Self-Determination and Data Protection by Design

The trend in data protection law and in fundamental legal protection of information pertaining to personality is moving in the direction of "X by design" - where X may stand for different approaches to protecting legal personality. The protection of data subjects is to be built into information systems and artifacts by the specification of design parameters, and their users are moved to reducing their risk by the targeted deployment of heuristics. In this paper, the concepts of self-determined and design-based data protection are briefly summarised, juxtaposed, and the transition from one regulatory concept to another is examined. The purpose of presenting this interplay is to show what we can gain through design, where threats to the rights of those concerned lurk, and what is at stake for the constitutionally protected freedoms.

Philip Glass, www.datalaw.ch/self-determination-and-design/

This article is a translated version of the paper that formed the basis for my talk on the same topic at the [IRIS 2019](https://www.univie.ac.at/RI/IRIS2019/) in Salzburg. The original German version is published in the conference proceedings and in [Jusletter IT of February 21, 2019](https://jusletter-it.weblaw.ch/issues/2019/IRIS.html).

1. Self-determination as a fundamental value of data protection law

1.1. Consent and legal processing authoritisation

[1] The dominant approach in Swiss law to date is that of data protection by means of an agreement on data processing processes between private individuals on the one hand and law-based processing of personal data by public bodies on the other.[1]

[2] The concept is based first of all on the principle of private autonomy, as it is enshrined in the Civil Code, but ultimately on the protection against personal injury guaranteed in Art. 28 ZGB[2].[3] At the level of the protection of constitutional individual rights, the protection of which must be exercised as far as possible by the state in Swiss law pursuant to Art. 35 para. 3 BV[4] both in the public and in the private sphere,[5] data protection by intent means the implementation of the fundamental right to informational self-determination by the persons concerned in individual cases. Consenting or permitting data processing - whether individually by consent or collectively by law - justifies the inherent personal injuries involved and (in principle) renders such processing legal.[6] From the point of view of data protection law, the requirement for consent can trigger a static momentum when such consent is treated as formal processing requirement or even as a legal base for processing, without providing guidance on how to conserve ("Schonung"[7]) the threatened rights. With a sig-

---

[1] See Art. 13 Abs. 1 DSG (Bundesgesetz über den Datenschutz vom 19. Januar 1992 [DSG; SR. 235.1]; federal data protection statute): «Eine Verletzung der Persönlichkeit ist widerrechtlich, wenn sie nicht durch Einwilligung des Verletzten, durch ein überwiegendes privates oder öffentliches Interesse oder durch Gesetz gerechtfertigt ist.»

[2] Schweizerisches Zivilgesetzbuch vom 10. Dezember 1907 (ZGB; SR 210; civil code part 1).

[3] See Botschaft des Bundesrates zur Änderung des Bundesgesetzes über den Datenschutz (DSG) und zum Bundesbeschluss betreffend den Beitritt der Schweiz zum Zusatzprotokoll vom 8. November 2001 zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Aufsichtsbehörden und grenzüberschreitende Datenübermittlung vom 19. Februar 2003 BBl 2003 2101, 2127.

[4] Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999 (BV; SR 101; Swiss federal constitution).

[5] BIAGGINI, BV Kommentar: Bundesverfassung der Schweizerischen Eidgenossenschaft, Orell Füssli, Zürich 2017, Art. 35 n. 4, 7 and 21.

[6] Art. 13 Abs. 1 DSG.

[7] On the principle of "Schonung" see DRUEY, Der Kodex des Gesprächs – Was die Sprechaktlehre dem Juristen zu sagen hat, Nomos, Baden-Baden 2015, p. 402 f.

nature applied, the system architecture in question and the relevant data processes are considered approved - without, however, providing a further incentive for continuous optimisation.

1.2. The idea of a quasi ownership of personal data

[3] One approach to strengthening the legal position of data subjects lies in the idea of qualifying data as the quasi-property of individuals for whom the data is considered to be personal data.[8] In the foreground is the person from whom the information in the data originated and to whom it still refers - the data subject. However, data rights are also conceivable for persons to whom aggregated data are applied by assigning information on the basis of certain characteristics as pseudo-personal data[9] - more like data objects. It is very questionable whether it would make sense to regard the relevant data as quasi-property of the individualised person when attributing information.

