Preliminarily Exploring the Possibility Toward a Holistic Legal Regime for Data Protection

Yuyun Ma(✉)

School of Law, The University of Warwick, Coventry, UK
mayuyun022@gmail.com

Abstract. Many jurisdictions have implemented data protective legislations. However, these rules of law accentuate personal data protection and it seems that the safeguard of other valuable data is neglected. Premised on the assumption that other data should be under the equal supervision like personal data, this essay deploys a holistic legal approach to briefly construct a data protective regime that incorporates other traditionally protected data including IP-protected data and confidential data in the specific data legislation for policymakers to regulate data comprehensively and effectively However, is this new regime practically feasible? The feasibility analysis demonstrates that the data within the protection of intellectual property (IP) law and confidential law are constrained to a small amount and the extant legislations have already been adequate to safeguard these data. The sufficiency analysis shows that the new regime is inadequate to safeguard various data and many data are out of its regulation. This essay firstly presents a simple holistic data protective regime that illustrates from the scope, process and enforcement regime aspects. The feasibility analysis is followed from necessity and sufficiency perspectives.

Keywords: Data protection · Holistic Legal Regime · Holistic Approach · Possibility

1 Introduction

Ongoing digitization and digitalization are making data grow at an unprecedently pace and increasingly impact people's daily life. Digitization refers to 'the conversion of information from analog to digital formats', and digitalization means 'the adoption of digitized data and tools' [1]. Data's economic value has been uncovered and it has been referred to be the new oil of the twenty-first century [2]. However, data is a double-edged sword. It also gives rise to the possibility of misuse and raises legal issues, which poses high burden on supervisors for data protection. In response to this problem, legislators in some jurisdictions have promulgated legal rules to protect personal data. The emblematic example is European General Data Protection Regulation (GDPR), which initiated a flurry of global legislative protection on privacy [3].

Z. Zhan et al. (Eds.): SEAA 2022, ASSEHR 675, pp. 1507–1513, 2023.
https://doi.org/10.2991/978-2-494069-05-3_181

However, the legislative practice exclusively emphasizes personal data protection. Personal data protection is only one aspect of the data protection. Other data also possess economic and social value and should be equally protected for their value creation. Some scholars have conducted research on protection of non-personal data. Tommaso Fia's (2021) contribution on the management of non-personal data through the commons [4]. Open data policies are also encouraged and supported worldwide and both academically and practically for enhancing government data accessibility and reuse, and for capturing the full social and economic value the data brings.

Therefore, it is possible that the current data protection is incomplete and inadequate. The legislative practice and scholarship highlight personal data protection and government data sharing via open data policies but neglect other non-personal valuable data protection such as IP data. This essay thus plans to deploy a holistic legal approach to briefly construct a data protective regime to regulate data comprehensively and effectively.

2 A Possible Holistic Data Protective Regime

2.1 A Holistic Legal Approach

The holistic legal research is not limited to the personal data. It involves various data into legal protection, including non-personal data. This is due to that an isolated focus on one particular data is likely to result in the gaps of data protection. Moreover, each field of law pursues a certain objective and rationale [5]. According to coherentism [6], namely applying the extant laws to regulate data, different fields of law should be considered as different data is governed by different law and even one kind of data is likely to be determined by various fields of law. Applying these sets of rules to a certain legal regime in data protection in an aggregate way guarantees that various objectives and rationales in different fields of law are or can be taken into consideration. Thus, a foundation is created for harmonizing divergent concerns [7].

2.2 The Traditionally Protected Data

Many data have become the subjects in a certain rule of law and thus these data fall into the protection of these legislations. These legislations include intellectual property (IP) law, personal privacy law, trade secret law and national secret law.

In terms of IP law, the digitization and digitalization generate a huge amount of IP-registerable or IP-registered data. For example, the interoperability information originating from the reverse engineering or decomplication is likely to be protected by patent [8]. Another example is the symbolic music data such as scores, MIDI note lists, and note onset sequences [9]. According to Cronin, the virtual scores that contains the original musical expression are regarded as copyrightable musical works [10]. These data are protected by IP law. Confidential data, including privacy, trade secret, and national secret are traditionally protected in English law. The purpose of privacy protection is to endow individuals with a right of 'respect for their private and family life' [11]. It involves information such as 'name, address, telephone numbers, location or video footage' [12]. Moreover, it is theoretically justified that there is overlap between personal privacy protection and personal data safeguard [13]. Trade secrets safeguard not only secret formulas, but also 'the highly confidential information of a non-technical nature, such as lists of names of customers' [14]. National secret concerns 'official secrets and other material' such as 'the internal workings of the state and its agencies' [15]. To sum up, different data have fallen within the jurisdictional remits of these traditional legislations.

2.3 The Possibility that Other Data in Addition to Personal Data Should Be Specifically Safeguarded

The content mentioned above shows that many data have been traditionally supervised, involving personal privacy. Nonetheless, the extant legislations promulgated personal data legislation particularly for personal data protection but there is no legislation specifically for IP-protected data or trade secret-protected data. It gives rise to the curiosity that whether it is necessary to establish a specific legislation or incorporate other data supervision into current data protection regimes such as GDPR.

