Targeting Reputation – Publication of Compliance as a Regulatory Concept in Comparative Data Protection Law

Sebastian J. Kasper and Timo Hoffmann

Abstract

In addition to direct sanctions, for example, in the form of levying fines, indirect measures like reputation-related measures might have a deterrent effect on companies. Particularly in data-driven industries, trust and having a good reputation seem to be important to acquire new customers and prevail over competitors. Therefore, it is not surprising that States may target companies' reputations to incentivise or compel them to comply with regulatory standards. This comparative paper shows that reputation-related measures are a common phenomenon across various data privacy legislations. However, this paper also demonstrates that the theory underlying reputation-related measures reveals many uncertainties when assessing the efficacy of those measures. By combining reputational literature, findings from the field of behavioural economics, and a comparative analysis, we further introduce structural elements for a typology to allow for future comparative assessments of regulatory concepts that target reputation.

1. Introduction

Legislation on data protection and informational privacy has become a global phenomenon,[1] with 157 countries having data privacy laws on their books as of mid-2022.[2] While laws aiming to protect individuals' personal information have existed for quite some time, data protection has steadily become more prominent. Particularly, the high fines that may be imposed under data protection laws, such as the European Union's (EU's) General

1 See Moritz Hennemann, 'Wettbewerb der Datenschutzrechtsordnungen' (2020) 84(4) RabelsZ 864.

2 Graham Greenleaf, 'Now 157 countries: Twelve data privacy laws in 2021/22' [2022] PrivL&BusIntlR 3.

https://doi.org/10.5771/9783748938743-79 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Data Protection Regulation (GDPR)[3] or the Brazilian General Personal Data Protection Law (LGPD)[4] have attracted attention.[5] However, many companies processing personal data fear not only (severe) monetary sanctions, but also the adverse effect on their reputation should the public become aware that they have violated data protection law[6].

We aim to identify and categorise regulatory instruments that impact companies' reputations directly or indirectly, in the context of data protection and informational privacy.

In an effort to account for the discussion and advancement in decolonial approaches to comparative law,[7] we attempt to reduce bias[8] by applying three strategies: Firstly, we employ a broad understanding of reputation-related measures in light of the concept of legal pluralism.[9] Secondly, we build our categorisation on an abstract typology which is derived from behavioural economics. Thirdly, we understand the various jurisdictions of our comparison as starting points to learn about different approaches to regulation, without being able to apply an all-encompassing comparison in this paper.[10]

Consequently, this article is structured as follows: We outline a theory of reputation (2), based on which we develop a typology for reputation-related measures (3). Thereafter, we compile a collection of regulatory

3 Article 83(4) and (5) Regulation (EU) 2016/679, OJ 2016 L 119/1.

4 Article 52(2) Lei Geral de Proteção de Dados Pessoais (*transl. General Law for the Protection of Personal Data*), Law No. 13.709 of 14 August 2018.

5 As an example, see BBC News, 'Three years of GDPR: the biggest fines so far' *BBC News* (24 May 2021) <https://www.bbc.com/news/technology-57011639> accessed 4 August 2023.

6 For a comprehensive analysis of reputational effects and countermeasures in the context of data breaches, see Kholekile L Gwebu, Jing Wang and Li Wang, 'The Role of Corporate Reputation and Crisis Response Strategies in Data Breach Management' (2018) 35(2) JMIS 683.

7 See only Lena Salaymeh and Ralf Michaels, 'Decolonial Comparative Law: A Conceptual Beginning' (2022) 86(1) RabelsZ 166.

8 Günter Frankenberg, 'Critical Comparisons: Re-thinking Comparative Law New Directions in International Law' (1985) 26(2) HarvIntlLJ 411.

9 For an introduction to the concept, see John Griffiths, 'What is Legal Pluralism?' (1986) 18(24) JLegPlurUnoffL, 1. Further, see Keebet von Benda-Beckmann and Bertram Turner, in: The Oxford Handbook of Global Legal Pluralism, 2020.

10 The 'traditional' structure of comparative legal research consists of the identification and comprehension of relevant legal rules in different jurisdictions followed by a comparative evaluation. See only Uwe Kischel, *Rechtsvergleichung* (C.H. Beck 2015) 109–111; Salaymeh and Michaels (n 7), passim.

https://doi.org/10.5771/9783748938743-79 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

concepts (4) and conclude with observations and a concept-oriented comparison (5).

2. Theory of Reputation

In this section, we outline what we understand under the concept of reputation. We therefore start by providing a working definition (2.1), before we demonstrate the mechanism of how reputation can or ought to influence human – and subsequently institutional – behaviour (2.2). Thereafter, we combine these mechanisms with various aspects stemming from the field of behavioural economics (2.3). We follow this approach to establish not only under which conditions the targeting of reputation as a regulatory concept could – ideally – work, but also where pitfalls might lie.

2.1 Notion and Structural Elements

When researching for a unified notion of reputation, the researcher quickly realises that such a notion does not exist.[11] The reason for this gap might be that various fields of research (e.g., psychology, economics, sociology, law) work with their own perceptions of reputation as a concept.

Coming from the field of law and economics, we build our arguments in this paper on a working definition that understands reputation as a "[…] set of beliefs that stakeholders hold regarding the company's quality."[12] This definition entails three main aspects: a group of stakeholders comprising more than one stakeholder, beliefs instead of knowledge, and perceived quality of the company in question, which usually includes the quality of the company's products or services. We apply these elements of a definition to the field of comparative data protection law.

In addition, if a company's reputation changes, it can influence at least two groups of parties. This links our understanding to the mechanisms described below.

11 Carolin Hümmer, *Die Reputation interner Dienstleister in Konzernen* (Business-to-Business-Marketing 2015) 39–49; John F Mahon, 'Corporate Reputation' (2002) 41(4) Bus&Soc'y 415, 438; Manfred Schwaiger and Sascha Raithel, 'Reputation und Unternehmenserfolg' (2014) 64(4) MRQ 225, 228–230; Kent Walker, 'A Systematic Review of the Corporate Reputation Literature: Definition, Measurement, and Theory' (2010) 12(4) CorpReputRev 357, 379.

12 Roy Shapira, *Law and Reputation* (Cambridge University Press 2020) 21.

https://doi.org/10.5771/9783748938743-79 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Group of Stakeholders. It is important to notice that a company's reputation is made up of the sum of various stakeholders' perceptions.[13] Consequently, it is not a matter of altering only one person's experience with or beliefs in a company or its products to effectively affect the company's reputation. Considering the pace in which positive and, more importantly, negative information disseminates on social media,[14] it is likely that the necessary group size of individuals who have personally experienced an incident shrinks.[15]

Aggregate of Beliefs. Stakeholders' perceptions consist of their beliefs about a company's past actions and situations[16], with the likelihood that the above-mentioned beliefs can be influenced by but are often distinct from actual knowledge. More importantly, the stakeholders' perceptions, their attitudes towards an industry or sector, their (factual) experiences with a company, and the media coverage[17] constitute important influences.

With a focus on data protection, stakeholders can experience a company's attitude towards data protection, for example, when they are (properly or improperly) confronted by cookie banners, when their access to certain webpages is (not) restricted by paywalls, or when they are burdened with extensive (or concise) data protection consent forms. Furthermore, stakeholders' attitude towards an industry might result from personal (factual) experience with data leakage or similar incidents. However, most of the time it is media coverage that is likely to influence stakeholders' attitude towards the data industry. Media coverage can validate but also invalidate previous perceptions. Furthermore, it can also verify, question, or falsify personal (factual) experience.[18]

Similarly, the stakeholders' perceptions of a company can be influenced by reputation management mechanisms. Therefore, it is not surprising that

13 Charles J Fombrun, 'The Buidling Blocks of Corporate Reputation: Definitions, Antecedents, Consequences' in Michael L Barnett (ed), *The Oxford handbook of corporate reputation* (1st edn, Oxford Univ Press 2012) 102; Thomas Noe, 'A Survey of the Economic Theory of Reputation: Its Logic and Limits' in Michael L Barnett (ed), *The Oxford handbook of corporate reputation* (1st edn, Oxford Univ Press 2012) 116.