[4] Apart from the practical problems surrounding this concept that have to do with the nature of data, information and their interaction, I think that in particular the rightful power of ownership speaks against it. THOUVENIN rightly points out that ownership of personal data could be transferred through sale to the acquirer who in turn could prohibit the data subject the use of his or her former personal data[10] Individuals would be able to sell their personal rights completely, which would run counter to the prohibition of excessive commitment.

[5] The crucial - and generally accepted - point seems to me that personal references within the information contained in data with respect to a particular individual can create a legal right of participation concerning the processing parameters for that data. This creative power results from the personality of this individual and is anchored in the personality right. It is not a question of claiming and locking away media, but of granting the right to participate as effectively as possible in defining the nature, extent, timing and purpose of personal data processing, and thereby affirming the legitimate expectations of the context-sensitive confidentiality of the information transmitted.[11] Because of their roots in personal rights, one can not completely forgo this right. For the same reason the legislator is called upon to intervene if the right can not be effectively implemented by the individual due to structural circumstances.

1.3. The danger of undermining self-determination through private-autonomous approaches

[6] The disadvantage of the autonomous security of privacy through self-determined authorisation for data processing is that it regularly does not work where the risks for those affected are particularly high.[12] Ironically, because the idea of data protection was born out of the need to reign in the increasingly confusing and complex nature of information systems and their use, and to provide individuals with tools to defend their self-perception and -representation.

[7] In fact, in many areas of data protection law, the realisation of private autonomy is limited to being able to choose which provider to choose (the same often goes for smaller to medium-sized municipalities as well as specialised administrative bodies). Particularly in mass transactions both accessory data processing and

---

[8] See FRÜH, Roboter und Privacy: Informationsrechtliche Herausforderungen datenbasierter Systeme, Aktuelle Juristische Praxis (AJP), 2/2017, 147 ff.; THOUVENIN, Wem gehören meine Daten? Zu Sinn und Nutzen einer Erweiterung des Eigentumsbegriffs, Schweizerische Juristenzeitung (SJZ) 113/2017, p. 21.

[9] Data attributed to a person by probability; see GLASS, Bearbeitung, p. 198.

[10] THOUVENIN, *ibid.* p. 31.

[11] NISSENBAUM, Privacy in Context – Technology, Policy, and the Integrity of Social Life, Stanford Law Books, Stanford California, 2010, p. 231: «a right to live in a world in which our expectations about the flow of personal information are, for the most part, met».

[12] HARTZOG, Privacy's Blueprint – The Battle to Control the Design of New Technologies, Harvard University Press 2018, p. 56 ff.; "*design gap*" in the torts pertaining to privacy.

further data processing (e.g. for marketing purposes, sociological experiments, sales to advertisers) are integrated as non-negotiable components of the general terms and conditions (GTC) in the contracts in question and this often only in an opaque way. The effect of such data protection is regularly limited to guaranteeing the client a minimal standard whose content is determined more by market structures than by legal requirements or even his own ideas for the protection of his digital personality.[13]

[8] Along with this, the (private and public) data processors have a legally wide open field for the technological control of users.[14] The law does not apply until a data breach has occurred; it is therefore a subsequent control, the effectiveness of which is uncertain inasmuch as it can only act when a remedy is being sought. In addition, "control" by consent does not affect third parties (e.g., cyberstalking, targeted disinformation) and, on the contrary, may limit liability for harmful third party action if such limitation has been contractually agreed.

1.4. Summary

[9] Essentially, legally motivated consent architectures for data protection are based on the idea of the right to informational self-determination and are intended to bring about implementation of this right through control over the processing or use of an individual's "own" personal data. The control thus affects the legal power of disposition regarding the manner and purpose of the use of personal information by certain third parties. It is an easy-to-understand concept that has been borrowed from civil law personality rights. The basic assumptions of the concept, however, are increasingly shown to not hold up to scrutiny. The concept opens up a great deal of room for data processors, who can subsequently only be legally restricted in cases of obvious personal injury - for example, if the consent appears as forced (monopoly problem) or immoral in the meaning of the civil code. This promotes a risk of undermining legal protection through consent as well as the "erosion of user autonomy"[15].

[10] Overall, there is much evidence to suggest that self-determined, deliberate control by consent to the processing of personal data both in the domain of civil and of public law, does not fulfil or insufficiently fulfils its function preventing personality harms.[16] Rather, due to the economic, political, technical and informational imbalance of power between the actors, it is often not suitable for exercising an actual control and decision-making function with regard to the realisation of informational self-determination.

