Human Biodata Governance: Addressing the Tension Between Innovation and Protection Through DPIAs

Esra Demir, LLM
PhD Candidate at Erasmus School of Law
Junior Fellow at Jean Monnet Centre of Excellence on Digital Governance
Rotterdam, The Netherlands
demir@law.eur.nl

2023 IEEE Conference on Computational Intelligence in Bioinformatics and Computational Biology (CIBCB) | 979-8-3503-1017-7/23/$31.00 ©2023 IEEE | DOI: 10.1109/CIBCB56990.2023.10264903

***Abstract*— In the area of human biodata governance, one of the most pressing questions is how to address the trade-off between promoting innovation and safeguarding the fundamental rights and freedoms that arise from the development, deployment, and use of AI and data processing. This paper considers that this trade-off poses a dilemma and raises the question of how to achieve governance that promotes biotechnological innovation and research while protecting the fundamental rights and values of individuals and groups. The aim of this paper is to explore regulatory instruments in the EU data protection law that can strike a balance between innovation and protection in the governance of human biodata. To this end, it focuses on meta-regulation as a regulatory technique and examines data protection impact assessment (DPIA) as a method for addressing the tension between innovation and protection. Based on doctrinal legal analysis, it argues that while DPIA is a useful instrument to seek a solution in this dilemma, further reflection and clarification are needed to improve the methods of conducting the impact assessment.**

Keywords*— *biodata, biotechnology, data protection, DPIA, innovation, meta-regulation

I. Introduction

More and more biological material is being collected by individuals to use for various purposes such as treatment, ancestry testing, and research. These collected biomaterials are stored in biobanks in the form of material and data. This storage is indeed crucial for biotechnological innovation and biomedical research as it offers many possible opportunities, especially for predictive, preventive, personalized and participatory medicine. Meanwhile, improper handling of these data may cause many legal and ethical issues related to the development, deployment, and use of AI and data processing in a biological context, which can have profound implications on fundamental rights and freedoms [1].

This paper argues that the trade-off between the promise of biodata and the ethical and legal concerns surrounding them presents a kind of dilemma, referred to here as the innovation and protection dilemma. On the one hand, biological datasets have led to revolutionary changes in many fields through a combination of breakthrough advances in machine learning and artificial intelligence [2]. For example, with the increasing availability of genome-wide expression data and in vitro drug sensitivity data for cancer cell lines, a data-driven approach to identifying molecular markers by establishing robust statistical associations between genes and drugs has become possible [3]. Achieving innovation through a data-driven approach requires processing large amounts of data. As experienced first-hand during the Covid 19 pandemic, viral surveillance and the development of new tests, treatments, and vaccines depend on the collection of and access to large amounts of biodata, including clinical, epidemiological, and public health data that can be collected from laboratories, medical records, wearables, and smartphone apps [4]. On the other hand, there are myriad ethical and legal concerns about possible infringement of fundamental rights and freedoms, including autonomy, transparency, distributive justice, privacy, and the risk of misuse through discrimination and stigma [5]. The improper handling of data, such as through data leaks, which was one of the problems during the pandemic, reinforces these concerns. An example of such handling in the Netherlands, where Department of Public Health employees sold the data of individuals who had been tested for coronavirus under the health service's coronavirus testing system, was widely publicized in the media [6]. Such incidents raise questions about the level of data security and the adequacy of protection of the data collected by the facilities and equipment.

Within this context, data governance is seen as a key concept to address the tension between innovation and protection, as it serves to harness the potential of data-driven innovation while protecting fundamental rights and freedoms [7]. The purpose of this paper is to explore how innovation and protection can be reconciled in the governance of human biodata by scrutinizing the regulatory tools of the EU data protection law. To this end, it focuses on meta-regulation as a regulatory technique and takes a close look at data protection impact assessment (DPIA) as a method for addressing the tension between innovation and protection. In terms of limitations, this paper confines itself to the governance of human biodata. The term 'biodata' refers to all data generated, created, or collected, and stored in relation to life and living organisms. The definition of biodata takes a holistic approach to ensure better and comprehensive protection of data in a biological context. And it carries out a legal analysis within the framework of European data protection law.

To achieve the objective of the paper, this paper comprises four steps. First, it introduces the concept of data protection law and examines the regulatory techniques and tools in the General Data Protection Regulation (GDPR) to underpin the balancing mechanism between the dilemma of innovation and protection. Second, it takes a closer look at the rationale for impact assessment, which is a meta-regulatory instrument in the GDPR. Third, it analyzes DPIAs with regard to scope, timing, risk factors, and process. And finally, it discusses the role of DPIA in addressing the tension in human biodata governance. Based on the doctrinal legal analyses, this paper

argues that while DPIA is a useful tool to address the tension, further reflection and clarification are needed to improve the methods of conducting DPIA.

