DOI: 10.1007/s10272-019-0829-9

Max von Grafenstein, Alina Wernick and Christopher Olk*

Data Governance: Enhancing Innovation and Protecting Against Its Risks

Big Data is expected to unleash data-driven innovation,[1] which is supposed to better address and solve challenges in our society.[2] As a so-called non-rival good, the sharing and re-using of data by one actor does not diminish its value for other actors and can create significant spillover effects.[3] However, data is still often stored in data silos. Releasing data from silos and sharing it may therefore enhance social and economic welfare. Of course, digitisation and data-driven innovation also entail risks. For decades, experts have discussed, depending on the discipline, the risks that result from the accumulation of informational power: risks for individuals, for example, for their privacy, autonomy or freedom and equality, but also for the society as a whole, for example, for its democratic constitution, solidarity principle or free markets.[4]

Data governance in Smart Cities

This basic conflict can be illustrated using the example of Smart Cities. On the one hand, data-driven innovations are designed to help improve urban living conditions, such as urban traffic management: with more precise information, we hope to gain more knowledge about how people move in a city in order to reduce traffic chaos and emissions.[5] On the other hand, numerous risks are discussed under the heading 'Smart Cities'. These risks range from the concern that urban supply will depend on individual IT service providers (so-called 'lock-in effects')[6] to the citizens' fear of a digital surveillance state.[7]

Such a basic conflict raises the question of how to enhance data-driven innovation while at the same time protecting against its potential perils.[8] This is a complex question because it encompasses many different, often conflicting interests, especially in a city that has a multiplicity of actors with different roles. Citizens may have different concerns as, for instance, voters, consumers, employees, drivers, cyclists and so on.[9] Similarly, depending on the context, the city administration may perform the various functions of a political decision-maker, state enforcement body, data donor and so on.[10] In a Smart City, all these interests must be reconciled to not only profit from the benefits of data-driven innovation, but also effectively protect against its risks. This is the goal of successful data governance.

Data governance and legal regulation

Focusing on the governance of data means taking a broader view than that of just legal regulation. While the approach of legal regulation concentrates on the state's use of legal instruments to achieve a certain conduct of actors, the governance perspective focuses on the coordination efforts by these ac-

* This contribution is based on the research project "Data Governance" at the Alexander von Humboldt Institute for Internet and Society (HIIG) and corresponds to the introduction of the HIIG Discussion Paper "Data Governance: Towards a Conceptual Framework", forthcoming, available at http://www.hiig.de/paper-Data-Governance-Towards-Conceptual-Framework/.

1 See V. Mayer-Schönberger, K. Cukier: Big Data: A Revolution that Will Transform How We Live, Work, and Think, New York 2013, Houghton Mifflin Harcourt Publishing Company, p. 30.

2 See M. Hilbert: Big Data for Development: A Review of Promises and Challenges, in: Development Policy Review, Vol. 34, No. 1, 2016, pp. 135-174, p. 142.

3 OECD: Data-Driven Innovation: Big Data for Growth and Well-Being, Paris 2015, OECD Publishing, p. 179.

4 See M. von Grafenstein, J. Hölzel, F. Irgmeier, J. Pohle: Nudging: Regulierung durch Big Data und Verhaltenswissenschaften, Berlin 2018, ABIDA (Assessing Big Data), p. 46.

Max von Grafenstein, Alexander von Humboldt Institute for Internet and Society, Berlin; Einstein Center Digital Future, Berlin, Germany.

Alina Wernick, Alexander von Humboldt Institute for Internet and Society, Berlin; Ludwig Maximilian University, Munich, Germany.

Christopher Olk, Alexander von Humboldt Institute for Internet and Society, Berlin; Technische Universität, Berlin, Germany.

5 See A. Habenstein, S. D'Onofrio, E. Portmann, M. Stürmer, T. Myrach: Open Smart City: Good Governance für smarte Städte, in: A. Meier, E. Portmann (eds.): Smart City: Strategie, Governance und Projekte, Wiesbaden 2016, Springer Vieweg, pp. 47-71, p. 48.

