 I and II, Art. 20 II, and Art. 27 I APPI.

[210] Due to legal uncertainty of other grounds of authorization, especially when it comes to a weighing of interests, controllers are more likely to choose consent between various possible grounds of authorization. Even when not assuming such primacy of consent (*Veil,* Einwilligung oder berechtigtes Interesse? – Datenverarbeitung zwischen Skylla und Charybdis, NJW (2018), p. 3337), some legislations place consent in a position that claim primacy over

Art. 18 III, 20 II, and 27) names exemptions to consent, none of which being overriding private interest. Thusly, consent has a *de facto* greater importance in relation to other bases for authorization of information handling. In opposition to such trends some jurisdictions like Brazil[211] have created incentives not to rely solely on consent when handling personal information. Such incentives can also be the possibility to always withdraw consent, which is possible in every examined jurisdiction except for Ghana and Japan.

As Californian and US law does not focus on prohibiting or restricting the collection of information, pre-disclosure consent holds no relevance in these jurisdictions, except for sector specific peculiarities such as the protection of children's privacy[212].

When it comes to prerequisites of valid consent, the maximum (and to this extent regular) requirements are that the consent must be freely given[213], for a specific case and purpose, informed, and unambiguous. Such comprehensive requirements can be found in Brazil, California, China, and Germany[214]. Only Japan and especially Switzerland negatively deviate from this standard, because they allow for implicit consent in certain cases[215]. Despite the authorization in Art. 94 I lit. b) DPA, Ghana has not yet specified upon its consent requirements.

other bases of authorization that are only stipulated as exceptions to consent, cf. Art. 20 I DPA (Ghana) or Art. 27 APPI (Japan).

[211] For example, Art. 7 § 5 LGPD, which requires to obtain consent before third party transfer, if the original collection was based on consent, or Art. 9 § 2 LGPD, which requires to always give an option to opt-out, when the original collection was based on consent.

[212] Cf. on federal level 15 USC § 6502 (b)(1)(ii) (COPPA) or on Californian level § 1798.120 (d) CCPA.

[213] This often includes the prohibition to unnecessarily couple consent with other services.

[214] See for Brazil Art. 5 XII LGPD, for California § 1798.140 (h), for China Art. 14, 16 PIPL, and for Germany Art. 4 I Nr. 11 and 7 IV GDPR. Ghana is only not listed here, because the specifications on consent referred to in Art. 94 I (b) DPA are not yet enacted.

[215] See for Switzerland Art. 6 VII FADP, which requires explicit consent only for handling sensitive information and high-risk profiling. In Japan, the APPI is silent on further requirements of consent. However, the PPC has indicated, that implied consent may be possible in certain cases, cf. *Paulger,* Japan – Status of Consent for Processing Personal Data (7.9.2022), p. 7, accessible under https://fpf.org/wp-content/uploads/2022/09/ABLI-FPF-Consent-Project-Japan-Jurisdiction-Report.pdf (last accessed 04.03.2024).

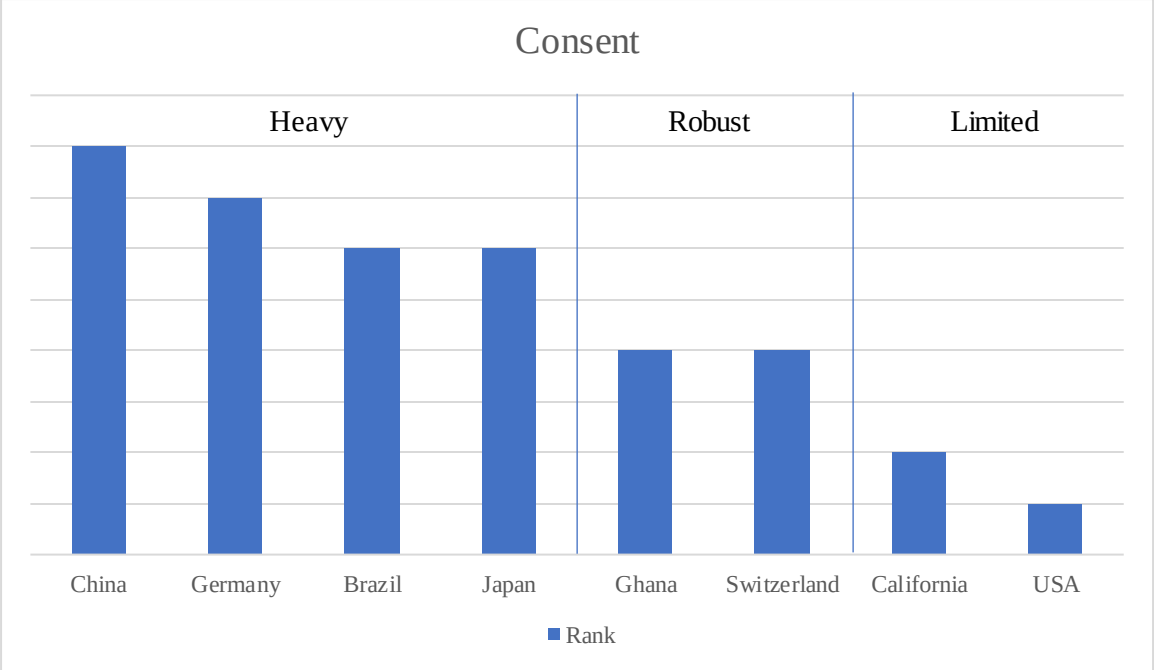

Figure 18: Ranking of regulation concerning consent

2. Right to Object / Opt-Out

While consent is a method of empowering the individual to decide on the handling of their personal information before such information was collected, the counterpart for co-determination after the information collection is regulation giving the individual a right to object or opt-out from the information handling. Enacting such right would terminate the legal allowance to further handle personal information.

But only Ghana comes even remotely close to this extent by giving the individual the right to always (i.e. without prerequisites) object unless otherwise provided by law.[216] This is to be understood as meaning that the objection is only inadmissible if the law provides for the irrelevance of opposing will.[217] Similar to this is the regulation in California[218], where it is always allowed to opt-out from selling or sharing personal information, which encompasses most third-party transfers. While this individual right is certainly a formidable one and provides for the core of notice-and-choice-based regulation, it is not a general right comparable to other jurisdictions that applies to any information handling activity. However, this right to opt-out is accompanied by a right to restrict handling sensitive information to that use which is necessary for the legitimate (i.e. benefiting the individual) purpose[219]. Both rights having no notable exemptions[220] and being central to the Californian approach to privacy protection, the possibilities of individual co-determination rank higher than general rights to objection in most other jurisdictions. Even if not codified, that does also apply for

[216] Cf. Art. 20 II DPA.

[217] This could be, for example, a disclosure obligations or information handling for public purposes (listed in Art. 60 et seqq. DPA).

[218] Cf. § 1798.120 CCPA.

[219] Cf. § 1798.121 CCPA.

[220] Only the general very specific exemptions of § 1798.145 CCPA apply.

the federal level of the US: FTC case law, by embracing the "notice and choice"[221] approach, lends great relevance to the possibility to opt-out as means of "choice".[222]

Most common design of a right to object/opt-out is the weighing of interests, whether the individual shall be granted the possibility to terminate otherwise lawful information handling. This is most apparent in Switzerland, where information handling despite opposition constitutes a violation of personality that can be justified by overriding interest[223]. Leaning slightly more to the interests of the controller is the German right to objection, which only allows objection for reasons relating to the particular situation of the individual such as occurred data breaches and also then allows for exemptions due to compelling overriding interests of the controller[224], which can be archive, research, or other public purposes[225]. Only Japan grants a less restrictive right by only allowing objection in cases of violation of law, data breaches, incompatible secondary purposes, and impending harm[226]. This less restrictive nature is completed by – in contrast to the aforementioned jurisdictions – not including a right to revoke consent.

Other jurisdictions relying on a prohibition subject to permission only[227] provide for a right to objection in the form of revocation of consent, which naturally enables objection only for cases where information handling was (solely) based on consent. Examples for such regulation are Brazil and China[228], even though both name a right to oppose/refuse information handling, which is, however, mostly of declaratory nature[229].

Lastly, it should be mentioned that in every jurisdiction (mostly in appearance of purpose limitation, specified consent or information handling authorization in relation to performance of contract) allow for a reflexive control option for the individual to co-determine the manner in which

---

[221] See on this model already above, → C.I.3.

[222] *Solove/Hartzog,* The FTC and the New Common Law of Privacy, Columbia Law Review (2014), pp. 583, 634. The underlying concept of enabling the individual to have agency over information about him especially prohibits commercial third-party transfers or publicizations without giving opportunity to opt-out, cf. *Keegan/Schroeder,* Unpacking Unfairness: The FTC's Evolving Measures of Privacy Harms, Journal of Law, Economics & Policy (2019), pp. 19, 29, 34.

[223] Cf. Art. 30 II lit. b) and 31 II FADP. This is not exactly a "right" but enables the individual to express his disregard of information handling activities. If such disregard is also of legitimate and overriding interest, it would lead to a prohibition of information handling.

[224] Cf. Art. 21 GDPR. On the "particular situations" giving rise to the right, see *Schulz,* in: Gola/Heckmann (eds.), Datenschutz-Grundverordnung – Bundesdatenschutzgesetz (3rd edition 2022) Art. 21 DSGVO N 10. One must also keep in mind that this right does only include information handling based on legitimate interest, as opposed to Art. 7 III GDPR, which provides for an opt-out possibility in cases of consent (revocation of consent).

[225] When talking about exemptions to a right granted to the individual by the GDPR, one must always consider the modifications made by §§ 27 et seqq. BDSG (including modification and restrictions to protect certain privileged interests, such as research, public archives, or legal confidentiality) enacted pursuant to Art. 23 GDPR. In this case §§ 27 II; 28 IV; and 36 BDSG become relevant.

[226] Cf. Art. 35 I, V APPI. In comparison to the GDPR, this is a more precise and therefore final definition and does also not include direct marketing purposes (cf. Art. 21 II GDPR).

[227] This is a difference to Germany, Switzerland and the US, where revocation of consent and objection are possible parallelly (and sometimes synonymous), and Ghana and Japan, where only objection is possible.

[228] See for Brazil Art. 8 § 5 and Art. 9 § 2 LGPD and for China Art. 15 PIPL.

[229] See for Brazil Art. 18 § 2 LGPD and for China Art. 44 PIPL: for both, the right to objection is nothing more than a right to deletion, which can be interpreted as aiming at one and the same function. Therefore, in both jurisdictions, the right to objection and deletion can be understood as identical.

their personal information is handled. This does not *per se* constitute a right to object or opt-out, but rather a (very limited) right to opt-in.

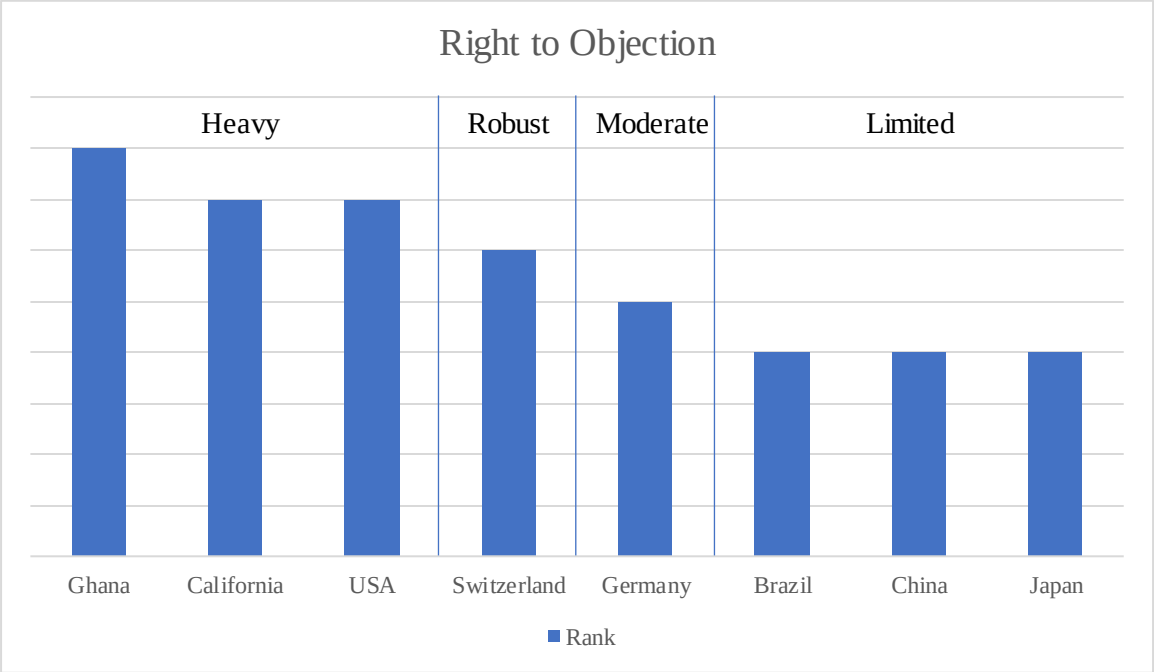

Figure 19: Ranking of regulation on objection rights

3. Right to Deletion

While objecting information handling activities prohibits the controller to use the information available to them and generally withdraws the authorization to handle personal information, a right to deletion requires the controller to dispose of all available personal information. Throughout all examined jurisdictions common grounds for requesting deletion are unauthorized information handling, revocation of consent (where applicable), objection (where applicable), and excessive/unnecessary information handling[230]. An exception to this is Japan, only requiring certain violations[231], and Switzerland, requiring unlawful violation of personality. Only the latter does not notably lower the restrictiveness of the regulation, because nearly all principle of the FADP are included in the concept of personality violation.

Especially California and the US stand out in this regard: § 1798.105 (a) CCPA grants the consumer the right to always request deletion of all collected personal information about him. This is only restricted by § 1798.105 (d), allowing for wide reaching examples such as (amongst others) free speech, necessity for performance of contract, or internal use, which could potentially limit deletion by a great extent, but they do not surpass other exemptions from other jurisdiction by a lot. However, this does not compensate the restrictiveness of not having any prerequisites. As far as the federal US is concerned, the right to deletion without further prerequisites is also vital part of the

[230] Cf. for Brazil Art. 18 IV and VI LGPD, for China Art. 47 PIPL, for Germany Art. 17 GDPR, for Ghana Art. 33 DPA, for Japan Art. 35 APPI, and for Switzerland Art. 32 II FADP.

[231] Art. 35 I, III APPI refers insofar to Art. 18, 19, 20, 26 and 27 APPI (purpose limitation, appropriateness, handling of sensitive information, third party transfers).

"notice and choice"[232] approach and can therefore be seen not different then in context of a right to opt-out. Such trends can also be observed in federal statutory privacy laws[233].

Switzerland does require a violation of their respective privacy legislation, but in turn does not prescribe exemptions to deletion requests (apart from justifications of privacy violations, Art. 31 FADP), which is similar to Ghana with the exception that Art. 33 I DPA does only refer to data quality, data minimization, and authorization to obtain information. This is, in its restrictiveness, similar to Brazil, which knows exemptions only in such cases where information to be deleted were handled based on consent but encompass all aforementioned possible grounds for deletion[234].

Apart from that, more or less restrictive exemptions to a request for deletion may vary in their concrete scope. China, in Art. 47 II PIPL, only permits to securely store information where a retention period prescribed by law has not expired yet or deletion is technically hard to realize, which can be compared to exemptions in Japan[235]. The widest exemptions to a right to deletion are found in Germany, exempting deletion of information which are necessary for exercising the freedom of speech, fulfilling legal obligations, certain public interests and for invoking or defending legal claims[236].

It shall also be worth mentioning that jurisdictions often provide for alternatives to deletion after receiving a deletion request, often relating to solely internal use or safe retention for certain purposes as anonymized information[237].

---

[232] See on this model already above, → C.I.3.

[233] For example, 16 CFR § 312.6 (a)(2) (COPPA Rule) or 15 USC § 1681s-2 (b)(1)(E)(ii) (FCRA).

[234] Cf. Art. 18 IV LGPD ("processed in noncompliance with the provisions of this law"), which in contrast to Art. 18 VI LGPD does not refer to Art. 16 LGPD. However, the exemptions include lawful transfer to third parties and internal use, which are rather narrow, and are therefore suitable to restrict the right to deletion and ease compliance costs for Brazilian controllers.

[235] Cf. Art. 35 II, IV APPI: Information must not be deleted if deletion would require a costly expenditure or is otherwise hard to realize. Note that the Japanese right to deletion does only apply to certain violations, which are unlawful purpose, inappropriate use, unlawful handling of sensitive information, or unlawful third-party transfers, and is therefore ranked below China.

[236] Cf. Art. 17 III GDPR. Further exemptions (especially unreasonable expenses) to a right to deletion can be found in § 35 BDSG.

[237] Cf. for Brazil Art. 16 IV LGPD, for California § 1798.105 (c)(2) and § 1798.145 (a)(6) CCPA, for China Art. 47 II PIPL, and for Germany § 35 BDSG in combination with Art. 18 GDPR. This alternative for anonymization can factually also be derived from the common principle that anonymized information is not subject to privacy regulation (either due to not identifying an individual or being statutory excluded from regulation).

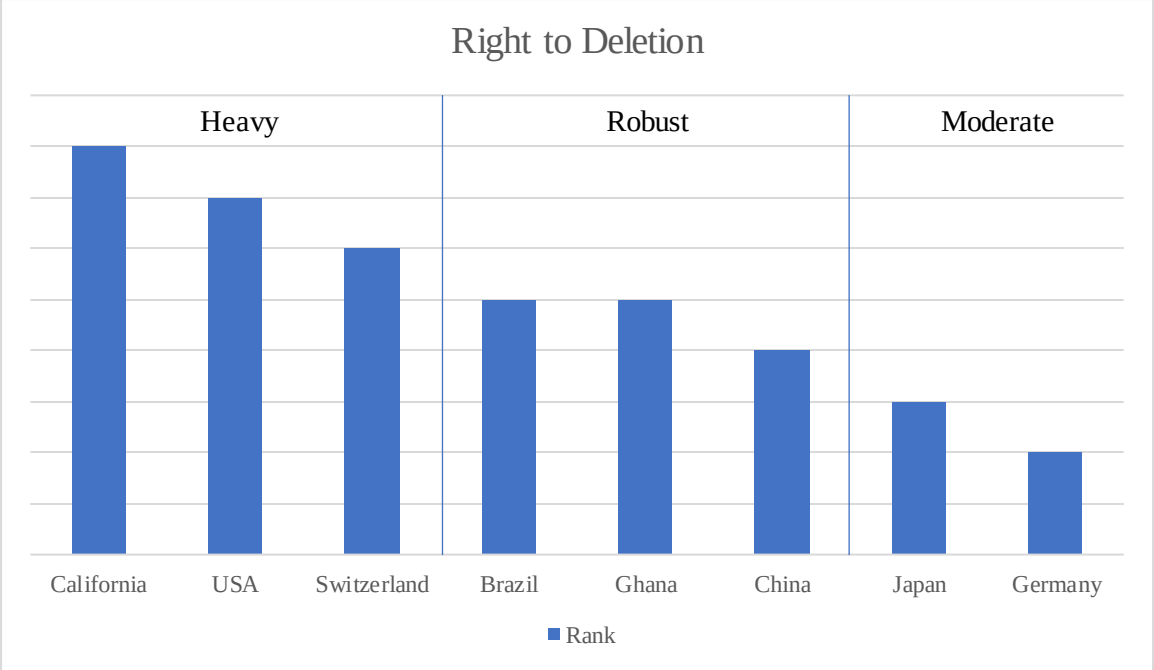

Figure 20: Ranking of regulation on deletion rights

4. Right to Rectification

As a right to deletion is addressing unauthorized information handling, a right to rectification addresses information that violate the data quality (→ I.9.) principle: Inaccurate, incomplete, or not up-to-date information must be corrected accordingly upon request. Such examples without mentionable exemptions can be found in Brazil, China, Germany, and Japan.[238]

This basic description is only surpassed by Ghana, which pairs the right to rectification with the right to deletion and additionally allows for correction of excessive, misleading or unlawful information.[239]

On the other hand, "accuracy" of personal information could be interpreted in the way that they are correct in relation to the purpose. This may especially exclude certain cases of factual incomplete or not up-to-date data. California and Switzerland implement such approaches and are also the only jurisdictions which allow for exemptions to the right to rectification.[240] Only the federal US, that does not place a lot of significance in accuracy of information ranks lower. Resembling

[238] See for Brazil Art. 18 III LGPD, for China Art. 46 PIPL, for Germany Art. 16 GDPR, and for Japan Art. 34 APPI. However, Germany explicitly provides for exemption when information is handled for research, or archive purposes, cf. §§ 27 II; 28 III BDSG.

[239] Art. 33 I lit. a) DPA.

[240] § 1798.106 (a) CCPA allows for rectification "taking into account the nature of the personal information", which is also subject to commercial reasonableness of the efforts, § 1798.196 (c) CCPA. In Switzerland, the relative approach originates not only from the relative definition of data quality in Art. 6 V FADP, but also from the exceptions of legal obligation and public archive purposes in Art. 32 I FADP.

the significance of a data quality principle, a right to rectification can only be found in sector specific regulation[241] or in the form of the false publicity tort.[242]

One should note that some jurisdictions require – accompanying a right to rectification – a contestation note in *non liquet* situations.[243]

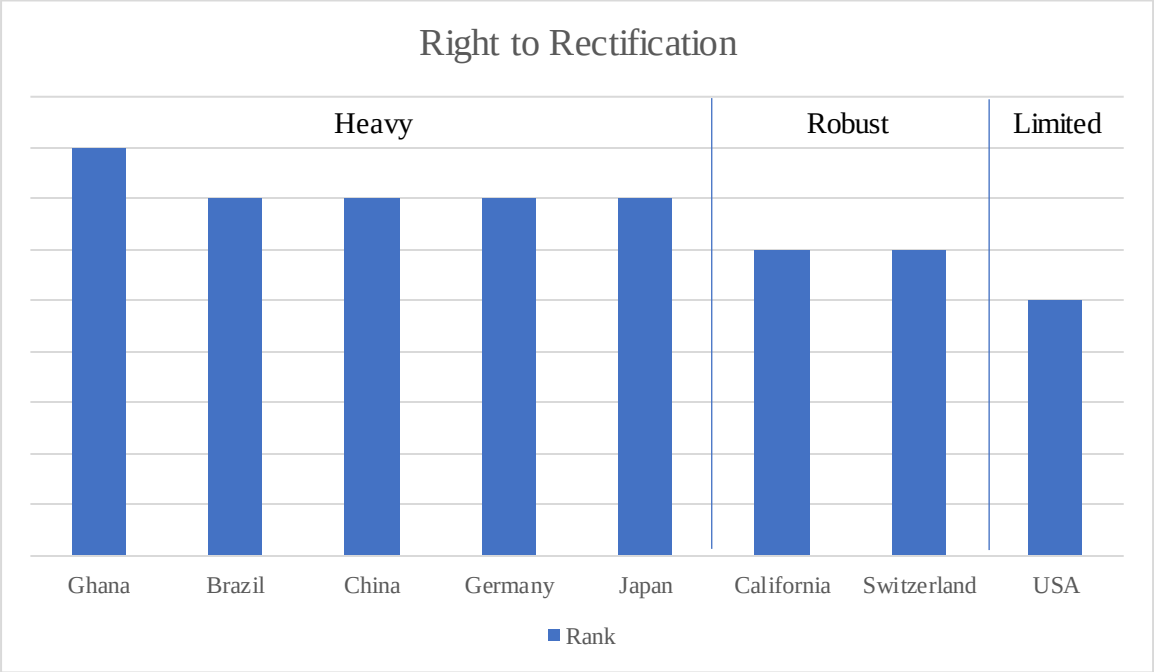

Figure 21: Ranking of regulation on rectification rights

5. Right to Access

The right to access holds central significance in all jurisdictions when it comes to empowering the individual regarding knowledge on information handling activities and the potential exercise of accompanying individual rights. As such, all jurisdictions require the controller to disclose information on the handled information to the individual on his request. Commonly, these are: confirmation of information handling as well as access to "raw" information, the categories of handled information, as well as sources of them, handling purposes, recipients in cases of third-party transfers, whether there is an automated decision-making, the individual rights, and applicable retention periods.[244] Japan and China (and to some extent Brazil) rather rely on only granting the individual direct, "raw" access to the handled information.[245] Note, however, that Japan refrains from any explanation on the handled information, while China does implement a right to "explain personal information handling rules"[246]. Due to the fragmented nature of its law, the US is difficult to classify

---

[241] Cf. 15 USC § 1681i (FCRA). This is due to the high damage potential of inaccurate information in contexts of credit reporting.

[242] Restatement (Second) of torts § 652E. This tortious liability is, however, not tailored to address handling of inaccurate information and is also not recognized in all states yet.

[243] See for Ghana Art. 33 III DPA and for Switzerland Art. 32 III FADP.

[244] At least, to this extent, this information is required in California (§ 1798.110 (a) CCPA), Germany (Art. 15 I GDPR), Ghana (Art. 35 I DPA), and Switzerland (Art. 25 II FADP). In Brazil, the catalogue in Art. 18 LGPD is comparable but misses certain vital information like handling purpose or recipients of third-party transfers.

[245] See for China Art. 45 PIPL and for Japan Art. 33 I APPI.

[246] Art. 48 PIPL.

especially in regards of access rights. This is because most federal legislation on privacy includes some form of a right to access, which is always slightly different in design[247]. While this shows a certain prominence of access rights in the US, it is also apparent that, where existent, such rights include access to "raw" information and explanation of basic circumstances. With that, the USA best resembles the regulation in China.

Clear order in the regimes of information access rights can be brought by examining the different exemptions to such rights.[248] Of course, all jurisdictions provide for exemptions because of some form of confidentiality of the requested information.[249] Besides rather neglectable exemptions (jeopardy of certain interests[250]), striking exemptions exist in Ghana and Japan: Ghana is the only country that restricts access requests of multi-referential information to the extent that accessing information that could identify another person often requires the consent of an also identifiable third person.[251] Somewhat even more restrictive, Japan allows to refuse access requests, where – amongst others – it would seriously interfere with the proper implementation of the controller's business.[252]

---

[247] For example, such regulation is to be found in 47 USC § 551 (d) (Cables Act); 15 USC § 1681g (FCRA); 15 USC § 6502 (b)(1)(B) in combination with 16 CFR § 312.6 (COPPA); or 45 CFR § 164.524 and 45 CFR § 164.520 (HIPAA).

[248] At this point, it is worth mentioning that the potential exemptions of all rights examined here are a clear indication for intensity of regulation.

[249] Cf. for California § 1798.145 China Art. 45, 18 I PIPL, for Germany § 29 I BDSG, for Ghana Art. 35 II, for Japan Art. 33 II (i) APPI, and for Switzerland Art. 26 I lit a) and b) FADP. Note that the latter two jurisdictions do not require explicit "confidentiality" but use the much wider terminus of third-party interest.

[250] Even though this can fall under the definition of confidentiality in some jurisdictions, such interests like research, or protection civil procedure, can be found for example in California (§ 1798.145 (a)(5) or § 1798.146 (a)(5)) and in Germany (§§ 27 II, 28 II, 33 BDSG).

[251] Cf. Art. 35 IV–VIII DPA.

[252] Cf. Art. 33 II (ii) APPI. However, this could be understood similarly to the Swiss exemption in Art. 26 I lit. c) FADP, that exempts "troublemaking" requests. But even then, the APPI can constitute exemptions beyond this "troublemaking" requirement.

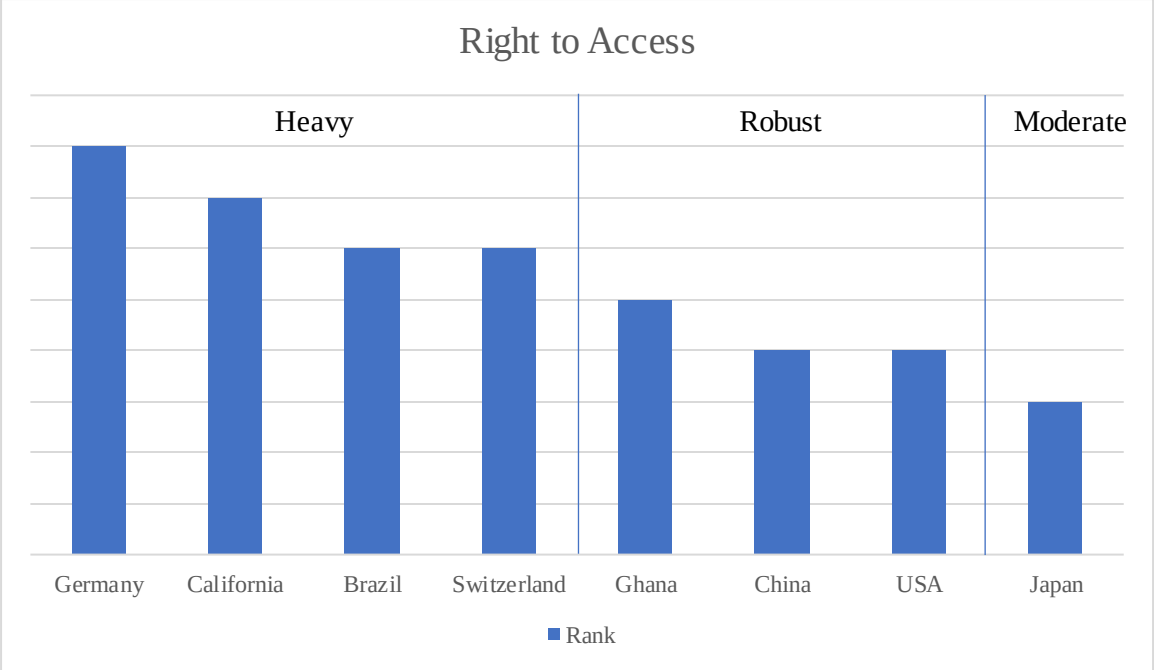

Figure 22: Ranking of regulation on access rights

6. Right to Data Portability

The right to data portability is somewhat a subcategory of the right to "raw" access. However, its implications for modern digital competition and utility of information attest a not negligible significance to such right to data portability. It enables the individual to receive a copy of the handled information in a readily readable format. Even more so, an individual may request to transfer information to a third party in an interoperable format.

As it is a subcategory of the right to access, some jurisdictions – mainly Ghana and Japan[253] – only provide for a factual data portability in the sense that an individual can request a copy of the "raw" information handled by one controller and then manually transfer this copy to another controller. This, however, does not constitute a sole "right to data portability", but only a modification to the right to access. Such modifications can *de facto* constitute a right to data portability, which is demonstrated by the example of California: The CCPA does not require the controller to transfer information directly, but to provide it in a format that allows the individual to transfer the information without further hinderance.[254] Adopting the rather specific exemptions of the right to access (→ 5.) and directly targeting the feasibility of third-party transfers, California ranks a lot higher than Ghana and Japan, despite also not requiring transfer itself.

Nonetheless, it is more common that there is a special modification that obligates the controller to transfer information directly, which one can observe in the fullest extent (meaning with low

[253] While Japan allows the individual to determine the means of access (Art. 33 II APPI), Ghana only prescribes provision of "a copy of the data in permanent form" (Art. 35 XII DPA).

[254] Cf. § 1798.130 (a)(3)(B)(iii) CCPA.

prerequisites[255] and no exemptions) in China[256] and a little lesser in Brazil[257]. Germany follows a more differentiating approach, to which the Swiss regulation is very similar,[258] and does only allow for data portability when information handling is based on consent or performance of contract and provides for more comprehensive exemptions such as technical feasibility/disproportionate effort or third-party rights and freedoms[259].

Lastly, the federal US constitutes similar classification problems as with the right to access. A right to data portability is not part of the FTC case law body. The Health Insurance *Portability* and Accountability Act, as well as comprehensive self-regulation initiatives[260] show the relative prominence of data portability in the US discussion on privacy. Nonetheless, this cannot justify a higher ranking than the Ghanaian and Japanese sole focus on a (consistent) right to access.

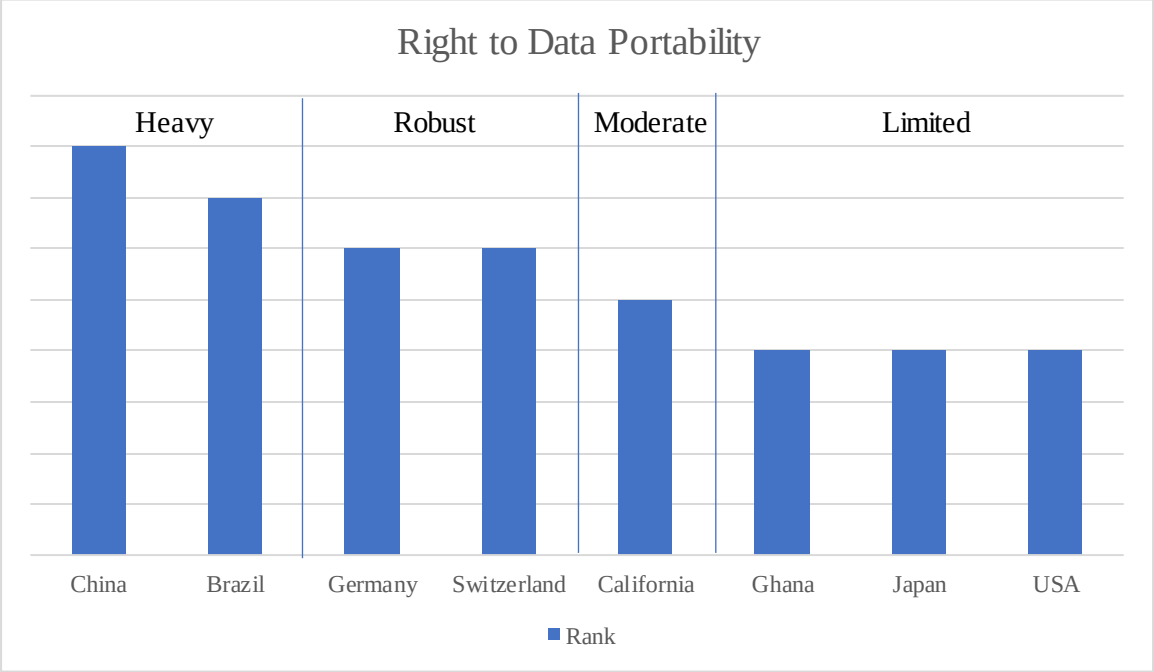

Figure 23: Ranking of regulation on data portability rights

7. Information Obligations

On first glance, information obligations don't quite fit with the other categories examined under "self-determined level of privacy": It is not a subjective right granted to the individual, but rather an objective obligation to the information handling entity notwithstanding any user interaction. Nonetheless, its main goals being transparency and empowerment of the individual, information

[255] The receiving party shall meet the condition of the State Cybersecurity and Information Department, which factually is likely to only forbid transfers abroad.