14 See only Tina McCorkindale and Marcia W Distaso, 'The Power of Social Media and Its Influence on Corporate Reputation' in Craig E Carroll (ed), *The Handbook of Communication and Corporate Reputation* (Blackwell Publishing Ltd 2013) 497–500.

15 Shapira (n 12) 26.

16 See only Mahon (n 11), 439.

17 This might also extend to non-traditional media, such as customer reviews on customer review platforms or social media.

18 See also Schwaiger and Raithel (n 11), 235–237, 251–252.

https://doi.org/10.5771/9783748938743-79 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

approximately 9.5 billion US dollars worldwide were spent on reputation management in the year 2019 alone.[19]

Focus on (Perceived) Quality of Company and Product. The third aspect pertains to the (perceived) quality of a company or product. When focusing on data protection, individual stakeholders can only assess the recency and frequency of a company's data leakages or data protection incidents. Apart from that, stakeholders can only trust in a company's fair, reasonable, and legal processing of their data, as described above.[20] Although it is possible to link trust to a company's prominence on the market and although an excellent reputation management highly influences trust,[21] we cannot focus on such a 'celebrity status' in our assessment of reputation in data protection laws.

Overall, trust in data-driven companies' handling of data, companies' attitude towards data protection, and the absence of data leakages become increasingly important for stakeholders to assess a company's quality, real or perceived, and integrity. Since the handling of data needs to be classified as a credence good or service instead of an experience good or service,[22] it is nearly impossible for stakeholders to factually assess such quality which is why believing in the handling of data becomes increasingly relevant. Owing to these information asymmetries, it can become even more pressing to have not only legal rules requiring companies to inform their customers about data leakages and other data protection incidents, but also media coverage.[23] Depending on a State's regulatory approach, also trust in data protection agencies, their efficacy, the companies' subsequent compliance, and transparency about the agencies' work can have their effects.[24]

Second and Third Parties. Should a State measure (e.g., mandatory information about a data leakage, acquiring a public or private certificate)

19 CHEQ and University of Baltimore, 'The Economic Cost of Bad Actors on the Internet: Fake News 2019' (November 2019), 11–13 <https://de.statista.com/statistik/daten/studie/1074000/umfrage/jaehrliche-kosten-durch-die-auswirkungen-von-fake-news/> accessed 4 August 2023.

20 Certifying companies' data processing might increase trust but highly depends on the frequency of or generally on continuous review mechanisms. Whether the triennial periodic review, outlined in Article 42 GDPR, is sufficient, will be seen.

21 Charles Fombrun and Mark Shanley, 'What's in a Name? Reputation Building and Corporate Strategy' (1990) 33(2) AMJ 233, 252–254.

22 Daniel Feser and Till Proeger, 'Knowledge-Intensive Business Services as Credence Goods—a Demand-Side Approach' (2018) 9(1) JKnowlEcon 62, 74.

23 See also below in section 4.2.

24 See also below in sections 4.3, 4.8, and 4.9.

https://doi.org/10.5771/9783748938743-79 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

target a company's reputation, we can identify two groups of parties on whom such reputation-related measures seem to have significantly different effects.

Firstly, there is the group of purported second parties. The second parties are customers, suppliers, investors, and other subjects that are directly dependent on a company.[25] Secondly, there is the group of third parties, which comprises the public, indirectly affected individuals, and other market players.

Armour et al. were able to demonstrate that reputation-related measures have up to nine times greater effect on the group of second parties than they have on the group of third parties.[26] Although their findings were limited to the capital market in the United Kingdom, some structural elements of financial markets and the markets for data-driven companies are comparable: Both fields are highly dependent on trust and their stakeholders' perception, both can be highly volatile depending on the current market situation; both build in large parts on reputation and information asymmetries. Consequently, the findings are at least in part transferable.

2.2 Mechanism

After having established what we understand by the term reputation and how it is built, we outline the (theoretical) mechanism that links reputation-related measures with intended effects. As *Figure 1* outlines, reputation-related measures (e.g., implemented by a State) are supposed to influence a company's behaviour preventively (before any incident might occur) or at least for the future (after an incident occurred).

25 Jonathan M Karpoff, 'Does Reputation Work to Discipline Corporate Misconduct?' in Michael L Barnett (ed), *The Oxford handbook of corporate reputation* (1st edn, Oxford Univ Press 2012) 372.

26 John Armour, Colin Mayer and Andrea Polo, 'Regulatory Sanctions and Reputational Damage in Financial Markets' (2017) 52(4) JFinancQuantAnal 1429.

https://doi.org/10.5771/9783748938743-79 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

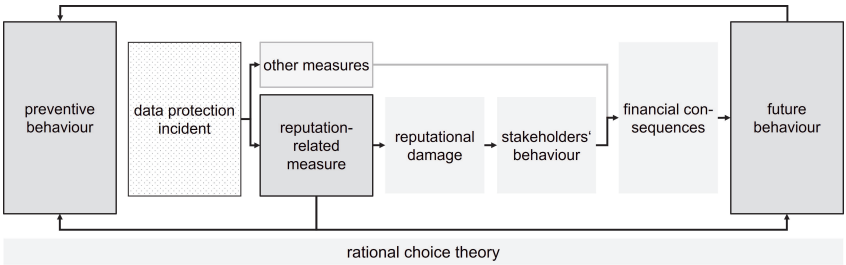

Figure 1 Structured Mechanism of Reputation and its Effects on Behaviour

Ideally, the mere threat of reputation-related measures alters a company's behaviour, because it adapts to avoid the measures' indirect[27] effects. This is because (effective) reputation-related measures that follow a data protection incident will lead to reputational damage. Consequently, the reputational damage alters the stakeholders' perception of a company, which, in turn, affects the company's returns negatively.[28] To avoid such financial repercussions, a company will – so goes the theory – do as much as economically possible and feasible to steer clear of reputational damage.

However, even if a company did not avoid a data incident, it will alter its conduct for the future to avoid further (reputational) losses. Sometimes, the company might also plan to demonstrate to the market and its shareholders that it has changed its behaviour. Such conduct signals market goodwill on the company's part and might restore some, if not all, of its reputational losses.[29]

Reputation-related measures rely on the market to evaluate the data incident and to react accordingly. This already indicates a fundamental obstacle of reputation-related measures: The market needs to be correctly, timely, and comprehensibly informed.[30] Consequently, when evaluating whether reputation-related measures might be effective, it is necessary to

27 In contrast, pecuniary fines can have a more direct, yet sometimes less damaging effect. See only ibid.

28 ibid 1440, 1442.

29 Mobin Fatma and others, 'Building company reputation and brand equity through CSR: the mediating role of trust' (2015) 33(6) IJBM 840, 850.

30 Mona N Lintvedt, 'Putting a price on data protection infringement' (2022) 12(1) IDataPrivL 1, 14.

https://doi.org/10.5771/9783748938743-79 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

consider findings relating to the risk of exposure.[31] In parallel, asymmetrical information might entail aspects of market failure, such as adverse selection and moral hazard.[32]

Additionally, the described mechanism of reputation-related measures is directly linked to the theory of (fully) rational behaviour. A fully rational and calculating individual would assess the risk of exposure and multiply it by the expected direct and indirect financial losses. If the calculated sum is higher than the costs of compliance, it will initiate the relevant changes, and vice versa.