II. Data Protection Law and Regulatory Techniques and Instruments

A. Data Protection Law in General

The concept of data governance is admittedly vague and broad, as it is difficult to operationalize and provides little guidance on the specific structures, processes, and actors [8,9]. In general, the concept refers to an organized system to effectively manage data. Indeed, it is an essential concept for reconciling conflicting interests in data with different values and risks for different stakeholders [7]. The concept of data governance consists of different layers, namely organizational, technological, and normative. Data protection law is part of the normative layer - consisting of the applicable laws on the processing of data - with strong links to the organizational and technological layers [7].

Data protection law is of fundamental importance as it addresses the question of how to strike a balance between the competing interests of promoting innovation and protecting fundamental rights and freedoms per se [10]. Such law contains a 'rights-based approach' with standards for regulating data processing that both protects the rights of individuals and imposes obligations on data controllers and processors [11,12]. It is framed from the vision of an informed and rational person making appropriate decisions about whether to consent to various forms of collection, use, and disclosure of personal data [13]. This has been seen as a transition from a 'paternalistic' to an 'autonomy-based' regime [14]. Currently, more than 100 countries have adopted data protection legislation [11].

In Europe, data protection is settled as a fundamental right in Article 8 of the Charter of Fundamental Rights of the European Union. Accordingly, everyone has the right to the protection of their personal data [15]. However, this right is not established as an absolute right [16]. Article 52 of the Charter states that the right to data protection may be restricted on the basis of the established proportionality criteria only if this is necessary and genuinely meets the general interest objectives recognized by the Union or the need to protect the rights and freedoms of others [15]. In addition, data protection is also protected by the European Convention on Human Rights under Article 8, the right to respect private and family life [17].

Regarding the regulation and protection of personal data at the EU level, the GDPR is the main legal framework, adopted in 2016 and became operational in 2018 [18,19]. The main objectives of the GDPR are to harmonize data protection laws in Europe, to protect and strengthen the data protection of all EU citizens and to improve the way organizations in the EU handle data protection [14,20]. The GDPR contains rules on the protection of individuals with regard to the processing of personal data and rules on the free flow of personal data [14,18]. The GDPR thus introduces a system that regulates the collection and further processing of personal data in Europe in order to protect fundamental rights while promoting a thriving European data economy [21]. In this context, the GDPR, as a governance framework, strongly encourages entities to handle data carefully and to shape their business strategy in a way that uses data responsibly [22].

To reconcile data protection with other fundamental rights, the GDPR adopts the principle of proportionality. Recital 4 of the GDPR states that the purpose of processing personal data should be to serve humankind and emphasizes that the right to the protection of personal data is not an absolute right. And it further states that the GDPR applies the principle of proportionality in order to balance the interests in view of its function in society and against other fundamental rights [18]. Proportionality is defined as a set of rules establishing the conditions for a restriction of constitutionally protected rights [23]. Although the principle of proportionality is a complex concept, it is widely accepted in the balancing of the various rights and interests at stake [24]. The principle of proportionality consists of two tests, namely necessity and proportionality. Once a legislative measure has been assessed as necessary, it should then be examined whether it is proportionate [25,26]. In data protection law, the principle of proportionality is based on a fact-based approach that requires a case-by-case assessment [25].

In light of the above information, the following subsection examines the regulatory techniques and instruments available in the GDPR to assess proportionality. This subsection serves to provide information on these techniques and instruments in order to achieve such a balance between innovation and protection.

B. Regulatory Techniques and Instruments in the GDPR: Moving from a Rights-Based to a Risk-Based Approach

The traditional categories of regulatory approaches are referred to as legal regulation, self-regulation, and co-regulation. Legal regulation is often understood as regulation by the state in the form of legal rules backed by criminal or civil sanctions, an approach sometimes referred to as command-and-control. In contrast, self-regulation refers to commitments that private actors make on their own behalf without any form of enforcement by the state or other external actors. In addition, co-regulation is a term generally used to refer to various types of cooperation between state and private actors on certain aspects of the regulatory process where there is at least some form of legal enforceability [27]. The GDPR provides for several types of regulatory techniques that fall into these traditional categories of regulatory approaches, namely command and control, design-based regulation, and meta-regulation [21]. Fig. 1 illustrates these various types of techniques enshrined in the GDPR.

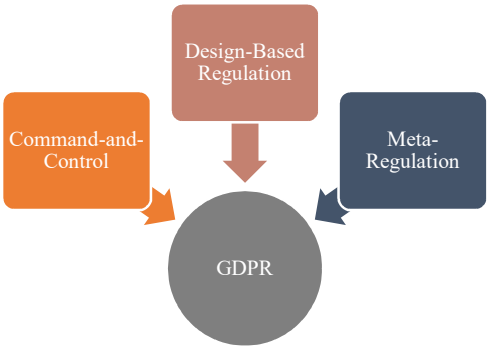

Fig. 1. Regulatory Techniques Anchored in the GDPR

The basic structure and starting point of the GDPR is a traditional command-and-control strategy. Command-and-control is a regulatory model where both the standards and the safeguards are set a priori by the legislator. It is an example of a rights-based approach to data protection, where data

processing either complies or does not comply with basic data protection principles. The legislator ensures compliance by imposing sanctions that act as threats [24]. This technique comprises a set of legal standards or orders that data controllers or processors must comply with. Accordingly, regulators assume that they know what good and bad behavior is embedded in the standards they set, and how best to apply the standards that address such behavior. Nevertheless, the linear processes of standard-setting and associated safeguards have not always succeeded in properly addressing the harm resulting from data processing practices. The command-and-control approach predicts that any breach can be sanctioned and that any sanction or the threat of it has a deterrent effect. However, the effectiveness of deterrence strategies can be misleading. The standards themselves may not lead to satisfactory regulatory outcomes and/or their adequate implementation may be more difficult than anticipated [24]. The shortcomings of this traditional regulatory model have led to a shift towards a risk-based regulatory model.