6 Regarding lock-in-effects, see E. Veronelli: Smart cities vs "locked-in" cities, CORDIS EU research results, 12 September 2016, available at https://cordis.europa.eu/news/rcn/135237/en.

7 Regarding smart cities and surveillance, see T. Wadhwa: Smart Cities: Toward the Surveillance Society?, in: D. Araya (ed.): Smart Cities as Democratic Ecologies, New York 2015, Palgrave Macmillan, pp. 125-141.

8 See W. Hoffmann-Riem, S. Fritzsche: Innovationsverantwortung – zur Einleitung, in: M. Eifert, W. Hoffmann-Riem (eds.): Innovation und Recht III – Innovationsverantwortung, Berlin 2009, Duncker & Humblot, p. 16.

9 See for example the smart city project in Toronto: J. Wakefield: The Google city that has angered Toronto, BBC News, 18 May 2019.

10 Regarding biomedical data, see J.L. Contreras: Leviathan in the Commons: Biomedical Data and the State, in: K.J. Strandburg, B.M. Frischmann, M.J. Madison (eds.): Governing Medical Knowledge Commons, Cambridge 2017, Cambridge University Press, pp. 19-45.

tors on an organisational and technical level.[11] The broad focus of the governance perspective can serve as a basis for the regulator to find out if actors are cooperating in a way that already leads to a desired outcome or if regulatory support is needed. This also applies to companies that seek to achieve a certain outcome through private ordering measures.[12] Thus, legislators should regulate the sharing and re-use of data only if the involved actors in a given context are unable to coordinate the data sharing themselves.

Benefits and disandvantages of data sharing from the perspective of companies

From the viewpoint of most actors, however, there are more obstacles than incentives to sharing and re-using data. At least on the European Single Market, private companies have few incentives to disclose data to third parties. While citizens display a so-called 'privacy paradox' behaviour, i.e. individuals value data protection and privacy but continue to disclose their data, companies are much more hesitant.[13] By sharing data, they fear not only violating data protection laws, but also disclosing information that is actually protected by their intellectual property rights or trade secrets.[14] At the very least, many companies fear that they will suffer a competitive disadvantage as the other companies could use the shared data to better position themselves in the market.[15] Even if it would be possible to overcome these obstacles – e.g. to create infrastructure for legally compliant data sharing without any competitive disadvantage – the necessary efforts to achieve this seem to outweigh the expected benefits.[16]

In addition, the expected benefits of innovation are rather vague compared to the disadvantages mentioned. The reason for this is that the value of data often only becomes apparent and more concrete in the course of the innovation process – i.e. after the data has been shared – when the potential usage of the data becomes clearer.[17] Thus, while the disadvantages before disclosure of the data are more specific, the expected benefits at this point are rather abstract.[18] The fact that actors give a specific disadvantage more weight than an abstract benefit corresponds to well-known decision heuristics and may explain why many companies hesitate to share their data.[19]

Last but not least, even if there are ways to overcome these obstacles, i.e. creating an infrastructure for sharing data legally, reducing transaction costs sufficiently and correctly assessing that there are more benefits than disadvantages, the so-called 'collective action problem' may remain: each actor is reluctant to invest in an infrastructure because each (wrongly) expects that there are already enough other parties to build it.[20]

11 See, regarding the perspective of the legal regulator, A. Voßkuhle: Neue Verwaltungsrechtswissenschaft, in: W. Hoffmann-Riem, E. Schmidt-Aßmann, A. Voßkuhle (eds.): Grundlagen des Verwaltungsrechts – Band I: Methoden – Maßstäbe – Aufgaben – Organisation, 2nd edition, Munich 2012, C.H. Beck, cip. 20; and regarding the governance perspective, J. Hofmann, C. Katzenbach, K. Gollatz: Between coordination and regulation: Finding the governance in Internet governance, in: New Media & Society, Vol. 19, No. 9, 2017, pp. 1406-1423.