2.3 Behavioural Economics and Reputation

However, it is well established that individuals do not behave fully rationally.[33] Instead, their behaviour is subject to heuristics (shortcuts), limited by their computational capacity, and prone to biases.[34] Consequently, it might well be that a company's representative does not act upon the introduction or enactment of reputation-related measures. At the same time, these measures build on the assumption and expectation that a broad audience[35] notices, (correctly) assesses, decides to act, and acts upon a data incident (e.g., a data leakage).[36] However, cognitive biases might interfere with each of these four steps (notice, assess, decide, act).

Noticing. Firstly, stakeholders need to become aware of the relevant pieces of information (e.g., about a data leakage). This is easier assumed than proven, since the mere magnitude of information stimuli to which stakeholders are exposed impedes noticing all relevant information. Especially when stakeholders are not directly informed about a data incident,

31 See Annika Selzer and others, 'Practitioners' Corner – An Economic Analysis of Appropriateness under Article 32 GDPR' (2021) 7(3) EDPL 456, 461.

32 See chapter by Kerber/Specht-Riemenschneider in this volume.

33 Gerd Gigerenzer and Reinhard Selten, 'Rethinking rationality' in Gerd Gigerenzer and Reinhard Selten (eds), *Bounded Rationality* (Dahlem Workshop Reports, MIT Press 2001) 1, 2–6.

34 See only the findings by Daniel Kahneman, *Attention and effort* (Prentice Hall series in experimental psychology, Prentice Hall 1973); Daniel Kahneman and Amos Tversky, 'Prospect Theory: An Analysis of Decision under Risk' (1979) 47(2) Econometrica 263; Amos Tversky and Daniel Kahneman, 'Judgment under Uncertainty: Heuristics and Biases' (1974) 185(4157) Science 1124.

35 See section 2.1 above.

36 Michael L Barnett, 'Why Stakeholders Ignore Firm Misconduct' (2014) 40(3) JManage 676, 683 et passim.

https://doi.org/10.5771/9783748938743-79 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

they often only learn of such a situation if an intermediary (e.g., the media) reports about it. In those cases, however, the link between an incident and a stakeholder noticing it is indirect and therefore unsure. Consequently, not every piece of information will reach the individual stakeholder and the market with the same intensity.

Furthermore, such information needs to be salient[37] enough to stand out from the magnitude of information that surrounds stakeholders every day. Especially, the level of harm (caused by a data incident), the stakeholders' personal or professional[38] interests in noticing a piece of information, their motivation to learn about (types of) information, and heuristics (e.g., availability heuristic) will determine whether they notice such information.[39]

Assessing. Secondly, stakeholders who have noticed a piece or pieces of information also need to assess it correctly. At this stage, primarily the way in which information is presented (e.g., framing effects[40]) determines how stakeholders will assess information. Moreover, there are a variety of heuristics and biases that originate from within a stakeholder (e.g., confirmation bias,[41] ambiguity aversion,[42] status quo bias[43]) and influence the way and likelihood to assess a (piece of) information correctly.

Deciding. Thirdly, and assuming that a stakeholder has noticed a piece or pieces of information and assessed it correctly, the stakeholder must decide whether to act on the information. At that stage, the market's status quo is as important as biases that originate from the stakeholder itself. Only if a market allows for equally suitable alternatives (e.g., alternative messenger services that at least most of a stakeholder's regular contacts use or might

37 Salience generally refers to the degree to which a particular attribute or piece of information is prominent or noticeable in the decision-making process of an individual or group, see Pedro Bordalo and others, 'Salience and Consumer Choice' (2013) 121(5) JPoliticalEcon 803, 3, 40.

38 An example might be system administrators who become aware of risks stemming form certain programmes, etc.

39 Barnett (n 36), 683 et passim.

40 Alan M Rubin, 'An Examination of Television Viewing Motivations' (1981) 8(2) Communication Research 141, 158.

41 Barnett (n 36), 688.

42 Daniel Ellsberg, 'Risk, Ambiguity, and the Savage Axioms' (1961) 75(4) QJEcon 643, 668.

43 William Samuelson and Richard Zeckhauser, 'Status quo bias in decision making' (1988) 1 JRiskUncertain 7, 47.

https://doi.org/10.5771/9783748938743-79 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

likely use) and only if the opportunity costs[44] that are incurred when switching to the alternative service are not prohibitive, is a stakeholder faced with a reasonable opportunity to switch service providers.[45]

Moreover, stakeholders are again subject to diverse biases (e.g., status quo bias, sunk costs fallacy[46], home bias[47]), which might prevent them from acting. Furthermore, stakeholders need to be motivated to switch services or service providers. The perception of how they personally assess the immaterial costs of changing current and practiced behaviour will influence their calculation of opportunity costs.

Acting. Fourthly, even if individuals noticed an incident that harms a company's reputation, assess the situation fully and correctly, and decide to take action, there remain three ways in which they can act: do nothing, voice their irritation, or exit the market or company's service.[48]

To sum up, the prima facie link between introducing a reputation-related measure and the aforesaid measure taking effect is all but straight and clear. Instead, there are multiple hurdles and obstacles that such measures need to overcome before becoming effective.

3. Structural Elements for a Typology

The following structural elements for a typology are meant to support a future comparison of regulatory measures. The elements are influenced by the above-described mechanism of reputation and are drawn from our comparison of eight data protection legal systems.[49] They lead towards

44 Opportunity cost is the value of the next best alternative forgone as a result of making a decision, see Nicholas G Mankiw, *Principles of macroeconomics* (Cengage Learning 2021) 4.

45 At this stage, competition laws came into play, see also Kerber/Specht-Riemenschneider in this volume.

46 Samuelson und Zeckhauser 1988, S. 35.

47 Bong-Chan Kho and others, 'Financial Globalization, Governance, and the Evolution of the Home Bias' (2009) 47(2) JAccountRes 597, 600.

48 For the purpose of assessing the (immediate) effects of reputation-related measures, future re-entries into the market can be ignored at this stage.

49 For a summary of our research project's legal comparison, see Timo Hoffmann, 'The Laws of Data Disclosure: Examining the Regulation of Individuals' Personal Data Disclosure in Brazil, China, the European Union, Ghana, Japan, Russia, Switzerland and the United States of America' in Moritz Hennemann and others (eds), *Data disclosure: Global developments and perspectives* (Global and Comparative Data Law Volume 2, De Gruyter 2023), 1.

https://doi.org/10.5771/9783748938743-79 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

the concept-oriented comparison (5). In this paper, we wish to describe eight such elements, knowing that this list can only be a starting point for future research.[50] With these elements, we attempt to categorise the reputation-related measures below (4).

3.1 Mode of Regulation

A first element pertains to the mode of regulation. Some reputation-related measures are the result of self-regulatory advances. Those self-regulatory measures might be developed by industry associations or companies themselves to signal compliance with high levels of data protection. Other measures are circumscribed by legislation, whereas the details are left to companies or industry associations to determine (i.e., regulated self-regulation). Then again, other measures are completely prescribed by law.

3.2 Actors

A second element focuses on the actors that are obligated under such regulation. Generally, this is either a private corporation or a State organ. However, there might be specific alternatives to or forms of such dichotomy. For example, industry associations – which can be State-owned, publicly organised, or founded as a privately owned association – might be required to act upon legislation.

3.3 Effects

A third element concerns the effects of a measure. When it comes to reputation-related measures, these effects can range on a continuum from very concrete effects (e.g., direct shaming) to rather diffuse effects (e.g., naming). Undoubtedly, the particular formulation, reach, and distribution of those measures will influence how a particular measure is assessed in terms of its effects.

50 For a link between these elements and the collection of concepts, see the concept-oriented comparison in and at 5 below.

https://doi.org/10.5771/9783748938743-79 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

3.4 Impact as a Sanction

A fourth element has to do with whether the reputation-related measure has an impact as a sanction. Again, this element should be understood as a continuum, ranging from no sanction intended through to measures that are structured to only have secondary sanctioning effects or measures that involve intended sanction. In practice, most measures could be argued to have at least secondary sanctioning effects.