2.4 A Simple Framework Toward a Holistic Data Protective Regime

A simple holistic data protective regime is thus constructed. The possible data supervisory regime uses a holistic approach for data regulation and protection. This is because jurisdictions across the globe safeguard sensitive information and intellectual property, making these forms of data regulation and protection simple, widespread, and cost-effective. This part will demonstrate a simple framework toward a new regime from the scope, process and enforcement aspects. This framework is based on the extant data protection legislations like GDPR and briefly proposes the possible improvement and advancement.

2.4.1 Scope

2.4.1.1 Scope with Regard to the Data Type

This new regime incorporates IP data, trade secret data, and national secret data in data protection and it gives these data equal attention. This completely deviates from the extant legislations that merely and highly stress the personal data protection such as GDPR. Moreover, the IP law, trade secret law and national secret law merely provide

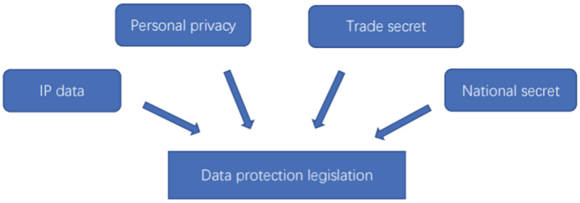

Fig. 1. Scope with regard to the data type

general legislative protection for these data. These general legal regimes are different from the specific legislative protection that customizes for personal data and provides detailed and strict rules. Incorporating IP etc. data takes the heterogeneities of these data into account and provides targeted protection for these data (Fig. 1).

2.4.1.2 Scope with Regard to the Data Subject, Data Controller and Data Processor

The extant legislations in data protection highlight personal data. Take the GDPR as an example. It applies to any processing of personal data and the personal data refers to all the information that is in relation to an identified or identifiable individual. And the controller is deemed to be 'a natural or legal person, public authority, agency or other body that, alone or jointly with others, determines the purposes and means of the processing of personal data'. The processor is defined as 'a natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller' [16]. Although it is interpreted in a broad manner for guaranteeing a high level of protection, its data subject constrains to the individual. As other types of data are added, this study expands data subjects to the legal person, public authority, agency or other bodies that, alone or jointly with others. There is no adjustment to controller and processor.

2.4.2 Process and Enforcement Mechanism

The extant data protection regimes have been relatively mature. They are embodied in applied legal institutions and thus 'automatically benefit from the processes and mechanisms in relation to enforce law and provide remedy for breaches' [17]. Even if the new elements are involved, the extant regimes still shoulder a certain degree of function. What is the difference is that more rules of law are included and the process and enforcement are more complex. For example, personal data protection merely refers to the private law. In comparison, national secret data protection falls within the jurisdiction of administrative law. Furthermore, involving private interests and public interests in a legal regime leads to that the balance between them should be struck, which complicates the situation (Fig. 2).

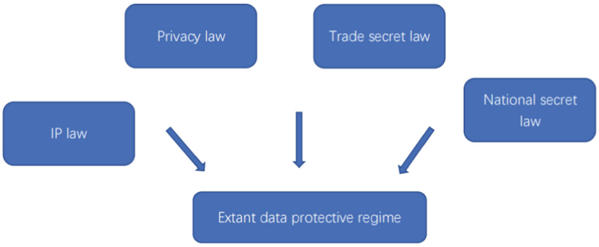

Fig. 2. Scope regarding process and enforcement mechanism

3 The Feasibility of the Holistic Data Protective Regime

3.1 IP-Protected Data and Confidential Data

Is IP law-protected or confidential data necessitated with a holistic data law? It should be said that both IP law and confidential law have set a high access threshold. Take IP as an example, IP is an intangible property right that aims to protect innovations and creations [18]. In general, United Kingdom statute provides four main forms of intellectual property, namely patent, copyright, design, and trademark. Patent protects the novel inventions. Copyright should guard the originality. The registered designs should demonstrate the novelty and specialty, whereas the unregistered designs should show its originality and non-commonplace. Trademarks should have the distinguishability [19]. As a result, although the digitization and digitalization have generated many IP-registerable or IP-registered data, in comparison to the huge amount of general data, it is merely a small number. Moreover, the IP legislation has been increasingly perfect both monitoring ex ante and relief and enforcement ex post. Even if publicity is the characteristic of registered IP property, and many registered IP properties are publicly available, the IP right is still protected. IF without permission, IP data could not be economically used or further processed. This is completely deviated from the personal data that economically exploitable, easily available by other subjects such as data controllers but not legally protected. For example, the information of consumer behavior and purchasing habits can be easily gained by data controllers. The controllers analyze when, where, and the product *per se*, which can be used to improve products and services, or explore the potential future profit streams. This may raise concerns that whether the controllers' actions in this example is legal. That is why the personal data protection legislations appears.

This is the case in confidential data. The American Uniform Trade Secret Act (UTSA) defines trade secret as enjoying independent economic value and being put the reasonable efforts of the subject for maintaining its secrecy [20]. Accordingly, the trade secret is held by owner and not publicly available. If not, the owner's interests are violated. As a result, it seems not necessary to add a special data protective law for trade secret data.