2. Design-based Data Protection

2.1. Privacy by design and other design approaches

[11] Data protection by design assumes that the personality of data subjects and objects can be better protected in many areas if the underlying information systems are designed with a view to enabling and realising privacy. Design-based data protection approaches use the property of code to function as a kind of law and thus to transport values. Of crucial importance is the insight that coded architectures and algorithms always carry values.[17] In addition to the data processing itself, the technical conditions of data processing now

---

[13] Baeriswyl, Neuer Datenschutz für die digitale Welt – Ein wirksames Datenschutzkonzept muss die tatsächlichen Risiken für die Privatheit minimieren können, digma – Zeitschrift für Datenrecht und Informationssicherheit, 2011.1, p. 7, as early as 2011 speaks in this context of a "de facto abolition of data protection rights"; Hartzog, Privacy's Blueprint, p. 62 ff.

[14] Hoffmann-Riem, Verhaltenssteuerung durch Algorithmen – Eine Herausforderung für das Recht, Archiv des öffentlichen Rechts (AöR) 142 1/2017, p. 23; Hartzog, Privacy's Blueprint, p. 57.

[15] Hoffmann-Riem, Verhaltenssteuerung, p. 21.

[16] See Baeriswyl, Neuer Datenschutz, p. 8.

[17] Lessig, Code Version 2.0, 2006, p. 6: «we can build, or architect, or code cyberspace to protect values that we believe are fundamental. Or we can build, or architect, or code cyberspace to allow those values to disappear. There is no middle ground»; Hildebrandt, Algorithmic Regulation and the Rule of Law, Phil.Trans. R. Soc. A 376: 2017035, 2018, p. 7.

come into the focus of legal assessment. These conditions, embodied by the respective information system, in combination with its application environment, should reduce the leeway for the use of personal data as close as possible to the legally permissible contextual relationships.[18] Data protection by design can stabilise risks to the rights of those affected by legally restricting and technically predefining the permissible scope of decision-makers with respect to data processing, which is usually outside the sphere of influence of the data subjects.

[12] In connection with design-oriented data protection, Swiss doctrine relies on the concept of *privacy by design*[19],[20] which has found its way into Art. 25 GDPR[21] and shall be incorporated into Swiss law in the form of a dual principle (by design and default) in the course of the revision of the federal data protection law statute.[22] The concept is attributed to ANN CAVOUKIAN and consists of seven principles. Data protection thus is a proactive concept that follows the guiding principle of privacy by default, is embedded in information systems (embedded privacy), geared towards win-win situations between supposedly divergent interests, is effective over the entire life cycle of information, transparent for all concerned and always user-centric in its approach.

[13] The basic idea of integrated data protection embodied by the system itself has been incorporated in a number of ways and made fruitful for similar legal and design issues. A more general method of value-oriented engineering design, for example, is the approach of *value sensitive design*[23] or *design for value*[24]. It is a methodology that combines conceptual, empirical, and technical investigations into a comprehensive tool for estimating consequences for the future realisation of (moral) values.[25] The key point remains a proactive approach, as already highlighted in the context of privacy by design. These evolved concepts assume that the values to be observed are not fixed from the outset, but must be determined and harmonised with each other in the course of the preparation of a project[26] - for example through discourse or *participative design*[27]. At their core, therefore, these are procedural theories[28] that should (also) be used in to further the values protected by data law and that the law can adopt and implement. The proceduralisation of data protection law gives it greater flexibility. The inclusion of the data subjects (regularly represented by the responsible data

[18] See HARASGAMA/TAMÒ, Smart Metering und Privacy by Design im Big-Data-Zeitalter: Ein Blick in die Schweiz, in: Weber/Thouvenin (Eds.), Big Data und Datenschutz – Gegenseitige Herausforderungen, Schulthess, Zürich/Basel/Genf 2014, p. 131.