The shift is reflected in the GDPR in the form of design-based regulation and meta-regulation. While most of the GDPR is rights-based, the only risk-based provisions are contained in Chapter IV (controller and processor). Accordingly, it can be said that a rights-based and a risk-based approach coexist in the GDPR [24]. What these approaches have in common is that both require a proportionality test to accommodate data protection with other fundamental rights and freedoms. It can thus be said that regulation and risk are closely intertwined. In the context of data protection, it is about regulating the risks arising from the processing of personal data [24].

The GDPR requires a risk-based approach, demanding the controller to carry out a contextual risk assessment of fundamental rights in order to determine the appropriate level of rigor of the technical and organizational measures to be taken to ensure that these risks do not materialize [21]. The risk-based approach to data protection can essentially be seen as the implementation of meta-regulation - a subset of co-regulatory strategies - at the level of data protection, using risk as a regulatory tool [24,27]. Meta-regulation consists of three dimensions, namely responsibility, standard setting, and implementation of safeguards. This means that regulators become internally and externally accountable bodies, committed to both the purpose of the organization and broader societal goals, and comply with their own initiative. Having been made accountable, regulators can be given some of their responsibilities, namely setting standards and operationalizing safeguards [24]. One of the main forms of meta-regulation using risk as a regulatory tool under the GDPR is conducting an impact assessment.

The following section will provide information on the rationale of impact assessments.

III. Rationale of Impact Assessments

Traditionally, impact assessments have been considered a self-regulatory tool. However, their status has changed with the introduction of the requirement to conduct impact assessments in data protection law. As it is a requirement created by state legislation and enforced by fines, with little discretion left to regulators, it has been said to resemble the category of legal regulation [27]. Impact assessments, however, differ from traditional legal regulation; they are a combination of rules imposed by the regulator and measures that regulators themselves must develop and enforce with stakeholder involvement. Impact assessments thus have elements of legal regulation, but the focus is on the regulatory authorities developing their own policies based on risk assessments [27]. In terms of regulatory techniques, it is therefore more accurate to classify impact assessments as a meta-regulatory instrument [24].

Impact assessments have so far been used in many regulatory areas for assessing the impact of risks posed by a specific technology or in a specific context. As an example, technology assessments were designed in the 1960s to examine the impact of technological inventions [28]. Impact assessments can be defined as a method for evaluating the impact of a project, policy, program, service, product, or other initiative on data processing and for taking remedial action, in consultation with stakeholders, to avoid or minimize negative impacts [29]. Impact assessments not only identify, describe, and analyze possible positive or negative, intended or unintended consequences of an initiative under consideration, but also identify, describe, and analyze possible solutions [30]. From this point of view, conducting an impact assessment is more than just a tool, a process that should start as early as possible, when there are still opportunities to influence the outcome of a project [29].

Carrying out an impact assessment is the primary risk management tool laid down in the EU data protection law [31]. According to Article 35 of the GDPR, data controllers are legally obliged to carry out an impact assessment when a data processing operation or a set of similar operations, in particular those using new technologies, is likely to present a high risk to the rights and freedoms of individuals [18,21,28]. This obligation echoes the main objective of the GDPR, that of ensuring a high level of protection of the fundamental rights and freedoms of natural persons on a general basis and in particular their right to the protection of personal data [28]. The main merits of carrying out an impact assessment can be seen as contributing to an informed decision on whether to implement a project and under which conditions and protection of societal concerns [30]. As such, it can be argued that conducting an impact assessment is a promising process for dealing with the tension between innovation and protection through risk assessment.

The following section will analyze DPIAs in terms of scope, timing, risk factors, and content.

IV. Analyzes of DPIAs: Scope, Timing, Risk Factors, and Process

A. Scope and Timing

Impact assessment is a systematic process carried out in accordance with an appropriate methodology and in a timely manner. It involves the analysis of the potential impact of an operation in terms of relevant societal concerns - both individual and collective - appropriate to the nature of the operation [30]. According to Article 35(1), the controller shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data prior to the processing where a type of processing, in particular using new technologies, is likely to result in a high risk to the rights and freedoms of natural persons, taking into account the nature, scope, context, and purposes of the processing [30]. In this sense, DPIA is an instrument which focuses on the types of processing likely to present a high risk to the rights and freedoms of natural persons [18,28].