12 See, regarding regulation by the state: A. Voßkuhle, op. cit.; and regarding regulation by private companies: J. Black: Decentring regulation: Understanding the role of regulation and self-regulation in a "post-regulatory" world, in: Current legal problems, Vol. 54, No. 1, 2001, pp.103-146; see the term 'private ordering' at Elkin-Koren who defines the term as a situation wherein "the rule-making process regarding the use of information is privatized, and the legal power to define the boundaries of public access to information is delegated to private parties." N. Elkin-Koren: A Public-Regarding Approach to Contracting over Copyrights, in: R. Dreyfuss, H. First, D. Zimmerman (eds): Expanding the Boundaries of Intellectual Property: Innovation Policy for the Knowledge Society, Oxford 2001, Oxford University Press, pp. 191, 192 as cited by S. Dusollier: Sharing Access to Intellectual Property through Private Ordering, in: Chicago-Kent Law Review, Vol. 82, 2007, pp. 1391, 1393, fn. 8; see S. Schwarcz: Private ordering, in: Northwestern University Law Review, Vol. 97, No. 1, 2002, p. 319.

13 Regarding the privacy paradox, see for example G. Müller, C. Flender, M. Peters: Vertrauensinfrastruktur und Privatheit als ökonomische Fragestellung, in: J. Buchmann (ed.): Internet Privacy: Eine multidisziplinäre Bestandsaufnahme, Heidelberg 2012, Springer Vieweg, pp. 143-188, p. 175.

14 See H. Richter, P.R. Slowinski: The Data Sharing Economy: On the Emergence of New Intermediaries, in: IIC-International Review of Intellectual Property and Competition Law, Vol. 50, No. 1, 2019, pp. 4-29, p. 7, fn 15, discussing the risk of liability of breaching data protection law.

15 Regarding coopetition, see D.R. Gnyawali, R. Madhavan, J. He, M. Bengtsson: The competition–cooperation paradox in inter-firm relationships: A conceptual framework, in: Industrial Marketing Management, Vol. 53, 2016, pp. 7-18; sometimes, the data donor also overestimates the value of its data due to an endowment effect, see D. Kahneman, J. Knetsch, R. Thaler: Anomalies: The Endowment Effect, Loss Aversion, and Status Quo Bias, in: Journal of Economic Perspectives, Vol. 5, No. 1, 1991, pp. 193-206.

16 Regarding transaction costs in law in general, see R.H. Coase: The problem of social cost, in: The Journal of Law and Economics, Vol. III, 1960, pp. 1-44. Bounded rationality, such as unwarranted fear of failing to comply with data protection law, may also contribute to the reluctance to share data, see, for example H.A. Simon: Bounded rationality and organizational learning, in: Organization science, Vol. 2, No. 1, 1991, pp. 125-134. Finally, excessive transaction costs may lead to a so-called tragedy of the anti-commons, see M.A. Heller: The Tragedy of the Anticommons: Property in the transition from Marx to markets, in: Harvard Law Review, Vol. 111, No. 3, 1998, pp. 621-688; and regarding patents, M.A. Heller, R.S. Eisenberg: Can patents deter innovation? The anticommons in biomedical research, in: Science, Vol. 280, No. 5364, 1998, pp. 698-701.

17 See similar reasons mentioned by V. Kathuria: Greed for data and exclusionary conduct in data-driven markets, in: Computer law & security review, Vol. 35, No. 1, 2019, pp. 89-102.

18 See M. von Grafenstein: The Principle of Purpose Limitation in Data Protection Laws, Baden-Baden 2018, Nomos, p. 77.

19 Regarding decision heuristics, see S. Mousavi, G. Gigerenzer: Risk, uncertainty, and heuristics, in: Journal of Business Research, Vol. 67, No. 8, 2014, pp. 1671-1678.