3.5 Starting Point

A fifth element is the starting point of a reputation-related measure. Whereas some measures are meant to have preventive effects, others are designed to operate repressively. Particularly, measures that operate based on information requirements can have both effects. Following such information, market participants might refrain from using a company's products or they might take measures to protect their data.

3.6 Reach

A sixth element has to do with a measure's reach. When it becomes necessary to inform aggrieved parties directly about, for example, a data leakage, the measure focuses on a definable group of individual subjects. However, if a measure is meant to inform the general public, it reaches an undefinable group and can be described as collective.

3.7 Point in Time

A seventh element pertains to the timeline or point in time when a measure is meant to take place. Particularly, measures that should have preventive effects usually also need to be conducted before a data incident occurs. Other measures function (primarily) repressively and have to be implemented in the aftermath of a data incident. Then again, there are measures that need to be activated during a data incident. Nonetheless, some measures might take effect at various points in time.

https://doi.org/10.5771/9783748938743-79 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

3.8 Reception

An eighth and last element has to do with the reception. Whereas some measures are meant to be noticed directly by market participants, others are aimed at intermediaries. In the latter case, it is left for such intermediaries (e.g., general press, news media outlets, academic literature, private website hosts, blogs) to further distribute the effects of a measure. Often, intermediaries such as the press or the media exercise discretion in whether and how they disseminate information. Aggravated individuals or the public might therefore not be the primary recipient.

4. Collection of Concepts

The following sections outline a total of ten concepts of reputation-related measures we identified in various legal systems.

4.1 Codes of Conduct

A common reputation-related measure pertains to a (standardised) code of conduct about processing personal data. Typically, industry associations prepare these codes for their members, and the codes are meant to guide how to protect personal data for industry-specific or area-specific acts of processing. Usually, companies add a reference that they comply with these codes.

Data protection legislation can reference such codes of conduct, giving incentives for subscription to such a code[51] or allowing for review by the regulatory authority.[52] Within legislation, codes of conduct may be linked to modes of certification.[53]

51 Under Article 52 § 1 IX of the Brazilian *Lei Geral de Proteção de Dados Pessoais* (LGPD), the regulator can positively consider the adoption of a code of conduct in the form of a 'good practices and governance policy' in the event of the imposition of a sanction. See Timo Hoffmann and Pietro L Pietrobon de Moraes Vargas, 'LGPD Et Al.: Report on the Law of Data Disclosure in Brazil' (2022) 22(6) University of Passau IRDG Research Paper Series, 45.

52 Article 40 GDPR.

53 See section 4.2 below.

https://doi.org/10.5771/9783748938743-79 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Article 53 of the Japanese data protection law, the Act on the Protection of Personal Information (APPI),[54] provides for the implementation of codes of conduct via the development of guidelines by 'accredited personal information protection organizations'. These guidelines must be forwarded to the Personal Information Protection Commission (PPC), which then publishes the guidelines.[55] The accredited organisation must then 'take action' towards the implementation of the act.[56] Accredited organizations like those referred to above are usually industry associations.[57] In addition, the PPC lists the companies covered by such organisations on their website.[58]

The mere existence or non-existence of codes of conduct can have signalling effects for market participants.[59] Particularly, if an industry standard has been developed and the public is familiar with it, companies that do not reference such a code of conduct or that do not comply with it might be subject to reputational effects.

4.2 Certification Mechanisms

To obtain certification, a party intending to process personal data must submit itself (as an organisation), certain procedures, or provided services to a review by a regulator or specialised agency. Upon positive review, the party processing personal data may then advertise itself as certified or alike.[60] This allows those parties to signal their compliance with data protection legislation to the public.

54 Act on the Protection of Personal Information, amended version, effective 1 April 2022. English translation available at Personal Information Protection Commission Japan, 'Laws and Policies' (2023) <https://www.ppc.go.jp/en/legal/> accessed 4 August 2023.

55 Article 53(2) and (3) APPI.

56 Article 53(4) APPI.

57 Personal Information Protection Commission Japan, 'List of Authorized Personal Information Protection Organizations (transl.)' (8 February 2023) <https://www.ppc.go.jp/personalinfo/nintei/list/> accessed 8 February 2023.

58 ibid.

59 Stephen Brammer and Gregory Jackson, 'How Regulatory Institutions Influence Corporate Reputations: A Cross-Country Comparative Approach' in Michael L Barnett (ed), *The Oxford handbook of corporate reputation* (1st edn, Oxford Univ Press 2012) 310.

60 Regarding Article 42(5) GDPR and the 'European Data Protection Seal', see also Hornung/Kohpeiß in this volume.

https://doi.org/10.5771/9783748938743-79 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

An example of such certification by recognised independent certification bodies can be found in Article 11 of the Swiss Data Protection Act (DSG)[61]. Upon positive evaluation, companies acquire a 'Data Protection Quality Seal'[62]. In practice, this specific certification mechanism has not proven particularly popular.[63] Under the revised version of the DSG[64], set to enter into force in September 2023, the certification of services will be possible (Article 13) too, while the overall certification system remains unchanged.[65]

Certifications can have a signalling effect for market participants, if they (can) trust the certifying institution. Once a certification has become well established in the market, the stakeholders will also notice the absence of a certificate for a product, service, or company, which then leads to reputational effects.

4.3 Public Data (Protection) Register

In Ghana, Section 27 of the Data Protection Act 2012 (DPA)[66] includes a wide-ranging obligation for all parties processing personal data to register with the Data Protection Commission (DPC), that is the Ghanaian regulator. Those covered by the DPA are required, *inter alia*, to provide comprehensive information on their data processing activities, contact information, and a 'general description of measures to be taken to secure the data'.[67] The DPC then checks the application and registers the applicant.[68]

---

61 Bundesgesetz über den Datenschutz (transl. *Data Protection Act*), enacted 19 June 1992 as amended 1 March 2019, SR 235.1. Not to be confused with the revised DSG set to enter into force on 1 September 2023, which will also be referred to hereafter.

62 Translated from German: '*Datenschutz-Qualitätszeichen*'.

63 The Swiss regulator has already spoken of 'difficulties' with certification in 2010: Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter, 'Stand der Produkt- und Dienstleistungszertifizierung' (2011) <https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/datenschutzzertifizierung/stand-der-produkt--und-dienstleistungszertifizierung.html> accessed 8 February 2023.

64 Bundesgesetz über den Datenschutz (transl. *Data Protection Act*), enacted 25 September 2020, BBl 2020, 7639.

65 See further Peer Sonnenberg and Timo Hoffmann, 'Data Protection Revisited: Report on the Law of Data Disclosure in Switzerland' (2022) 22(17) University of Passau IRDG Research Paper Series, 45.

66 Data Protection Act, 2012 (Act 843).

67 Section 47(1) DPA 2012.

68 Section 49 DPA 2012.

https://doi.org/10.5771/9783748938743-79 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Registration and the registration's biennial renewal are subject to a fee,[69] which is the major source of financing for the DPC.[70]

The DPC makes the register accessible to the public,[71] which, in practice, is done via a searchable webpage.[72] Anyone interested in a particular party's data processing activities may check whether it is properly registered. Non-registration or expired registration is easily identifiable, clearly indicating non-compliance with this obligation. In practice, however, only a minority of obligated parties are registered,[73] leading to a temporary amnesty in an effort to increase registration numbers,[74] followed by the announcement of enforcement measures.[75]

Public data (protection) registers can improve public credence and allow for public easy-access information. Depending on the information these registers collect and on the level of review by the responsible authority, stakeholders can trust the validity of certain information or believe that their data is processed in compliance with the law.