DPIA is carried out by data controller. Article 4(7) of the GDPR defines a controller as a natural or legal person, public authority, agency, or other body which alone or jointly with others determines the purposes and means of the processing of personal data [18]. As stated in Article 35(2), data controllers, if designated, shall carry out the DPIA following the advice of the Data Protection Officer (DPO) [18]. The advice and decisions taken by the controller should be documented in the DPIA [32]. In addition, the DPO should also monitor the implementation of the DPIA in accordance with Article 39(1)(c) [32]. Besides the controller, the DPIA may also be carried out by the data processor. Article 4(8) of the GDPR defines data processor as a natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller [18]. Where the processing is carried out in whole or in part by a data processor, the data processor should assist the controller in carrying out the DPIA and provide all necessary information in accordance with Article 28(3)(f) of the GDPR [18,32]. Even if the DPIA is carried out by another person, inside or outside the organization, the controller is responsible for ensuring that the DPIA is carried out and remains accountable for this task [18,32,33].

As regards the timing of the assessment, Article 35 of the GDPR requires data controllers to carry out an impact assessment before any type of processing of personal data is likely to present a high risk to the rights and freedoms of the data subject [27]. According to Recital 90, the controller should carry out an impact assessment prior to the processing in order to assess the particular likelihood and seriousness of the risk [18]. As such, conducting a DPIA obliges data controllers to establish internal control and compliance management systems before they start processing personal data. This reflects the GDPR's stronger emphasis on accountability and the role of DPIA as an accountability measure [21]. In this sense, DPIA is an ex-ante regulatory mechanism that serves as an early warning system which aims to detect potential negative consequences of processing activities at an early stage and mitigate the impact of the potential risks [28,31].

B. Risk Factors

In line with the risk-based approach of the GDPR, carrying out a DPIA is not mandatory for every processing operation. A DPIA is only required if the processing is 'likely to result in a high risk to the rights and freedoms of natural persons' [28,33]. While risk is at the core of this assessment, the GDPR does not contain a definition of risk, making the concept of risk in the GDPR difficult to grasp [24,31]. Nevertheless, the GDPR contains some constitutive elements of the concept of risk and a number of risk factors, namely the nature of the processing, new technologies, and the type of the data [31]. Article 35(3) contains an indicative list of risk factors for which an impact assessment must be carried out. Accordingly, the list includes the systematic and large-scale exploitation of personal data based on automated processing; the large-scale processing of special categories of data within the meaning of Articles 9(1) and 10 of the GDPR; and the systematic and large-scale monitoring of a publicly accessible area [18]. This list is not exhaustive and there may therefore be other processing operations that exceed the threshold of 'high risk to the rights and freedoms of natural persons' [33].

In practice, data controllers should conduct a preliminary assessment to determine whether the processing is likely to present a high risk and thus require a DPIA and should continuously assess the risks of their processing activities to determine whether a type of processing is likely to present a high risk to the rights and freedoms of natural persons [28,32]. In 2017, the Article 29 Working Party (WP29) provided guidance on DPIA, endorsed by the European Data Protection Board (EDPB), which sets out a series of nine non-legally binding criteria that should be taken into account when determining whether a data processing operation is likely to present a high risk. This non-exhaustive list includes evaluation or scoring, including profiling and prediction; automated decision-making with legal or similar significant effect; systematic monitoring; sensitive data or data of a highly personal nature; data processed on a large scale; matching or combination of datasets; data relating to vulnerable data subjects; innovative use or application of new technological or organizational solutions; where the processing in itself prevents data subjects from exercising a right or using a service or contract [32]. In accordance with the GDPR Article 35(4), in 2019, European Data Protection Supervisory (EDPS) has also prepared and published a non-exhaustive list of processing activities that are subject to the requirement of a DPIA. The list contains nine criteria, which are similar to the criteria developed by the WP29 [34]. As a result, if the controller ticks two or more of these criteria in the list, it is suggested that a DPIA is carried out. If the controller considers that the risk is not 'high' in the case at hand, even if s/he has ticked two or more of the criteria, s/he is asked to explain and justify why s/he considers that the processing does not in fact pose a 'high risk' [34]. In this context, risk is scalable and granular, meaning that it is less a question of 'yes or no' and more a question of 'how much' risk one is willing to take [31].

C. Process of DPIA

DPIA is a cyclical process and not a one-time exercise [35]. Such a process consists of several sub-processes to describe the risks and assess the legality of the system so that appropriate security measures can be taken to minimize the risks [36]. In this regard, DPIA is as an instrument for describing the processing, assessing its necessity and proportionality, and managing the risks to the rights and freedoms of natural persons arising from the processing of personal data by evaluating those risks and determining the measures to address them [32]. However, the GDPR does not provide a methodology for conducting a DPIA. Therefore, agencies may choose to use any compliant methodology as long as they comply with the provisions of the GDPR [35].