20 See M. Olson: Collective action, in: S.N. Durlauf, L.E. Blume: The New Palgrave Dictionary of Economics, 2nd edition, London 2008, Palgrave Macmillan, pp. 876-880.

Regulatory attempts to clarify data ownership, access and usage rights

To solve these problems, various legislative measures have been and are still being discussed. So far, there are few existing regulations that prescribe the sharing of data. Art. 20 of the EU General Data Protection Regulation (GDPR) on data portability may be considered such a law. According to this Article, data subjects may require the controller, to whom they have provided personal data, to transfer that data to another controller of their choice. The aim of this provision is to enable data subjects to switch more easily to another service provider.[21] Companies can thus use this rule – even if it functions only in an indirect way via data subjects – to gain access to certain data from another company.[22] Additional initiatives, however, have been limited.

In Germany, there was a relatively long-lasting discussion about data property rights.[23] Such rights should solve the (so far open) question of to whom the data should be legally assigned, i.e. to whom the data belongs regardless of a de facto power over data.[24] 'De facto power over data' means that an actor is able to exclude others from using its own data just by means of factual (not legal) powers. A legal allocation of data through a data property right could counteract such a de facto power. However, such a solution via a data property right carries the risk that it only further (legally) underpins an already existing de facto power. The reason for this concern is that the value of data depends, again, largely on its intended use, which can change constantly over time depending on the context and perspective of the actors. This kind of context-dependent transitoriness of the value of data let it seem more appropriate to focus, instead of on a one-time allocation of data to one actor by means of an exclusion right against all other actors, on more context-dependent access and usage rights.[25]

21 Regarding the rationale of Art. 20 GDPR, see for example T. Jülicher, C. Röttgen, M. von Schönfeld: Das Recht auf Datenübertragbarkeit: Ein datenschutzrechtliches Novum, in: Zeitschrift für Datenschutz, Vol. 6, No. 8, 2016, pp. 358-362.

22 R.H. Weber: Improvement of Data Economy Through Compulsory Licences?, in: S. Lohsse, R. Schulze, D. Staudenmayer: Trading Data in the Digital Economy: Legal Concepts and Tools, Baden-Baden 2017, Nomos, p. 151.

23 See, for example, M. Grützmacher: Dateneigentum – ein Flickenteppich, in: Computer und Recht, Vol. 32, No. 8, 2016, pp. 485-495; N. Härting: „Dateneigentum" – Schutz durch Immaterialgüterrecht?, in: Computer und Recht, Vol. 32, No. 10, 2016, pp. 646-649; N. Jentzsch: Dateneigentum – Eine gute Idee für die Datenökonomie, Berlin 2018, Think Tank für die Gesellschaft im technologischen Wandel, available at https://www.stiftung-nv.de/sites/default/files/nicola_jentzsch_dateneigentum.pdf.

24 See H. Richter, R.M. Hilty: Die Hydra des Dateneigentums – eine methodische Betrachtung, Discussion Paper No. 12, Munich 2018, Max-Planck-Institut für Innovation und Wettbewerb, in: Stiftung Datenschutz (ed.): Dateneigentum und Datenhandel, Schriftenreihe DatenDebatten, Vol. 3, Berlin 2018, Erich Schmidt Verlag, pp. 241-259.

25 Regarding this last aspect, see again, ibid., p. 15.

Interestingly, the position paper that the Social Democratic Party of Germany (SPD) has recently brought into discussion under the title "Daten-für-Alle-Gesetz" goes in this direction of context-dependent access and usage rights.[26] In this paper, the innovative power of competitors is seen as an important corrective against the market dominance of single companies.[27] However, this corrective loses its power the more innovation depends on the processing of data and if only individual companies have access to that data. In order to increase competitors' data-driven innovative capacities, they must hence be equally able to access sufficient (high-quality) data. The paper therefore proposes three parameters for a legal regulation of data:

1. 'Non-personal data' should, in principle, be usable as a common good;
2. 'Data monopolies' should be broken up by a data sharing obligation; and
3. General incentives to share data should be created.