4.4 Violation in Plain View

Another reputational effect of data protection may occur when a data protection law is violated in a manner that is clearly visible to a stakeholder. An example may be found in the non-fulfilment of information requirements under the GDPR.[76] The GDPR requires parties processing personal data to provide the data subject with information such as, *inter alia*, the purpose of

69 Section 59 DPA 2012.

70 See further Timo Hoffmann, 'Data Protection Act(ion): Report on the Law of Data Disclosure in Ghana' (2022) 22(1) University of Passau IRDG Research Paper Series, 15.

71 Section 54 DPA 2012.

72 Data Protection Commission Ghana, 'Data Protection Register – Entities Search' (2019) <http://app.dataprotection.org.gh/en/entities/search/> accessed 4 August 2023.

73 Ghanaian German Economic Association, 'Data controllers granted 6-month relief to regularize their operations' *Ghanaian German Economic Association* (12 October 2020) <http://ggea.net/news/data-controllers-granted-6-month-relief-to-regularize-their-operations/> accessed 4 August 2023.

74 Data Protection Commission Ghana, 'Amnesty' (2020) <https://dataprotection.org.gh/amnesty> accessed 4 August 2023.

75 Juliet Akyaa Safo, 'Register with Data Protection Commission or face prosecution – Adusei-Poku' *Graphic Online* (31 March 2022) <https://www.graphic.com.gh/news/general-news/register-with-data-protection-commission-or-face-prosecution-adusei-poku.html> accessed 4 August 2023.

76 Regulation (EU) 2016/679 of 2016, OJ L (2016) 119/1.

https://doi.org/10.5771/9783748938743-79 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

processing, categories of personal data processed, and the contact details of a data protection officer.[77] Data subjects who are aware of this requirement may notice non-compliance with the GDPR if asked to provide personal data. Failure to comply with such informational requirements may thus negatively affect the way in which the data subject witnessing this violation of the GDPR views the party processing personal data.

Depending on the stakeholders' data privacy literacy[78], they might be aware of missing information, the absence of cookie banners, or illegal dependencies between a company's request for personal data and access to its digital products. Consequently, the better the stakeholders know the relevant legal regime, the more severe the reputational loss suffered by non-compliant companies will be.

4.5 Notification Obligations after Data Breach

Obligations to report to the public are very common in the case of data leaks or data breaches. Where personal data is subjected to an incident such as hacking, data loss, or the like, the above-mentioned notification obligations require, with some variation, that the party informs the regulator, the data subjects affected, the public, or a combination of the former.

In the case of a 'personal data breach', for example, the GDPR requires notification of the relevant regulatory authority within 72 hours of awareness of the situation.[79] In severe cases,[80] the party affected by the breach is additionally required to inform the data subjects of the breach 'without undue delay',[81] alongside further information like the nature of the data breach, its consequences, and measures taken.[82] In cases where a great

77 Article 13 GDPR.

78 Data privacy literacy refers to the level of knowledge and understanding that stakeholders have about their data privacy rights, the risks associated with data collection and processing, and the measures they can take to protect their personal information, see Trepte and others, 'Do People Know About Privacy and Data Protection Strategies? Towards the "Online Privacy Literacy Scale"' in Serge Gutwirth and others (eds), *Reforming European Data Protection Law* (Springer Netherlands 2015) 333, 339.

79 Article 33(1) GDPR.

80 Article 34(1) GDPR.

81 Article 34(1) GDPR.

82 Article 34(3) GDPR.

https://doi.org/10.5771/9783748938743-79 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

number of individuals are involved, this may equate to a *de facto* publication requirement via media reception.[83]

Consequently, notification obligations are meant to allow data subjects not only to take appropriate measures to protect themselves from any harm (if feasible, e.g., changing of passwords), but also to allow them to take the data leakage into account when assessing whether a competitor might be better suited to protect their data. Since aggrieved subjects must often be personally informed, there is a very high probability that they at least notice the data incident, particularly when the responsible controller has taken further noticeable action to mitigate the impact of the breach.

4.6 Violation-Oriented Shaming as an Explicit Sanction

The explicit use of shaming as a sanction for violations of data protection laws is rare amongst data protection legislation, despite shaming being a widespread instrument in other areas of the law,[84] such as capital markets regulation, in the form of 'naming and shaming'.[85]

An exception can be found in the Brazilian LGPD.[86] In its catalogue of sanctions, the Brazilian data protection authority (ANPD)[87] may 'publicise the infraction after its accurate assessment and confirmation of its occurrence'.[88]

The ANPD has not yet published the guidelines for the application of sanctions. However, the comments on the sanction of publication in

83 Cédric Burton, *Article 34 Communication of a personal data breach to the data subject* (2020) 660.

84 Judith van Erp, '30 – Shaming and Compliance' in Daniel D Sokol and Benjamin van Rooij (eds), *The Cambridge Handbook of Compliance* (Cambridge University Press 2021) 439; Cullen S Hendrix and Wendy H Wong, 'When Is the Pen Truly Mighty? Regime Type and the Efficacy of Naming and Shaming in Curbing Human Rights Abuses' (2013) 43(3) BritJPolitSci 651, 671.

85 Judith van Erp, 'Naming and Shaming of Corporate Offenders' in Gerben Bruinsma and David Weisburd (eds), *Encyclopedia of criminology and criminal justice* (Springer Reference 2014) 3209, 3210; Edward F Greene and Joshua L Boehm, 'The Limits of "Name-and-Shame" in International Financial Regulation' (2012) 97(5) CornellLRev 1083, 1086.

86 Lei Geral de Proteção de Dados Pessoais (*transl. General Law for the Protection of Personal Data*), Law No. 13.709 of 14 August 2018.

87 Autoridade Nacional de Proteção de Dados (*transl. National Authority for the Protection of Personal Data*).

88 Article 52(4) LGPD.

https://doi.org/10.5771/9783748938743-79 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

the regulatory impact assessment concerning sanctions, which compares the sanction catalogue to other national and international legislation and comments on its operationalisation, implies that publication is to occur in the news media, such as in newspapers.[89] The offender is likely to also bear the costs of publication.[90]

Evidently, such shaming in the media has the potential of heavy reputational losses.[91] However, the specific effects will depend on details of the publication: the type and reach of the medium, whether publication occurs repeatedly, the size and presence of the publication, etc. In contrast to the previously described individual notification requirements, public shaming is less targeted at current customers but focuses on the public as a whole and potential future customers.

4.7 (Voluntary) Public Apology

In certain contexts, normative effects with regard to reputation in data protection contexts may arise not only from State law, but from societal expectations. Where there is strong social pressure, these expectations can constitute a form of law.[92] In data protection practice, a Japanese social 'obligation' may require a company to publicly apologise.[93] Such an apology may lead to more widespread awareness of a violation of law, but it may perhaps also soften the reputational blow as a countermeasure to negative public opinion. In Japan, public apologies are primarily made out of fear for the reputational impacts.[94]

In one case, this fear for the reputational impacts has extended to the granting of (low-value) vouchers to affected individuals.[95] This practice

89 Autoridade Nacional de Proteção de Dados, *Relatório de Análise de Impacto Regulatório: Construção do Modelo Regulatório Previsto Na LGPD com Relação à Aplicação de Sanções Administrativas e às Metodologias de Cálculo do Valor-Base das Sanções de Multa* (2022) 107–108.

90 This presumably relates to fees for advertisement space/time in such media.

91 See only Armour, Mayer and Polo (n 26); Sharon Yadin, 'Regulatory Shaming' (2019) 49(2) EnvtlL 407–451, 417.

92 For more detail on non-state normative ordering, refer to Griffiths (n 9), 1.

93 Flora Wang, 'Cooperative Data Privacy: The Japanese Model of Data Privacy and the EU-Japan GDPR Adequacy Agreement' (2020) HarvJL&Tech 661, 679–681.