According to Article 35(7), the impact assessment should include at least a systematic description of the envisaged processing operations and the purposes of the processing, including, where relevant, the legitimate interest pursued by the controller; a threshold analysis to determine whether an impact assessment is necessary and proportionate in relation to the purpose of processing operations; an assessment of the risks to the rights and freedoms of data subjects in terms of likelihood and severity; and a final report setting out the measures envisaged to address the risks and demonstrate compliance with the GDPR. Followingly, it must be carried out and constantly updated throughout the life cycle of the data processing operations [18,28,37]. The EDPS recommends a review cycle of two years, with an exceptional review in case of significant changes in the processing operations [35]. Fig. 2 exemplifies the cyclical process of the DPIA.

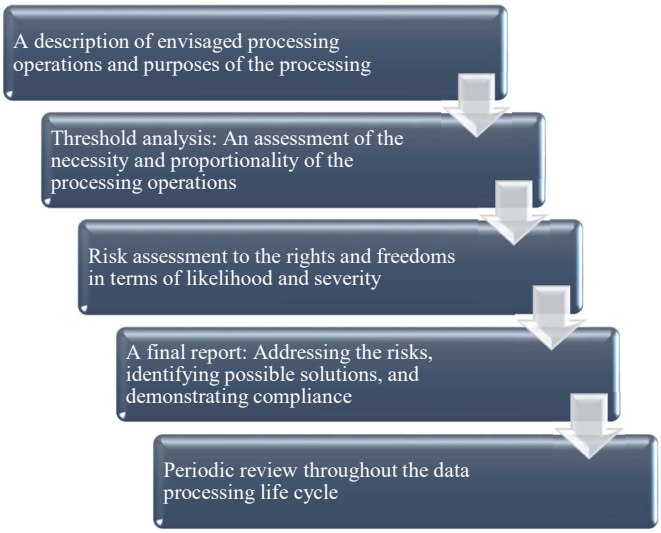

Fig. 2. Process of DPIA

Regarding the final report, Recital 90 states that it must include, in particular, the measures, safeguards, and mechanisms considered to mitigate that risk, ensure the protection of personal data and demonstrate compliance with the GDPR [18]. As set out in Recital 84, consultation with the supervisory authority should take place prior to the processing if a DPIA indicates that the processing presents a high risk that the controller cannot mitigate by appropriate measures in terms of available technology and implementation costs [18]. The GDPR does not explicitly require the publication of DPIA reports. However, the EDPS considers that the publication of DPIA reports, at least in the form of a summary, is a good practice that allows to show the work done to make processing operations compliant and can foster trust among stakeholders and the public in general [35].

The following section will discuss the role of DPIAs in human biodata governance with regard to the tension between innovation and protection.

V. The Role of DPIAs in Human Biodata Governance

Impact assessments are an important area for managing innovation and protecting fundamental rights and freedoms [37]. They can play a key role in addressing the tension between innovation and protection, as the assessment process requires necessity and proportionality analyzes throughout the data processing period, followed by a risk assessment for rights and freedoms in terms of the likelihood and severity of the risk. Within this context, DPIAs are of crucial importance in human biodata governance. On the one hand, the information stored in biological datasets are key components for biotechnological innovations and biomedical research [38]. Human biodata potentially offer opportunities for research and development and innovation, and bring benefits to public health and the health system, e.g., new areas of research, operational and cost-effective health care, improved data-driven strategies for health promotion and prevention, emergency preparedness, improved quality of health services, etc. [39, 40]. On the other hand, biological datasets contain perhaps the most sensitive and valuable information about individuals [41]. This information can be informative for all issues that may directly and profoundly affect the lives of the source of the information, the person's biologically related family members and people living in the same environment [42]. Therefore, the processing of human biodata may have a deep impact on fundamental rights and freedoms. Hence, the dichotomy between innovation and protection in human biodata governance is evident and requires special attention to ensure the balance between innovation and protection. In this context, DPIA as a regulatory tool can be seen as a useful instrument to strike this balance.

The general requirements mentioned above apply to the performance of a DPIA in the context of human biodata. Thus, if the processing of biodata is based on a systematic and comprehensive assessment of personal aspects of natural persons, based on automated processing; processing on large-scale of special categories of data; or processing on large-scale systematic monitoring of a publicly accessible area, the controller is required to conduct a DPIA. Considering that human biodata are vast and diverse and include genetic data, biometric data, and health-related data, which are among the sensitive categories of data highlighted in the GDPR, it can be said that the processing of data will most likely require the performance of a DPIA. However, not all processing of biodata requires a DPIA. For example, if a doctor processes the data of a patient, a DPIA does not need to be carried out as the processing is not on a large scale. On the other hand, a DPIA is required if a hospital wants to set up a new health database containing patients' health data [43].

Although conducting DPIAs is an important instrument for human biodata governance, particularly to address the tension between innovation and protection, there are still some aspects that need to be considered and clarified in order to improve DPIAs and achieve sound data governance. The following paragraphs identify some of these aspects which need to be taken into account when conducting DPIAs for human biodata processing. These aspects are not limited to human biodata but may be relevant to conducting DPIAs in general.