[19] For the concept see CAVOUKIAN, Privacy by design, The 7 Foundational Principles, revised version 2011; see also the updated tabular overview in TAMÒ-LARRIEUX, Designing for Privacy and its Legal Framework – Data Protection By Design and Default for the Internet of Things, Springer Nature, Cham 2018, p. 85; SCHAAR, Privacy by design, IDIS (2010) 3:267, https://doi.org/10.1007/s12394-010-0055-x; for the further development see HARTZOG, Privacy's Blueprint, p. 179 ff.; HILDEBRANDT, Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology, Edward Elgar Publishing Inc. 2015, p. 214 ff.: "legal protection by design"; GLASS, Die rechtsstaatliche Bearbeitung von Personendaten in der Schweiz – Regelungs- und Begründungsstrategien des Datenschutzrechts mit Hinweisen zu den Bereichen Polizei, Staatsschutz, Sozialhilfe und elektronische Informationsverarbeitung, Diss. Univ. Basel, Dike, Zürich /St. Gallen 2017, p. 197 ff.; and a new addition with *contestability by design* as a design parameter for securing automated decision-making systems in ALMADA, Contesting Automated Decisions: Limits to the Right to Human Intervention in Automated Decision-Making, SSRN Electronic Journal (2018), 10.2139/ssrn.3264189, p. 11 f.

[20] BAERISWYL, Neuer Datenschutz, p. 7; GASSER, Perspectives on the Future of Digital Privacy, Zeitschrift für Schweizerisches Recht (ZSR) 2015 II 335, p. 378 ff.; HARASGAMA/TAMÒ, Smart Metering, p. 131 ff.

[21] See EDPS, Preliminary Opinion on privacy by design, Opinion 5/2018, 31 May 2018.

[22] Botschaft des Bundesrates zum Entwurf eines revidierten Datenschutzgesetzes vom 15. September 2018, BBl 2017 6941, 7029.

[23] FRIEDMAN, Value-Sensitive Design: A Research Agenda for Information Technology – A Report on the May 20-21, 1999 Value-Sensitive Design Workshop, https://vsdesign.org/outreach/pdf/friedman99VSD_Research_Agenda.pdf; FRIEDMAN/KAHN JR./BORNING, Value Sensitive Design and Information Systems, in: Zang/ Galetta (Eds.), Human-Computer Interaction and Management Information Systems: Foundations, 2nd Ed. London New York 2015, p. 348 ff.

[24] VAN DEN HOVEN/VERMAAS/VAN DE POEL, Design for Values: An Introduction, in: Van den Hoven/Vermaas/Van De Poel (Eds.), Handbook of Ethics, Values, and Technological Design – Sources, Theory, Values and Application Domain, Dordrecht 2015, *passim*.

[25] FRIEDMAN/KAHN JR./BORNING, Value Sensitive Design and Information Systems, p. 351.

[26] For the debate see DAVIS/NATHAN, Value Sensitive Design: Applications, Adaptations, and Critiques, in: Van den Hoven/Vermaas/Van De Poel (Eds.), Handbook of Ethics, Values, and Technological Design – Sources, Theory, Values and Application Domain, Dordrecht 2015, p. 20 ff.

[27] VAN DER VELDEN/MÖRTBERG, Participatory Design and Design for Values, in: Van den Hoven/Vermaas/Van De Poel (Eds.), Handbook of Ethics, Values, and Technological Design – Sources, Theory, Values and Application Domain, Dordrecht 2015, p. 41 ff.

[28] For the concept see TSCHENTSCHER, Prozedurale Theorien der Gerechtigkeit – Rationales Entscheiden, Diskursethik und prozedurales Recht, Nomos, Baden-Baden 2000, p. 132 ff.

protection authorities) as well as other sources of legitimacy (experts, NGOs, commissions, round tables) can thus produce information technology artifacts (databases, access matrixes, user interfaces) and infrastructures with greater legitimacy.

[14] It is common to the various design-based concepts that the values and their interdependent weighting as well as the resulting evaluation pattern, which serves as a basis or target value for the functional orientation of an information system, are disclosed within the design process. Overall, design data protection opens up the possibility of a legally informed system design that integrates the rights of participation and the right to an explanation of those affected.

2.2. Data security as a design specification

[15] At this point, I would like to list data security as a significant, albeit ambiguous design aspect of information systems.[29] Data security pursues the threefold goal of confidentiality, integrity and availability of data - but not the goal of "data protection" (or privacy).[30] The goals mentioned form the operational prerequisites for the meaningful use - and thus intrinsic protective motives - of information systems.