94 Regarding willingness to disclose data, see Daniela Wawra and others, 'Cultural Influences on Personal Data Disclosure Decisions – Japanese Perspectives' [2022] SSRN Journal <https://ssrn.com/abstract=4079634> accessed 4 August 2023.

95 Wang (n 93), 680.

https://doi.org/10.5771/9783748938743-79 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

must be understood in the context of the generally observed aversion to litigation[96] and hard enforcement[97] in Japan[98] in favour of a focus on cooperation and communal reputation.

Public apologies can be out of the reputation management playbook.[99] Often, such apologies do not only disclose that a data breach has occurred, but also include information about the steps a company has already taken and is about to take to prevent future leaks. The additional information is meant to mitigate reputational losses. Consequently, apologies are open to exploit framing effects. At the same time, the fear of having to apologise to the public after a leakage can incentivise companies to take precautionary steps.

4.8 Public Relations Work by Supervisory Authorities

In some cases, supervisory authorities' publications and public relations work can have reputational effects. Often, such activities are required to enhance governmental transparency and are not necessarily considered a sanction from a legal perspective.

An example is the United Kingdom Information Commissioner's Office (ICO). The ICO makes its actions public – extensively – on its website, naming individual companies that have been fined, going as far as offering an 'action we've taken e-newsletter'.[100] In its press releases, the ICO, apart from naming the companies, even provides testimonials by victims, thereby making use of emotional responses to violations.[101]

---

96 Giorgio F Colombo and Hiroshi Shimizu, 'Litigation or Litigiousness? Explaining Japan's "Litigation Bubble" (2006-2010)' [2016] Oxford University Comparative Law Forum <https://ouclf.law.ox.ac.uk/litigation-or-litigiousness-explaining-japans-litigation-bubble-2006-2010/> accessed 4 August 2023.

97 Wang (n 93), 680.

98 See further Timo Hoffmann, 'Data Protection by Definition: Report on the Law of Data Disclosure in Japan' (2022) 22(3) University of Passau IRDG Research Paper Series.

99 Tulika M Varma, 'Responsible Leadership and Reputation Management During a Crisis: The Cases of Delta and United Airlines' (2021) 173(1) JBusEthics 29, 40.

100 UK Information Commissioner's Office, 'Action we've taken' (2023) <https://ico.org.uk/action-weve-taken/> accessed 4 August 2023.

101 UK Information Commissioner's Office, 'Five businesses fined a total of £435,000 for making nearly half a million unlawful marketing calls' (7 December 2022) <https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/12/five-busin

https://doi.org/10.5771/9783748938743-79 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

In a blog post, a law firm makes reference not only to the ICO's practice of 'naming and shaming', stating the importance of publicity as a concern of involved companies, but also to the 'lack [of] a clear appeals mechanism once a reprimand has been imposed'. The latter aspect is particularly problematic because such informational action by the ICO cannot, as opposed to other sanctions, be appealed to the relevant tribunal.[102] This hints at the high practical relevance of such public relations work by authorities and demonstrates the reputation effects companies fear.

4.9 Transparency in the Judicial or Administrative Process

Another notable reputation-related measure can come as a side effect of judicial or administrative transparency. By allowing for a high degree of transparency in judicial or administrative proceedings, the public can gain insight into alleged or actual breaches of data protection or privacy legislation. Such publications might include information on how (effectively) the situation was handled.

Where the United States' Federal Trade Commission enforces privacy laws in the US, documents regarding enforcement are made public, and thus transparent, to a great degree.[103] Comprehensive publication of case documents takes place, which allows for easily accessible insights into wrongdoing. This subjects the party processing personal data, conditional on enforcement action, to the 'court' of public opinion[104] alongside other applied sanctions.

The effect of such judicial or administrative transparency highly depends on the reception by major media outlets and the relevant public. Reputational effects are therefore usually rather indirect and dependent on the

---

esses-fined-a-total-of-435-000-for-making-nearly-half-a-million-unlawful-marketing-calls/> accessed 4 August 2023.

102 Giles Pratt and others, 'Naming and shaming? The UK ICO is now naming most organisations it investigates' (31 January 2023) <https://technologyquotient.freshfields.com/post/102i6m7/naming-and-shaming-the-uk-ico-is-now-naming-most-organisations-it-investigates> accessed 4 August 2023.

103 Federal Trade Commission, 'Privacy and Security Enforcement' 107–108 <https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement> accessed 4 August 2023.

104 See, for example, media reporting: Frank Bajak, 'FTC fines GoodRx for unauthorized sharing of health data' *CBS News* (1 February 2023) < https://www.cbsnews.com/sacramento/news/goodrx-unauthorized-sharing-of-health-data/> accessed 4 August 2023.

https://doi.org/10.5771/9783748938743-79 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

distribution by intermediaries should the judicial or administrative organ not enhance publication themselves.

4.10 Governmental Warnings

In certain situations, supervisory authorities may warn the public of certain companies or products that are considered harmful. While the sanctioning effect is not the primary goal, being subject to such a warning can have significant reputational impact.

In Germany, the Federal Office for Information Security (BSI)[105] may warn the public or affected groups in the event of a loss of or unauthorised access to data.[106] Although related to a slightly different context,[107] such a warning by the BSI was recently subject to much debate after it issued a warning against a Russian antivirus software provider[108] following the Russian invasion of Ukraine[109].[110]

In particular, if a government or its individual institutions are (highly) trusted by the citizens, a governmental or administrative warning can have detrimental effects on a company's reputation, presuming that such warnings are used rarely and as a measure of last resort. In such a case, it is likely not only that the warning itself is received, but also that the media will report about the warning to make it commonly known. Apart from that, the reputation effects resemble those described with regard to notification obligations (4.5 above), but furnished with a seal of a public warning.

105 Bundesamt für Sicherheit in der Informationstechnik (*transl. Federal Office for Security in Information Technology)*.

106 § 7(1)(1)(c) of the Act on the Federal Office for Information Security (BSIG).

107 This incident concerned security concerns and was based on § 7(1)(1)(a) BSIG.

108 Bundesamt für Sicherheit in der Informationstechnik, 'Warnung vor Kaspersky-Virenschutzsoftware nach § 7 BSIG' (30 September 2022) <https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Technische-Sicherheitshinweise-und-Warnungen/Warnungen-nach-Par-7/Archiv/FAQ-Kaspersky/faq_node.html> accessed 4 August 2023.

109 UNGA, *Aggression against Ukraine* (01.03.2022) UN Doc A/ES-11/L.1; UNGA, *Principles of the Charter of the United Nations underlying a comprehensive, just and lasting peace in Ukraine* (16.02.2023) UN Doc A/ES-11/L.7.