To begin with, performing DPIAs is not a silver bullet for addressing the tension between innovation and protection. DPIAs are a decision-support method that needs to be taken into account throughout the data processing when it is likely to result in a high risk to individuals' rights and freedoms [30]. Furthermore, impact assessments are not a one-size-fits-all solution; they should not be applied in a blanket manner but should be a tailored approach that allows entities to link regulatory objectives with their other business objectives and operations [27]. The key is to choose an appropriate assessment method that provides the best understanding and treatment of the potential impacts of the proposed initiative [30]. Within this direction, like the other risk-based reforms, impact assessments will not succeed in achieving the ultimate goal if the objectives are unclear or controversial and failure is difficult to predict in advance [44].

The quality of an assessment is by no means guaranteed, but it is an ideal to which regulators should aspire [27]. In fact, the quality of impact assessment highly depends on the way controllers use it, on the support they receive from policymakers, and - ultimately - on oversight by data protection authorities and courts [30]. In this respect, impact assessments should not only be used to meet a legal requirement, to be carried out with as little effort as possible, or to legitimize drastic initiatives [30]. Although impact assessments include a compliance check, they should go beyond a simple compliance check and involve stakeholders

in the risks and impacts of data processing [29]. Otherwise, this leads to a number of general criticisms similar to those of the command-and-control approach, including the risk that they become legitimacy exercises rather than risk assessment [27,47,48].

In order to make a realistic assessment, one needs to know where the data is located, how the data moves in the data environment and where the data processing is most vulnerable to risky activities. Once the data processing context is known, risk tolerance can be assessed by deciding which activities are potentially outweighed by their value - and which are unacceptable. In order to assess how to trade off, contextual information is first required [49]. In the assessment, the data controller should take into account how the processing might affect the individuals whose biodata are being processed and what might go wrong with the processing with respect to their fundamental rights and freedoms [33,50]. It is therefore important to proactively provide adequate information on high risks and risk assessment methods that are coherent with the nature, scope, context, and purposes of the processing [45]. Only on the basis of this contextual information can it be judged whether a data activity is a risky data activity and whether the risk is acceptable [49].

The Regulation, however, leaves open how the risks to the rights and freedoms of data subjects should be calculated in practice. Although Recital 76 requires that the risk assessment should be based on the application of an objective assessment method, the GDPR does not specify how the risk analysis should be carried out [31]. Therefore, providing further clarification and a methodological guide with standards may help to achieve the ultimate goal of conducting a DPIA. In this context, the process-oriented approach to conducting an impact assessment should be improved [46]. In this direction, data controllers should reassess the assessment during the other phases, as risks may have changed, or new risks may arise as a result of design and/or implementation decisions [46].

VI. Conclusion

This paper aimed to explore regulatory techniques and tools in EU data protection law that can help to address the tension between innovation and protection in human biodata governance. To this end, it focused on meta-regulation as a regulatory technique and examined DPIA as a method. Accordingly, DPIA is an ex-ante regulatory mechanism adopted in the GDPR with a view to moving to a risk-based approach to data protection. The rationale behind conducting a DPIA is to contribute to an informed decision on whether and under what conditions a project should be implemented and to ensure the protection of societal concerns. In this context, DPIA refers to a cyclical process that identifies not only the potential consequences of an initiative under consideration, but also possible solutions.

The tension between innovation and protection is not a zero-sum game. Innovation and protection can exist simultaneously. DPIAs can help to understand the risks to fundamental rights and freedoms at stake and offer some solutions to mitigate them before data processing. It is therefore a promising tool to address the tension between innovation and protection at an early stage. Based on the doctrinal legal analyses conducted above, this paper concludes that while DPIA is a useful instrument for addressing the tension between innovation and protection, further reflection and clarification are needed to improve the methods of conducting the impact assessment. In particular, this relates to the need for a clear methodology and assessment benchmarks, which have remained unclear in the law. DPIAs are thus not a panacea, but they can contribute to more robust human biodata governance.

Acknowledgment

E. D. thanks Prof. Dr. Lee A. Bygrave, Dr. Shu Li, and anonymous reviewers for their valuable feedback on the earlier version of the text.

References

[1] E. Demir, "Big Biological Data: Need for a Reorientation of the Governance Framework," IEEE Conference on Computational Intelligence in Bioinformatics and Computational Biology (CIBCB), Ottawa, ON, Canada, pp. 1-7, August 2022.

[2] T. Davenport and R. Kalakota, "The potential for artificial intelligence in healthcare," Future Healthcare Journal, vol. 6(2), pp. 94-98, 2019.

[3] S. Lee, S. Çelik, B. A. Logsdon, S. M. Lundberg, T. J. Martins, V. G. Oehler, et al., "A machine learning approach to integrate big data for precision medicine in acute myeloid leukemia," Nature Communications, vol. 9(42), pp. 1-13, 2018.

[4] C. Staunton, E. Hannay, O. John, M. Johnson, R. Kadam, and R. Sampath, "The governance of personal data for COVID-19 response: perspective from the Access to COVID-19 Tools Accelerator," BMJ Global Health, Commentary, pp. 1-3, 2021.