3.2 The Sufficiency Analysis

The proposed data protective regime is not comprehensive and inadequate. There are some valuable data that are not taken into account. For example, the technologies leveraged on farms have generated large amount of site-specific and farm-level data, which may be substantially useful at the aggregate level. However, there is no statutory or other legal protections for it [21]. And it is not safeguarded in the new regime.

4 Conclusion

This essay has presented a simple data protective regime based on a holistic legal approach. It is presupposed that various traditionally protected data should be involved in a specific data protective legislation. Then it designs a regime that added other traditionally protected data into extant personal data protective regime. Ultimately, Rationality test is conducted in this regime from the necessity and sufficiency perspectives, concluding that there is other valuable data should be legally protected and there is no need to incorporate traditionally protected data as they have been perfectly safeguarded.

This study is only a preliminary regime design and check. Many points could be delved in in future works. For example, are there any other data except the genres mentioned above that should be protected? Holistic data protection in this study is just a beginning.

References

1. Office of the Chief Economist, 'Data, Digitalization, and Governance'. (2021). The World Bank ECA Economic Update Spring 2021.
2. Chrobak, L. (2018). Proprietary rights in digital data? Normative perspectives and principles of civil law. In M. Bakhoum, et al. (Ed.), *Personal data in competition, consumer protection and intellectual property law: Towards a holistic approach?* Springer (2018). https://doi.org/10.1007/978-3-662-57646-5_10
3. World Bank Group, 'Data for Better Lives'. (2021). World Development Report 2021. Accessed August 17, 2021, https://www.worldbank.org/en/publication/wdr2021
4. Fia, T. (2021). An alternative to data ownership: Managing access to non-personal data through the commons. *Global Jurist, 21*. Accessed May 20, 2022, https://www.degruyter.com/document/doi/10.1515/gj-2020-0034/html
5. Bakhoum, M. (2018). Introducing a holistic approach to personal data. In M. Bakhoum et al. (Ed.), *Personal data in competition, consumer protection and intellectual property law*. Springer. https://doi.org/10.1007/978-3-662-57646-5_1
6. Brownsword, R. (2019). Law disrupted, law re-imagined, law re-invented. *Technology and Regulation.*
7. Mackenrodt, M.-O. (2018). Personal data after the death of the data subject—Exploring possible features of a holistic approach. In M. Bakhoum, B. C. Gallego, M.-O. Mackenrodt, & G. Surblytė-Namavičienė (Eds.), *MSIPCL: Personal data in competition, consumer protection and intellectual property law* (Vol. 28, pp. 273–302). Springer.https://doi.org/10.1007/978-3-662-57646-5_11

8. Ciani, J. (2018). A competition-law-oriented look at the application of data protection and IP law to the internet of things: Towards a wider 'holistic approach. In M. Bakhoum, B. C. Gallego, M.-O. Mackenrodt, & G. Surblytė-Namavičienė (Eds.), *MSIPCL: Personal data in competition, consumer protection and intellectual property law* (Vol. 28, pp. 215–249). Springer.https://doi.org/10.1007/978-3-662-57646-5_9
9. Chuang, Y.-C., & Su, L. (December 2020). Beat and downbeat tracking of symbolic music data using deep recurrent neural networks. In *APSIPA annual summit and conference*, Auckland.
10. Cronin, C. (2004). Virtual music scores, copyright and the promotion of a marginalized technology. *Columbia Journal of Law & the Arts, 28*. Accessed May 20, 2022, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2457442
11. Torremans, P. (2018). *Holyoak and Torremans, Intellectual Property Law* (9th ed.). Oxford University Press.
12. Madir, J. (2018). Smart Contracts: (How) do They Fit under Existing Legal Frameworks? Accessed August 27, 2021, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3301463
13. Tan, D. (2021). Privacy, confidence & data protection in the 21th century. *Singapore Journal of Legal Studies*. Accessed 20 2022
14. Intelsec Systems Ltd. v. Grech Cini [1999] 4 All ER 11
15. Karapapa, S., & McDonagh, L. (2019). *Intellectual property law*. Oxford University Press.
16. Voigt, P., & von dem Bussche, A. (2018). *The EU general data protection regulation (GDPR): A practical guide*. Springer. https://doi.org/10.1007/978-3-319-57959-7
17. Lehdonvirta, V. (2004). European union data protection directive: Adequacy of data protection in Singapore. *Singapore Journal of Legal Studies*. Accessed May 20, 2022, https://www.jstor.org/stable/24869492
18. US Council for International Business. (1985). A New MTN: Priorities for Intellectual Property.
19. Brown, A., et al. (2019). *Contemporary intellectual property: Law and policy* (5th ed.). Oxford University Press.
20. Quinto, D. W., et al. (2022). *Trade secrets: Law and practice.*
21. Ellixson, A., et al. (2019). Legal and economic implications of farm data: Ownership and possible protections. *Drake Journal of Agricultural Law, 24*.