110 For a comprehensive overview, see Tilmann Dittrich, 'Die "Akte Kaspersky": kritische Betrachtungen zur Warnung vor einer Virenschutzsoftware' (2022) NJW 2971.

https://doi.org/10.5771/9783748938743-79 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

5. Concluding Observations with Concept-Oriented Comparison

Table 1 below merges the above-described structural elements for a typology (3 above) with the collection of concepts described immediately above (4 above). In this last section, we therefore share some concluding observations that follow a concept-oriented comparison.

regulatory instruments	mode of regulation	actors	effects	Impact as a sanction	starting point	reach	point in time	reception
codes of conduct	(regulated) self-regulation	private	diffuse	none	preventive	collective	before incident	direct
certification mechanisms	(regulated) self-regulation	private/ public	diffuse	none	preventive	individual/ collective	before incident	direct/ indirect
public data (protection) register	statutory regulation	public	diffuse	secondary effect	preventive	collective	before incident	direct/ indirect
violation in plain view	statutory regulation	private	concrete	secondary effect	preventive/ repressive	individual	during incident	direct
notification obligations after data breach	statutory regulation	private/ public	concrete	secondary effect	preventive/ repressive	individual/ collective	after incident	direct
violation-oriented shaming as an explicit sanction	statutory regulation	public	concrete	intended	preventive/ repressive	collective	after incident	indirect
(voluntary) public apology	self-regulation	private	concrete	intended	(preventive/) repressive	collective	after incident	indirect
public relations work by supervisory authorities	statutory regulation	public	concrete/ diffuse	secondary effect/intended	preventive/ repressive	collective	after incident	indirect
transparency in the judicial or administrative process	statutory regulation	public	diffuse	secondary effect/none	preventive/ repressive	individual/ collective	after incident	(direct/) indirect
governmental warnings	statutory regulation	public	concrete/ diffuse	secondary effect/intended	Preventive (/repressive)	collective	during incident	direct/ indirect

Table 1 Reputation-related Measures Assessed by Elements of Typology

When assessing the efficacy of reputation-related measures, a common determinant is that the relevant public first needs to notice and process the given information before there is a chance that such information leads to reputational losses. Even if the relevant public notices and processes such information, reputation-related measures can only have an effect if there is sufficient relevant competition that allows stakeholders to switch, for example, service providers.[111]

The link between a reputation-related measure and its effects is rather indirect and often requires intermediaries to play their role. Furthermore, dissemination of information via the media will reach second and third parties alike.[112] Therefore, it will be difficult to evaluate such measures' effects precisely. Consequently, the preventive effects of reputation-related measures are equally uncertain.

From a comparative point of view, we realise that several measures are not primarily meant to have reputation-related effects. However, many

111 See Kerber/Specht-Riemenschneider in this volume.
112 See above following n 24.

https://doi.org/10.5771/9783748938743-79 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

accept such reputation-related effects as side effects. Thus far, we could also not identify reputation-related measures with which supervisory authorities explicitly address second parties.

Apart from informational obligations that are often required to obtain consent from data subjects for processing their data, most reputation-related measures are repressive by nature. Furthermore, most measures build on disseminating information in one way or another and can be identified as descriptive by nature. Consequently, stakeholders need to be sufficiently knowledgeable to assess the risk based on such factual and descriptive information. However, such assessment requires a high level of data protection literacy.

Overall, reputation-related measures are common to all reviewed jurisdictions, be it either as direct and intended measures or as indirect side effects.

Acknowledgement

The presented research is part of an interdisciplinary research project 'Vectors of Data Disclosure – A comparative study on the disclosure of personal data from the perspectives of legal, cultural studies, and business information systems research', https://www.bidt.digital/en/vectors-data-disclosure, supported by the Bavarian Research Institute for Digital Transformation (an Institute of the Bavarian Academy of Sciences and Humanities). We would like to thank the participants of the Jahrestagung Forum Privatheit 2022 in Berlin for their feedback and many discussions. Furthermore, we would like to thank the student research assistant Nico Göbel for supporting us with finalising this paper.

References

Akyaa Safo J, 'Register with Data Protection Commission or face prosecution - Adusei-Poku' *Graphic Online* (31 March 2022) <https://www.graphic.com.gh/news/general-news/register-with-data-protection-commission-or-face-prosecution-adusei-poku.html> accessed 4 August 2023.

Armour J, Mayer C and Polo A, 'Regulatory Sanctions and Reputational Damage in Financial Markets' (2017) 52(4) JFinancQuantAnal 1429.

https://doi.org/10.5771/9783748938743-79 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Autoridade Nacional de Proteção de Dados, *Relatório de Análise de Impacto Regulatório: Construção do Modelo Regulatório Previsto Na LGPD com Relação à Aplicação de Sanções Administrativas e às Metodologias de Cálculo do Valor-Base das Sanções de Multa* (2022).

Bajak F, 'FTC fines GoodRx for unauthorized sharing of health data' *CBS News* (1 February 2023) <https://www.cbsnews.com/sacramento/news/goodrx-unauthorized-sharing-of-health-data/> accessed 4 August 2023.

Barnett ML, 'Why Stakeholders Ignore Firm Misconduct' (2014) 40(3) JManage 676.

BBC News, 'Three years of GDPR: the biggest fines so far' *BBC News* (24 May 2021) <https://www.bbc.com/news/technology-57011639> accessed 4 August 2023.

von Benda-Beckmann K, Turner B, 'Anthropological Roots of Global Legal Pluralism' in Paul Schiff Berman (ed), *The Oxford Handbook of Global Legal Pluralism* (1st edn, Oxford Univ Press 2020).

Bordalo P, Gennaioli N and Shleifer A, 'Salience and Consumer Choice' (2013) 121(5) JPoliticalEcon 803.

Brammer S and Jackson G, 'How Regulatory Institutions Influence Corporate Reputations: A Cross-Country Comparative Approach' in Michael L Barnett (ed), *The Oxford handbook of corporate reputation* (1st edn, Oxford Univ Press 2012).

Bundesamt für Sicherheit in der Informationstechnik, 'Warnung vor Kaspersky-Virenschutzsoftware nach § 7 BSIG' (30 September 2022) <https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Technische-Sicherheitshinweise-und-Warnungen/Warnungen-nach-Par-7/Archiv/FAQ-Kaspersky/faq_node.html> accessed 4 August 2023.

Burton C, *Article 34 Communication of a personal data breach to the data subject* (2020).

CHEQ and University of Baltimore, 'The Economic Cost of Bad Actors on the Internet: Fake News 2019' (November 2019) <https://de.statista.com/statistik/daten/studie/1074000/umfrage/jaehrliche-kosten-durch-die-auswirkungen-von-fake-news/> accessed 4 August 2023.

Colombo GF and Shimizu H, 'Litigation or Litigiousness? Explaining Japan's "Litigation Bubble" (2006-2010)' [2016] <https://ouclf.law.ox.ac.uk/litigation-or-litigiousness-explaining-japans-litigation-bubble-2006-2010/> accessed 4 August 2023.

Data Protection Commission Ghana, 'Data Protection Register – Entities Search' (2019) <http://app.dataprotection.org.gh/en/entities/search/> accessed 4 August 2023.

— 'Amnesty' (2020) <https://dataprotection.org.gh/amnesty> accessed 4 August 2023.

Dittrich T, 'Die "Akte Kaspersky": kritische Betrachtungen zur Warnung vor einer Virenschutzsoftware' [2022] 2971.

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter, 'Stand der Produkt- und Dienstleistungszertifizierung' (2011) <https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/datenschutzzertifizierung/stand-der-produkt--und-dienstleistungszertifizierung.html> accessed 8 February 2023.

Ellsberg D, 'Risk, Ambiguity, and the Savage Axioms' (1961) 75(4) QJEcon 643.

https://doi.org/10.5771/9783748938743-79 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

van Erp J, 'Naming and Shaming of Corporate Offenders' in Gerben Bruinsma and David Weisburd (eds), *Encyclopedia of criminology and criminal justice* (Springer Reference 2014).

— '30 – Shaming and Compliance' in Daniel D Sokol and Benjamin van Rooij (eds), *The Cambridge Handbook of Compliance* (Cambridge University Press 2021).

Fatma M, Rahman Z and Khan I, 'Building company reputation and brand equity through CSR: the mediating role of trust' (2015) 33(6) IJBM 840.

Federal Trade Commission, 'Privacy and Security Enforcement' (2018) <https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement> accessed 4 August 2023.

Feser D and Proeger T, 'Knowledge-Intensive Business Services as Credence Goods—a Demand-Side Approach' (2018) 9(1) JKnowlEcon 62.

Fombrun C and Shanley M, 'What's in a Name? Reputation Building and Corporate Strategy' (1990) 33(2) AMJ 233.