[5] D. J. van Leeuwen, "Ethical and Legal Aspects of Pandemics During COVID-19 and Beyond for the Hepatology Community," CLD Clinical Liver Disease A Multimedia Review Journal (CLD), vol. 18(4) pp. 211-217, July 2021.

[6] NL Times, "Private data leak in GGD Covid system existed for months: report," 28 January 2021 <https://nltimes.nl/2021/01/28/private-data-leak-ggd-covid-system-existed-months-report> accessed 27 March 2023.

[7] M. von Grafenstein, "Reconciling Conflicting Interests in Data through Data Governance: An Analytical Framework (and a Brief Discussion of the Data Governance Act Draft, the AI Regulation Draft, as well as the GDPR)," HIIG Discussion Paper Series 2022-2, pp. 1-44, 2022.

[8] J. Hofmann, C. Katzenbach, and K. Gollatz, "Between coordination and regulation: Finding the governance in Internet governance," New media & society, vol. 19(9), pp. 1406-1423, 2017.

[9] L. A. Bygrave, Internet Governance by Contract. Oxford University Press, 2015.

[10] S. Wachter, "The GDPR and the Internet of Things: A Three-Step Transparency Model," Law, Innovation, and Technology, pp. 266-294, 2018.

[11] World Health Organization, "Ethics and Governance of Artificial Intelligence for Health: WHO Guidance," Geneva: World Health Organisation, Licence: CC BY-NC-SA 3.0 IGO, pp. 1-148, 2021.

[12] S. Wachter and B. Mittelstadt, "A Right to Reasonable Inferences: Re-thinking Data Protection Law in the Age of Big Data and AI," Columbia Business Law Review, vol. 2, pp. 494-620, 2019.

[13] D. J. Solove, "Introduction: Privacy Self-Management and the Consent Dilemma," 126 Harvard Law Review, vol. 126, pp. 1880- 1903, 2013.

[14] L. Marelli and G. Testa, "Scrutinizing the EU General Data Protection Regulation: How will new decentralized governance impact research?" Science, vol. 360(6388), pp. 496-498, May 2018.

[15] European Union, "Charter of Fundamental Rights of the European Union," 2012/C 326/02, 26 October 2012 <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=EN> accessed 17 January 2023.

[16] T. Naef, Data Protection without Data Protectionism - The Right to Protection of Personal Data and Data Transfers in EU Law and International Trade Law, 28 EYIEL Monographs – Studies in European and International Economic Law, Springer, 2023.

[17] Council of Europe, "European Convention on Human Rights," 4 November 1950 <https://www.echr.coe.int/documents/convention_eng.pdf> accessed 02 June 2023.

[18] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.

[19] J. Bell, S. Aidinlis, H. Smith, M. Mourby, H. Gowans, S. E. Wallace, and J. Kaye, "Balancing Data Subjects' Rights and Public Interest Research," European Data Protection Law Review, vol. 5(1), pp. 43-53, 2019.

[20] L. Floridi, "Soft Ethics: Its Application to the General Data Protection Regulation and Its Dual Advantage," Philos. Technos., vol 31, pp. 163-167, 2018.

[21] K. Yeung and L. A. Bygrave, "Demystifying the Modernized European Data Protection Regime: Cross-disciplinary insights from legal and regulatory governance scholarship," Regulation & Governance, vol. 16, pp. 137-155, 2022.

[22] C. J. Hoofnagle, B. van der Sloot, and F. Z. Borgesius, "The European Union General Data Protection Regulation: what it is and what it means," Information & Communications Technology Law, vol. 28(1), pp. 65-98, 2019.

[23] A. L. Bendor and T. Sela, "How proportional is proportionality?" International Journal of Constitutional Law, vol. 13(2), pp. 530-544, 2015.

[24] R. Gellert, The Risk-Based Approach to Data Protection. Oxford University Press, 2020.

[25] European Data Protection Supervisor (EDPS), "EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data," 19 December 2019 <https://edps.europa.eu/sites/default/files/publication/19-12-19_edps_proportionality_guidelines2_en.pdf> accessed 17 November 2022.

[26] Article 29 Data Protection Working Party (Art29 WP), "Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector," 536/14/EN WP 211, Adopted on 27 February 2014, pp. 1-22 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp211_en.pdf> accessed 03 June 2023.

[27] R. Binns, "Data protection impact assessments: a meta-regulatory approach," International Data Privacy Law, vol. 7(1), pp. 22-35, 2017.

[28] E. Kosta, "Article 35. Data protection impact assessment," in Christopher Kuner and others, Eds. The EU General Data Protection Regulation (GDPR): A Commentary, New York, 2020, online edn, Oxford Academic, pp. 665-679 <https://doi.org/10.1093/oso/9780198826491.003.0072> accesse d 5 April 2023.

[29] D. Wright, "The State of the Art in Privacy Impact Assessment," Computer Law & Security Review, vol. 28, pp. 54-61, 2012.