[16] In this context is the judgment of 27 February 2008 of the first Senate of the German Federal Constitutional Court is of interest, in which the court linked the two aspects of data security and data protection to a right to privacy-oriented system integrity. According to the ruling, the fundamental right to privacy-oriented integrity and confidentiality of information technology systems is to be applied in addition to the right of informational self-determination if the legal authorisation concerns systems that, by themselves or in conjunction with other systems within their technical network, make available personal data of the data subject to an extent and in a variety that access to this system allows an insight into essential parts of a person's life style or even to get a meaningful picture of the subject's personality.[31] The connection of the two aspects from the point of view of the constitutional personality rights clearly shows that these are two different aspects of information systems whose goals are not automatically congruent. From this realisation it follows that data security as a system component must be design for data protection values in the same way as the information system as a whole - the method of privacy by design is therefore also to be observed for data security and is not automatically fulfilled by the latter's implementation.

[17] The goals of data protection for information systems are therefore always extrinsic integrity motives - i.e. they are realised outside the information system, namely in the protection of the personality of persons to whom data or information is assigned - that nevertheless inform the design of system security and co-determine the importance and scope of system integrity.[32] Data security is therefore an important basis for data protection. In particular, it constitutes the technical prerequisite for the enforcement of data protection objectives.[33] On the other hand, an information system that meets all data security requirements may be inadequate in terms of data protection or may cause unnecessary risks to personality rights.[34]

2.3. The aim of design-based data protection

[18] For data protection-oriented design of information systems, the goals in a state adhering to the rule of law must be based on the fundamental principles of the constitution, in particular on the informational aspects of fundamental rights as well as private rights. For Switzerland, this includes the fundamental rights as

---

[29] See the references to the historical development in Tamò-Larrieux, Designing for Privacy, p. 84.

[30] For the differences in goals see Glass, Bearbeitung, p. 138 f.

[31] Judgment from the first Senate from February 27. 2008, 1 BvR 370/07; 1 BvR 595/07, para. 203.

[32] See Glass, Singularisation and Identification, www.datalaw.ch, February 27. 2018, DOI: 10.5281/zenodo.1436396.

[33] Hartzog, Privacy's Blueprint, p. 104.

[34] Wildhaber, Informationssicherheit, p. 28: «Datensicherung ohne Datenschutz ist ohne weiteres möglich, Datenschutz ohne Datensicherung hingegen undenkbar».

a whole, but especially informational self-determination, freedom of expression and information, as well as basic communication rights.[35] Likewise, the privacy rights, especially legal ones, are conveyed by the obligation to fulfil obligations in Art Private autonomy.[36] The overarching goal is the constitutionally informed structuring of networked information systems - and thus the technical ambient intelligence[37]. This structuring sets out the permitted contexts for the processing of personal data afforded by the legal system.[38] Data protection thus becomes an environmental problem with regard to the information environment or *infosphere*[39]. The problem is shifting away from a mere defence against unwanted data processing towards the setting of rules for the joint design of an autonomy-promoting informational environment.

[19] It is therefore important for data protection law to note that privacy is always only a means to the end of achieving autonomy, which, in turn, is the basis for the legal guarantee of personal development and human dignity.[40] Accordingly, *X by Design* must be interpreted and understood in the light of constitutional rights and subsequently as a central design principle promoting the rule of law for information systems - for example, in the form of *legal protection by design*[41] or more broadly, *autonomy by design*[42].

3. The added value of design-based data protection

3.1. Legitimisation of data processing according to public interest

[20] The added value of a design-based approach lies in the fact that in this way legal decision-making power can be shifted from the parties involved (data subjects/objects and data processors) to social decision-making structures. In other words, the transition from a private-autonomous to a design-oriented approach transforms a personal question into a question of infrastructure design and the weight of private and public interests involved. Thus those value judgments of most importance to society as a whole can be anticipated by translation in law and subsequently into system architectures. At the same time, the abandonment of concrete self-determination and shaping power requires the building of trust in the legitimacy and function of information systems.[43]

[21] The proceduralisation of data protection standards frees the individual data subject from justifying forms of data processing that are the result of structural phenomena and therefore rarely negotiable in individual cases. On the other hand, the data processor is relieved of the *quasi-ecological legal responsibility*[44] to design processes that are in his or her interest in a way that is compatible with the common good. In other words, a design-based approach allows for the procedural, continuous development of the relevant processes based on discursive reconciliation of mutual interests over time - and beyond the scope of individual data handlers. Thus, data protection law is switching from a question of permission to a question of designing data processing systems under constant feedback from both society and the interested parties, facilitating a transparent, continuous optimisation of the balance between the values and interests involved.

---

[35] Glass, Bearbeitung, p. 179 ff. with further references.