As an overarching objective, the position paper underlines the fact that all measures must respect data protection and other protected goods as well as suggests that the involvement of trusted third parties in the data sharing may be a suitable means of ensuring compliance with these requirements. However, the paper leaves open the specific question of how such trusted third parties, i.e. their data governance structures, should look exactly.

Data governance for controlling data usage: Privacy by design in Smart Cities

In fact, whether data sharing is compatible with legal requirements such as data protection law depends largely on the design of the implemented data governance structure – and in this respect, a trusted third party solution can be very promising. The reason for this can be seen in the example of the research project 'Data Protection by Design in Smart Cities' conducted at the Alexander von Humboldt Institute for Internet and Society (HHIG).[28] This project is based on a hypothetical Smart City scenario: Public WiFi is available for free throughout Berlin; closed-circuit television (CCTV) cameras measure – 'anonymously' – how many vehicles and people move from A to B, when and how fast; and parking space sensors report in real time where and which parking spaces are available. All of this data should be freely accessible so that researchers,

26 See A. Nahles: Digitaler Fortschritt durch ein Daten-für-Alle-Gesetz, Positionspapier der Parteivorsitzenden der Sozialdemokratischen Partei Deutschlands, Berlin 2019, available at https://www.spd.de/aktuelles/daten-fuer-alle-gesetz/.

27 See T. Ramge, V. Mayer-Schönberger: Das Digital: Markt, Wertschöpfung und Gerechtigkeit im Datenkapitalismus, 3rd edition. Berlin 2017, Ullstein.

28 Information on the project 'Privacy by design in smart cities' available at https://www.hiig.de/en/project/privacy-by-design-in-smart-cities/.

startups, larger companies, journalists or public authorities could use this data for innovative services such as better urban traffic management. A key element of this research project is the so-called legal-scientific Data Protection Impact Assessment (DPIA), which was used to assess the risks caused by the hypothetical Smart City application.[29] One of the most surprising results of the DPIA was that it in fact was impossible to completely anonymise the personal data and maintain its value for later use. There was always a data usage scenario in which the collected data could be related to an individual.

For example: Even if the CCTV camera images are pixelated in such a way that it is no longer possible to tell whether a truck or a cyclist is moving at 30 km/h on a certain street, it is still possible that the recorded action may be related to the driver of that object by the additional knowledge of a third party. For instance, if records show that a moving object drove over a traffic light after it has turned red, a witness on site who may not have noticed that action could have possibly seen the moving object, such as a car with its specific license plate. If it was the only object at that location at that time, the recorded 'anonymised' action could be related to the driver of the car via the witness (mediated via the vehicle license plate register and the vehicle owner listed therein). The only way to prevent making such a reference would be to pixelate the recording in such a way that even the action could no longer be recognised. This reduces the informational content of the data to zero, however, rendering it useless. Therefore, if one wants to preserve the information and still prevent it from being related to individuals, one must ensure that the data is only used in a way that does not de facto relate to an individual.

The need for controlling the data usage raises, in turn, the question of who exactly controls it with what kind of mechanisms, i.e. what data governance applies. With regards to data protection, for example, a clear distinction is made in whether the data is stored centrally by a government agency and kept for future purposes or whether the data may in principle only be used by the respective service provider for the purpose of the service (e.g. the CCTV camera data only for counting vehicles, the WiFi data only for providing public WiFi access and the parking space sensor data only for displaying free parking spaces); the data may solely be combined, in this second case, in exceptional cases and used for other purposes only if a trusted third party gives its consent under specific usage conditions. However, even then the question arises as to who actually makes the decisions in such a trusted third party: Data protection experts? With the participation of the actors who actually want to share and use the data? Does this happen under the control of a data protection authority? And might the data subjects be involved? The answers to such questions determine, in essence, whether or not the data processing is compatible with data protection laws.