[30] D. Kloza, N. van Dijk, R. Gellert, I. Böröcz, A. Tanas, E. Mantovani, and P Quinn, "Data Protection Impact Assessments in the European Union: complementing the new legal framework towards a more robust protection of individuals," d.pia.lab Policy Brief No. 1/2017, pp. 1-4, 2017.

[31] R. Gellert, "Understanding the Notion of Risk in the General Data Protection Regulation," Computer Law & Security Review, vol. 34, pp. 279-288, 2018.

[32] Article 29 Data Protection Working Party (Art29 WP), "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679," WP 248 rev.01, Adopted on 4 April 2017, pp. 1-22 <https://ec.europa.eu/newsroom/article29/items/611236> accessed 4 March 2023.

[33] European Data Protection Supervisor (EDPS), "Accountability on the ground Part I: Records, Registers and when to do Data Protection Impact Assessments," July 2019 <https://edps.europa.eu/sites/edp/files/publication/19-07-17_accountability_on_the_ground_part_i_en.pdf> accessed 10 June 2023.

[34] European Data Protection Supervisor (EDPS), "Decision Of The European Data Protection Supervisor Of 16 July 2019 on DPIA Lists Issued Under Articles 39(4) and (5) of Regulation (EU) 2018/1725," 16 July 2019, pp. 1-8 <https://edps.europa.eu/data-protection/our-work/publications/guidelines/data-protection-impact-assessment-list_en> accessed 16 June 2023.

[35] European Data Protection Supervisor (EDPS), "Accountability on the ground Part II: Data Protection Impact Assessments & Prior Consultation," July 2019 <https://edps.europa.eu/sites/edp/files/publication/19-07-17_accountability_on_the_ground_part_ii_en.pdf> accessed 16 June 2023.

[36] G. Gültekin Várkonyi and A. Gradišek, "Data Protection Impact Assessment Case Study for a Research Project Using Artificial Intelligence on Patient Data," Informatica, vol. 44, pp. 497-505, 2020.

[37] N. van Dijk, R. Gellert, and K. Rommetveit, "A risk to a right? Beyond data protection risk assessments," Computer law & Security Review, vol. 32, pp. 286-306, 2016.

[38] B. J. Evans, "Big data and individual autonomy in a crowd," in I. Glenn Cohen, Holly Fernandez Lynch, Effy Vayena, Urs Gasser Eds. Big Data, Health Law, and Bioethics, pp. 19-29. New York: Cambridge Univ. Press, 2018.

[39] S. Marjanovic, I. Ghiga, M. Yang, and A. Knack, "Understanding value in health data ecosystems - A review of current evidence and ways forward," RAND Health Q uar., vol. 7(2), 29 January 2018 <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5798965/> accessed 18 March 2023.

[40] Y. Li and L. Chen, "Big Biological Data: Challenges and Opportunities," Genomics Proteomics Bioinformatics, vol. 12, pp. 187-189, 2014.

[41] A. Ballantyne, "How should we think about clinical data ownership?" Journal of medical ethics, vol. 46(5), pp. 289-294, 2020.

[42] P. Bronwyn and B. Greenhough, Bioinformation, John Wiley & Sons, 2017.

[43] European Commission, "When is a Data Protection Impact Assessment (DPIA) required?" <https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/when-data-protection-impact-assessment-dpia-required_en> accessed 15 June 2023.

[44] A. L. Beaussier, D. Demeritt, A. Griffiths, and H. Rothstein, "Accounting for Failure: risk-based regulation and the problems of ensuring healthcare quality in the NHS, Health," Risk & Society, vol. 18(3-4), pp. 205-224, 2016.

[45] European Commission, "White Paper on Artificial Intelligence – A European Approach to Excellence and Trust," COM(2020) 65 final, 19 February 2020, Brussels <https://commission.europa.eu/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en> accessed 20 February 2023.

[46] J. van Puijenbroek and J. H. Hoepman, "Privacy Impact Assessment in Practice - The Results of a Descriptive Field Study in the Netherlands," pp. 1-8, 2017.

[47] A. Warren, R. Bayley, C. Bennett, A. Charlesworth, R. Clarke, and C. Oppenheim, "Privacy Impact Assessments: International experience as a basis for UK Guidance," Computer Law & Security Report, vol. 24, pp. 233-242, 2008.

[48] D. Wright, "Privacy impact assessments should be integrated into the overall approach to risk management with other strategic planning instruments," Communications of the ACM, vol. 54(8), pp. 121-131, 2011.

[49] Harvard Business Review, "How to Find the Balance Between Empowering Innovation and Protecting Company Data," 20 May 2021 <https://hbr.org/sponsored/2021/05/how-to-find-the-balance-between-empowering-innovation-and-protecting-company-data> accessed 10 January 2023.

[50] European Data Protection Supervisor (EDPS), "EDPS Survey on Data Protection Impact Assessments under Article 39 of the Regulation (case 2020-0066)," February 2020, pp. 1-31 <https://edps.europa.eu/data-protection/our-work/publications/reports/edps-survey-data-protection-impact-assessments-under_en> accessed 15 June 2023.