[36] See Glass, The protective parameters of civil and constitutional personality rights in Swiss law, www.datalaw.ch, Mai 29 2018, DOI: 10.5281/zenodo.1436387.

[37] Hoffmann-Riem, Rechtliche Rahmenbedingungen für und regulative Herausforderungen durch Big Data, in: Hoffmann-Riem (Ed.), Big Data – regulative Herausforderungen, Baden-Baden 2018, p. 22 w.f.r.

[38] Glass, Bearbeitung, p. 126 ff.

[39] Floridi, The Fourth Revolution: How the Infosphere is Reshaping Human Reality, Oxford University Press 2014, p. 119.

[40] Glass, Bearbeitung, p. 172.

[41] Hildebrandt, Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology, Edward Elgar, Cheltenham UK/Northampton MA 2015, p. 218.

[42] Glass, Bearbeitung, p. 197; Friedman, Introduction, in: Friedman (Ed.), Human Values and the Design of Computer Technology, CSLI Publications/Cambridge University Press 1997, p. 5: «At the same time, such systems can help users to realize their goals and intentions through their use of the technology – a human value which Nissenbaum and I […] refer to as autonomy».

[43] Cavoukian, Privacy by design: the definitive workshop. A foreword by Ann Cavoukian, Ph.D, IDIS (2010) 3: 247.

[44] Druey, Der Kodex des Gesprächs, p. 397 ff.

3.2. Promotion of a cyclical understanding of data protection

[22] As a further advantage, the design approach also leads away from a legally formulaic, static data view of protection requiring discrete, usually unique decisions, towards a more substantive, dynamic data protection law based on ongoing, legally guided risk assessment legitimised by procedurally binding feedback pertaining to legally protected interests. In particular, such dynamic data protection allows for the temporal component to be taken into account and thus to accompany and assess the processing and its effects in the context of risk assessments over the entire life cycle of information and data. For this to work properly, the tool box has to be adapted to the different phases of the data and information cycle.[45]

[23] For public sector data processors, this will allow a more flexible application of data protection and substantive laws involving various stakeholders which may result in the assessment of projects depending not so much on the quality of the legal base but on the interaction of the legitimation of this legal base with the respective risk profile of a project over time, including measures for the ongoing optimisation of that profile towards better data protection. In particular, it also means that identified risks can be accepted as residual risk over a certain period of time - for example as part of a pilot project - if specific measures to mitigate risks are mature or available in the foreseeable future.

[24] For private data processors, a procedural understanding of data law additionally opens up the possibility of a publicly negotiated, flexible minimum legal standard that leaves room for strategic differentiation from other participants in the relevant market.

4. The ambivalent protection of self-determination through design

[25] When introducing and implementing procedural data protection concepts, it should not be forgotten that the design of information systems and interfaces with regard to the optimisation of public interests (such as data protection issues) interferes with the fundamental and personal rights of all parties involved and can lead to a societal relativisation of central components of the previous constitutional order.[46] On the one hand, those parties are limited in their shaping power, which could determine the system architecture largely without consultation of contractual counterparts due to the power or market conditions. On the other hand, the optimisation of user or customer behaviour through the targeted use of heuristics has a highly manipulative component, even if this is done for the benefit of those affected. It is therefore important to ensure that those whose behaviour (here: mediated by information systems) should be changed by and large remain "authors of their own actions".[47] For Swiss law, this means that such interventions must be legitimised by the rule of law and respect the personality of those affected. Due to their encroaching nature, the regulation of design requirements for information systems by the state only appears legitimate where this is done in the exercise of fundamental rights protection obligations according to Art. 35 BV (federal constitution),[48] is made transparent and appears proportionate. The latter criterion also requires that state regulations of design choices resulting in a relatively low impact on fundamental rights should only be taken into consideration subsidiarily, while the preservation of the rights of structurally weaker parties would initially burden the structurally stronger contracting parties.[49]

---

[45] See Tamò-Larrieux, Designing for Privacy, p. 149 ff.; EDPS, Preliminary Opinion, p. 15 f.

[46] Hildebrandt, Smart Technologies, S. 216, warns that the inevitable alignment of legal mechanisms of law with the new information environment should not erode the substance of the previous legally protected system of values.

[47] Hildebrandt, Algorithmic Regulation, p. 5; «treated as authors of their own actions».

[48] Biaggini, BV Kommentar, Art. 35 n. 7 w.f.r.

[49] Glass, Schutzparameter, n. 18 w.f.r.

5. Final remarks

[26] By implementing design-based data protection, the power to make decisions regarding data processing will increasingly be shifted to the technical sphere. As a result, deficits in autonomy and trust are more evident and must be addressed, in particular through feedback loops to compatible networks of constitutional legitimacy[50], by strengthening and emphasising the information and justification obligations regarding data, purposes, models, risk assessments, output expectations and further use. Especially valuable would be the development of a constitutionally supported dialogue culture between data subjects and objects as well as data processors who would ideally be able to plausibly redeem the original promise of data protection law as an instrument for the realisation of informational self-determination and autonomy. Along with this evolution, the role of data protection authorities is shifting towards supervising service providers who advise administrations on the design, development and continued integration of their information systems, in each case representing the interests of those who are not appropriately involved in the discussions pertaining to the functionality of system architectures and processes - the general public.

[27] The limits of possible legitimacy of the new technical approaches to data protection are not yet fully apparent. From the aim of of design-based data protection it can be deduced that the line will run along individual cases and typical case groups as a constitutional response to the distortions in the information landscape and the realisation of corresponding risks for those affected. Over time , a clear picture should emerge from the practice of data protection authorities and courts, showing which design approaches sufficiently protect the privacy rights and fundamental rights of those affected, and under what circumstances - without patronising them. Conversely, it will also be shown which forms of data processing are typically considered to be excessively binding in the sense of the Civil Code or as violations of core constitutional principles of the protection of personality rights, and should be avoided. Finally, the drafting and adoption of design requirements as a form of legislation or application will have to be closely linked to the legislative power involved and subject to the rules governing the delegation of such power.

6. Literature

ALMADA MARCO, Contesting Automated Decisions: Limits to the Right to Human Intervention in Automated Decision-Making, SSRN Electronic Journal (2018), 10.2139/ssrn.3264189.

BAERISWYL BRUNO, Neuer Datenschutz für die digitale Welt – Ein wirksames Datenschutzkonzept muss die tatsächlichen Risiken für die Privatheit minimieren können, digma – Zeitschrift für Datenrecht und Informationssicherheit, 2011.1, p. 6–11.

BIAGGINI GIOVANNI, BV Kommentar: Bundesverfassung der Schweizerischen Eidgenossenschaft, Orell Füssli, Zürich 2017.

CAVOUKIAN ANN, Privacy by Design, The 7 Foundational Principles, May 2010; http://www.ontla.on.ca/library/repository/mon/24005/301946.pdf (aufgerufen am 6. Januar 2019).

CAVOUKIAN ANN, Privacy by design: the definitive workshop. A foreword by Ann Cavoukian, Ph.D, IDIS (2010) 3: 247.

DAVIS JANET/NATHAN LISA P., Value Sensitive Design: Applications, Adaptations, and Critiques, in: Van den Hoven/Vermaas/Van De Poel (Eds.), Handbook of Ethics, Values, and Technological Design – Sources, Theory, Values and Application Domain, Springer, Dordrecht 2015.

DRUEY JEAN NICOLAS, Der Kodex des Gesprächs – Was die Sprechaktlehre dem Juristen zu sagen hat, No-

[50] See HOFFMAN-RIEM, Innovation und Recht – Recht und Innovation, Recht im Ensemble seiner Kontexte, Mohr Siebeck, Tübingen 2016, p. 104 f.

mos, Baden-Baden 2015.

FLORIDI LUCIANO, The Fourth Revolution: How the Infosphere is Reshaping Human Reality, Oxford University Press 2014.

FRIEDMAN BATYA, Introduction, in: Friedman (Ed.), Human Values and the Design of Computer Technology, CSLI Publications/Cambridge University Press 1997, p. 1–13.

FRIEDMAN BATYA, Value-Sensitive Design: A Research Agenda for Information Technology – A Report on the May 20-21, 1999 Value-Sensitive Design Workshop, August 23 1999; https://vsdesign.org/outreach/pdf/friedman99VSD_Research_Agenda.pdf (aufgerufen am 06. Januar 2019).

FRIEDMAN BATYA/KAHN JR. PETER H./BORNING ALAN, Value Sensitive Design and Information Systems, in: Zang/ Galetta (Eds.), Human-Computer Interaction and Management Information Systems: Foundations, 2nd Ed. M.E. Sharpe, London/New York 2015.

FRÜH ALFRED, Roboter und Privacy: Informationsrechtliche Herausforderungen datenbasierter Systeme, Aktuelle Juristische Praxis (AJP), 2/2017, p. 141–151.

GASSER URS, Perspectives on the Future of Digital Privacy, Zeitschrift für Schweizerisches Recht (ZSR) 2015 II 335–448.

GLASS PHILIP, Die rechtsstaatliche Bearbeitung von Personendaten in der Schweiz – Regelungs- und Begründungsstrategien des Datenschutzrechts mit Hinweisen zu den Bereichen Polizei, Staatsschutz, Sozialhilfe und elektronische Informationsverarbeitung, Diss. Univ. Basel, Dike, Zürich /St. Gallen 2017.

GLASS PHILIP, Die Schutzparameter des zivilrechtlichen und des verfassungsrechtlichen Persönlichkeitsrechts, www.datalaw.ch, 29. Mai 2018; engl. Version DOI: 10.5281/zenodo.1436387.

GLASS PHILIP, Singularisierung und Identifizierung, www.datalaw.ch, 27. Februar 2018; engl. Version DOI: 10.5281/zenodo.1436396.

HARASGAMA REHANA/TAMÒ AURELIA, Smart Metering und Privacy by Design im Big-Data-Zeitalter: Ein Blick in die Schweiz, in: Weber/Thouvenin (Hrsg.), Big Data und Datenschutz – Gegenseitige Herausforderungen, Schulthess, Zürich/Basel/Genf 2014, p. 117–150.

HARTZOG WOODROW, Privacy's Blueprint – The Battle to Control the Design of New Technologies, Harvard University Press 2018.

HILDEBRANDT MIREILLE, Algorithmic Regulation and the Rule of Law, Phil. Trans. R. Soc. A 376: 2017035.

HILDEBRANDT MIREILLE, Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology, Edward Elgar, Cheltenham UK/Northampton MA 2015.

HOFFMAN-RIEM WOLFGANG, Innovation und Recht – Recht und Innovation, Recht im Ensemble seiner Kontexte, Mohr Siebeck, Tübingen 2016.

HOFFMANN-RIEM WOLFGANG, Rechtliche Rahmenbedingungen für und regulative Herausforderungen durch Big Data, in: Hoffmann-Riem (Hrsg.), Big Data – regulative Herausforderungen, Baden-Baden 2018, S. 11–80.

HOFFMANN-RIEM WOLFGANG, Verhaltenssteuerung durch Algorithmen – Eine Herausforderung für das Recht, Archiv des öffentlichen Rechts (AöR) 142 1/2017, p. 1–42.

LESSIG LAWRENCE, Code: And Other Laws of Cyberspace, Version 2.0, Basic Books, New York 2006.

NISSENBAUM HELEN, Privacy in Context – Technology, Policy, and the Integrity of Social Life, Stanford Law Books, Stanford California 2010.

SCHAAR PETER, Privacy by design, IDIS (2010) 3:267. DOI: 10.1007/s12394-010-0055-x.

TAMÒ-LARRIEUX AURELIA, Designing for Privacy and its Legal Framework – Data Protection By Design and Default for the Internet of Things, Springer Nature, Cham 2018.

THOUVENIN FLORENT, Wem gehören meine Daten? Zu Sinn und Nutzen einer Erweiterung des Eigentumsbegriffs, Schweizerische Juristen-Zeitung (SJZ) 113/2017, p. 21–32.

TSCHENTSCHER AXEL, Prozedurale Theorien der Gerechtigkeit – Rationales Entscheiden, Diskursethik und prozedurales Recht, Nomos, Baden-Baden 2000.

VAN DEN HOVEN JEROEN/VERMAAS PIETER E./VAN DE POEL IBO, Design for Values: An Introduction, in: Van den Hoven/Vermaas/Van De Poel (Eds.), Handbook of Ethics, Values, and Technological Design – Sources, Theory, Values and Application Domain, Springer, Dordrecht 2015.

VAN DER VELDEN MAJA/MÖRTBERG CHRISTINA, Participatory Design and Design for Values, in: Van den Hoven/Vermaas/Van De Poel (Eds.), Handbook of Ethics, Values, and Technological Design – Sources, Theory, Values and Application Domain, Springer, Dordrecht 2015.

WILDHABER BRUNO, Informationssicherheit – rechtliche Grundlagen und Anforderungen an die Praxis, Diss. Univ. Zürich, Schulthess, Zürich 1994.