The challenge of complexity: Coordination on legal, organisational and technical levels

The question of who actually oversees data use through which type of mechanisms equally determines whether the reconciliation of potential conflicts of interest works. The normative expectations of the various actors must be reconciled on different governance levels, including the technical and organisational levels. This can be illustrated again by an example in data protection law.

At the normative level of data protection, the legal requirements are usually not only specified by courts and data protection authorities, but also depend on the privacy and risk expectations of the data subjects.[30] Thus, already on the normative level, controllers of personal data must meet the expectations of a variety of actors. In addition, the principles of 'data protection and security by design' according to Art. 25 and 32 GDPR (also Art. 24 GDPR) require that the controller and, partly the processor as well, incorporate the legal requirements into the technical and organisational design of its data processing. In business practice, however, legal responsibility and technical capabilities often diverge. The main responsibility lies with the actor who determines the purposes of the data processing, i.e. the controller (see Art. 4 No. 7 and Art. 5 sect. 2 GDPR). To achieve its processing purposes, however, the controller usually has to rely on third parties that either provide the IT (as so-called manufacturers) or process the data on behalf of the controller based on their own IT (as processors, for example, providing 'software as a service'). This means that the entities who carry the legal responsibility and who are technically able to apply the legal requirements are not the same. The various actors must therefore cooperate – with the help of the other actors, i.e. the processors and/or manufacturers – in their different roles to ensure that the controller meets the legal requirements.

In conclusion, if a trusted third party controls the use of data, it must ensure that coordination can take place at the normative (legal), organisational and technical levels by filling its deci-

29 Alexander von Humboldt Institute for Internet and Society: Data Protection by Design in Smart Cities, HIIG Discussion Paper, forthcoming, available at https://www.hiig.de/paper-Data-Protection-by-Design-in-Smart-Cities.

30 For more on 'reasonable expectations', see Article 29 Data Protection Working Party: Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, 2014, p. 51; regarding risk expectations, see Art. 35 (9) GDPR: "Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations."

sion-making body with the necessary actors and implementing the appropriate decision-making processes.

This example addresses only the challenges of coping with the complexity of data protection law. Due to its broad scope, particularly of the GDPR, the application of data protection law should be included in data governance.[31] This means that successful data governance should always maintain structures that enable various actors to comply with data protection law.[32] Ultimately, however, successful data governance means that other protected interests, such as trade secrets, intellectual property rights, and even state organisational law, must also be respected for making data sharing work. This diversity of actors, roles and interests makes the question of successful data governance extremely complex.

Findings on interorganisational data governance models

Against this background and building upon the results of the research project 'Data Protection by Design in Smart Cities', the HIIG research group 'Data Governance' initiated an additional project to assess which data governance models actually exist in different contexts. It focused on developing appropriate concepts to grasp the relevant aspects of interorganisational data governance. To understand current data-sharing practices and the incentives or disincentives of data holders to share data, the group reviewed the legal and economic literature focusing on the governance of intellectual property,[33] the economics of privacy,[34] competition in data-driven industries,[35] open (and user) innovation[36] and coopetition.[37] Relevant concepts from these bodies of literature have been identified and ordered based on their relation to each other and to the phenomena encountered in tentative studies of specific industries. On the conceptual level, the research focused on open models for managing intellectual property.[38] On the empirical level, researchers studied particular literature on the advertising, automotive, eHealth and smart city sectors and interviewed experts in these fields in order to map the possible constellations of actors, conflicts of interest and sharing practices in different legal, economic and technological contexts. The group alternates between the conceptual work and these industry studies to ensure that each was grounded in and tested against the other.

The group has identified a number of typical data governance models in its research to date. However, the literature review and preliminary examination of existing data governance models has resulted in three particular findings:

1. The existing terminology for interorganisational data governance models is very heterogeneous and inconsistent both in literature and in practice. It also fails to reflect the core features that distinguish the diverse data governance solutions from each other.

2. Data governance models with similar features are present in different industries. These data governance models may be described using different terms or there may not be any terms to describe even one particular constellation.

3. Based on their core features, data governance models may be grouped into a number of different types.

Therefore, the HIIG research project proposes in its discussion paper a conceptual framework for data governance that may provide a foundation for subsequent research on data governance.[39]

31 See N. Purtova: The law of everything. Broad concept of personal data and future of EU data protection law, in: Law, Innovation and Technology, Vol. 10, No. 1, 2018, pp. 40-81.

32 See also W. Kerber: Digital markets, data, and privacy: competition law, consumer law and data protection, in: Journal of Intellectual Property Law & Practice, Vol. 11, No. 11, 2016, pp. 856-866.

33 M.A. Heller: The Tragedy of the Anticommons: Property in the transition from Marx to markets, in: Harvard Law Review, Vol. 111, No. 3, 1998, pp. 621-688; M.A. Heller, R.S. Eisenberg: Can patents deter innovation? The anticommons in biomedical research, in: Science, Vol. 280, No. 5364, 1998, pp. 698-701; R.P. Merges: Contracting into liability rules: Intellectual property rights and collective rights organizations, in: California Law Review, Vol. 84, No. 5, 1996, pp. 1293-1393; M.J. Barnett: The anti-commons revisited, in: Harvard Journal of Law & Technology, Vol. 29, No. 1, 2015, pp. 127-203.

34 A. Acquisti, C. Taylor, L. Wagman: The economics of privacy, in: Journal of Economic Literature, Vol. 54, No. 2, 2016, pp. 442-92.

35 M.E. Stucke, A.P. Grunes: Big data and competition policy, Oxford 2016, Oxford University Press; N. Srnicek: Platform Capitalism, London 2017, Polity; V. Kathuria: Greed for data and exclusionary conduct in data-driven markets, in: Computer law & security review, Vol. 35, No. 1, 2019, pp. 89-102.

36 H.W. Chesbrough: Open innovation: The new imperative for creating and profiting from technology, Boston 2006, Harvard Business School Press; E. von Hippel: Democratizing innovation: The evolving phenomenon of user innovation, in: Journal für Betriebswirtschaft, Vol. 55, No. 1, 2005, pp. 63-78; E. von Hippel, G. von Krogh: Open source software and the "private-collective" innovation model: Issues for organization science, in: Organization Science, Vol. 14, No. 2, 2003, pp. 209-223.

37 R.B. Bouncken, J. Gast, S. Kraus, M. Bogers: Coopetition: a systematic review, synthesis, and future research directions, in: Review of Managerial Science, Vol. 9, No. 3, 2015, pp. 577-601.

38 See, for example, G. van Overwalle, E. van Zimmeren, B. Verbeure, G. Matthijs: Models for facilitating access to patents on genetic inventions, in: Nature Reviews Genetics, Vol. 7, No. 2, 2006, pp. 143-148; M. Mattioli: The data-pooling problem, in: Berkeley Technology Law Journal, Vol. 32, No. 1, 2017, pp. 179-236; B. Lundqvist: Competition and data pools, in: Journal of European Consumer and Market Law, Vol. 7, No. 4, 2018, pp. 146-154; M. Finck: Blockchains and the GDPR, in: European Data Protection Law Review, Vol. 4, 2018, pp. 17-35; H. Richter, P.R. Slowinski: The Data Sharing Economy: On the Emergence of New Intermediaries, in: IIC-International Review of Intellectual Property and Competition Law, Vol. 50, No. 1, 2019, pp. 4-29.

39 See the proposed terminology and a first categorisation of interorganisational data governance models in Alexander von Humboldt Institute for Internet and Society: Data Governance: Towards a Conceptual Framework, HIIG Discussion Paper, forthcoming, available at http://www.hiig.de/paper-Data-Governance-Towards-Conceptual-Framework/.