[256] Art. 45 III PIPL.

[257] Cf. Art. 18 V LGPD. There are no prerequisites of a right to portability and only the exemptions of commercial and industrial secrecy as well as anonymization (Art. 18 § 7 LGPD).

[258] Cf. Art. 20 GDPR for Germany and Art. 28 FADP for Switzerland.

[259] See for Germany Art. 20 II, IV GDPR and for Switzerland Art. 26 et seq. FADP.

[260] Cf. the "Data Transfer Project" allowing for data portability between Google, Meta, Microsoft, X, and Apple, accessible under https://dtinit.org/ (last accessed 04.03.2024).

obligations take central role in conceptualizing the user as the responsible entity to adjust their own privacy needs.[261]

Having this function in mind, all examined jurisdictions require the controller to inform of at least the handled information, the handling purposes, identification and contact information of the controller, third-party transfers and the existence of individual rights.[262] Beyond this extent, other popular information requirements are legal basis of information handling and where applicable invoked legitimate interest[263], retention periods[264], automated decision making[265], adopted security measures[266], and the source of the handled information[267]. In general, Brazil, China and Germany provide for the broadest scope of required information, and the Japan the narrowest.

Other important factors to categorizing information obligations are the modalities, how the information must be given, and the exemptions to them. In general, the required information must be provided in a readily accessible form to the individual at the time of collection/reception. This is, however, not true for Brazil, Ghana and Japan, where the individual must merely be "made aware of" or "accessible" to the individual. When it comes to exemptions, Brazil, California, Germany and Japan stand out by not providing for any notable exemptions[268]. While China only restricts the information obligation where confidentiality is prescribed by law, Ghana excludes it where there is a necessity for certain purposes[269] and Switzerland goes even further by implementing a broad variety of exemptions[270].

So far, this classification has not taken the US (and to a certain extent California) into account. As previously mentioned, it is central to the US approach to privacy regulation, that the individual is informed and therefore empowered to choose their own level of privacy. Thus, information obligations must carry great relevance in relation to the overall regulation in the USA. And indeed, the CCPA provides for one of the most detailed regimes on information to be given to the individual. While this does not include information such as retention periods or adopted security measures, 11 CCR § 7011 (e) comprehensively specifies on key information such as on the controller, handled information, its purposes, and sources as well as recipients. The generally applicable exemptions in

---

261 *Richthammer/Widjaja,* The Effect of Regulatory Measures on Individual Data Disclosure: A Country Comparison, ECIS Research-in-Progress Papers (2023) 83, p. 6.

262 See for Brazil Art. 9 LGPD; for California §§ 1798.110, 1798.130 (a)(5) CCPA in combination with 11 CCR § 7011 (e); for China Art. 17 PIPL in combination with Nr. 5.5 of the 2020 Specifications; for Germany Art. 12 et seqq. GDPR; for Ghana Art. 27 II DPA; for Japan Art. 21, 27 II, 32 APPI; and for Switzerland Art. 19 et seqq. FADP.

263 As is the case in Brazil, Germany, and Ghana.

264 As is the case in Brazil, China, and Germany.

265 As is the case in China, Germany, and Switzerland.

266 As is the case in Brazil and China.

267 As is the case in California and Germany.

268 Germany, however, provides for the exemption that the individual already has obtained the information in question, cf. Art. 13 IV, 14 V GDPR.

269 Art. 27 IV DPA allows for exemptions where it is necessary for avoiding to prejudice law enforcement, or other public or lawful purposes as well as when the information is handled for research, historical or statistical purposes.

270 Art. 20 FADP allows for exemptions where – amongst others – the individual does already have access to the information, information handling is prescribed by law, providing information is not possible or reasonably feasible, or when there is a necessity for overriding third party interests. The only reason Switzerland ranks higher than Ghana despite these wide exemptions is the larger scope of required information and the direct information at the time of collection.

§ 1798.145 CCPA are not tailored to exempt information obligation but are comparable to the scope in Ghana[271]. What is making California so remarkable in this regard is § 1798.130 (a)(5) CCPA: Rather than individually informing the persons the information is collected from, the Californian law additionally requires giving general notice every 12 months on their privacy practices not only in relation to the individual but to all consumers the controller handles information from. Thus, the CCPA requires both, individual and collective information, providing for maximum transparency[272].

On federal US level, every notable privacy legislation contains the obligation to provide the central information necessary to enable the user's choice ("notice and choice model"[273])[274]. This is also reflected in FTC case law, that prescribes to sufficiently inform the individual of potentially invasive practices.[275] In its scope (providing for such information that are necessary for the individual to invoke his rights) the US regulation resembles the Swiss approach. As notice is so important in the regulatory approach of the USA, practical exemptions to it can be assumed as rather low.

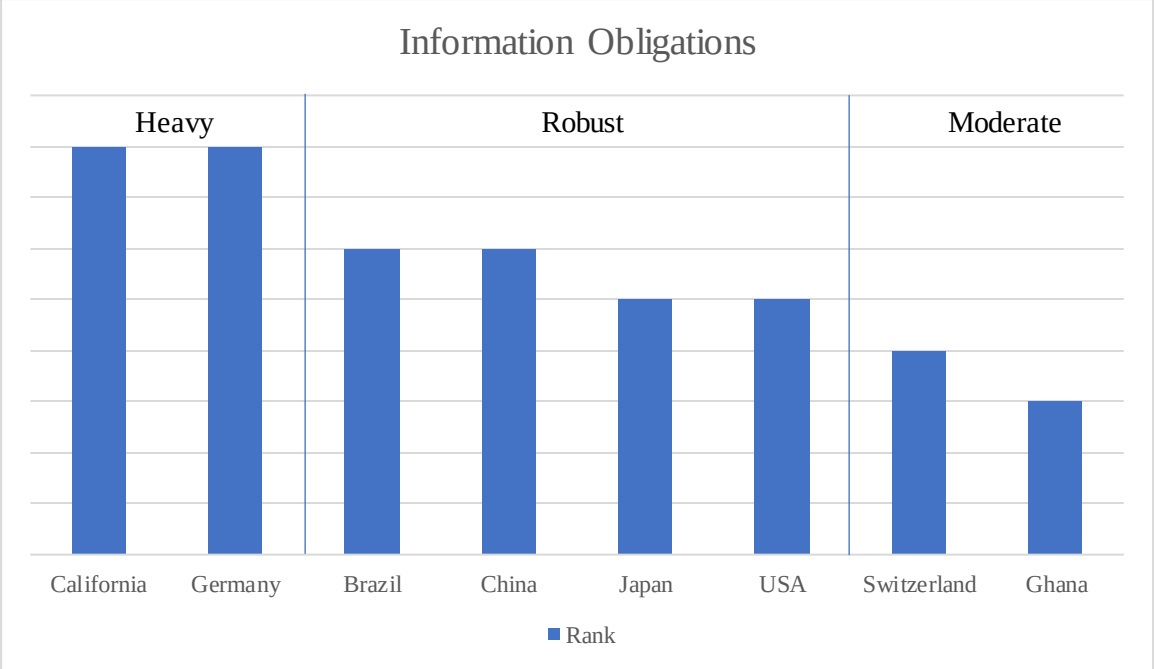

Figure 24: Ranking of regulation on individual information

8. Data Breach Notification

The requirement of controllers who suffered from a security incident to inform the individual as well as the supervisory authority is difficult to classify as instrument of assured or self-determined level of privacy. On first sight, it is a self-restrictive objective obligation to the controller, who must

---

[271] Especially, the information obligation shall not hinder the controller's ability to comply with legal obligation and administrative orders as well as conduct research or exercise/defend legal claims including evidentiary privilege.

[272] While one should note that this is a common practice in other jurisdictions requiring individual information by linking a general privacy policy in every collection notice, the CCPA is the only legislation to make this duality a hard requirement.

[273] See on this model already above, → C.I.3.

[274] For a broad overview only *Glocker,* Der California Consumer Privacy Act (2022), pp. 19 et seqq., 150 et seq.

[275] *Solove/Hartzog,* The FTC and the New Common Law of Privacy, Columbia Law Review (2014), pp. 583, 634 et seqq.

take action irrespective of user involvement. One can argue that in requiring to notify the supervisory authority of the data breach, the controller presents himself as object of enforcement and that therefore, such obligations solely serve as preventive measure as well as to provide a high level of objective transparency and enforceability and therefore protection. On the other side, the data breach notification does have a lot of similarities with the general information obligation: in requiring to notify the affected individual, they get empowered to enact their control rights, as one could assume that one would not want to have their personal information stored in a system that is frequent subject to cybercrime or technical malfunctions. In this function, the data breach notification rather aims at subjective transparency and constitutes a necessary precursor of user involvement. It is therefore necessary to draw a coherent parallel with the previous chapter, according to which the general information obligations, which also apply *ex lege*, primarily serve to enable user involvement.[276]

When it comes to legal pluralism and privacy protection law, literature frequently discusses publicity and "naming & shaming" as means of enforcement[277]. Besides publicity work of supervisory authorities, the main instrument of such regulation targeting reputation is the concept of data breach notification, which originated in Californian law, but by now has reached every of the examined jurisdictions. Notification obligations only diverge in whom the breach must be declared to and whether there are exceptions from the obligation.

Most restrictive in terms of prerequisite are California, China and Ghana, only requiring a data breach or security incident[278], followed by Germany, requiring a high risk for individual rights only when notifying the individual[279], and Brazil, Japan, and Switzerland, requiring a high risk both for notifying the individual and the supervisory authority[280]. These differences are minimal because there are likely few scenarios where a "data breach" does not also constitute a high risk for the individual's rights – and *vice versa*. It must also be noted that California (and the federal US) is the only jurisdiction, which does not require notifying a supervisory authority. Other jurisdictions do put the supervisory authority as primary addressee of data breach notifications – which subsequently often uses their channels to inform the public of it.

---

[276] *Tschider,* International Cybersecurity and Privacy Law in Practice, (2017), p. 387 describes the instrument as "facilitating self-help". Other indications for such classification can be found, for example, in Recital 86 of the GDPR, or in *Solove/Schwartz,* Information Privacy Law (7th edition 2021), p. 1014.

[277] Cf. only *Kasper/Hoffmann,* Targeting Reputation – Publication of Compliance as a Regulatory Concept in Comparative Data Protection Law, in: Friedewald et al. (eds.), Daten-Fairness in einer globalisierten Welt (2023), p. 79.

[278] See for California § 1798.82 Civil Code of California, for China Art. 57 PIPL, and for Ghana Art. 31 DPA. Of the three only Ghana does not require further prerequisites: California does not require to notify the supervisory authority and China allows for an exemption to notify the individual where sufficient measures avoiding harm were implemented.

[279] Cf. Art. 33 et seq. GDPR. The supervisory authority must be notified regardless of high risk. Art. 33 I 1 GDPR still does exempt notification if it can be reasonably expected that there will not be any risk for individual rights.

[280] Cf. for Brazil Art. 48 LGPD, for Japan Art. 26 APPI, and for Switzerland Art. 24 FADP.

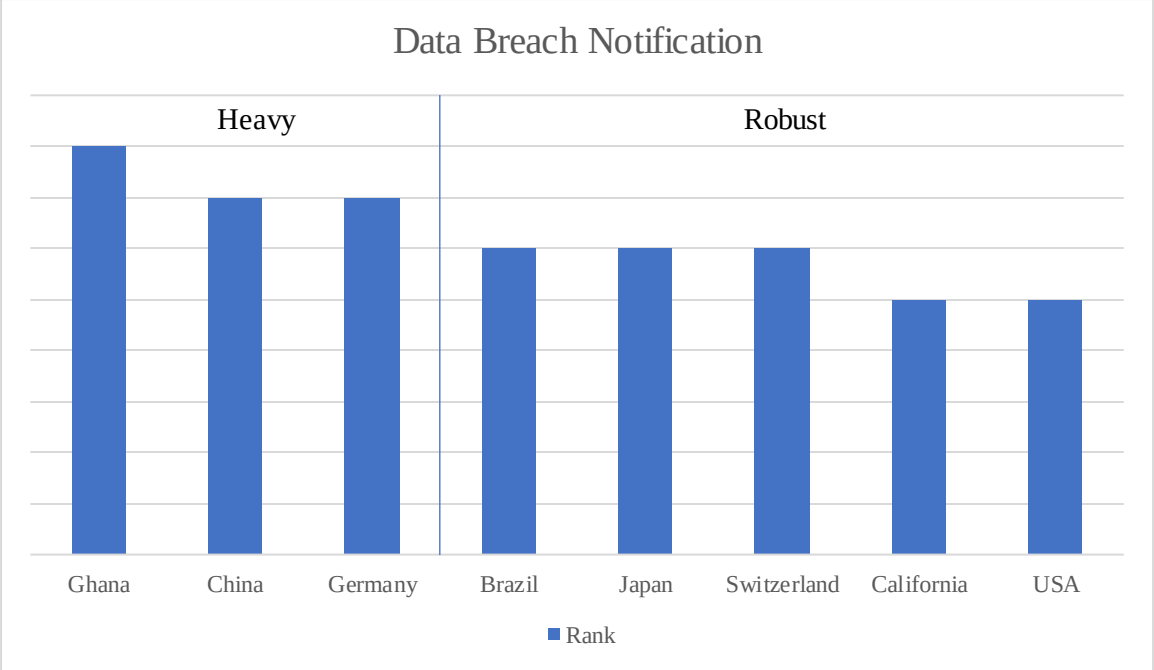

Figure 25: Ranking of regulation on data breach notifications

III. 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.

For example, one must also consider when disclosing personal information, that most jurisdictions provide for special, less restrictive regulation, if the controller deidentifies or anonymize the information: Often, anonymized information will not count as "personal information" as defined by the law[281] and is therefore not even subject of regulation, or jurisdictions provide for comprehensive exemptions for anonymized/deidentified information[282]. Most prominent in this regard is Japan, where there are lower (but existent!) regulatory standards for handling pseudonymized[283], and even less so when handling anonymized information[284]. One must also note that the biggest

[281] A codified example of this can be found in Art. 12 LGPD.

[282] An example for the former approach can be found in recital 26 of the GDPR and an example of the latter in § 1798.145 (a)(6) CCPA. However, it is more likely that international regulation on handling anonymized information is more likely to resemble the GDPR approach, because most jurisdictions use the same definition for "personal information", cf. *Hoffmann,* Data Disclosure, in Hennemann, von Lewinski, Wawra, Widjaja (eds.), The Laws of Data Disclosure (2023) pp. 1, 14.

[283] Art. 41, 42 APPI.

[284] Art. 43-46 APPI.

difficulty here is the different requirements for information to be anonymized, pseudonymized or deidentified.[285]

Concerning one of the biggest questions of privacy in a modern digital economy, jurisdictions around the world approach the commercialization of information very differently. Ghana, for example, entirely prohibits to sell or purchase personal information relating to another person[286]. Similar, but not as restrictive, Germany and Switzerland handle the provision of information as payment for an unrelated service as generally not sufficient basis for authorization.[287] Such sufficiency of context is often expressed by law in a prohibition of coupling.[288] An entirely different approach to this can be found in California and in the USA in general, following a market-driven approach.[289] Most remarkably, California has adopted a financial incentives program, which encourages the tangibility of personal information as means of payment.[290] Such commercial marketability of personal information has always been an important part of the US privacy regulation, which has resulted in the explicit regulation of "data brokers" for example in Vermont, followed by other state legislation.[291] China is also a good example of addressing personal information not only as matter of protection, but also societal good. While the US relies on monetization, China, however, incentivizes sharing of personal information in connection with state interests, for example their social credit system.[292]

With the adoption of the GDPR, a new instrument appeared in the privacy regulatory landscape: privacy by design and privacy by default.[293] They require the controller to consider the most privacy-protective technologies and default settings when designing a product to ensure maximum privacy protection capabilities before the controller even enters the market. While some

---

[285] To start with, it is not even clear in a technical sense (let alone legal), at which point an information can be deemed "anonymous", cf. only *Rubinstein/Hartzog,* Anonymization and Risk, Washington Law Review (2016), pp. 703, 714 et seqq.

[286] Cf. Art. 88, 89 DPA.

[287] CJEU, 4.7.2023, C-252/21, NZKart (2023) p. 430 – *Meta Platforms*; cf. also *Wiedemann,* Datenschutz- und Kartellrecht auf Facebook und andernorts, NZKart (2023), pp. 601, 603. Even though this is based on the GDPR, Switzerland must be mentioned in the same breath, because at least for high profile litigation such as this, Swiss authorities tend to adopt the decisions of the bigger EU authorities as part of a so called "copycat litigation". See on this matter *Sonnenberg/Hoffmann,* Data Protection Revisited – Report on the Law of Data Disclosure in Switzerland, in IRDG Research Paper Series, No. 22-17, p. 33.

[288] See for Brazil Art. 7 XI Marco Civil Law of the Internet (MCI); for China Art. 16 PIPL; for Germany Art. 7 IV GDPR, and for Switzerland Art. 6 VI FADP, as coupling is considered to be not voluntary under Swiss case law, cf. *Sonnenberg/Hoffmann,* Data Protection Revisited – Report on the Law of Data Disclosure in Switzerland, in IRDG Research Paper Series, No. 22-17, p. 26.

[289] *Bradford,* Digital Empires: The Global Battle to Regulate Technology (2023), pp. 33 et seqq. However, such competition affinity can also be observed in Switzerland, cf. Art. 31 II lit. b) FADP.

[290] See on the CCPA addressing current monetization trends *Determann,* California Privacy Law Vectors for Data Disclosures, in Hennemann, von Lewinski, Wawra, Widjaja (eds.), Data Disclosure (2023), pp. 121, 124 et seqq. See also § 1798.125 (b) CCPA.

[291] See for the Vermont Data Broker Act 9 VSA §2430. See on data broker regulation trends in general *Determann/Johnson,* Data Broker Regulation – Competition v. Privacy Considerations: Trade-Offs, accessible under https://insightplus.bakermckenzie.com/bm/attachment_dw.action?attkey=FRbANEucS95NMLRN47z%2BeeOgEFCt8EGQJsWJiCH2WAWuU9AaVDeFgpCdzlkUxiWH&nav=FRbANEucS95NMLRN47z%2BeeOgEFCt8EGQbuwypnpZjc4%3D&attdocparam=pB7HEsg%2FZ312Bk8OIuOIH1c%2BY4beLEAeoUASUHJpPzQ%3D&fromContentView=1 (last accessed 04.03.2024).

[292] *Hünting,* Endeavour to contain Chinas' Tech Giants – Country Report on China, in IRDG Research Paper Series No. 22-15, p. 20.

[293] Art. 25 GDPR.

jurisdictions have implemented such or similar regulation[294], the suitability and expediency of an exact transplantation is internationally not unanimously viewed uncritically.[295]

Other rather remarkable specifics are the explicit regulation on multi-referential information in Ghana[296], the corporate privilege in Switzerland easing information transfer within the same company group[297], automated decision-making (especially scoring)[298], restrictions of direct marketing[299], or the principle of habeas data in Brazil, which raises the individual's control of personal information vis-a-vis the government to a constitutionally protected good[300].

Ultimately, the aforementioned 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 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.

IV. Conclusion for Regulatory Intensities

1. Overall Assured Level of Privacy

Assessing the rank of every privacy related instrument of one jurisdiction in relation to the same instrument of 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 provides for a proposal, how different legislation

---

[294] In Brazil Art. 46 and 49 LGPD are understood to promote the same principles as Art. 25 GDPR, cf. *Hoffmann*, LGPD Et Al. – Report on the Law of Data Disclosure in Brazil, in IRDG Research Paper Series, No. 22-06, p. 45. See for a more pronounced transplantation in Switzerland Art. 7 FADP.

[295] *Gadoni Canaan,* Stimulating Innovation through Personal Data Protection Regulation: Assessing the Replication of GDPR into LGPD, June 1, 2022, 4.2.2. accessible under https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4154500 (last accessed 04.03.2024); *Waldmann,* Data Protection by Design? A Critique of Article 25 of the GDPR, Cornell International Law Journal (2020), p. 147. See for a general discussion on the potential criticism of privacy by design in general *Klitou,* A Solution, But Not a Panacea for Defending Privacy, in: Breneel/Ikonomou (eds.), Privacy Technologies and Policy (2021), pp. 100 et seqq.

[296] Art. 35 IV DPA.

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

[298] It is popular to grant a right to request review of decisions, that were based entirely on an automated process. Examples of such rights 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). The most far-reaching regulation in this regard can be found in Germany, in Art. 22 I GDPR, entirely forbidding automated individual decisions-making, subject to the permissions in Art. 22 II GDPR.

[299] Direct marketing is a practice that does often come into conflict with individual privacy concerns. Some jurisdictions have therefore found it necessary to include specific regulation on direct marketing, including Germany (granting an unconditional right to object in Art. 21 II GDPR) and Ghana (prohibiting direct marketing without prior consent of the individual (Art. 40 DPA). This cautious approach is in no way universal: On the contrary, California, in § 1798.140 (e)(6) CCPA explicitly qualifies advertising and marketing as (legitimate) business purpose. It even provides for specific regulation (thus explicitly allowing under the named circumstances) cross-context behavioral advertising, cf. § 1798.140 (ah)(1) CCPA.

[300] Cf. Art. 5 LXXII of the Constitution of the Federative Republic of Brazil.

can be clustered into relation to each other. Accordingly, a clustering of a combined assured level of privacy as examined in this paper does look like this:

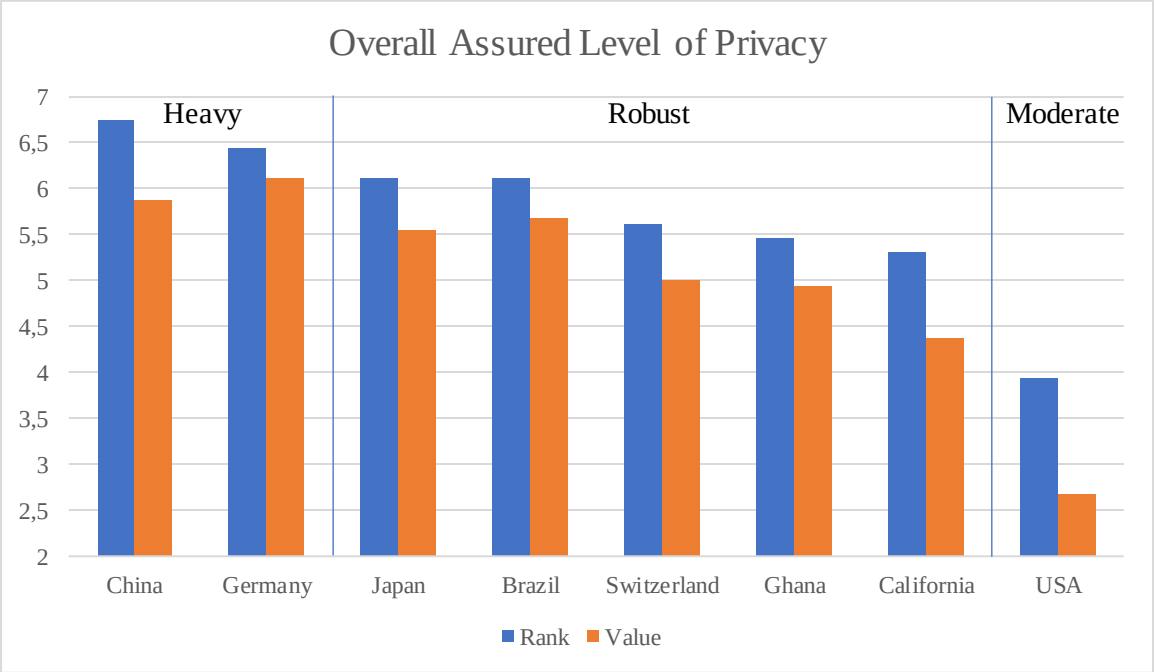

Figure 26: Overall ranking of the assured level of privacy in different jurisdictions

This ranking is led by China despite having a lower average value than the second placed Germany. This is due to the main instance that causes China to lose average value is 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 as Brazil, which outperforms the Japanese regulation in terms of prerequisites of information handling and internal responsibility management. Nevertheless, this would not pay attention to the peculiarity of the Japanese system, focusing on regulation of subsequent information handling, third party transmissions, and sensitive information. In these categories, the Japanese ranking scores significantly higher than Brazil. It follows, that Japan is despite the same ranking overall slightly higher than Brazil.

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

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:

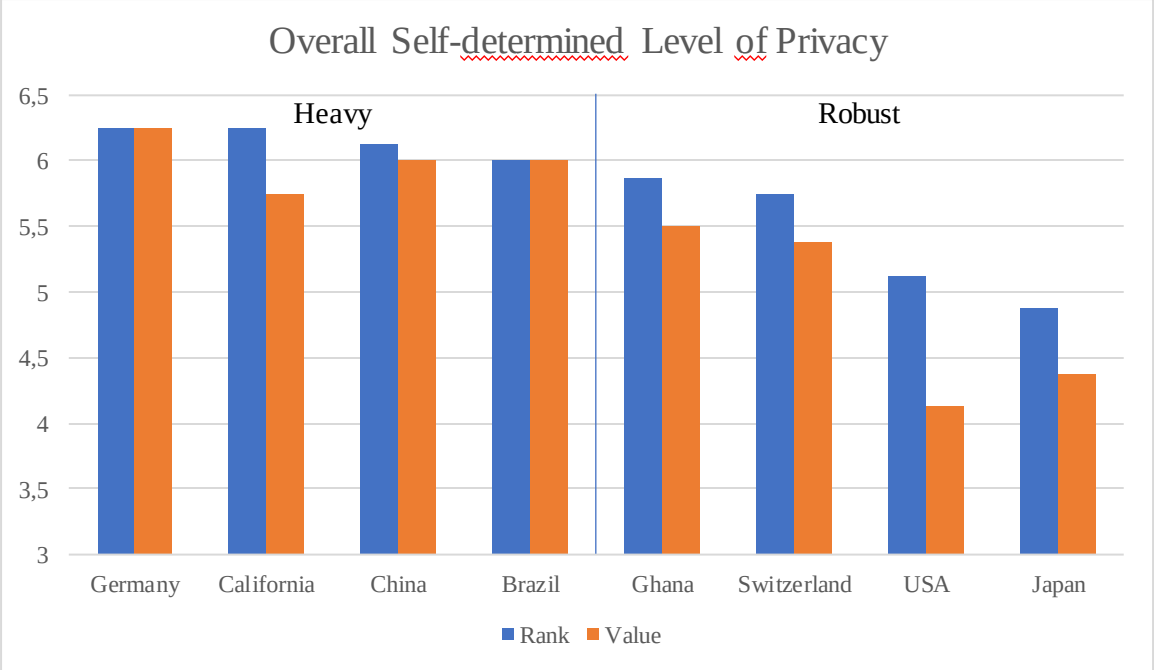

Figure 27: Overall ranking of the self-determined level of privacy in different jurisdictions

This time, Germany unambiguously takes the first place. California is 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[301]. Having this in mind, it seems reasonable to adhere to the high overall ranking and place California second, before China and Brazil.

Ghana and Switzerland follow with rather 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.

3. Overall Ranking of Privacy Laws

If combining the average rank and the average value[302] consisting of all examined legal instruments, the Regulatory Clustering produces the following (final) ranking on regulatory intensity:

[301] See on this model already above, → C.I.3.

[302] 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.

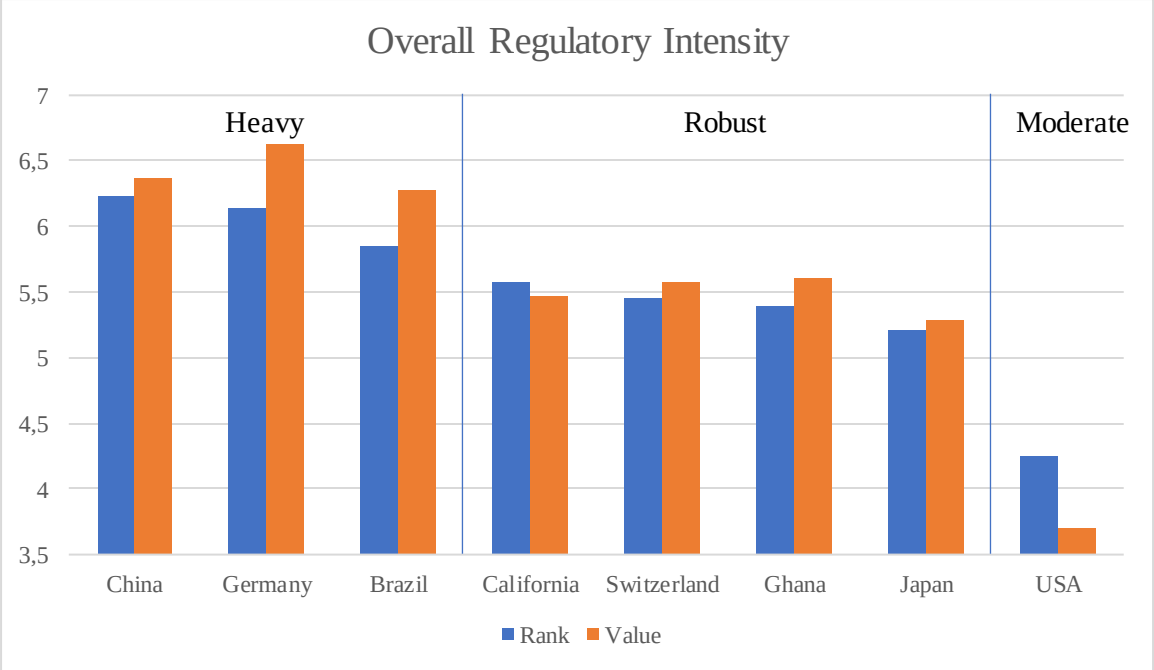

Figure 28: Overall ranking of the regulatory intensity of the examined jurisdictions of privacy.

For the same reasons as already above, China ranks very close before Germany, shortly followed by Brazil. The order of California, Switzerland and Ghana is rather difficult to assess, since they all score differently in rank and value. One must assess whether the relative significance of the factor mainly contributing to their respective value ranking justifies a rearrangement in contradiction to the ordinal ranking. Having this in mind, Ghana must rank 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 surpasses California in many instruments implementing a level of protection regardless of user involvement. Consequently, the autonomy-based approach in California grants the individual greater autonomy than in Switzerland. It is not the goal of the Regulatory Clustering to normatively take a side for 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.

D. 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 (→ B.IV.) – regulatory intensities as analyzed above,

do only describe the law in the books. Closing the gap between law in action requires further factors.[303] One of them can be the "efficiency" of enforcement.

Thus, this Regulatory Clustering must find a variable which can describe enforcement intensity to the most objective degree possible. This excludes the subjectively charged terminology of "good" or "effective" enforcement. It is also not sufficient to assess the degree of behavioral restrictions as it was done with the regulatory intensity: enforcement does not *per se* restrict the individual but is only a mean of making sure that actual restrictions imposed by material law are adhered to. Nonetheless, enforcement activities are in this sense restrictive, as they can "hurt" the perpetrator.[304] Therefore, enforcement intensity can be best described as the possibilities that a jurisdiction offers to act on the perpetrator in a way, that is intrusive and thereby causes negative effects. But because 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 must be collected. Due to the incomparable nature of empirical evidence and possibilities of enforcement, the two sub-categories cannot be accumulated, which results in a rather splintered 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.[305] However, this Regulatory Clustering is not based on empirical data (as this is not the goal of it, see above → B.III./IV.), which is why this section must remain a vague approximation of an objective standard of theoretical protection.

I. Instruments of Enforcement

1. Powers of the Supervisory Authority

First and foremost, privacy protection in a digitalized world is a complex topic. Such complexity is best addressed and overlooked by governmental bodies with the accompanying resources, competence and authority. All the examined jurisdictions – and for that matter all other jurisdictions implementing comprehensive privacy legislation – have also come to this conclusion and have introduced supervisory authorities[306]. All of them were assigned three central functions to:

---

[303] *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, 996.

[304] 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.

[305] 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)).

[306] Art. 55-A LGPD created the National Data Protection Authority (ANPD) in Brazil; § 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. 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. Having no comprehensive privacy legislation, the main regulator of privacy in the USA is the Federal Trade Commission (FTC). 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 of the relevant authorities.

Investigation of suspected incompliance, remedy of actual violations, and public guidance on privacy matters.

In terms of investigative powers, most jurisdictions provide their respective supervisory authority with the authority to request information on information handling activities, to receive the handled information, to interview persons responsible for information handling, to access documents and to access premises of the controller, as well as (external) auditing of them[307]. Only the USA and California provide for slightly less intrusive investigative powers: Investigations are conducted via formal hearing[308] where the hearing authority is also empowered to request access to all handled information and other relevant documents but is not empowered to access premises. Such shortcomings, however, are compensated by the wide array of remedial instruments given to the FTC ("consent order") and CPPA ("cease and desist order").

There are also large similarities in terms of public guidance. All supervisory authorities are obliged to participate in some way in public discourse, including the issuance of guidance or specifications to clarify legislation, to cooperate with and advice information handling entities, or to raise awareness on privacy matters.

When it comes to remedial powers, the differences between the jurisdiction crystalize: Higher ranking jurisdictions (California, China, Germany, USA)[309] empower their supervisory authority to directly impose binding obligations to – among others – create security audits, implement certain security measures, comply with an individual right, making violations public, refrain from or change the handling personal information, or to pay a fine. From this catalogue, China stands out in particular because it provides for the popular remedial power to terminate service provision.

The other lower ranking jurisdictions follow a tiered approach: While the Brazilian legislation is very similar to more restrictive regulations[310], the ANPD does only enforce according to a four-step classification of violations[311]. Such "responsive regulation"[312] focuses on cooperation with the perpetrator: Only when the non-compliant controller does not react to communication and complies with guidance of the ANPD, more and more restrictive remedial measures including fines and suspension of processing can be imposed. Very similar "responsive regulation" can also be found in Japan, where the PPC does always first issue a non-binding recommendation and only where such recommendations are not adhered to, it issues binding orders of action, and only in a third

---

[307] Cf. for China Art. 63 et seq., for Germany Art. 58 I GDPR, for Japan Art. 146 APPI. In the cases of Brazil and Ghana, no concrete information on investigative powers could be found. However, both jurisdictions provide for the vague requirement to monitor compliance (Art. 5 XIX LGPD; Art. 3 lit. a) DPA), which can rationally be expected to be similar to the other mentioned jurisdictions.

[308] See for the federal level 15 USC § 57b-1 (FTCA), and for California § 1798.199.65 CCPA.

[309] Cf. for China Art. 66 PIPL, and for Germany Art. 58 II GDPR. California and the USA allow for an issuance of "cease and desist" orders (§ 1798.199.55 (a)(1) CCPA), which can be individually settled and are therefore interpreted widely by the issuing supervisory authority. See on this settlement practice by the FTC on federal level *Solove/Hartzog,* The FTC and the New Common Law of Privacy, Columbia Law Review (2014) pp. 583, 610 et seqq.

[310] Art. 52 LGPD.

[311] This layered concept was foreshadowed in Art. 52 § 6 LGPD, and further specified on in the ANPDs Rules to Calculate and Enforce Administrative Penalties, CP/ANPD no. 4/2023, 27.2.2023.

[312] See on the foundations of this regulatory concept *Ayres/Braithwaite,* Responsive Regulation: Transcending the Deregulation Debate (1992). On the usage as privacy enforcement tool, cf. *Raghavan/Chugh/Kumar,* Effective Enforcement of a Data Protection Regime, Dvara Research Paper Series, WP-2018-01, pp. 12 et seqq. and *Greenleaf,* Asian Data Privacy Laws (2014), pp. 67 et seqq.

step reach out to the criminal investigation authority to file a criminal charge for monetary fines and publicizes such action.[313] Lastly, Ghana and Switzerland also follow a cooperative approach, even though not as layered as in Japan and Brazil: in both jurisdictions, the supervisory authority only enacts its remedial powers in the form of binding orders to take steps to rectify shortcomings of the controller.[314] If the controller does not comply, the supervisory authorities will take the matter to the criminal court. It should lastly be noted that out of all of these jurisdictions implementing a tiered approach to supervision, only Brazil allows the supervisory authority to directly impose fines, while all other systems are subsidiary to judicial enforcement.

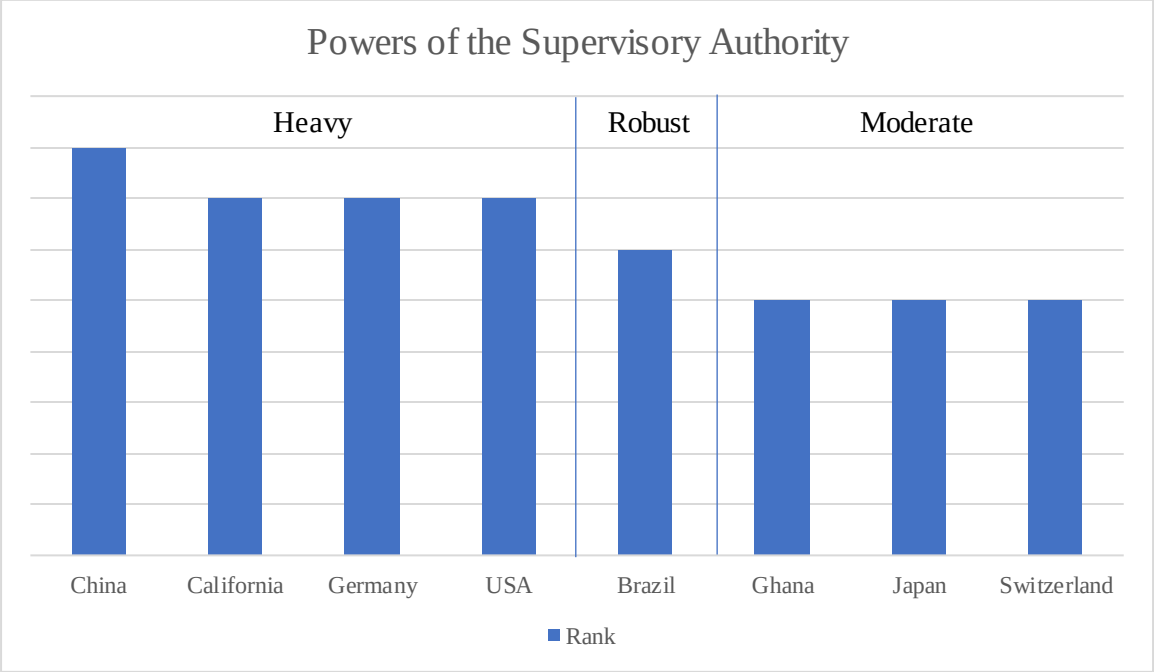

Figure 29: Ranking of regulation granting powers to a (privacy) supervisory authority

2. Administrative Fines

Technically, this category of "administrative fines" is already part of the powers of supervisory authorities, as they are regularly the only authority that can impose fines relating to violations of privacy laws. However – as far as the purely theoretical understanding of the possibilities of intensive enforcement relevant here is concerned – the scope of financial sanctions constitutes a central pillar of enforcement potency, as monetary loss is most suitable to result in "hurtful" sanctions.[315]

---

[313] Cf. Art. 148 APPI. Note that Art. 148 I APPI stipulates a general clause of recommending "necessary measures to rectify the violation" and thusly grants the PPC great freedom to design their remedial measures.

[314] In Ghana, the DPC issues "enforcement notices" cf. Art. 75 DPA. In Switzerland, the FDPIC issues "administrative measures", Art. 41 FADP.

[315] Of course, not only monetary sanctions can result in financial loss. Requiring costly security measures or restricting profitable business activities may also impose "hurtful" costs on the controller. However, such remedial measures are often aimed at restoring a lawful state and therefore, accompanying costs can hardly be defined as "hurtful" to the controller, as they have cost savings due to the breach of law. In contrast to that, administrative sanctions are not aimed at restoration of a lawful state, but rather at sanctioning the perpetrator for his shortcomings. This is also true for sanctioning of other assets unrelated to the violation of law; such rules, however, can only be found in China, in the termination of services. Nonetheless, monetary fines may even be the more attractive option between different enforcement measures as the transatlantic data flow problem exemplifies: Global Big Data players may want to rather pay (or more suiting get sanctioned) monetary fines than to implement data localization

Central characteristic to the notion of administrative fines is the fact that the supervisory authority can directly impose a monetary fine or other sanction not related to restoration of an unlawful status which can be costly for the controller. Thus, countries like Ghana and Switzerland, that only provide for criminal sanctions, cannot rank in this category. Even though Japan does also primarily rely on criminal prosecution, the APPI provides for the possibility of a "civil fine"[316]. However, such fines can only reach up to 100.000 yen (ca. $650 USD) and are only applicable in very specific situations, such as the deception of trading partners in cases of third-party transfers or misleading information concerning certification and are therefore close to neglectable.

The next less intrusive administrative fine is stipulated in the CCPA reaching up to $2.500 USD per violation per person, or $7.500 USD for intentional violations or violations involving minors.[317] Yet another giant leap take those jurisdictions, which – alternatively to an absolute height – base sanctions on the annual revenue of an controller.[318] These immensely large sums can only – in theory – be topped by the federal US, which empowers the FTC to recover a civil penalty of up to $10.000 USD per day of repeated violation of an FTC order and per affected person through the Attorney General.[319] This is not capped, and therefore has the potential to exceed the capped numbers of other jurisdictions, especially if the case takes place in California which is subject to two jurisdictions.[320]

measures in Europe. Unfortunately, assessing such effectivity of different enforcement measures is primarily an economical question and cannot be depicted in this Regulatory Clustering.

316 Art. 185 APPI. Even though the terminology of "civil" might be misleading ("過料" can also be translated as "non-penal"), this is classified as administrative measure in the sense of this Regulatory Clustering.

317 § 1798.155 (a) CCPA. One should note, that besides the CCPA, the much heavier regulation of the federal FTCA does also apply in California. However, in data privacy matters, it is more likely that the CPPA or the Californian Attorney General will take action, which can be backed up by the FTC.

318 These are Brazil, with up to R$ 50.000.000 (roughly $10.000.000 USD) or 2% of the annual revenue "only" in Brazil, cf. Art. 52 II LGPD; China, with up to RMB 50.000.000 (roughly $7.000.000 USD) or 5% of the annual revenue (not specified whether global or in China), cf. Art. 66 II PIPL; and Germany, with up to 20.000.000 € (roughly $22.000.000 USD) or 4 % of the worldwide (!) annual revenue, cf. Art. 83 V, VI GDPR.

319 15 USC § 45 (l) and § 56 (a) (FTCA).

320 Even though in head-to-head comparison, the federal US regulation is more intrusive than the Californian regulation, one must consider that parallel actions on federal and state level are theoretically possible (→ B.V.5.) and that the CCPA is therefore an addition to already applicable US law. Therefore, if any, the also applicable fines from the CCPA must rank California nonetheless higher than the US.

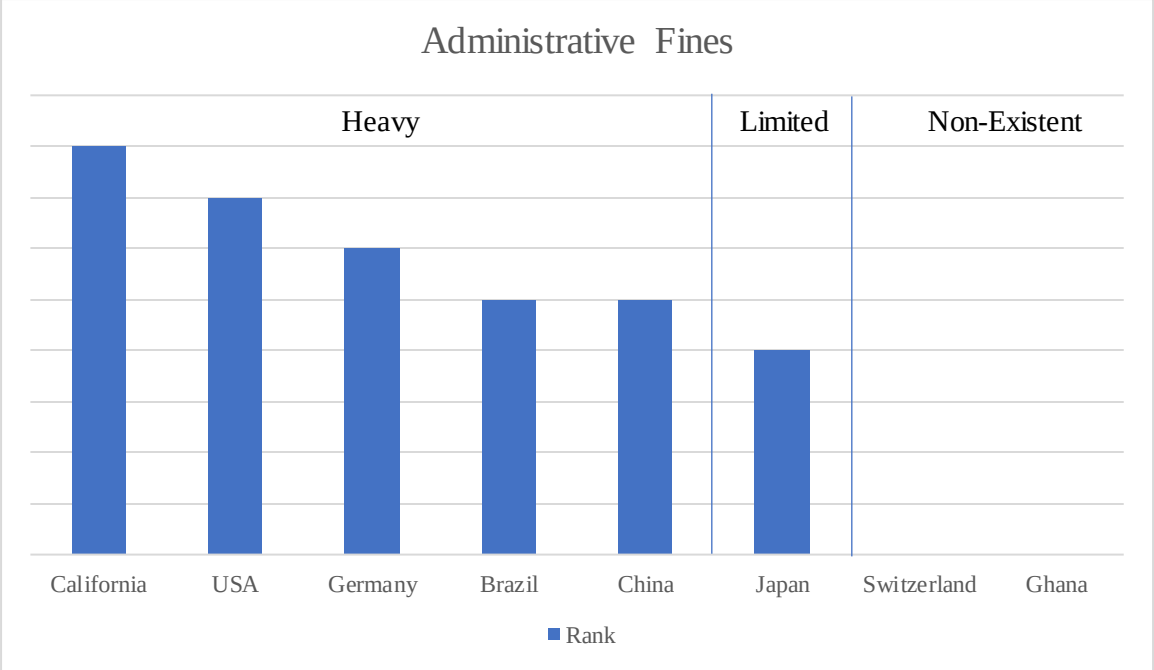

Figure 30: Ranking on regulation on administrative fines following a violation of privacy law

3. Penal Sanctions

Contrary to the preceding instrument, penal sanctions are not inflicted upon the controller by an administrative authority, but rather by a court as part of the countries criminal law regime. In general, there are two categories of jurisdictions on privacy criminal law: Those that rely on administrative sanctions and therefore only criminalize especially reprehensible privacy related offences such as hurtful invasion of privacy or unlawful mass publicization;[321] and those that criminalize non-compliance with any order of the supervisory authority and therefore use criminal law as main means of enforcement[322]. Of the latter category, Ghana imposes the lowest sanctions of up to ca. $5.000 USD[323] and only ca. $150 USD in cases of non-compliance with an enforcement notice. The opposite example would be Switzerland that imposes a fine of approximately $285.000 USD when FDPIC orders were not adhered to.[324] Even though Japan only imposes a personal fine of roughly $6.800 USD (or imprisonment of up to one year) on non-compliance with PPC orders, there is also the possibility of fining the perpetrators corporation up to $680.000 USD, which ranks Japan the highest.[325]

---

[321] Those jurisdictions include Brazil, cf. Art. 151 et seqq. of the Brazilian Penal Code (Decree-Law 2.848/1940); California and the federal US, cf. Sec. 647(j) of the Californian Penal Code or 18 USC § 1801 (US Penal Code); China, cf. Art. 285-287b Criminal Code of the PRC; and Germany, cf. Art. 84 GDPR in combination with § 42 BDSG, and Art. 201 et seqq. of the German Penal Code.

[322] Those jurisdictions include Ghana, cf. Art. 80 DPA; Japan, cf. Art. 178 APPI; and Switzerland, cf. Art. 63 FADP. One should note that these jurisdictions do also provide for additional penal provisions similar to the one of the aforementioned jurisdictions and very often even more detailed, because they aim to replace administrative enforcement and therefore aim at specific violations of the respective legislation.

[323] Art. 94 II, 95 DPA. One penalty unit amounts for approximately $1 USD, cf. Schedule 1 of the Fines (Penalty Units) Act of 2000 (Act 572).

[324] Art. 63 FADP (and surrounding articles for various other offences).

[325] Cf. on the penal provisions of the APPI Art. 176 et seqq. APPI. On the criminal liability of corporations, cf. Art. 184 APPI.

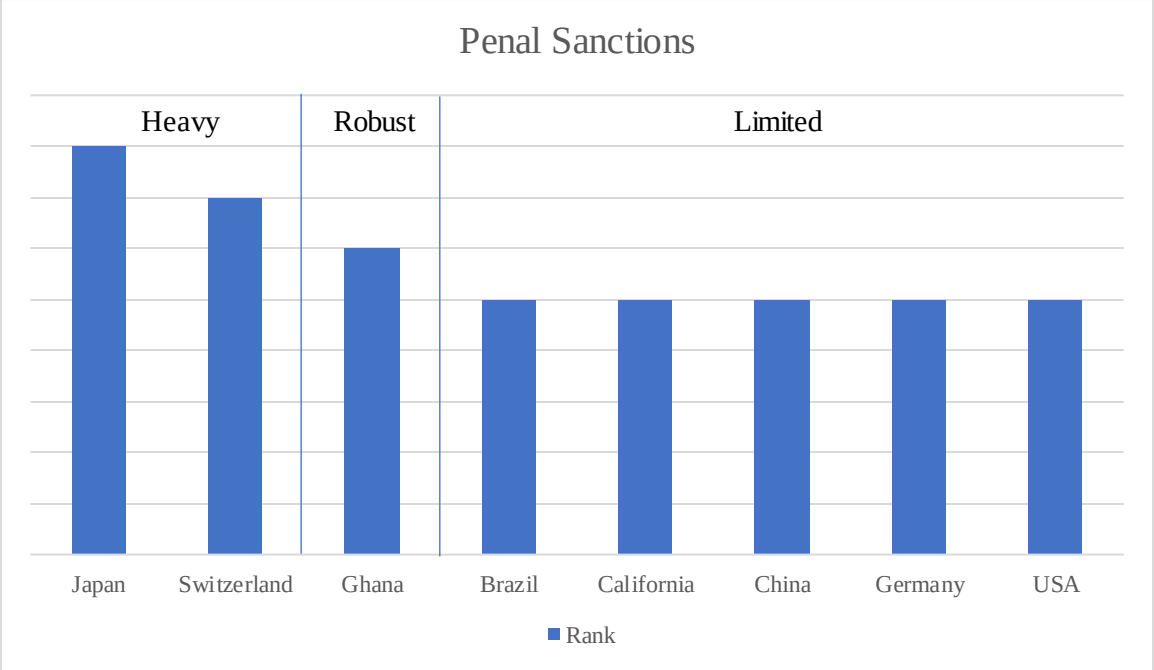

Figure 31: Ranking of regulation on penal sanctions following a violation of privacy law

4. Private Enforcement

Every jurisdiction also implements an instrument that allows the individual to recover suffered damages and to obtain an injunction following violations of privacy legislation. Contrary to the aforementioned sanctions, such private enforcement does (mostly) not aim at remedy or punishment, but simply at the protection and restitution of the individual. In this regard, there are no significant differences between the examined jurisdictions; they all provide for causes of action either (partially) in the privacy legislation itself[326] or in the general body of (civil) law[327]. Switzerland offers the best example of why privacy-specific bases for claims are generally more intrusive than general ones: Art. 32 II FADP references the general regulation for civil claims based on personality violations (Art. 28 et seqq. Of the Swiss Civil Code). However, this assumes in advance – and this statement does not apply to all jurisdictions – that any violation of the FADP already fulfils the elements of an infringement of personality rights and that it is only the causal damage at question. Causal damage constitutes the main obstacle for most jurisdictions, as their private enforcement mechanisms aim at the restoration of a status quo and it is difficult to prove that a privacy violation has directly caused monetary loss or similar.[328] The reason why the US ranks higher than other jurisdictions is, because – even though bases for civil compensation are narrower – US law circumvents the problem of calculable causal damage by allowing for punitive damages as only examined jurisdiction to do so. In addition to that, California allows for a rough quantification of suffered damage at between $100 and $750 USD per security incident (or actual damage, whichever is

[326] 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.

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

[328] Cf. also *Hoffmann,* The Laws of Data Disclosure in: Hennemann, von Lewinski, Wawra, Widjaja (eds.), Data Disclosure (2023), pp. 1, 23.

greater). Having outlined this ranking, it should also be noted that Switzerland and China stand out by allowing for additional private enforcement mechanisms.[329]

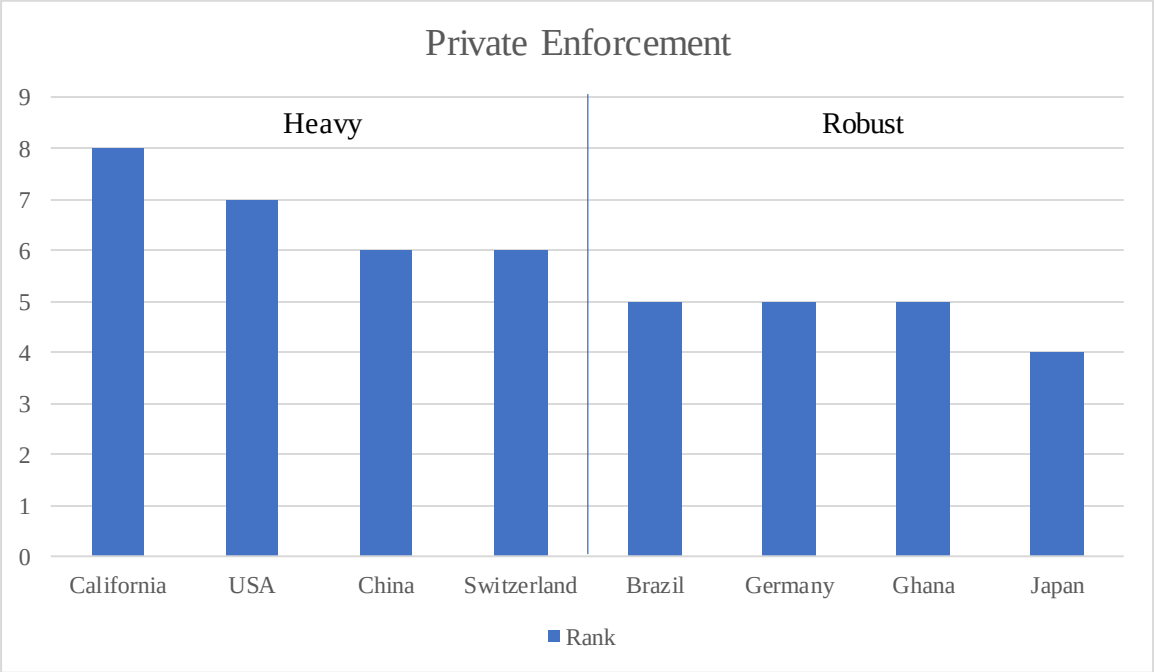

Figure 32: Ranking of regulation on private enforcement of privacy laws

5. Extent of Liability

It is crucial for the intrusiveness of sanctions who can be held liable. It is either the natural person standing behind the information handling entity (personal liability), or the entity itself, if it is not a natural person (corporate liability). Both options have advantages and disadvantages: Personal liability can certainly be more "hurtful" as the perpetrator cannot hide behind liable capital but is prone to individual over-penalization and cannot reach the heights of corporate liability. Corporate liability is easier to determine and can reach greater sums but may not be sufficiently "hurtful" or individually adjustable.

Generally, jurisdictions can be divided into those that rely on penal sanctions (which holds the natural person liable)[330] and those that rely on administrative fines (which holds the information handling entity liable)[331]. As this ranking looks at the raw potential to be hurtful to the controller, personal liability must usually rank higher than corporate liability. However, Japan and China rank even above that, because they allow for parallel liability of both, the information handling entity and the natural person(s) behind it.[332] Such dual liability does also exist in Switzerland in the form

---

[329] In China, Art. 69 II PIPL allows to calculate the suffered damage also according to the received benefits of the controller, thus implementing a sort of profit forfeiture. In Switzerland, especially Art. 32 IV FADP stands out, because it empowers the individual to request publication of compensatory measures and consequently of the shortcomings of the controller.

[330] This encompasses Ghana, Japan, and Switzerland.

[331] This encompasses Brazil, California (and the USA), China, and Germany. As already mentioned above, these jurisdictions do also provide for individual liability in the form of specific privacy offences. But this liability is nowhere near the prominence of individual liability in jurisdictions solely relying on penal sanctions.

[332] In China Art. 66 PIPL (which primarily relies on administrative fines) allows for an additional fine of up to RMB 1.000.000 (roughly $140.000 USD) on each responsible person in charge or other directly responsible personnel. China does also provide for a corporate criminal liability in Art. 31 of the Criminal Law of the People's Republic of

of corporate criminal liability, but it is subsidiary to individual liability[333] and therefore only alternatively and not parallelly. One can argue that such duality may result in more just penalization (in cases where the individual perpetrator cannot be identified), but in context of this Regulatory Clustering it means that the Swiss sanctioning system can be (ever so slightly) less "hurtful" or intrusive as the Ghanaian one, because it may allow for some cases, where personal liability is refrained from.

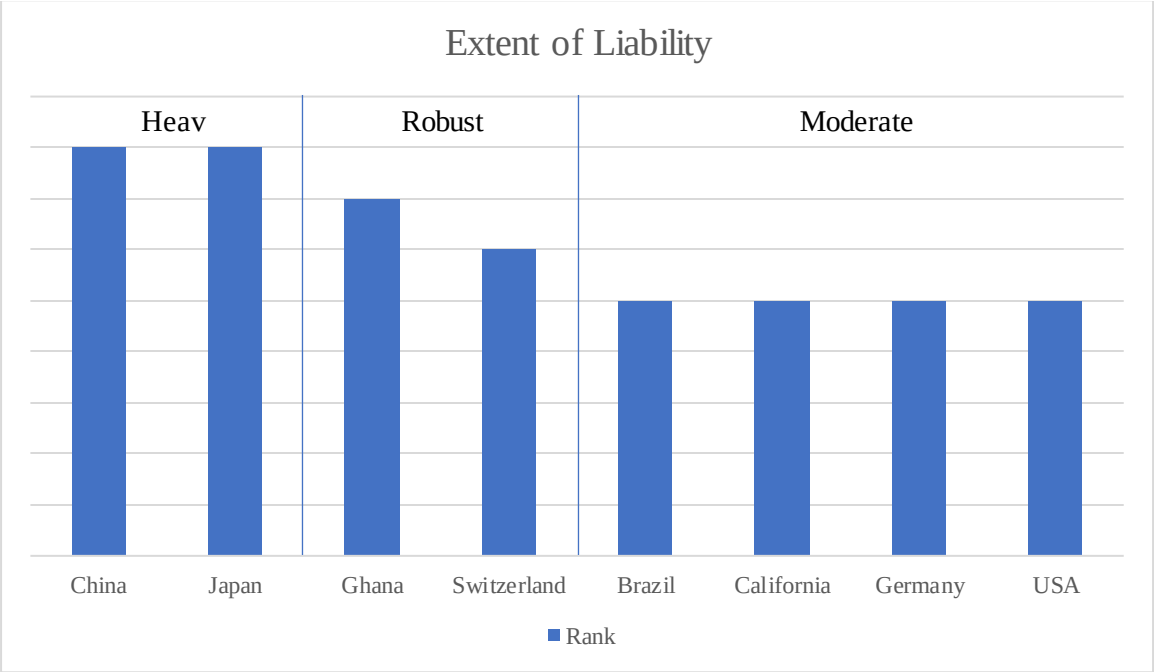

Figure 33: Ranking of the extent of liability

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[334], means of dispute settlements[335], collective redress mechanisms[336], or cost shifting[337]. Such factors may have great

China. In Japan, Art. 184 APPI allows the court to fine the corporation the individual perpetrator was acting for up to 100.000.000 yen (roughly $680.000 USD).

[333] Cf. Art. 102 of the Swiss Penal Code.

[334] Accessibility of justice can be influenced by factual (i.e. physical and financial availability of courts) or legal (i.e. the existence of a right to complain/petition and a right to referral) circumstances.

[335] It may be that in some legal cultures, disputes are more prominently settled through other institutions rather than the court. Such institutions could be the public or alternate dispute resolution (ADR) instruments such as arbitration and mediation. Such heightened prominence of ADR can be found in Brazil with its litigiousness, the US with its common practice of settlements, and Switzerland with the legal obligation to consult "judges of peace" in Art. 197 of the Swiss Civil Procedure Code.

[336] It is often more efficient to collect a variety of small claims by individually weak actors and collectively exercise them at once against a big player. However, such collective redress is not equally common in different privacy regulations: Some jurisdictions do not provide for any collective redress mechanism or do only enable consumer associations to enforce antitrust and competition law (such as Germany, Japan, and Switzerland). Other jurisdictions, however, have a more prominent history of collective litigation. The latter includes the USA and California with its popularity of class actions and Brazil with its public civil action (cf. Art. 42 § 3 LGPD in combination with Law 9.099/1995 on Public Civil Actions).

[337] Rules on who bears the costs of the court proceedings (including court fee and counsel fees of the opposing party) might influence enforcement insofar, as individual action might be (dis-)incentivized by such rules.

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.

II. 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*. Thusly, this section shall serve as inspiration for further empirical research on efficiency of privacy enforcement. Figure 34, at the end of this chapter, provides for an overview of the resulting ranking.

1. Ghana

Most strikingly, Ghanaian enforcement practices must rank last: The DPA entered into force in 2012 (more than 10 years ago), but the DPC has only very recently announced to pick up enforcement activities.[338] This recency is mirrored in the Ghanaian data protection registry, which by now has 2.388[339] entries, most of whom were added since 2021, shortly after the announcement of enforcement actions.[340] It remains to be seen, if such an increase in compliance and the associated enforcement will continue. At the moment, the empirical evidence does not give much reason to believe so.

2. Switzerland

As the FDPIC was only very recently equipped with its power to issue binding orders, enforcement numbers are difficult to assess. The FDPIC has announced in its last activity report, that it plans to conduct only 12 comprehensive investigations in one year.[341] In recent years, supervisory activities have only made up ca. 12 % of all the FDPIC resources, which focused more on advice to public and private entities, information, and arbitration (this part is not limited to privacy protection, but to (freedom of) information law in general).[342] In general, the Swiss enforcement system does face criticism because the FDPIC is understaffed for sufficiently handling privacy protection

Commonly, the losing party must bear the costs of the court and the prevailing party to the extent that they were reasonably necessary. This disincentivizes individual actions in legally uncertain cases but provides for more just distribution of costs and potentially relieves courts. Another approach would be the one of the USA: Attorney's fees can generally not be recovered from the opposing side. While this allows for a level-playing field, it may disincentivize individual action in legally certain cases. However, this approach has produced the practice of contingent fees, which may grant a more affordable access to justice than other systems.

338 *Data Protection Commission Ghana,* Public Announcement of July 21, 2023, accessible under https://www.dataprotection.org.gh/media/attachments/2023/07/24/bnft-publication.pdf (last accessed 04.03.2024).

339 As of 04.03.2024.

340 The data protection register is accessible under https://app.dataprotection.org.gh/en/entities/search/?q=%20 (last accessed 04.03.2024).

341 *FDPIC,* 30. Tätigkeitsbericht 2022/23, 31.03.2023, p. 86.

342 Ibid, p. 90.

issues[343], and because the final decision remains with the cantonal criminal prosecution agencies which are not regarded as suitable to regulate privacy.[344]

In terms of private enforcement, material damages were never recovered referring to the FADP. Switzerland does allow for compensation of immaterial damages ("satisfaction"). Even though this is more frequently used[345], cases are most likely situated in the area of protection of honor, not personal information *per se*. Other cases which constitute a violation of the FADP (such as the publication of the name of a rehabilitated criminal[346]) are so intrusive that there is no need to fall back on privacy regulation.

3. Brazil

The Brazilian supervisory authority – the ANPD – was not just revisited (like the Swiss FDPIC), but rather completely new introduced. Since the LGPD entered into force in 2020, the ANPD picked up enforcement activities only recently (middle of 2023) and has so far issued three sanctions[347] and has announced to investigate on the Meta application "Threads".[348] Most likely, the rare enforcement activities can be reasoned due to the still not completed specifying ordinances required (or rather allowed) by the LGPD.[349]

In contrast to most other jurisdictions, Brazil earns its ranking not because of public, but rather its private enforcement system: first of all, Brazilian people are regarded as very litigious.[350] In 2022, there have been well over 400 civil cases in second instance involving the LGPD.[351] in these cases,

---

[343] *Rosenthal,* Switzerland's DP Act revised, Privacy Laws & Business International Report (October 2020), pp. 1, 4. The FDPIC at the moment has 33 employees responsible for privacy oversight. This is, however, 10 employees more than 10 years ago, cf. *FDPIC,* 30. Tätigkeitsbericht 2022/23, 31.03.2023, p. 85.

[344] Amongst many *Rosenthal,* Das neue Datenschutzgesetz, Jusletter 2020, p. 70; *Sonnenberg/Hoffmann,* Data Protection Revisited – Report on the Law of Data Disclosure in Switzerland, in IRDG Research Paper Series, No. 22-17, p. 57.

[345] Satisfaction can (rarely) reach up to 10.000 – 40.000 Swiss francs (roughly $45.000 - $57.000 USD), cf. *Landolt,* Genugtuung für mediale Persönlichkeitsverletzungen, medialex 04/2021, accessible under https://medialex.ch/2021/05/06/genugtuung-fuer-mediale-persoenlichkeitsverletzungen/#post-5704-_Toc69055175 (last accessed 04.03.2024).

[346] *BGer,* Judgement of 23.10.2003 – 5C.156/2003.

[347] Two of them have been addressed to public bodies, which are not subject to monetary fines (Art. 52 § 3 LGPD). The only fine against a private entity amounted for 14.400 R$ (roughly $3.000 USD), cf. *ANPD,* Administrative Process No. 00261.000489/2022-62.

[348] *ANPD,* ANPD fiscaliza a rede social Threads, accessible under https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-fiscaliza-a-rede-social-threads (last accessed 04.03.2024).

[349] Another point of criticism arises from the questionable autonomy of the ANPD together with rule of law concerns: The Board of Directors of the ANPD is chosen and appointed by the President (Art. 55-D LGPD, which also stipulates that the senate must approve of this). In practice, this could undermine the ANPD's trustworthiness to protect citizen's rights, if the Directors of the ANPD were chosen by a president, who violates citizen's rights himself (such as former president Jair Bolsonaro), cf. on this *Erickson,* Comparative Analysis of the EU's GDPR and Brazil's LGPD: Enforcement Challenges with the LGPD, Brooklyn Journal of International Law (2019), pp. 869, 887.

[350] *Armour/Schmidt,* Building Enforcement Capacity for Brazilian Corporate and Securities Law, European Corporate Governance Institute – Law Working Paper No. 344/2017, p. 5; *Takahashi,* Why Do We Have So Many Social Security Claims in Brazil? (2019) Shinshu University Economic Law Collection 5, pp. 94 et seqq.; *Deffenti,* Laws of Brazil: Dispute Resolution, accessible under https://lawsofbrazil.com/dispute-resolution/#:~:text=Brazil%20is%20one%20of%20the,hundreds%20of%20thousands%20every%20year. (last accessed 04.03.2024).

[351] *Opice Blum,* LGPD_Lookout: Annual Jurimetrics Report 2022, accessible under https://opiceblum.com.br/wp-content/uploads/2019/07/09-relatorio-jurimetria-2022.pdf (last accessed 04.03.2024).

the awarded compensation ranged from 280 R$ to 25.849 R$ (roughly $60 USD to $5.300 USD).[352] Even though this speaks for a strong private enforcement, such high case numbers are often regarded as counterproductive:[353] for example, the average length of a civil trial in Brazil is ca. 24 months (707 days) and the duration until actual enforcement upon the judgement is even higher.[354] With such high intensity of private enforcement and to be expected (intervening) activity of the ANPD, Brazil ranks higher than Switzerland. Nonetheless it remains on the bottom of the ranking due to systematical shortcomings as Brazil is a country shaken by corruption scandals[355] and other rule of law concerns[356], which – for example – manifests in the position of the ANPD being subordinate to the president.

4. Japan

Next in line, the Japanese PPC does also have a low record of "hard" enforcement actions: between April 2021 and March 2022, the PPC issued only one (binding) administrative order.[357] The non-compliance of this binding order was only recently (in January 2023) brought to criminal investigation. On the other hand, the PPC was in the same period very active as an advisory organ, issuing 217 guidance/advice notices, 326 information submission requests, and 3 administrative (non-binding) recommendations.[358]

In terms of private enforcement, the Japanese people are considered not very litigious[359], which is why private enforcement is not very frequent. In practice, compensation for privacy infringements have yet just reached roughly $310 USD.[360] Nonetheless, one should also bear in mind that Japanese companies are known to voluntarily offer compensation despite not being required to.[361]

With its non-litigious people and non-binding activity of the FDPIC, Japanese privacy enforcement should be less effective than Swiss and Brazilian enforcement. However, Japan does not suffer from systematic deficits like Brazil, and especially in comparison with the FDPIC provides for a

---

[352] Ibid, p. 17.

[353] See on a comprehensive analysis only *Zimmermann,* How Brazilian Judges Undermine the Rule of Law: A Critical Appraisal, International Trade and Business Law Review (2008), p. 179.

[354] *Castelliano/Guimaraes,* Court Disposition Time in Brazil and in European Countries, Revista Direito GV (2023) V.19, p. 9.

[355] *Hoffmann,* LGPD Et Al. – Report on the Law of Data Disclosure in Brazil, in IRDG Research Paper Series, No. 22-06, p. 1.

[356] *World Justice Program,* Brazil's Incoming Government Faces Rule of Law Challenges, But Also Opportunities, December 11, 2022, accessible under https://worldjusticeproject.org/news/brazil%E2%80%99s-incoming-government-faces-rule-law-challenges-also-opportunities (last accessed 04.03.2024).

[357] *Personal Information Protection Commission Japan,* Annual Report 2022, June 9, 2023, accessible under https://www.ppc.go.jp/files/pdf/050609_annual_report.pdf (last accessed 04.03.2024).

[358] Ibid.

[359] *Colombo/Shimizu,* Litigation or Litigiousness? Explaining Japan's "Litigation Bubble (2006-2010), Oxford University Comparative Law Forum (2016), no. 4; *Hoffmann,* Data Protection by Definition – Report on the Law of Data Disclosure in Japan, in 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, Electronic Journal of Contemporary Japanese Studies (2003), no. 5.

[360] *Greenleaf/Shimpo,* The puzzle of Japanese data privacy enforcement, International Data Privacy Law (2014), pp. 139, 145.

[361] *Miyashita,* The evolving concept of data privacy in Japanese law, International Data Privacy Law (2011), pp. 229, 233. The author quotes a case where Mitsubishi UFJ Securities offered 50.000 customers a compensation of 10.000 yen each (roughly $100 USD).

very active guidance organ with the PPC, which consequently ranks Japan higher than these two countries. In this regard, one should also consider the hypothetical effectiveness of extra-judicial instruments such as voluntary self-restriction or cooperation with the supervisory authority.[362]

5. Germany

As Germany is only one single part of the enforcement network provided for by the GDPR[363], privacy enforcement in Germany must be assessed together with practices of other EU members, especially Ireland (since many global players have their main establishment there). Fines from European DPAs have reached up to 1,2 billion € (ca. $1,3 billion USD)[364] and have on average fined 1.755 € (ca. $1.900 USD).[365] In total, European DPAs have issued around 500 fines, about 50 of which originated in Germany.[366] In addition to these supervisory authorities, the CJEU has recently granted competition authorities the competence to enforce data protection law as part of competition regulation[367], thus adding an enforcement body similar to the FTC in the USA.

While the activities of the DPAs paint a rather clear picture, the matter of private enforcement is not as clear. This is reflected in the widespread disagreement as to when and how much damage is eligible for compensation.[368] Consequently, there is an unpredictable vastness of judiciary decisions granting compensation, which can reach up to 15.000 € (ca. $16.250 USD).[369]

In comparison to the USA, such private enforcement may be less intrusive for the controller (as there are no class actions that can reach high collective sums), but more protective from the perspective of the individual (as individual compensation is many times higher than in the USA). At last, two factors cast a shadow on the EU's capacities to give practical relevance to its vast

---

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

[363] Cf. on the structure of GDPR enforcement by oversight authorities *von Lewinski,* Datenschutzaufsicht in Europa als Netzwerk, NVwZ (2017), p. 1483.

[364] *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 04.03.2024). Other notable litigation includes a 746.000.000 € (roughly $800.000.000 USD) fine for Amazon, a 345.000.000 € (roughly $370.000.000 USD) fine for TikTok, and a 90 million € (roughly $97.000.000 USD) fine for Google.

[365] *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 04.03.2024).

[366] For an overview of GDPR enforcement activities, cf. *CMS,* GDPR Enforcement Tracker, accessible under https://www.enforcementtracker.com/ (last accessed 04.03.2024).

[367] *CJEU,* Judgement of 04.07.2023 – C-252/21, GRUR 2023, p. 1131.

[368] The CJEU has recently decided that the individual must have suffered actual damages which must not be significant in any sense (CJEU, Judgement of 04.05.2023, C-516/21, BeckRS 2023, 8968), but did not specify on any further prerequisites of "actual damage". On an overview of the state of discussion, cf. *Quaas,* in: Wolff/Brink/v. Ungern-Sternberg (eds.), BeckOK Datenschutzrecht, (46th edition 2023), Art. 82 DSGVO, N 23 et seqq.

[369] A collection of such court decisions can be found in *Matthiesen et al.,* DSGVO-Schadensersatz: Übersicht über aktuelle Urteile und Entwicklungen (laufend aktualisiert) #018, accessible under https://www.cmshs-bloggt.de/tmc/datenschutzrecht/dsgvo-schadensersatz-uebersicht-ueber-aktuelle-urteile-und-entwicklungen-laufend-aktualisiert/ (last accessed 04.03.2024). Another overview shows, that there have been at least 17 decisions of courts in second instance out of at least 50 relevant cases in 2022 granting damages, *Noerr,* GDPR Damages Tracker, accessible under https://www.noerr.com/de/themen/gdpr-damages-tracker (last accessed 04.03.2024).

regulatory body: Extraterritorial efficiency and small-scale enforcement. As the cases of Threads and X[370] exemplifies (even though this concerns the DSA and DMA and not the GDPR), the sparring on the field of digital regulation with multinational big tech companies may well result in their withdrawal from the European market. It also seems common practice that US companies postpone adhering to imposed sanctions as long as possible.[371] In terms of small-scale enforcement, a Meta study suggests that there is a significantly low compliance and consequently low enforcement rate to the GDPR.[372]

6. California

The CPPA was even more recently introduced than the ANPD. It was legally appointed with the entering into force of the CPRA in January 2023. However, it picked up advisory activities by the end of 2021 and in its recency of activities is therefore very similar to the ANPD. Still, the CPPA is set to start enforcement activities only in March 2024 by decision of the Superior Court of California, which the CPPA has filed to overturn.[373] Nonetheless, the CCPA does not only equip the CPPA with enforcement authority, but also the Attorney General. Its most significant enforcement activity was a settlement agreement with Google worth $93 million USD.[374]

Similar to Brazil, the aspect of private enforcement is relatively very important in California: This is especially due to the combination of class actions and punitive damages that is commonly used in US legal systems, as well as the common practice that lawsuits are often privately settled. In California, there have already been strong examples for such settlements: For example, an online retailer settled for $400.000 USD[375], and an art trader platform settled for $5.000.000 USD[376]. In addition, since the enactment of the CCPA, there has been a trend in nationwide class actions to

---

[370] Meta's instant messaging service "Threads" has not launched in Europe due to "complexities with complying" with EU law, cf. *Heath,* Why Instagram is taking on Twitter with Threads, accessible under https://www.theverge.com/2023/7/5/23784870/instagram-threads-adam-mosseri-interview-twitter-competitor (last accessed 04.03.2024). Likewise, Elon Musk reportedly considered withdrawing his instant messaging service "X" for similar reasons, cf. *Hays,* Elon Musk is considering taking X out of Europe amid EU compliance investigation, accessible under https://www.businessinsider.com/elon-musk-considering-taking-twitter-x-out-of-europe-dsa-2023-10?IR=T#:~:text=The%20Tesla%20billionaire%2C%20who%20acquired,accessing%20it%2C%20the%20person%20said (last accessed 04.03.2024).

[371] *Daigle/Khan,* The EU General Data Protection Regulation: An Analysis of Enforcement Trends by EU Data Protection Authorities, Journal of International Commerce and Economics (2020), pp. 1, 22 et seq.

[372] *Lancieri,* Narrowing Data Protection's Enforcement Gap, Maine Law Review (2022) pp. 16, 65 et seqq. Note that this meta study does also include compliance with the CCPA. Main target of the investigated studies, however, where EU companies subject to EU law.

[373] Superior Court of California, 34-2023-80004106-CU-WM-GDS; *CPPA,* Announcement of August 4, 2023: CPPA seeks to Overturn Superior Court Decision Delaying Enforcement of Consumer Privacy Regulations, accessible under https://cppa.ca.gov/announcements/2023/20230804.html (last accessed 04.03.2024).

[374] Cf. on privacy enforcement activities of the Californian Attorney General *Rob Bonta – Attorney General,* Privacy Enforcement Actions, accessible under https://oag.ca.gov/privacy/privacy-enforcement-actions (last accessed 04.03.2024).

[375] US District Court N.D. Cal., *Barnes v. Hanna Andersson, LLC et al.,* (2020) Case No. 3:20-cv-00812.

[376] US District Court N.D. Cal., *Atkinson et al v. Minted, Inc.,* (2020) Case No. 3:20-cv-03869.

create a California subclass that receives up to $100 USD more per member.[377] The total amount of CCPA-related actions filed vary between 50 – 100 per year.[378]

7. USA

The federal US is very similar to California as both jurisdictions rely on the same basic enforcement structures. In fact, Californian controllers can also be subject to federal enforcement (see above → B.V.5.). Such federal enforcement by the FTC goes beyond the (current) capabilities of the CPPA: In June 2019, the FTC issued a $5 billion USD fine (alongside other remedial measures) against Facebook for violations of their users' privacy.[379] Despite such and other prestigious enforcement actions, the FTC decides on not more than 25 cases relating to privacy (in 2022, there have only been 3 of such cases) per year.[380]

Also, in terms of private enforcement, the USA does qualitatively surpass California: The most expensive class action lawsuit/settlement so far has reached ca. $600 million USD involving 147 million customers[381], which has just recently been surpassed as as a class action lawsuit worth $5 billion USD has been settled by Google.[382] There have been 42 other not as expensive, but still large-scale nationwide class actions concerning data breaches in 2022, which is an increasing trend likely to continue in the future.[383] Of course, there are various other civil claims (mostly arising from (mass) tort law) which are a vital part of US private enforcement. Even though concrete numbers on this aspect could not be found, individual compensation can be expected to be rather high, as punitive damages are popular in privacy tort law and disputes are also often privately settled. Altogether, the federal enforcement system in terms of capacities, quality and quantity is more intrusive than the Californian one. However, as many Californian cases are potentially subject to federal (FTC) enforcement on one side, and class action lawsuits are potentially costlier with more Californian members on the other side, California and the USA can be ranked the same.

8. China

China is the only jurisdiction that does not rely on a single supervisory authority (or supervisory network as in Europe). Rather, the PIPL empowers "departments fulfilling personal information

---

[377] *Perkins Coie,* California Consumer Privacy Act Litigation. 2022 Year in Review (May 2023) p.9, accessible under https://www.perkinscoie.com/images/content/2/6/263321/2023-CCPA-YIR-FINAL-2.pdf (last accessed 04.03.2024).

[378] *Perkins Coie,* CCPA Litigation Tracker, accessible under https://www.perkinscoie.com/en/ccpa-litigation-tracker.html (last accessed 04.03.2024).

[379] *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 04.03.2024).

[380] Cf. *FTC,* Legal Library: Cases and Proceedings, accessible under https://www.ftc.gov/legal-library/browse/cases-proceedings (last accessed 04.03.2024). In the case of the 2022 enforcement, one should note, that the three actions included one $500.000 USD fine for covering up a data breach, and a $150 million USD fine for deceptively collecting data.

[381] *FTC,* Equifax Data Breach Settlement, December 2022, accessible under https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement (last accessed 04.03.2024).

[382] *Stempel,* Google settles $5 billion consumer privacy lawsuit, 29.12.2023, accessible under https://www.reuters.com/legal/google-settles-5-billion-consumer-privacy-lawsuit-2023-12-28/ (last accessed 04.03.2024).

[383] *Wyatt/McDermott,* Privacy Litigation 2022 Year in Review: Data Breach Litigation, January 25, 2023, accessible under https://www.mofo.com/resources/insights/230125-year-in-review-data-breach-litigationY (last accessed 04.03.2024); *Norton Rose Fulbright,* 2023 Annual Litigation Trends Survey – Perspectives from Corporate Counsel, pp. 6, 17. Such upward trends are – consequently – also apparent in California.

protection duties and responsibilities". Likewise, other legislations provide for a fragmented supervisory landscape as a whole[384], which causes some difficulties in the assessment.

Nonetheless, Chinese enforcement practices are notable: The highest administrative fine was worth RMB 8,026 billion (roughly $1,2 billion USD). Strikingly, the same enforcement action provided for an additional RMB 1.000.000 fine (Roughly $145.000 USD) each on the company's chairman, CEO, and president.[385] On a quantitative level, the Supreme People's Procuratorate has claimed, that between January and September 2022, 5.188 cases of public interest litigation in the area of personal information protection have been filed.[386] Such and other lawsuits arising from privacy violations may be rather efficient because it is reported that it takes only 1-2 months for a Chinese court to commence trial.[387] Finally, one should keep in mind, that the Chinese approach to law is a law by rule one, rather than – as in all other examined jurisdictions – a rule of law one. It follows, that Chinese regulation is not as prone to practical hurdles like material justice, low compliance rates, or insufficient supervisory powers as other examined jurisdictions. Therefore, it can be concluded that China has the broadest practical means to enforce its supervisory powers under the law (and even beyond, as public organs are not necessarily bound to law).

---

[384] Such enforcement bodies are for example the Cyberspace Administration of China (CAC), the Ministry of Public Security, or the Ministry of Industry and Information Technology (MIIT), as well as their regional/provincial counterparts and subdivisions, cf. also *Hünting,* Endeavour to Contain Chinas' Tech Giants – Country Report on China, IRDG Research Paper Series (22/15), pp. 31 et seq.

[385] *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 04.03.2024).

[386] Ibid. Note, that such litigation is, nonetheless, actively discouraged by China's Supremes People's Court, cf. *Han,* Background Memorandum: Public Interest Litigation in China, June 2017, accessible under https://law.yale.edu/sites/default/files/area/center/china/document/public_interest_litigation_china_background_memo.pdf (last accessed 04.03.2024).

[387] *Hongji/Qiang,* China: Litigation, Question 4, accessible under https://www.legal500.com/guides/chapter/china-litigation/ (last accessed 04.03.2024). However, these numbers could not be verified. They also do not include the time between commencing the trial and passing final judgement.

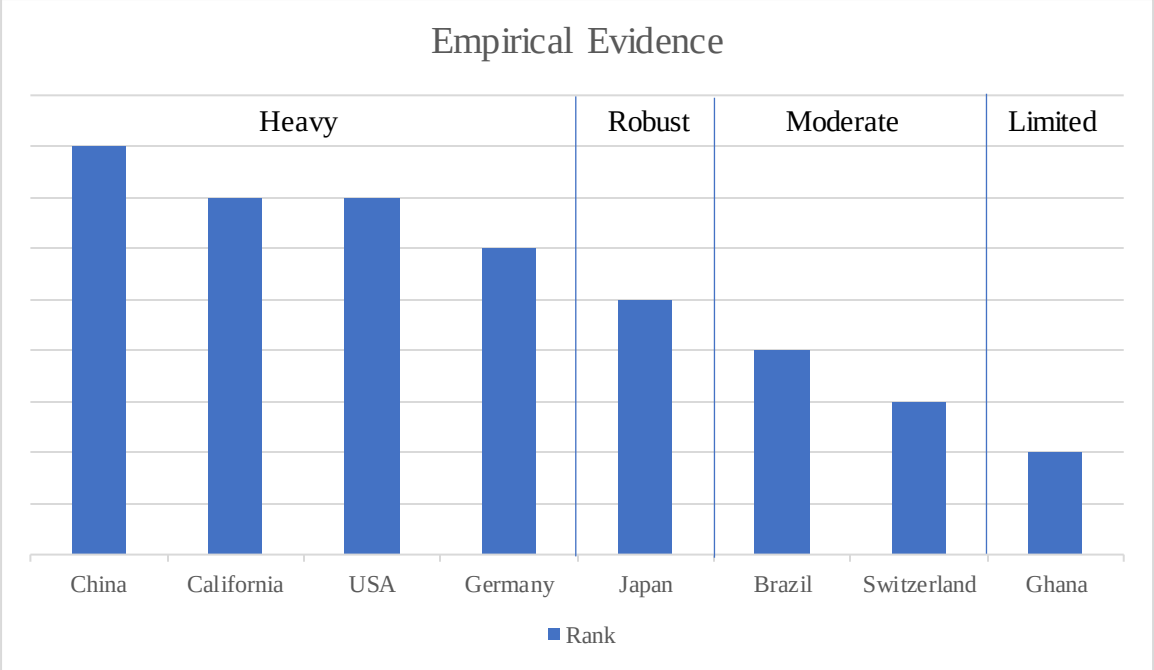

Figure 34: Ranking of the empirical evidence of privacy enforcement activities in different countries

III. Conclusion for Enforcement Intensities

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

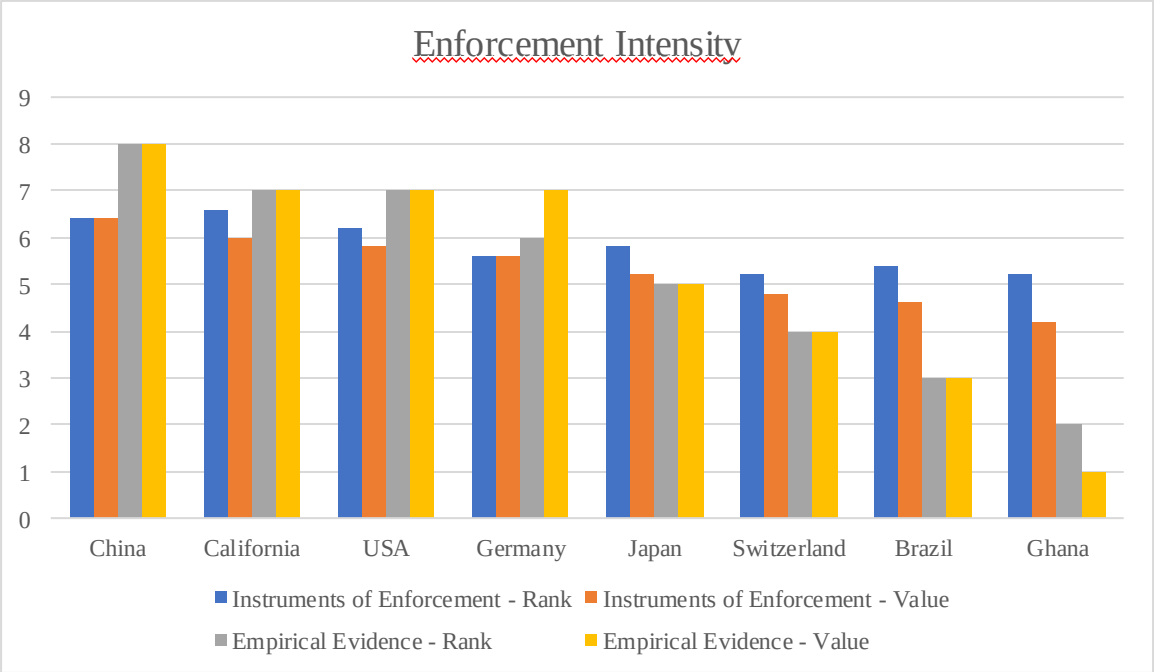

Figure 35: Overall ranking of enforcement intensities

California, the USA, and foremost China provide for the most intensive/intrusive enforcement system, both when it comes to theoretical possibilities and actual activities of enforcement. The same is true for Germany, even though it is overall slightly less intensive. Despite the Japanese systems being slightly better equipped with enforcement instruments than the German system, it lacks actual practical implementation. The remaining jurisdictions, led by Brazil and especially,

show a large discrepancy between what their jurisdiction allows them to enforce and what enforcement they actually exercise. While the Swiss and Brazilian ranking may be subject to change due to the novelty of both, the ANPD and the revisited FDPIC, Ghana has no so such excuse.

E. 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 privacy law.

I. China

As has already come up several times, China is a cluster of its own. It is a techno-authoritarian regime that utilizes 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. Nonetheless, the Chinese law provides for extensive means of protection in the private sector. In fact, China provides for the highest assured and overall level of privacy protection in this ranking: The PIPL casts heavy restrictions on information handling activities such as collection and sharing of information and alteration of the handling purpose. Often, the Chinese law requires prior consent of the individual above all else.[388] This undisputed supremacy of consent is tipping the scales in favor of China ranking first in this Regulatory Clustering. The Chinese system is also very capable of enforcing its strict regulation, as its high ranking in both, enforcement possibilities and actual enforcement, shows. Art. 13 PIPL is a good representation of the whole Chinese system: 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 do actually need to adhere to such restrictions of the private sector, which is why China – in practice – cannot be reasonably put on first place, even though the data of this paper imply so.

II. Germany

Unsurprisingly, Germany and the GDPR lead the democratic regimes in this Regulatory Clustering. It has always been the main point of criticism on the GDPR, that it imposes too much and too uncertain restrictions on the utility of personal data and raises compliance expenses for the controller to an unreasonable extent.[389] This criticism has manifested 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

---

[388] 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.

[389] Amongst many *Veil,* Die Datenschutz-Grundverordnung: des Kaisers neue Kleider, NVwZ (2018), p. 686; *Roßnagel,* Die Evaluation der Datenschutz-Grundverordnung, MMR (2020), p. 657; *Determann,* California Privacy Law Vectors for Data Disclosures, in Hennemann, von Lewinski, Wawra, Widjaja (eds.), Data Disclosure (2023), pp. 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, Journal of Law and Economics (2020), p. 349.

of objective (legal, technical, and organizational) obligations on how to handle collected information. The only notable anomaly arises from 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 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, uncertainty as to how to interpret 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.[390]

III. Brazil

The LGPD was greatly inspired and influenced by the GDPR. This is also reflected by its regulatory intensity ranking just below Germany. Its substantive regulation, in its intensity, does often not largely deviate from the one of the GDPR. Where the Brazilian legislator negatively deviates from the GDPR standard, it is only a little change from the design of the counterpart GDPR provisions. In a lot of aspects, the LGPD can be described as the "little brother of the GDPR". With that, a regulatory concept of the post-industrial west (global north) has been transplanted into a lesser developed country of the global south. Consequently, such regulation supposedly cannot fit the needs and regulatory goals of a developing economy like the one of Brazil, which is why this uncritical transplantation is the main point of criticism of the LGPD.[391]

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[392], this might also hinder proper access to justice, as the Brazilian judiciary struggles to deal with the vast amount of civil actions.[393] The ANPD does not promise any substantial improvement in near future, since it (a) was established only very recently and still needs time to take its place as proper supervisory authority, and (b) is subject to concerns regarding its independency as it is a body of the federal administration, which in turn is subject to criticism due to recurring cases of corruption and other rule of law concerns.

---

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

[391] *Gadoni Canaan,* Stimulating Innovation through Personal Data Protection Regulation: Assessing the Replication of GDPR into LGPD, June 1, 2022, accessible under https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4154500 (last accessed 04.03.2024).

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

[393] *Zimmermann,* How Brazilian Judges Undermine the Rule of Law: A Critical Appraisal, International Trade and Business Law Review (2008), p. 179.

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.

IV. Switzerland

Until very recently, Switzerland followed a very liberal approach to privacy regulation that was, in its regulatory intensity, very comparable to the US one. In an effort to uphold the EU adequacy decision, this rather lax legislation was completely overhauled in 2023, which has also boosted the regulatory intensity ranking in Switzerland. The main approach to privacy regulation remains a different one than the one of the GDPR: The Swiss abuse legislation[394] generally allows information handling but requires adherence to certain fundamental principles.[395] 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.[396] Nonetheless, the new FADP has introduced some comprehensive objective obligations such as internal documentation or individual information along with strong fundamental principles, which puts Switzerland's regulatory intensity well in the middle of this ranking.

Interestingly, Switzerland is the only country of the global north that notably struggles with enforcement of 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.[397] This practice refers technically and legally challenging questions on privacy to cantonal criminal prosecution authorities, instead of the FDPIC which was created precisely for answering such questions. 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 underequipped and does only rarely engage in criminal prosecution matters. This cannot be compensated by private enforcement due to its respective lack of prominence.

V. Ghana

At least on a textual level, Ghana has sought inspiration from the EU Data Protection Directive and also partly of the US approach[398]. 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

---

394 Cf. on this terminology *Stark*, "Der Gesetzgeber hat mehr Bürokratie geschaffen". Interview mit David Rosenthal, 2021, p. 2, accessible under https://www.computerworld.ch/social/interview/gesetzgeber-buerokratie-geschaffen-2713114.html (last accessed 04.03.2024).

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

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

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

398 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.

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 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.[399] 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 the jurisdictions (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[400], 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, one could have thought that a supervisory authority and therefore privacy protection law itself, did not exist in Ghana.

VI. 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.[401] The same is true for basic 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, it leaves 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

[399] Art. 18 II DPA.

[400] See above, N 396.

[401] 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 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.

most other jurisdictions – be replaced by legitimate private interest. Apart from 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.[402] 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.

VII. 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 level. 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.[403]

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.[404] 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"[405]. 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 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

---

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

[403] *Norton Rose Fulbright,* 2023 Annual Litigation Trends Survey – Perspectives from Corporate Counsel, pp. 6, 17.

[404] 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, Boston University Law Review (2022), p. 793, 862.

[405] See on this model already above, → C.I.3.

Consumer Online Privacy Rights Act (COPRA)[406]). Similar proposed legislation, however, has so far never been successful.

VIII. California

California cannot stand alone besides the federal USA and must be assessed as part of its jurisdiction. 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.[407]

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. *Vice versa*, and only consequential, publicly accessible information are 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.

F. Approximating an Overall Rating

The findings of this paper potentially allow for building different clusters: 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. Lastly, Japan fails to 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.

---

[406] Legislative initiative of the 117th Congress (2021 – 2022) – S.3195, accessible under https://www.congress.gov/bill/117th-congress/senate-bill/3195 (last accessed 04.03.2024).

[407] 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.

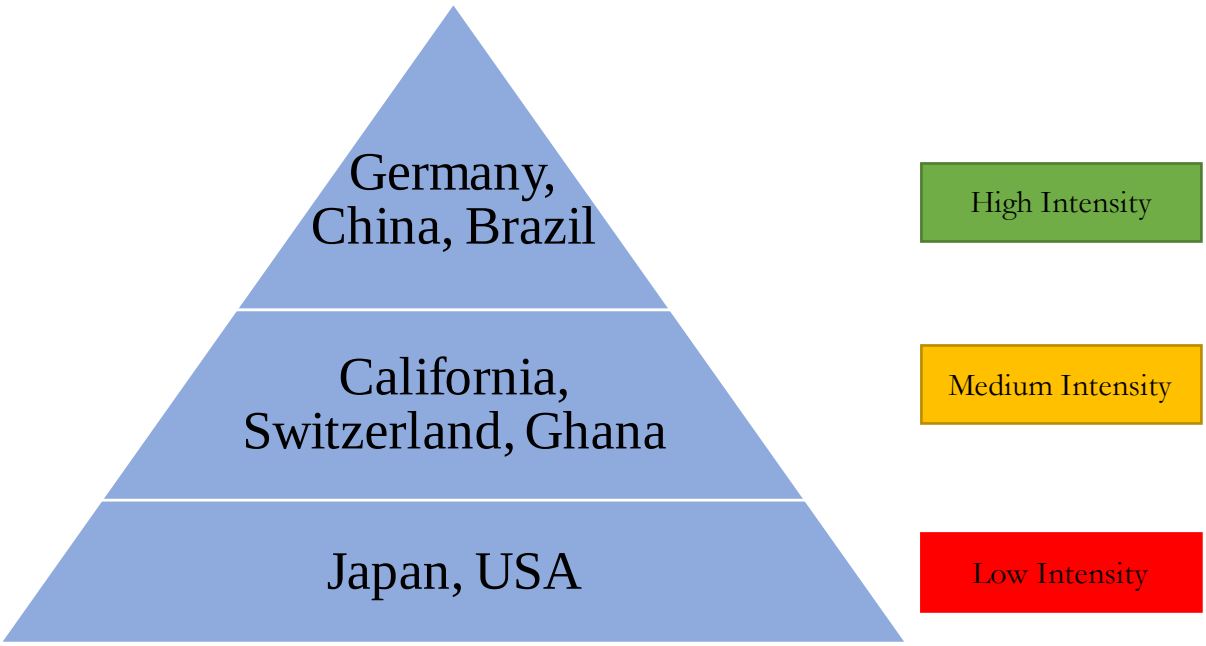

Figure 36: Final clustering of regulatory intensities

However, the additional remarks on enforcement intensities might change this picture: The USA and in particular California seem very capable of enforcing its rather lax substantive law, which might give raise to the assumption, 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 strikes as very intensive regulation that is, however, implemented in a system of weak or unfitting enforcement. Therefore, law in action is likely to be far below the standard provided for by law in the books. Such "Enforcement Gap"[408] is also apparent in higher developed jurisdictions such as Germany, Switzerland and even the US.[409] Only China with its techno-authoritarian system, and Japan with its extra-judicial settlement culture might be a little less prone to such systematic shortcomings of enforcement (be it of judicial or extra-judicial nature). However, assessing the capabilities and activities of a country's enforcement mechanism in combination with regulatory intensities may offer a more realistic view on the examined jurisdiction's privacy laws:

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

[409] Ibid, pp. 25 et seqq.

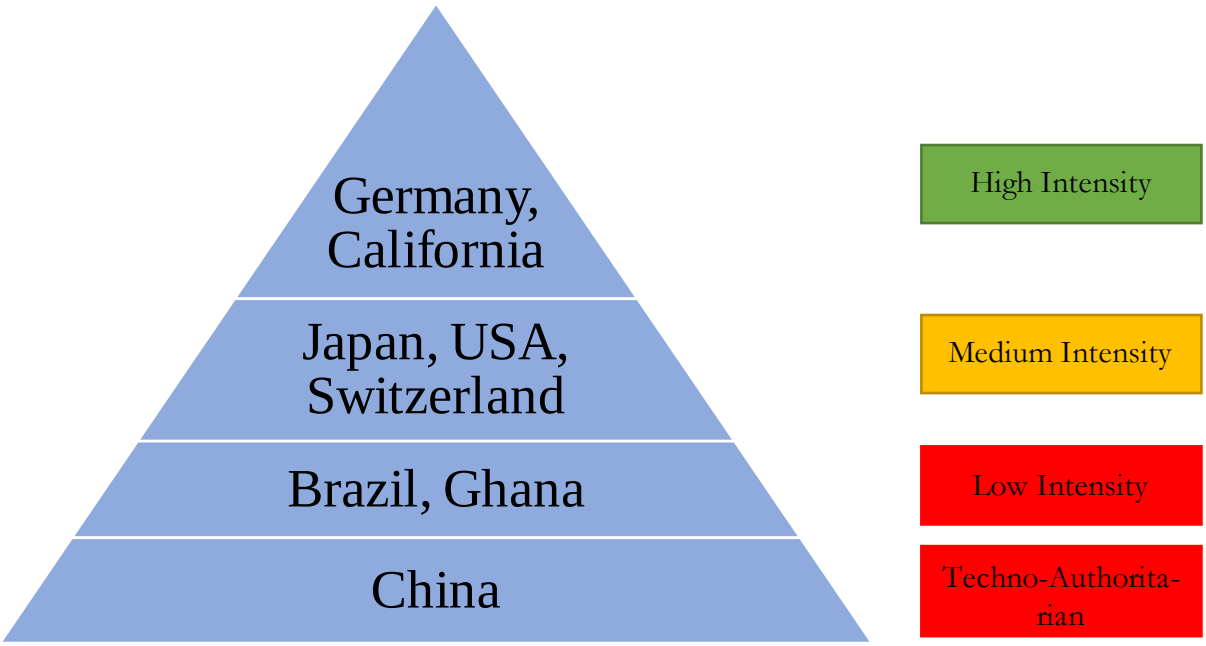

Figure 37: final clustering of regulatory intensities after consideration of the enforcement level

A Regulatory Clustering may not be limited to a ranking of any sorts. It could also (maybe even more fittingly) describe a number of categories which different jurisdictions can then be assigned to. An example would be the clustering of basic approaches to privacy regulation. In fact, this would create five different clusters, as most jurisdictions have a different, unique touch to it. China would constitute 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 in the same category of intensive risk-based regulation. These jurisdictions minimize privacy threats by implementing preventive restrictions. Switzerland does only partly fall within 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, relatively sweepingly allowing information collection, but restricting handling activities post-collection. The last cluster – let's call it "autonomy-based" approach – comprises of the USA and California and describes the basic concept of allowing all handling activities on the one side but giving the individual comprehensive information and rights to control such information handling activities.

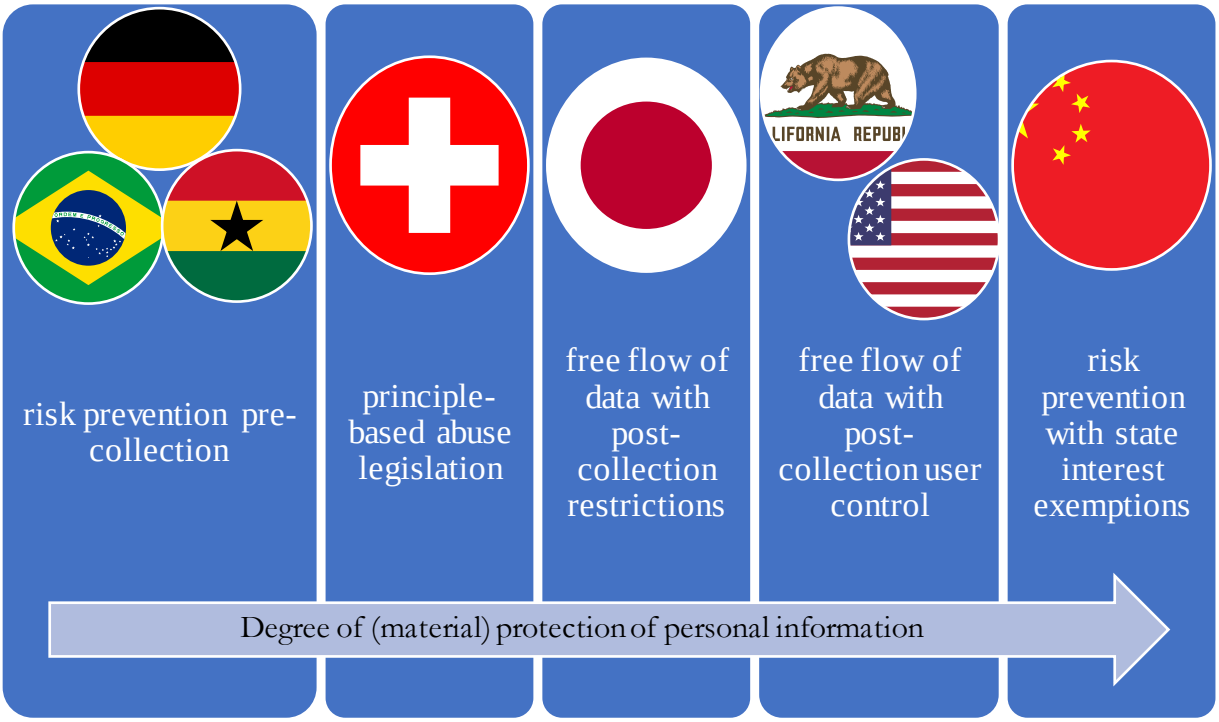

Figure 38: Regulatory approaches to privacy protection

Other clustered variables could be the proximity to each other[410], economic reference[411], the time at which regulation takes effect[412], or the role of governmental information handling[413].

Ultimately, this Regulatory Clustering shows that different jurisdictions all have their own advantages, disadvantages, approaches, and problems when addressing the matter of privacy. Depending on the variable to be researched, as well as the purpose of the research, the Regulatory

---

[410] 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.

[411] 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.

[412] The definition of such variable could be the main number 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).

[413] 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.

Clustering might be a good starting point for interdisciplinary research and law: Despite its frictions with conventional comparative law, building clusters of different jurisdictions might enable 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. Maybe, 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.