Fombrun CJ, 'The Buidling Blocks of Corporate Reputation: Definitions, Antecedents, Consequences' in Michael L Barnett (ed), *The Oxford handbook of corporate reputation* (1st edn, Oxford Univ Press 2012).

Frankenberg G, 'Critical Comparisons: Re-thinking Comparative Law New Directions in International Law' (1985) 26(2) HarvIntlLJ 411.

Ghanaian German Economic Association, 'Data controllers granted 6-month relief to regularize their operations' *Ghanaian German Economic Association* (12 October 2020) <http://ggea.net/news/data-controllers-granted-6-month-relief-to-regularize-their-operations/> accessed 4 August 2023.

Gigerenzer G and Selten R, 'Rethinking rationality' in Gerd Gigerenzer and Reinhard Selten (eds), *Bounded Rationality* (Dahlem Workshop Reports, MIT Press 2001).

Greene EF and Boehm JL, 'The Limits of "Name-and-Shame" in International Financial Regulation' (2012) 97(5) CornellLRev 1083.

Greenleaf G, 'Now 157 countries: Twelve data privacy laws in 2021/22' [2022] 3.

Griffiths J, 'What is Legal Pluralism?' (1986) 18(24) JLegPlurUnoffL 1.

Gwebu KL, Wang J and Wang L, 'The Role of Corporate Reputation and Crisis Response Strategies in Data Breach Management' (2018) 35(2) JMIS 683.

Hendrix CS and Wong WH, 'When Is the Pen Truly Mighty? Regime Type and the Efficacy of Naming and Shaming in Curbing Human Rights Abuses' (2013) 43(3) BritJPolitSci 651.

Hennemann M, 'Wettbewerb der Datenschutzrechtsordnungen' (2020) 84(4) RabelsZ 864.

Hoffmann T, 'Data Protection Act(ion): Report on the Law of Data Disclosure in Ghana' (2022) 22(1) University of Passau IRDG Research Paper Series.

— 'Data Protection by Definition: Report on the Law of Data Disclosure in Japan' (2022) 22(3) University of Passau IRDG Research Paper Series.

https://doi.org/10.5771/9783748938743-79 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

— 'The Laws of Data Disclosure: Examining the Regulation of Individuals' Personal Data Disclosure in Brazil, China, the European Union, Ghana, Japan, Russia, Switzerland and the United States of America' in Moritz Hennemann and others (eds), *Data disclosure: Global developments and perspectives* (Global and Comparative Data Law Volume 2, De Gruyter 2023).

Hoffmann T and Pietrobon de Moraes Vargas PL, 'LGPD Et Al.: Report on the Law of Data Disclosure in Brazil' (2022) 22(6) University of Passau IRDG Research Paper Series.

Hümmer C, *Die Reputation interner Dienstleister in Konzernen* (Business-to-Business-Marketing, 2015).

Kahneman D, *Attention and effort* (Prentice Hall series in experimental psychology, Prentice Hall 1973).

Kahneman D and Tversky A, 'Prospect Theory: An Analysis of Decision under Risk' (1979) 47(2) Econometrica 263.

Karpoff JM, 'Does Reputation Work to Discipline Corporate Misconduct?' in Michael L Barnett (ed), *The Oxford handbook of corporate reputation* (1st edn, Oxford Univ Press 2012).

Kho B-C, Stulz RM and Warnock FE, 'Financial Globalization, Governance, and the Evolution of the Home Bias' (2009) 47(2) JAccountRes 597.

Kischel U, *Rechtsvergleichung* (C.H. Beck 2015).

Lintvedt MN, 'Putting a price on data protection infringement' (2022) 12(1) IDataPrivL 1.

Mahon JF, 'Corporate Reputation' (2002) 41(4) Bus&Soc'y 415.

Mankiw NG, *Principles of macroeconomics* (Cengage Learning 2021).

McCorkindale T and Distaso MW, 'The Power of Social Media and Its Influence on Corporate Reputation' in Craig E Carroll (ed), *The Handbook of Communication and Corporate Reputation* (Blackwell Publishing Ltd 2013).

Noe T, 'A Survey of the Economic Theory of Reputation: Its Logic and Limits' in Michael L Barnett (ed), *The Oxford handbook of corporate reputation* (1st edn, Oxford Univ Press 2012).

Personal Information Protection Commission Japan, 'Laws and Policies' (2023) <https://www.ppc.go.jp/en/legal/> accessed 4 August 2023.

— 'List of Authorized Personal Information Protection Organizations (transl.)' (8 February 2023) <https://www.ppc.go.jp/personalinfo/nintei/list/> accessed 8 February 2023.

Pratt G, Annear R and Gillert A, 'Naming and shaming? The UK ICO is now naming most organisations it investigates' (31 January 2023) <https://technologyquotient.freshfields.com/post/102i6m7/naming-and-shaming-the-uk-ico-is-now-naming-most-organisations-it-investigates> accessed 4 August 2023.

Rubin AM, 'An Examination of Television Viewing Motivations' (1981) 8(2) Communication Research 141.

Salaymeh L and Michaels R, 'Decolonial Comparative Law: A Conceptual Beginning' (2022) 86(1) RabelsZ 166.

https://doi.org/10.5771/9783748938743-79 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Samuelson W and Zeckhauser R, 'Status quo bias in decision making' (1988) 1 JRiskUncertain 7.

Schwaiger M and Raithel S, 'Reputation und Unternehmenserfolg' (2014) 64(4) MRQ 225.

Selzer A, Woods D and Böhme R, 'Practitioners' Corner – An Economic Analysis of Appropriateness under Article 32 GDPR' (2021) 7(3) EDPL 456.

Shapira R, *Law and Reputation* (Cambridge University Press 2020).

Sonnenberg P and Hoffmann T, 'Data Protection Revisited: Report on the Law of Data Disclosure in Switzerland' (2022) 22(17) University of Passau IRDG Research Paper Series.

Trepte S and others, 'Do People Know About Privacy and Data Protection Strategies? Towards the "Online Privacy Literacy Scale"' in Serge Gutwirth and others (eds), *Reforming European Data Protection Law* (Springer Netherlands 2015).

Tversky A and Kahneman D, 'Judgment under Uncertainty: Heuristics and Biases' (1974) 185(4157) Science 1124.

UK Information Commissioner's Office, 'Action we've taken' (2023) <https://ico.org.uk/action-weve-taken/> accessed 4 August 2023.

— 'Five businesses fined a total of £435,000 for making nearly half a million unlawful marketing calls' (7 December 2022) <https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/12/five-businesses-fined-a-total-of-435-000-for-making-nearly-half-a-million-unlawful-marketing-calls/> accessed 4 August 2023.

United Nations General Assembly (UNGA), *Aggression against Ukraine* (01.03.2022) UN Doc A/ES-11/L.1.

— *Principles of the Charter of the United Nations underlying a comprehensive, just and lasting peace in Ukraine* (16.02.2023) UN Doc A/ES-11/L.7.

Varma TM, 'Responsible Leadership and Reputation Management During a Crisis: The Cases of Delta and United Airlines' (2021) 173(1) JBusEthics 29.

Walker K, 'A Systematic Review of the Corporate Reputation Literature: Definition, Measurement, and Theory' (2010) 12(4) CorpReputRev 357.

Wang F, 'Cooperative Data Privacy: The Japanese Model of Data Privacy and the EU-Japan GDPR Adequacy Agreement' (2020) 33(2) HarvJL&Tech 661.

Wawra D and others, 'Cultural Influences on Personal Data Disclosure Decisions – Japanese Perspectives' [2022] <https://ssrn.com/abstract=4079634> accessed 4 August 2023.

Yadin S, 'Regulatory Shaming' (2019) 49(2) EnvtlL 407–451.

https://doi.org/10.5771/9783748938743-79 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY