The effectiveness of the GDPR's Data Protection Impact Assessment as a mechanism to establish algorithmic accountability in order to reduce bias

Master thesis Law & Technology

Primary supervisor: Shakya Wickramanayake

Secondary supervisor: Gert Meyers

Student number: 2067644

Date: 18-5-2022

Contents

Chapter 1 – Introduction

The emerging information society is increasingly driven by big data.[1] Meaningful processing of big data is made possible by algorithms: systems that can analyze large datasets, find patterns and make decisions.[2] Nowadays, algorithms have been integrated into virtually all aspects of modern life.[3] Applications include predictive policing[4], autonomous driving[5], language translation[6], and many others[7].

Additionally, algorithms have entered the decision-making domain. Algorithms nowadays make decisions that have a large influence on individuals' lives. They are used to decide whether a loan is granted[8], what is shown on someone's digital news feed,[9] and whether an applicant is invited for an interview.[10] Algorithms thus support or autonomously take part in important decision-making. Although algorithms are often believed to be neutral, they contain biases.[11] The data that forms the basis for the algorithm's decision-making largely reflect the values and ideas of the algorithm's developers that are mostly white and male, as was for instance shown in Apple's diversity report of 2017.[12] This lack of diversity makes algorithms prone to bias against particularly marginalized groups that are historically the target of incorrect assumptions.[13] These marginalized groups can consequently fall victim to a so-called feedback loop.[14] The decisions based on biased historical data then produce decisions that subsequently form new datasets that equally contain this bias.[15] Algorithmic decisions, therefore, are capable of causing serious harm particularly when it concerns high-impact decisions, such as the evaluation of credit scores.[16] Bias can be considered problematic when

---

[1] RH Weber and E Studer, 'Cybersecurity in the Internet of Things: Legal aspects' [2016] 32(5) Computer Law and Security Review 715-728

[2] C Adriaansz and E Studer, 'Betekenisvolle transparantie voor algoritmische besluitvorming' [2020] 43(2) Computerrecht 83-91

[3] Finale Doshi-velez and others, 'Accountability of AI Under the Law: The Role of Explanation' [2017] SSRN Electronic Journal <DOI:10.2139/ssrn.3064761> accessed 16 May 2021

[4] Aaron Shapiro, 'Reform predictive policing' [2017] 541(7638) Nature <http://dx.doi.org/10.1038/541458a> accessed 16 May 2021

[5] Mohammed Al-qizwini and others, 'Deep learning algorithm for autonomous driving using GoogLeNet' [2017] 2017 IEEE Intelligent Vehicles Symposium

[6] Nguyen Ha vo and others, 'The NL2KR Platform for building Natural Language Translation Systems' [2015] 1(1) ACL <DOI:10.3115/v1/P15-1087> accessed 16 May 2021

[7] E.g. Yan Guo and others, 'An Interactive Personalized Recommendation System Using the Hybrid Algorithm Model' [2017] 9(10) Symmetry; Kazi Mahmud Hasan and others, 'Path planning algorithm development for autonomous vacuum cleaner robots' [2014] 1(1) Conference: 2014 International Conference on Informatics, Electronics & Vision (ICIEV) <DOI:10.1109/ICIEV.2014.6850799> accessed 16 May 2021

[8] N Metawa, M Elhoseny, MK Hassan and AE Hassanien, 'Loan Portfolio Optimization using Genetic Algorithm: A case of credit constraints' [2016] 12th International Computer Engineering Conference 95-64

[9] Paige Cooper, 'How the Facebook Algorithm Works in 2021 and How to Make it Work for You' (Hootsuite, 10th February) <https://blog.hootsuite.com/facebook-algorithm/> accessed 18 April 2021

[10] S Pan, K Larson, J Bradshaw and E Law, 'Dynamic task allocation algorithm for hiring workers that learn' [2016] Proceedings of the Twenty-Fifth International Joint Conference on Artificial Intelligence 3825-3831

[11] Alina Köchling and Marius Claus Wehner, 'Discriminated by an algorithm: a systematic review of discrimination and fairness by algorithmic decision-making in the context of HR recruitment and HR development' [2020] 13(3) Business Research 795

[12] Joni R Jackson and Marco Marabelli, 'Algorithmic Bias' [2018] 15(4) Accountability & Ethics 56

[13] Nicol Turner Lee, 'Detecting racial bias in algorithms and machine learning' [2018] 16(3) JICES 252

[14] Kiana Alikhademi and others, 'A review of predictive policing from the perspective of fairness' [2022] 30(1) Artificial Intelligence and Law 2

[15] Kiana Alikhademi and others, 'A review of predictive policing from the perspective of fairness' [2022] 30(1) Artificial Intelligence and Law 2

[16] David Danks and Alex John London, 'Algorithmic Bias in Autonomous Systems' [2017] 1(1) Proceedings of the 26th International Joint Conference on Artificial Intelligence 1

it leads to a violation of human rights, such as the right not to be discriminated on basis of race, and when it has major impact on people's lives.[17] Algorithmic decision-making, therefore, raises public concern.[18]

It is particularly the machine learning algorithm that causes public concern. This is because machine learning algorithms have an opaque character. This makes it difficult to understand not only the algorithm itself, but also its related power relations.[19] The latter means that the algorithm has a large impact on society, but regulation may be unable to keep pace and impose the checks and balances which are required for such powerful processes.[20] This is where accountability issues arise. Accountability can be defined as the responsibility of a body or person to explain and justify their actions to another body or person.[21] It is important for subjects of algorithmic decision-making to hold a body or person accountable for the decision-making, particularly because the algorithm tends to be biased and its decisions can have large impact on people's lives. Accountability is considered to be instrumental in correcting bias in algorithms and decrease the harm that biased algorithms cause by making biased decisions, such as the rejection of a loan.[22] Accountability is instrumental to correct bias, since it allows exercising control over the conduct of the private sector.[23] It provides the possibility of a learning circle where an actor behaves according to instructions of a forum under the threat of a sanction.[24] It can therefore further protect natural persons against human rights violations as a consequence of algorithmic bias.

There are legal mechanisms in place that intend to increase accountability. One of these regulatory instruments in the European Union is the General Data Protection Regulation (GDPR).[25] The GDPR is important to study as it is the first legal document to specifically address how algorithmic discrimination affects the fundamental rights and freedoms of natural persons, including algorithmic discrimination.[26] Its successes and failures will be incorporated into future regulation. The GDPR specifically addresses accountability concerns that arise from algorithmic decision-making. One of its mechanisms, the Data Protection Impact Assessment (DPIA), has been largely studied in environmental law, but overlooked in the data protection regulation research. It can be questioned to what extent the DPIA successfully contributes to accountability. It is important for the data subjects to be protected effectively from the risks that arise from algorithmic decision-making, such as the risks of discrimination. This thesis will shed light on the extent to which the DPIA addresses algorithmic accountability.

---

[17] UN Human Rights Committee (HRC) 'CCPR General Comment No. 18: Non-discrimination' (10 November 1989), para 6

[18] Hetan Shah, 'Algorithmic accountability' [2018] 376(1) Philosophical Transactions of The Royal Society A Mathematical Physical and Engineering Sciences 2

[19] A Rosenblat, T Kneese and D Boyd, 'Algorithmic Accountability' [2014] The Social, Cultural & Ethical Dimensions of "Big Data" OSF Preprints

[20] A Rosenblat, T Kneese and D Boyd, 'Algorithmic Accountability' [2014] The Social, Cultural & Ethical Dimensions of "Big Data" OSF Preprints 3

[21] Colin Scott, 'Accountability in the Regulatory State' [2000] 27(1) Journal of Law and Society 38-60

[22] Bruno Lepri and others, ' "Fair, Transparent, and Accountable Algorithmic Decision-Making Processes' [2018] 31(4) Philosophy & Technology 611-627

[23] Mark Bovens, 'Analysing and Assessing Accountability: A Conceptual Framework' [2007] 13(4) European Law Journal 453

[24] Mark Bovens, 'Analysing and Assessing Accountability: A Conceptual Framework' [2007] 13(4) European Law Journal 452

[25] Article 29 Working Party, 'Opinion 3/2010 on the principle of accountability' (WP 173, 13 July 2010) 8-9

[26] B Goodman, 'A Step Towards Accountable Algorithms? Algorithmic Discrimination and the European Union General Data Protection' [2016] 29th Conference on Neural Information Processing Systems 1

1.1 Literature review

The academic literature did not remain silent on this topic. Particularly extensive literature exists around algorithmic accountability. A variety of disciplines, including legal and computer science, have engaged with this topic.[27] Of those, many authors have pleaded for more algorithmic accountability. [28] Discussion in the literature exists on the questions of who is to be held accountable[29], to whom the actor should be accountable[30], and for what the actor should be accountable[31]. However, this discussion does not include an evaluation of existing accountability tools.

A large body of literature is dedicated to the GDPR. Especially its challenges have been explored.[32] The right not to be subject to automated individual decision-making particularly caused large debate in the literature. Many scholars have dedicated their works to establishing whether or not there is a right to explanation embedded in this and other articles in the GDPR.[33] The thesis will not take part in this debate, as it has already been subject to extensive research.

The other tools of the GDPR that were mentioned above did not have similar attention in the literature. However, it has been researched whether impact assessments outside the GDPR are an effective tool to address accountability.[34] Before the existence of the GDPR, impact assessments were already adopted in environmental law. An environmental impact assessment

---

[27] E.g. Deborah G Johnson and Helen Nissenbaum, Computers, ethics & social values (Prentice Hall 1995); A Rosenblat, T Kneese and D Boyd, 'Algorithmic Accountability' [2014] The Social, Cultural & Ethical Dimensions of "Big Data" OSF Preprints; Lawrence Lessig, Code: and other laws of cyberspace (Basic Books 1999)

[28] L Rainie and J Anderson, 'Code-Dependent: Pros and Cons of the Algorithm Age' [2017] Pew Research Center; Joshua New and Daniel Castro, How Policymakers can foster Algorithmic Accoutability (Center for Data Innovation 2018); A Rosenblat, T Kneese and D Boyd, 'Algorithmic Accountability' [2014] The Social, Cultural & Ethical Dimensions of "Big Data" OSF Preprints

[29] E.g. Maranke Wieringa, 'What to account for when accounting for algorithms: a systematic literature review on algorithmic accountability' [2020] FAT* '20: Conference on Fairness, Accountability, and Transparency; Kristen Martin, 'Ethical Implications and Accountability of Algorithms' [2019] 160(1) Journal of Business Ethics; Han Yu and others, 'Building Ethics into Artificial Intelligence' [2018] IJCAI

[30] E.g. Maranke Wieringa, 'What to account for when accounting for algorithms: a systematic literature review on algorithmic accountability' [2020] FAT* '20: Conference on Fairness, Accountability, and Transparency; Jakko Kemper and Daan Kolkman, 'Transparent to whom? No algorithmic accountability without a critical audience' [2019] 22(14) Information, Communication & Society; Mark Bovens, 'Analysing and Assessing Accountability: A Conceptual Framework' [2007] 13(4) European Law Journal 447-468

[31] E.g. Maranke Wieringa, 'What to account for when accounting for algorithms: a systematic literature review on algorithmic accountability' [2020] FAT* '20: Conference on Fairness, Accountability, and Transparency; Joshua Kroll and others, 'Accountable Algorithms' [2016] 165(1) University of Pennsylvania Law Review; Daniel Neyland, 'Bearing Account-able Witness to the Ethical Algorithmic System' [2016] 41(1) Science, Technology, & Human Values 50-76

[32] E.g. E Politou and others, 'Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions' [2018] 4 J Cybersecur; Iskander Sanchez-rola and others, 'Can I Opt Out Yet?: GDPR and the Global Illusion of Cookie Control' [2019] 1(1) In Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security (Asia CCS '19); Tal Zarsky, 'Incompatible: The GDPR in the Age of Big Data' [2017] 4(2) Seton Hall Law Review

[33] B Casey, A Farhangi and R Vogl, 'Rethinking Explainable Machines: The GDPR's 'Right to Explanation' Debate and the Rise of Algorithmic Audits in Enterprise' [2019] 34 Berkeley Technology Law Journal; B Goodman, 'A Step Towards Accountable Algorithms? Algorithmic Discrimination and the European Union General Data Protection' [2016] 29th Conference on Neural Information Processing Systems; ME Kaminski, 'The Right to Explanation, Explained' [2019] 34(1) Berkeley Technology Law Journal; S Wachter, B Mittelstadt and L Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' [2017] (2) Harvard Journal of Law & Technology 841-887

[34] D Cilliers and others, 'The perceived benefits of EIA for government: a regulator perspective' [2020] 38(5) Impact Assessment and Project Appraisal 358-367; David P. Lawrence, Environmental Impact Assessment: Practical Solutions to Recurrent Problems (1 edn, John Wiley & Sons, Inc 2003) 165

(EIA) is required under the EIA directive[35] when a project is likely to have a significant effect on the environment (article 1). The EIA is regularly viewed as supporting greater accountability.[36] While the tool of EIA has been researched extensively[37], similar studies do not yet exist for the DPIA. It is, therefore, useful to study whether this tool of impact assessments is similarly useful in the context of data protection and algorithmic decision-making.

Discussion in the literature about the DPIA exists over what constitutes a 'high risk' as is required in article 35 GDPR.[38] The meaning of 'high risk' is not clarified in article 35 GDPR and has thus led to differing conceptual interpretations.[39] The concept of 'high risk' leaves considerable room for interpretation by the data controller.[40] It can therefore be challenging to determine whether a certain algorithmic data processing is high risk. How this impacts algorithmic accountability has nonetheless been largely overlooked. The concept of high risk will be touched upon in this thesis.

Further relevant for the thesis in the literature is the analysis of the DPIA as an obligation that interacts with the other rights and obligations in the GDPR.[41] The particular possibilities and limitations of the DPIA for algorithmic accountability have, however, only been reviewed in light of this interaction. This framework provides an overarching view. Nevertheless, the literature has not looked specifically at the DPIA as an individual tool to increase accountability. A study of the problems arising from deploying a DPIA to address algorithmic accountability issues has not yet been conducted in the literature.

At the same time, accountability can be instrumental in creating control over de conduct of private parties and therefore play a part in correcting bias.[42] It is therefore important to evaluate the tools that intend to contribute to accountability. The literature has not yet tapped into this issue, which is consequently the topic of this thesis.

---

[35] Directive 2011/92 on the assessment of the effects of certain public and private projects on the environment, [2012] OJ L 26/1, repealing Directive 85/337, [1985] OJ L 175/40 as amended. Directive 2011/92 was last amended by Directive 2014/52, [2014] OJ L 124/1

[36] D Cilliers and others, 'The perceived benefits of EIA for government: a regulator perspective' [2020] 38(5) Impact Assessment and Project Appraisal 358-367; David P. Lawrence, Environmental Impact Assessment: Practical Solutions to Recurrent Problems (1 edn, John Wiley & Sons, Inc 2003) 165

[37] E.g. Richard Morgan, 'Environmental impact assessment: The state of the art' [2012] 30(1) Impact Assessment and Project Appraisal 1-10; Stephen Jay and others, 'Environmental impact assessment: Retrospect and prospect' [2007] 27(4) Environmental Impact Assessment Review 287-300; Leonard Ortolano and Anne Shepherd, 'Environmental impact assessment: challenges and opportunities' [1995] 13(1) Impact Assessment 3-30

[38] S Bu-Pasha, 'The controller's role in determining 'high risk' and data protection impact assessment (DPIA) in developing digital smart city' [2020] 29(3) Information & Communications Technology Law 391-402; K Demetzou, 'Data Protection Impact Assessment: A tool for accountability and the unclarified concept of 'high risk' in the General Data Protection Regulation' [2019] 35(6) Computer Law & Security Review

[39] Felix Bieker and others, 'A Process for Data Protection Impact Assessment under the European General Data Protection Regulation' [2016] 1(1) Conference: 4th Annual Privacy Forum; Müge Fazlioglu, 'What's Subject to a DPIA under the GDPR? EDPB on Draft Lists of 22 Supervisory Authorities' [2018] IAPP; Camden Woollven, '7 Key Stages of the Data Protection Impact Assessment (DPIA)' [2021] IT Governance (4 September 2019) <https://www.itgovernance.co.uk/blog/gdpr-six-key-stages-of-the-data-protection-impact-assessment-dpia> accessed 3 May 2021.

[40] Shakila Bu-pasha, 'The controller's role in determining 'high risk' and data protection impact assessment (DPIA) in developing digital smart city' [2020] 29(3) Information & Communications Technology Law

[41] ME Kaminski and G Malgieri, 'Multi-layered explanations from algorithmic impact assessments in the GDPR' [2020] Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency 68-79

[42] Mark Bovens, 'Analysing and Assessing Accountability: A Conceptual Framework' [2007] 13(4) European Law Journal 453; Bruno Lepri and others,' "Fair, Transparent, and Accountable Algorithmic Decision-Making Processes' [2018] 31(4) Philosophy & Technology 611-627

1.2 Research questions

The research question that will be answered in this thesis is: "*To what extent does a data protection impact assessment, as required under article 35 GDPR, contribute to the accountability of data controllers in the private sector to data subjects with respect to machine learning algorithms that make decisions?"* The following sub-questions will be answered.

1. *What accountability problems arise from applying algorithmic decision-making?*
2. *What is a data protection risk assessment as is required in article 35 GDPR?*
3. *How does a data protection risk assessment increase the accountability of data controllers with respect to algorithmic decision-making?*
4. *What are the limitations of increasing accountability of data controllers with respect to algorithmic decision-making by means of a data protection risk assessment?*

1.3 Limitations, methods, and methodology

The scope of the thesis will be **limited** by the following elements. First, the assessment in this thesis will be limited to data controllers in the private sector. The public sector will therefore be excluded from the scope. This is because of two reasons. The first reason to look at the private sector is that public sector accountability has already been discussed in the literature to a larger extent than the private sector.[43] It is therefore useful to now turn to the private sector. The second reason to limit the scope to the private sector is that the private sector raises various transparency questions that are irrelevant to the public sector, as different interests are at play. For instance, trade secrecy may form a barrier to algorithmic transparency.[44] These transparency issues are central to the accountability question. Furthermore, the accountability structures that are present in the public sector, such as accountability of representatives to their voters, are not present in the private sector.[45] The impact of the algorithmic decision-making in the private sector, however, has as much an impact on the lives of people.[46] Therefore the scope is limited to the private sector.

The concept of algorithm is, for this thesis, narrowed down to machine learning algorithms. Other types of algorithms, such as expert systems, fall outside the scope of this thesis. As has been demonstrated, machine learning algorithms are particularly opaque, thereby raising accountability issues. More transparent algorithms are less problematic in light of accountability. It is therefore important to look at machine learning algorithms.

As the GDPR has come into force on 25 May 2018, most research will be limited to the period from 2018 to 2021. However, there are several reasons why documents from before this period may be included. First, research has been conducted before the official coming into force of the GDPR. Second, impact assessments have existed before they became

---

[43] E.g. Michael Veale and others, 'Fairness and Accountability Design Needs for Algorithmic Support in High-Stakes Public Sector Decision-Making' [2018] Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI'18); Anna Brown and others, 'Toward Algorithmic Accountability in Public Services: A Qualitative Study of Affected Community Perspectives on Algorithmic Decision-making in Child Welfare Services' [2019] 1(1) CHI '19: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems; Katherine Fink, 'Opening the government's black boxes: freedom of information and algorithmic accountability' [2017] 21(1) Information Communication and Society 1-19

[44] Mariateresa Maggiolino, 'EU Trade Secrets Law and Algorithmic Transparency' [2019] 1(1) Bocconi Legal Studies Research Paper No 3363178

[45] Nicholas Diakopoulos, 'Accountability in Algorithmic Decision Making' [2016] 59(2) Communications of the ACM 58

[46] Ruotong Wang and others, 'Factors Influencing Perceived Fairness in Algorithmic Decision-Making: Algorithm Outcomes, Development Procedures, and Individual Differences' [2020] 1(1) Conference: CHI '20: CHI Conference on Human Factors in Computing Systems 684

mandatory under the conditions of article 35 GDPR. Research that considers these impact assessments may be relevant as well.

To answer the main research question, doctrinal legal research will be conducted on the GDPR and academic literature on the DPIA and algorithmic accountability. Literature review from various disciplines, such as legal, technical, and sociological, on the concept of algorithmic accountability will be conducted. This will be followed by a black letter law analysis of Article 35 GDPR, subsequently supported by an analysis of the Article 29 Working Party (WP29) Guidelines. Further analysis of academic literature on the DPIA will be conducted to obtain a full understanding of the parts of Article 35. These findings will form the baseline to compare to the elements of accountability to establish whether they increase or limit accountability. The snowball method will be deployed to acquire other relevant academic literature. For the recommendation, a black letter analysis of the proposal for an AI Act will be conducted.

1.4 Structure

The thesis will consist of the following structure. **Chapter 2** will explain algorithmic accountability. The Chapter first delves into machine learning algorithms, followed by an analysis of algorithmic accountability. **Chapter 3** will describe the DPIA as required in article 35 GDPR. It will consist of a description of when the DPIA is required and what the contents of a DPIA are. Together with Chapter 2, this Chapter will form a descriptive basis for Chapters 4 and 5. **Chapter 4** will explain how the DPIA increases algorithmic accountability. The following topics will be explored: the contribution of the DPIA to transparency, the timing of the DPIA, the choice of legislative instrument, and the forums capable of passing judgment. **Chapter 5** will look into the limitations of a DPIA in increasing algorithmic accountability. This Chapter consists of two parts: the limitations in relation to the DPIA and the limitations in relation to algorithms. This categorizes limitations for the DPIA in increasing accountability and particularly forms the basis for how the DPIA may be adjusted to increase accountability and where more research on algorithms is required. Chapters 4 and 5 thus show opposing views to give a full account of how the DPIA does and does not increase algorithmic accountability. These arguments will be revisited and analyzed, followed by a recommendation, in **Chapter 6**. The thesis will end with a conclusion in **Chapter 7**.

Chapter 2 – Algorithmic accountability

To answer the main research question, it is first important to explore the concept of algorithmic accountability. This analysis will lay the basis for the substantive Chapters 4, 5, and 6. This chapter will first look into algorithmic decision-making, followed by an account of algorithmic accountability.

2.1 Algorithmic decision-making

This Chapter is divided into two parts; the first describes algorithms and the second explores accountability. Now, this chapter will elaborate on the meaning of algorithmic decision-making.

2.1.1 Machine Learning Algorithms

The legal literature contains a large variety of definitions of algorithm. Various sciences, such as computer and social sciences, look at the definition of algorithms differently, causing terminological anxiety.[47] Social scientists took a particular interest in "algorithms" of a monstrous size with great societal impact, such as Google Search and Facebook's newsfeed.[48] Computer scientists, however, claimed these "algorithms" were not in fact algorithms according to basic computer science.[49] It may be tempting to adopt the computer scientists' definition as most valid, since they technically have the most intimate knowledge of algorithms.[50] Computer scientists themselves, however, also cannot agree on the meaning of the term algorithm.[51] They are furthermore prone to overlook the social context that algorithms function within and stem from.[52] Algorithms are cultural objects that result from and respond to human action.[53] As explained strikingly by Nick Seaver, algorithms are not "technical rocks in a cultural stream, but are rather just more water".[54]

While not disregarding the cultural character of algorithms, it is useful to obtain a basic understanding of what an algorithm is technically. Combining various definitions in the legal, social, and computer science literature, gives the following definition of algorithm: *a set of instructions, that are sufficiently precise for a computer to run, to achieve a desired outcome*.[55] Defining the desired outcome includes a process of formalization, where a

---

[47] Nick Seaver, 'Algorithms as culture: Some tactics for the ethnography of algorithmic systems' [2017] 4(2) Big Data & Society 2

[48] Nick Seaver, 'Algorithms as culture: Some tactics for the ethnography of algorithmic systems' [2017] 4(2) Big Data & Society 2

[49] Nick Seaver, 'Algorithms as culture: Some tactics for the ethnography of algorithmic systems' [2017] 4(2) Big Data & Society 2

[50] Nick Seaver, 'Algorithms as culture: Some tactics for the ethnography of algorithmic systems' [2017] 4(2) Big Data & Society 2

[51] Nick Seaver, 'Algorithms as culture: Some tactics for the ethnography of algorithmic systems' [2017] 4(2) Big Data & Society 2-3

[52] Nick Seaver, 'Algorithms as culture: Some tactics for the ethnography of algorithmic systems' [2017] 4(2) Big Data & Society 2

[53] Nick Seaver, 'Algorithms as culture: Some tactics for the ethnography of algorithmic systems' [2017] 4(2) Big Data & Society 4-5

[54] Nick Seaver, 'Algorithms as culture: Some tactics for the ethnography of algorithmic systems' [2017] 4(2) Big Data & Society 5

[55] Robyn Caplan and others, 'Algorithmic Accountability: A Primer' [2018] 1(1) Tech Algorithm Briefing: How Algorithms Perpetuate Racial Bias and Inequality 2; A Rosenblat, T Kneese and D Boyd, 'Algorithmic Accountability' [2014] The Social, Cultural & Ethical Dimensions of "Big Data" OSF Preprints 1-2; Matthew Fuller, Software Studies: A Lexicon (1 edn, MIT Press 2008) 16; Maja Brkan, 'Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond' [2019] 27(2) International Journal of Law and Information Technology 94-95; C Adriaansz and E Studer, 'Betekenisvolle transparantie voor algoritmische besluitvorming' [2020] 43(2) Computerrecht 83-84

problem or goal is expressed in computer language.[56] This formalization is subsequently converted to variables, instructions, and indicators.[57] Input data is inserted into the algorithm, which then generates output data based on a set of instructions.[58] This entire procedure is carried out to allow the algorithm to find patterns, classifications, and correlations in the data to complete its task to achieve the goal.[59]

Machine learning algorithms are a type of algorithms that allow the computer to learn by itself, allowing the algorithm to solve more complex issues.[60] Since the introduction of machine learning by Arthur Samuel in 1959, the use of 'Big Data' has increased and the demand for complex analytical tools flourished.[62] This caused the field of machine learning to quickly become one of the most trendy technologies nowadays and simultaneously, a complex one.[63] It involves the utilization of large historical datasets to make an accurate classification or prediction of prospective cases.[64]

Algorithms can be useful to society as they are vital in processing the large amount of data that increasingly drives society.[65] They can detect the information in the data that is found useful in a sea of data that is found useless.[66] This ability to sort data can be beneficial for society.[67] For instance, an algorithm has been developed by the University of Hawaii Cancer Center to examine tumor samples to select what treatment is best fit for a cancer patient.[68] However, significant issues can simultaneously be identified. These will be explained later in this Chapter.

2.1.2 Algorithmic decision-making

The applications of algorithms are becoming increasingly widespread.[69] Particularly their application in decision-making has increased and broadened with applications ranging from policing to housing.[70] This increasing use of algorithms for high-impact decisions, such as the evaluation of a loan application, has a large influence on the lives of natural persons.[71] Biased decisions are capable of structurally reinforcing social inequalities.[72] In the context of

---

[56] Tarleton Gillespie, Algorithm. in Benjamin Peters (ed), Digital Keywords: a vocabulary of information society and culture (Princeton University Press 2016) 19

[57] Tarleton Gillespie, Algorithm. in Benjamin Peters (ed), Digital Keywords: a vocabulary of information society and culture (Princeton University Press 2016) 19-20

[58] Reuben Binns, 'Algorithmic Accountability and Public Reason' [2018] 31(4) Philosophy & Technology 545

[59] Tarleton Gillespie, Algorithm. in Benjamin Peters (ed), Digital Keywords: a vocabulary of information society and culture (Princeton University Press 2016) 20

[60] Rajan Gupta and Saibal Kumar Pal, Introduction to Algorithmic Government (1 edn, Palgrave Macmillan 2021) 40

[62] Jianlong Zhou and Fang Chen, Human and Machine Learning (Springer International Publishing 2018) vii; Stan Franklin, History, motivations, and core themes. in Keith Frankish (ed), The Cambridge handbook for artificial intelligence (Cambridge University Press 2014) 18-19

[63] Jianlong Zhou and Fang Chen, Human and Machine Learning (Springer International Publishing 2018) v

[64] Reuben Binns, 'Algorithmic Accountability and Public Reason' [2018] 31(4) Philosophy & Technology 545

[65] Tarleton Gillespie, The Relevance of Algorithms. in Gillespie and others (eds), Media Technologies: Essays on Communication, Materiality, and Society (MIT Press 2014) 167, 190

[66] Tarleton Gillespie, The Relevance of Algorithms. in Gillespie and others (eds), Media Technologies: Essays on Communication, Materiality, and Society (MIT Press 2014) 167, 190

[67] Alex Rosenblat and others, 'Algorithmic Accountability' [2014] The Social, Cultural & Ethical Dimensions of "Big Data" March 2014 <http://dx.doi.org/10.2139/ssrn.2535540> accessed 6 September 2021

[68] University of Hawaii Cancer Center. "Algorithm to find precise cancer treatments." ScienceDaily. ScienceDaily, 9 August 2016. <www.sciencedaily.com/releases/2016/08/160809185854.htm>.

[69] Reuben Binns, 'Algorithmic Accountability and Public Reason' [2018] 31(4) Philosophy & Technology 543

[70] Reuben Binns, 'Algorithmic Accountability and Public Reason' [2018] 31(4) Philosophy & Technology 543

[71] Reuben Binns, 'Algorithmic Accountability and Public Reason' [2018] 31(4) Philosophy & Technology 546

[72] Reuben Binns, 'Algorithmic Accountability and Public Reason' [2018] 31(4) Philosophy & Technology 546

high-impact decisions, the use of algorithmic decision-making is therefore particularly concerning.

Algorithmic decision-making consists of entities resorting to the output of an algorithm to make a decision without or with little human input.[73] The definition is broad and includes a large variety of decisions of both high and low impact. A decision is low impact when it is not a binding decision and does not touch upon the legitimate rights of the individuals.[74] High impact decisions do include binding decisions and decisions that touch upon the legitimate rights of individuals.[75] Different types of algorithmic decision-making include prioritization, classification, association, and filter.[76]

Algorithmic decision-making has the potential to have a large impact on the lives of individuals, but is simultaneously prone to bias. This will explained in the next.

2.2. Algorithmic accountability

Now that algorithmic decision-making has been explained, this chapter will turn to algorithmic accountability.

2.2.1 Algorithmic bias

Algorithms are often considered neutral.[79] A source of this presumption of neutrality lies in the algorithm's opaque character that causes incorporated bias to become invisible.[80] As will be demonstrated, a biased algorithm that appears neutral may cause serious harm.[81] However, what precisely is this potentially harmful bias and where do biases in algorithms come from?

The word "bias" can be defined in many ways. It includes both intended and unintended characteristics.[82] Broadly and more neutrally defined, bias means the deviation of a standard.[83] This standard can be of many different kinds, including statistical, moral, or legal.[84] For instance, a bias concerning the statistical standard appears in aerospace engineering, where 7.8% of its professionals are women, thereby clearly deviating from the percentage of women in the overall population.[85]

---

[73] Reuben Binns, 'Algorithmic Accountability and Public Reason' [2018] 31(4) Philosophy & Technology 543

[74] Maja Brkan, 'Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond' [2019] 27(2) International Journal of Law and Information Technology 93-94

[75] Maja Brkan, 'Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond' [2019] 27(2) International Journal of Law and Information Technology 93-94

[76] Nicholas Diakopoulos, 'Accountability in Algorithmic Decision Making' [2016] 59(2) Communications of the ACM 57

[79] Alina Köchling and Marius Claus Wehner, 'Discriminated by an algorithm: a systematic review of discrimination and fairness by algorithmic decision-making in the context of HR recruitment and HR development' [2020] 13(3) Business Research 796

[80] Joni R Jackson and Marco Marabelli, 'Algorithmic Bias' [2018] 15(4) Accountability & Ethics 56

[81] David Danks and Alex John London, 'Algorithmic Bias in Autonomous Systems' [2017] 1(1) Proceedings of the 26th International Joint Conference on Artificial Intelligence 1

[82] Jean Garcia-Gathright and others, 'Assessing and Addressing Algorithmic Bias - But Before We Get There' [2018] ArXiv

[83] Shahriar Akter and others, 'Algorithmic bias in data-driven innovation in the age of AI' [2021] 60(1) International Journal of Information Management 1

[84] David Danks and Alex John London, 'Algorithmic Bias in Autonomous Systems' [2017] 1(1) Proceedings of the 26th International Joint Conference on Artificial Intelligence 2

[85] David Danks and Alex John London, 'Algorithmic Bias in Autonomous Systems' [2017] 1(1) Proceedings of the 26th International Joint Conference on Artificial Intelligence 2

This meaning of bias does not incorporate the negative connotations of the word 'bias'.[86] The legal literature on algorithms, particularly of the machine learning kind, does regularly define bias in a more normative manner.[87] It is, for instance, defined as unfair discrimination.[88] This means that the algorithm systematically and unfairly favors some people over other people.[89] For instance, algorithmic decision-making is used in assessing the probability of recidivism that decides who is to remain in prison and who is to be set free.[92] The algorithm was later proved to be biased against African American defendants, who consequently obtained longer prison sentences.[93]

Thus, some algorithmic bias is deeply problematic, but this cannot be stated for all types of algorithmic bias. Some algorithmic bias enters valuable factors into the algorithm.[94] For instance, bias can be entered into the algorithm to correct unwanted bias.[95] It cannot be stated definitively and precisely what bias is problematic, since this is part of a society-wide and value-laden discussion on what should be part of high impact decision-making on, for instance, employment.[96] Factors that may have been found unproblematic in the 1900s may be considered deeply problematic in modern times. For example, during the racial segregation in the 1900s in the United States, African American people were found second-class citizens by many and therefore hired less for good jobs [97] In modern times, this is considered problematic by many and algorithms can be made biased to not follow this historic data. It is consequently not possible to state that all forms of bias are inherently problematic.

A possible manner to determine whether algorithmic bias is problematic, is by applying human rights considerations.[98] Here, an algorithmic bias is problematic when it leads to a human rights violation, such as a violation of the right not to be discriminated on basis of race.[99] A human rights based approach to determine whether algorithmic bias is problematic, is useful, because it allows evaluation of bias in a principled and structured manner, while holistically looking at different topics, such as racial discrimination and freedom of

---

[86] David Danks and Alex John London, 'Algorithmic Bias in Autonomous Systems' [2017] 1(1) Proceedings of the 26th International Joint Conference on Artificial Intelligence 2

[87] Jean Garcia-gathright and others, 'Assessing and Addressing Algorithmic Bias - But Before We Get There' [2018] ArXiv

[88] Jean Garcia-gathright and others, 'Assessing and Addressing Algorithmic Bias - But Before We Get There' [2018] ArXiv

[89] Jean Garcia-Gathright and others, 'Assessing and Addressing Algorithmic Bias - But Before We Get There' [2018] ArXiv 1

[92] Julia Angwin and others, 'Machine Bias: Risk assessments in criminal sentencing' [2016] ProPublica <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing> accessed 6 September 2021

[93] Julia Angwin and others, 'Machine Bias: Risk assessments in criminal sentencing' [2016] ProPublica <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing> accessed 6 September 2021

[94] David Danks and Alex John London, 'Algorithmic Bias in Autonomous Systems' [2017] 1(1) Proceedings of the 26th International Joint Conference on Artificial Intelligence 2

[95] David Danks and Alex John London, 'Algorithmic Bias in Autonomous Systems' [2017] 1(1) Proceedings of the 26th International Joint Conference on Artificial Intelligence 3

[96] David Danks and Alex John London, 'Algorithmic Bias in Autonomous Systems' [2017] 1(1) Proceedings of the 26th International Joint Conference on Artificial Intelligence 2

[97] Library of congress, 'Brown v Board at Fifty: "With an Even Hand"' (Library of Congress) <http:/loc.gov> accessed 16 May 2022; Library of congress, 'The Civil Rights Act of 1964: A Long Struggle for Freedom' (Library of Congress) <http:/loc.gov> accessed 16 May 2022

[98] UN Human Rights Committee (HRC) 'CCPR General Comment No. 18: Non-discrimination' (10 November 1989)

[99] UN Human Rights Committee (HRC) 'CCPR General Comment No. 18: Non-discrimination' (10 November 1989), para 6

religion.[100] It is furthermore particularly useful, because the human rights-based approach provides notions that have been developed over a long time and are widely understood.[101] Racial discrimination is, for instance, defined in the Human Rights Committee's General Comment .[102] The Human Rights Committee also explain what types of differentiation do not amount to discrimination and requires, for instance, objective criteria for the differentiation.[103] These notions can provide guidance in determining what bias is problematic. It needs to be noted that this approach is not completely sufficient, due to competing human rights and, for example, the practical difficulty of translating abstract human rights principles into concrete considerations.[104] The common language that the human rights framework provides, however, allows for a discussion in a common language.

Taken together, bias can be understood as: *an intended or unintended deviation from the standard that may constitute unfair discrimination*.

There are different sources of algorithmic bias. First, the data that is used to train or evaluate the algorithm may be biased. Datasets are at the center of particularly machine learning algorithms and the bias that are embedded in the datasets will therefore deeply impact the performance of the algorithms.[105] Datasets may be biased when they do not adequately or correctly represent the relevant population.[106] The datasets may additionally be biased when they under- or over-represent important characteristics of the relevant population.[107] The algorithm may furthermore reflect historical bias that is embedded in the historical training data.[108] Racial bias that appears in historical bias may for instance be adopted by the algorithm and replicated in future outcomes.[109] Bias in the training data is often not visible, particularly since training data regularly remains nondisclosed.[110] As the evaluation data that stems from the biased algorithm verifies the bias, a feedback loop further confirms and intensifies this bias.[111]

An algorithm in itself can therefore be inherently non-biased, but 'made' biased by the training and evaluation data. However, the algorithm itself can also be biased. For instance,

---

[100] Barrie Sander, 'Freedom of Expression in the Age of Online Platforms: The Promise and Pitfalls of a Human Rights-Based Approach to Content Moderation' [2020] 43(4) Fordham International Law Journal 966-967

[101] Barrie Sander, 'Freedom of Expression in the Age of Online Platforms: The Promise and Pitfalls of a Human Rights-Based Approach to Content Moderation' [2020] 43(4) Fordham International Law Journal 967-968

[102] UN Human Rights Committee (HRC) 'CCPR General Comment No. 18: Non-discrimination' (10 November 1989), para 6

[103] UN Human Rights Committee (HRC) 'CCPR General Comment No. 18: Non-discrimination' (10 November 1989), para 13

[104] Barrie Sander, 'Freedom of Expression in the Age of Online Platforms: The Promise and Pitfalls of a Human Rights-Based Approach to Content Moderation' [2020] 43(4) Fordham International Law Journal 968-969

[105] Shahriar Akter and others, 'Algorithmic bias in data-driven innovation in the age of AI' [2021] 60(1) International Journal of Information Management 5-6

[106] Shahriar Akter and others, 'Algorithmic bias in data-driven innovation in the age of AI' [2021] 60(1) International Journal of Information Management 5-6

[107] Shahriar Akter and others, 'Algorithmic bias in data-driven innovation in the age of AI' [2021] 60(1) International Journal of Information Management 5-6

[108] Nicol Turner Lee, 'Detecting racial bias in algorithms and machine learning' [2018] 16(3) Journal of Information, Communication and Ethics in Society 252-255

[109] Nicol Turner Lee, 'Detecting racial bias in algorithms and machine learning' [2018] 16(3) Journal of Information, Communication and Ethics in Society 252-255

[110] David Danks and Alex John London, 'Algorithmic Bias in Autonomous Systems' [2017] 1(1) Proceedings of the 26th International Joint Conference on Artificial Intelligence 1

[111] Shahriar Akter and others, 'Algorithmic bias in data-driven innovation in the age of AI' [2021] 60(1) International Journal of Information Management 6

the creators of the algorithm are human and therefore biased.[112] The values of the human creator are incorporated into the algorithm in the development stage and later reflected in its decisions.[113] The creator may adapt the algorithm to be biased on purposed, for instance to correct unwanted bias from the training data.[114] However, values can also be unintended and become unwanted bias in the algorithm. This is particularly an essential type of bias as creators of algorithms are largely white and male.[115] Algorithms will therefore largely reflect white and male values and ideas and thereby the algorithm is prone to bias against non-white and non-male groups.[116] This is particularly problematic for algorithms that make high-impact decisions, such as the evaluation of credit scores by banks or the prediction of recidivism risk, as explained above.

2.2.2 Defects in the algorithm and user bias

Algorithms can furthermore contain defects or user bias. These defects can lead to structural bias as explained in the previous paragraph, but can furthermore make wrongful decisions in isolated cases or for non-marginalized groups of people. The coding may contain defects, or a margin of error may lead to incorrect outcomes.[117] Furthermore, the algorithms may confuse correlations with causation.[118] This was the case for an algorithm used by an insurance company to create a risk profile for consumers that formed the basis for the determination of the premium. Consumers that lived at house number 186A were structurally offered a higher premium than consumers that lived at house number 186, as the algorithm found a high risk for consumers living at house number 168A.[119] This created a faulty risk profile that was based on correlation instead of causation.[120]

Moreover, incorrect decision-making may occur when the system is deployed by the user in ways or for purposes for which the algorithm was not intended or the outcome may be interpreted wrong by the user of the system or the larger system within which the algorithm functions.[121] Here, the algorithm itself and its training data are unbiased, but its outcome is used incorrectly. It can therefore be seen more as a ‘user bias’ than an algorithmic bias.[122]

---

[112] C Adriaansz and E Studer, 'Betekenisvolle transparantie voor algoritmische besluitvorming' [2020] 43(2) Computerrecht 84; Tarleton Gillespie, Algorithm. in Benjamin Peters (ed), Digital Keywords: a vocabulary of information society and culture (Princeton University Press 2016) 19-20

[113] C Adriaansz and E Studer, 'Betekenisvolle transparantie voor algoritmische besluitvorming' [2020] 43(2) Computerrecht 84; Tarleton Gillespie, Algorithm. in Benjamin Peters (ed), Digital Keywords: a vocabulary of information society and culture (Princeton University Press 2016) 19-20

[114] David Danks and Alex John London, 'Algorithmic Bias in Autonomous Systems' [2017] 1(1) Proceedings of the 26th International Joint Conference on Artificial Intelligence 3

[115] Joni R Jackson and Marco Marabelli, 'Algorithmic Bias' [2018] 15(4) Accountability & Ethics 55-57

[116] Joni R Jackson and Marco Marabelli, 'Algorithmic Bias' [2018] 15(4) Accountability & Ethics 55-57

[117] C Adriaansz and E Studer, 'Betekenisvolle transparantie voor algoritmische besluitvorming' [2020] 43(2) Computerrecht 84

[118] Shahriar Akter and others, 'Algorithmic bias in data-driven innovation in the age of AI' [2021] 60(1) International Journal of Information Management 6

[119] Nos, 'De verzekering is bij huisnummer 186A duurder dan bij 186' (NOS, 26-08-2015) <https://nos.nl/artikel/2054035-de-verzekering-is-bij-huisnummer-186a-duurder-dan-bij-186> accessed 9 September 2021

[120] Anna Gerbrandy and Bart Custers, 'Algoritmische besluitvorming en het kartelverbod' [2018] 21(3) Markt en Mededinging 102-103

[121] David Danks and Alex John London, 'Algorithmic Bias in Autonomous Systems' [2017] 1(1) Proceedings of the 26th International Joint Conference on Artificial Intelligence 4

[122] David Danks and Alex John London, 'Algorithmic Bias in Autonomous Systems' [2017] 1(1) Proceedings of the 26th International Joint Conference on Artificial Intelligence 4

Particularly problematic is that entities making use of algorithms for decision-making often neglect attempting to understand how the decision is made by the algorithm.[123] Therefore, bias can easily infiltrate the decision-making process and mistakes remain unnoticed. At the same time, the decisions made by the algorithm can have a large impact on the individuals.[124] For instance, a mistake in an algorithm deployed by a bank to determine the height of a mortgage, may structurally lead to consumers with too high debt to pay. As has been stated previously, however, not all bias is problematic. The previously proposed human rights approach can be taken to determine what algorithmic bias can be considered problematic.

2.2.3 Algorithmic accountability as a solution

Algorithms therefore may contain biases that have an adversarial impact on and potentially harm particularly marginalized groups or contain defects or user bias that lead to incorrect outcomes. This has fueled the call for algorithmic accountability.[125] Algorithms have the potential to make crucial decisions and thus have a large societal impact, but their underlying power structures remain largely invisible particularly due to the algorithm's complexity.[126] Especially the private sector has the potential to remain devoid of accountability. This is partly because the accountability structures for the public sector, such as accountability through the election of the government by citizens, do not apply to the private sector.[127] Determining accountability may enable the exercise of control over the conduct of entities in relation to algorithms.[128] Therefore accountability can be perceived as a means to correct bias and prevent or decrease harm done by the algorithm.[129]

Accountability has previously been defined as the responsibility of a body or person to explain and justify their actions to another body or person.[130] The widely accepted[131] analysis of Bovens of accountability identifies seven elements of accountability:[132]

"1. there is a relationship between an actor and a forum
2. in which the actor is obliged
3. to explain and justify
4. his conduct;
5. the forum can pose questions;
6. pass judgement;
7. and the actor may face consequences"

---

[123] Sue Newell and Marco Marabelli, 'Strategic opportunities (and challenges) of algorithmic decision-making: A call for action on the long-term societal effects of 'datification'' [2015] 24(1) Journal of Strategic Information Systems 4

[124] Reuben Binns, 'Algorithmic Accountability and Public Reason' [2018] 31(4) Philosophy & Technology 546

[125] Reuben Binns, 'Algorithmic Accountability and Public Reason' [2018] 31(4) Philosophy & Technology 543

[126] Alex Rosenblat and others, 'Algorithmic Accountability' [2014] The Social, Cultural & Ethical Dimensions of "Big Data" March 2014 <http://dx.doi.org/10.2139/ssrn.2535540> accessed 6 September 2021

[127] Nicholas Diakopoulos, 'Accountability in Algorithmic Decision Making' [2016] 59(2) Communications of the ACM 58

[128] Mark Bovens, 'Analysing and Assessing Accountability: A Conceptual Framework' [2007] 13(4) European Law Journal 453

[129] Bruno Lepri and others, ' "Fair, Transparent, and Accountable Algorithmic Decision-Making Processes' [2018] 31(4) Philosophy & Technology 611-627

[130] Colin Scott, 'Accountability in the Regulatory State' [2000] 27(1) Journal of Law and Society 38-60

[131] Maranke Wieringa, 'What to account for when accounting for algorithms: a systematic literature review on algorithmic accountability' [2020] FAT* '20: Conference on Fairness, Accountability, and Transparency

[132] Mark Bovens, 'Analysing and Assessing Accountability: A Conceptual Framework' [2007] 13(4) European Law Journal 452

Algorithmic accountability, accordingly, is accountability as Bovens identifies it, where algorithms are the subject of explanation.[133] To illustrate this definition, an example of a bank that deploys an algorithm to evaluate credit score applications can be given. If a loan is rejected on basis of the credit score, the customer may request the bank to justify its decision. The bank provides the requested justification and the customer may then judge the adequacy of the justification.[134] This justification can form the basis for legal action, or even societal action. It can be questioned whether the bank may face consequences for its decision on basis of its account. The possibility of facing sanctions, however, is a notion that should be interpreted broadly.[135] The possibility, for instance, of facing television cameras to explain its decision to the public, forms a possible sanction for the bank.[136] Thus, the possible consequences may be formal, for instance, fines or civil remedies, but may additionally be informal, such as the threat of negative publicity or a bad reputation.[137] Negative publicity has large impact on the views of consumers on the private entity. Consumers are less satisfied and evaluate the brand negatively in response to negative publicity.[138] It furthermore changes the purchase intentions of consumers which results in lower revenues for the private entity.[139] Private entities will consequently want to avoid negative publicity and thus put in place ex-ante measures.

Accountability contributes to combating algorithmic bias and other defects. As will be argued in Chapter 4, transparency brings to light information that contributes to accountability. By making information about algorithms visible and available, actors are prone to behave more responsibly.[140] Accountability then is instrumental to accomplish a reduction in algorithmic bias and defects.[141] This is because accountability can constitute a learning circle, where the actor can obtain insight into its conduct according to the feedback of the forum.[142] A well-natured actor that is oblivious to its algorithm's bias or defects can accordingly learn from the forum's feedback and adjust the algorithm.[143] Actors that are less inclined to improve their algorithms are more likely to do so, because of the threat of consequences. This provides at least a minimal form of control over the conduct at stake.[144]

---

[133] Maranke Wieringa, 'What to account for when accounting for algorithms: a systematic literature review on algorithmic accountability' [2020] FAT* '20: Conference on Fairness, Accountability, and Transparency 2

[134] Reuben Binns, 'Algorithmic Accountability and Public Reason' [2018] 31(4) Philosophy & Technology 544

[135] Mark Bovens, 'Analysing and Assessing Accountability: A Conceptual Framework' [2007] 13(4) European Law Journal 452

[136] Mark Bovens, 'Analysing and Assessing Accountability: A Conceptual Framework' [2007] 13(4) European Law Journal 452

[137] Mark Bovens, 'Analysing and Assessing Accountability: A Conceptual Framework' [2007] 13(4) European Law Journal 452

[138] Revadee Vyravene and Fazlul K Rabbanee, 'Corporate negative publicity – the role of cause related marketing' [2016] 24(4) Australasian Marketing Journal 323

[139] Revadee Vyravene and Fazlul K Rabbanee, 'Corporate negative publicity – the role of cause related marketing' [2016] 24(4) Australasian Marketing Journal 323

[140] Maranke Wieringa, 'What to account for when accounting for algorithms: a systematic literature review on algorithmic accountability' [2020] FAT* '20: Conference on Fairness, Accountability, and Transparency 2

[141] Maranke Wieringa, 'What to account for when accounting for algorithms: a systematic literature review on algorithmic accountability' [2020] FAT* '20: Conference on Fairness, Accountability, and Transparency 2

[142] Mark Bovens, 'Two Concepts of Accountability: Accountability as a Virtue and as a Mechanism' [2010] 33(5) West European Politics 954-955

[143] Mark Bovens, 'Two Concepts of Accountability: Accountability as a Virtue and as a Mechanism' [2010] 33(5) West European Politics 954-955

[144] Mark Bovens, 'Two Concepts of Accountability: Accountability as a Virtue and as a Mechanism' [2010] 33(5) West European Politics 954-955

It is additionally notable that transparency and accountability are occasionally used as synonyms. However, transparency cannot be equated to accountability.[145] Transparency may for instance be achieved without the need for a specific forum to pose questions. Issues of accountability are therefore not merely issues of transparency.[146] Transparency may however form a mechanism that assists accountability and therefore may form a concept that relates to accountability.[147]

2.2.4 Accountability in the GDPR

This thesis focuses on accountability in relation to the data protection impact assessment of the GDPR. Accountability is one of the key principles of the GDPR.[148] According to the WP29, accountability in this context is referred to as the implementation of measures to be taken by data controllers to ensure compliance with the data protection principles.[149] It includes both the measures taken to comply with the data protection principles and the obligation to demonstrate these measures to data protection authorities.[150] The principle intends to bridge the theoretical data protection principles and actual data protection.[151] This notion of accountability can be compared to the definition of accountability that is provided by Bovens. To demonstrate the similarities, the forum is the data protection authorities, and they have a relationship with the actor, which is the data controller. The data controller is obliged to explain or justify his conduct, which is the measures taken to comply with the data protection principles. The data protection authority may then interact with the data controller about its explanation or justification and has furthermore the power to impose sanctions.[152] The definition of Bovens of accountability, therefore, corresponds with the concept of accountability in the GDPR. The relation between the concept of accountability and the GDPR's data protection measures will be explained more elaborately in Chapter 3.

2.3 Conclusion

In this Chapter, the concepts of algorithmic decision-making and algorithmic accountability have been explored. It has been stated that algorithmic decision-making may be problematic, due to its proneness to bias, its ability to make mistakes, and the possibility to be used in the wrong way. Accountability was then introduced as a mechanism to correct bias and detect mistakes. Finally, the principle of accountability in the GDPR was explained. The next chapter will explain the second concept central to the research question: the Data Protection Impact Assessment.

---

[145] Mark Bovens, 'Analysing and Assessing Accountability: A Conceptual Framework' [2007] 13(4) European Law Journal 453

[146] Mark Bovens, 'Analysing and Assessing Accountability: A Conceptual Framework' [2007] 13(4) European Law Journal 453

[147] Nicholas Diakopoulos, 'Accountability in Algorithmic Decision Making' [2016] 59(2) Communications of the ACM 58

[148] Article 5(2) GDPR

[149] Article 29 Working Party, 'Opinion 3/2010 on the principle of accountability' (WP 173, 13 July 2010) 8

[150] Article 29 Working Party, 'Opinion 3/2010 on the principle of accountability' (WP 173, 13 July 2010) 9

[151] Article 29 Working Party, 'Opinion 3/2010 on the principle of accountability' (WP 173, 13 July 2010) 10

[152] Article 29 Working Party, 'Opinion 3/2010 on the principle of accountability' (WP 173, 13 July 2010) 17

Chapter 3 – Data Protection Impact Assessment

This chapter will explain the Data Protection Impact Assessment (DPIA) as required in Article 35 GDPR and will answer the second sub-question: *What is a data protection impact assessment as is required in article 35 GDPR?* It is necessary to explain the DPIA and understand its obligations in order to examine its impact on algorithmic accountability. This chapter will first elaborate on the GDPR itself and its relation to algorithms. Then, the background of the DPIA will be discussed, followed by when the DPIA is required and what it entails.

3.1 The GDPR and algorithms

Personal data has become increasingly valuable and commercialized.[153] The many possibilities to process and commercialize data call for a strong regulatory regime and have created a need for harmonization.[155] This has led to the development of the GDPR, which constitutes an important milestone in the improvement of data protection in the European Union.[156] It replaced the 1995 Data Protection Directive (DPD), which was developed and put in place in the early stages of the internet.[157] The GDPR came into force on 25 May 2018 and its goal is to protect the fundamental rights, particularly the right to privacy, of subjects of data processing.[158]

The GDPR applies to the processing of personal data which is fully or partially automated processing of personal data or processing of personal data which forms part of a filing system.[159] Algorithms make use of personal data at different stages. In the training stage, personal data can be used in the form of training data.[160] Not all training data contains personal data. An algorithm that is trained to recognize dogs, for instance, may require training data with pictures of dogs. This is not personal data, since the data does not concern a natural person.[161] An algorithm for facial recognition, on the other hand, will be trained on a large amount of personal data.[162] Second, the input data for an operating algorithm may contain or consists of personal data.[163] For instance, an algorithm that has been trained on the basis of personal data for facial recognition, then received input data in the form of passports to apply its facial recognition capacities.[164] Lastly, the output data may contain personal data. For example, an algorithm that receives input data that a person has a European last name and

---

[153] Daniel Rücker and Tobias Kugler, New European General Data Protection Regulation: A Practitioner's Guide (1 edn, Hart Publishing 2017) 1

[155] Daniel Rücker and Tobias Kugler, New European General Data Protection Regulation: A Practitioner's Guide (1 edn, Hart Publishing 2017) 1

[156] Daniel Rücker and Tobias Kugler, New European General Data Protection Regulation: A Practitioner's Guide (1 edn, Hart Publishing 2017) 1

[157] European data protection supervisor (EDPS), 'The History of the General Data Protection Regulation' (EDPS Europe, 2021) <https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en> accessed 8 September 2021

[158] Bart W Schermer and others, Handleiding Algemene verordening gegevensbescherming (Ministerie van Justitie en Veiligheid 2018) 9

[159] Article 2(1) GDPR

[160] Michael Veale and others, 'Algorithms that remember: model inversion attacks and data protection law' [2018] 376(1) Philosophical Transactions of the Royal Society A

[161] Article 4(1) GDPR

[162] Dirk Brand, 'Algorithmic Decision-making and the Law' [2020] 12(1) EJournal of eDemocracy and Open Government 122

[163] Tobias D Krafft and others, 'How to regulate algorithmic decision-making: A framework of regulatory requirements for different applications' [2022] 16(1) Regulation & Governance 123

[164] Dirk Brand, 'Algorithmic Decision-making and the Law' [2020] 12(1) EJournal of eDemocracy and Open Government 122

a many Dutch Facebook friends and consequently produces output data that claims the person is likely Dutch, produces personal data. The GDPR, therefore, applies in these situations. The data protection impact assessment, as adopted in the GDPR, is therefore also relevant to algorithmic decision-making.

3.2 Background of the DPIA

The first privacy impact assessments were carried out in Canada, New Zealand, and Australia in the 1990s.[165] Privacy impact assessments have since then spread widely across various regulatory areas.[166] Unsurprisingly, an impact assessment has also been included in the GDPR, as it has often been thought of as best practice by regulators[167] and has proven effective in environmental law[168].

Article 35 GDPR requires data controllers to conduct a DPIA when they are engaged in the processing of data that is likely to result in a high risk to the rights and freedoms of natural persons. This requirement is in line with the objective of the GDPR to safeguard the protection of fundamental rights and freedoms, especially those relating to data protection, of natural persons.[169] As stated in recital 84 GDPR, it serves as a mechanism to evaluate the origin, nature, particularity, and severity of the risks of data processing activities. It furthermore constitutes an accountability mechanism, as the outcomes of the DPIA are part of demonstrating compliance with the GDPR. A failure of conducting or correctly conducting the DPIA, for instance by lacking implementation of mitigation measures, may lead to a fine of up to 10 million or, if higher, 2 percent of the total worldwide annual turnover of the preceding financial year.[170]

3.3 When is a DPIA required?

A DPIA is required when there is a high risk to a natural person's rights and freedoms. This includes risks that are physical, material, or non-material[171] and of a social or economic nature[172]. Article 35 GDPR further provides a non-exhaustive list of personal data processing activities that are considered high risk: systemic and extensive personal data processing on which decisions are based that produce legal effects or similarly significantly affect natural persons, processing on a large scale of special categories of data or personal data relating to criminal convictions and offenses and finally, systemic monitoring of a publicly accessible area on a large scale. This list is non-exhaustive and other data processing activities can also be considered high risk. The WP29, a body of the European Data Protection Board that

---

[165] Eleni Kosta, Data protection impact assessment. in , The EU General Data Protection Regulation (GDPR): A Commentary (Oxford University Press 2020) 668-669

[166] Eleni Kosta, Data protection impact assessment. in , The EU General Data Protection Regulation (GDPR): A Commentary (Oxford University Press 2020) 668-669

[167] It governance privacy team and others, EU General Data Protection Regulation (GDPR) - an Implementation and Compliance Guide (4 edn, ITGP 2020) 201

[168] Yifat Nahmias and Maayan Perel, 'The Oversight of Content Moderation by AI: Impact Assessments and Their Limitations' [2021] 58(1) Harvard Journal on Legislation 158

[169] Eleni Kosta, Data protection impact assessment. in The EU General Data Protection Regulation (GDPR): A Commentary (Oxford University Press 2020) 668

[170] Eleni Kosta, Data protection impact assessment. in The EU General Data Protection Regulation (GDPR): A Commentary (Oxford University Press 2020) 666; Article 29 Working Party, '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, 4 April 2017) 4

[171] Recital 75 GDPR

[172] Paul Reuter, The General Data Protection Regulation (GDPR): An EPSU briefing (1 edn, EPSU 2019) 25

handles data protection issues since the GDPR has been in force[173], has published guidelines on the DPIA.[174] The following ten criteria have been identified to establish high risk:

- "Evaluation or scoring
- Automated decision-making with legal or similar significant effect
- Systemic monitoring
- Sensitive data
- Data processed on a large scale
- Datasets that have been matched or combined
- Data concerning vulnerable data subjects
- Innovative use or applying technological or organizational solutions
- Data transfer across borders outside the European Union
- Preventing data subjects from exercising a right or using a service or a contract"[175]

According to WP29, high risk is more likely to occur as more criteria are met.[176] Data processing activities are likely to constitute a high risk and therefore require a DPIA, when it meets at least two criteria.[177] However, the criteria reflect cases that frequently possibly generate high risk. Therefore, it may be advisable to consider data processing high risk and carry out a DPIA when any one criteria is met.[178] Aside from the WP29 guidelines, National Data Protection Authorities may provide lists of processing activities that do or do not constitute a high risk.[179]

3.4 What is a DPIA?

It will now be explained what a DPIA is. Article 35 GDPR states the responsible actor for conducting a DPIA is the data controller. The DPIA needs to be conducted prior to the processing activities.[180] The WP29 advises launching the conducting of the DPIA in the early stages of the design of the processing activities to adequately protect the rights and freedoms of the data subjects.[181] After a DPIA has been conducted, the data controller needs to monitor whether new risks that have not been addressed in the DPIA arise. In case these new risks arise, an assessment is required to determine whether the processing is still in accordance with the DPIA. Assessing the risks of data processing is therefore a continuous process that covers the entire life span of the processing activities.[184]

---

[173] European data protection board, 'Article 29 Working Party' (EDPB Europa) <https://edpb.europa.eu/about-edpb/more-about-edpb/article-29-working-party_en> accessed 8 September 2021

[174] Article 29 Working Party, '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, 4 April 2017)

[175] Article 29 Working Party, '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, 4 April 2017) 7-9

[176] Article 29 Working Party, '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, 4 April 2017) 9

[177] Article 29 Working Party, '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, 4 April 2017) 9-10

[178] Eleni Kosta, Data protection impact assessment. in , The EU General Data Protection Regulation (GDPR): A Commentary (Oxford University Press 2020) 674

[179] Article 4 GDPR; Article 5 GDPR

[180] Article 35(1) GDPR; Article 10 GDPR

[181] AH Pool, 'Artikel 35 Gegevensbeschermingseffectbeoordeling' [2019] Arbeidsovereenkomst 18

[184] AH Pool, 'Artikel 35 Gegevensbeschermingseffectbeoordeling' [2019] Arbeidsovereenkomst 18

Article 35 GDPR lays down what is minimally required in the GDPR: a systemic description of the purposes and envisaged processing operations and, where applicable, the legitimate interest pursued by the controller; an assessment of the necessity and proportionality; an assessment of the risks to the rights and freedoms of the data subject; and the measures envisaged to address the risks. Addressing the risks must include safeguarding security measures and mechanisms establishing data protection and demonstrating compliance. The controller is obliged to consider the views of data subjects or their representatives. In seeking the views of the data subjects, the data controller may take into account the protection of commercial or public interests or the security of processing operations.[185] It is not required to seek the views of the data subject where it is not appropriate to do so.[186] According to the WP29, this is for instance the case where seeking the views of the data subjects is not proportional or where the confidentiality of the company plans may be compromised.[187] Seeking the views of data subjects does not prevent the data controller from deviating from the views of the data subjects in its final decision. However, their reasoning for deviation must be documented.[188] Lastly, advice will be sought from the data protection officer (DPO), in case one has been designated.[189] The advice of the DPO must be documented.

National supervisory authorities need to be consulted when the DPIA exposes high residual risks.[190] High residual risks arise when the data controller is unable to put in place measures that sufficiently mitigate the risks that are revealed by the DPIA.[191] This is, for instance, the case where the data processing can lead to irreversible consequences with large impact on the lives of data subjects.[192]

3.5 Conclusion

This chapter has answered the second sub-question: *what is a data protection risk assessment as is required in article 35 GDPR?* In summary, a DPIA is required when the processing of data is likely to result in a high risk to the rights and freedoms of natural persons. When a DPIA is required, it needs to be conducted prior to data processing and then the processing needs to be continuously monitored for new risks. The GDPR provides a list of what is minimally required for the DPIA, including an assessment of the necessity and proportionality and an assessment of the risks to the rights and freedoms of the data subject.

---

[185] Article 35(9) GDPR

[186] Article 35(9) GDPR

[187] AH Pool, 'Artikel 35 Gegevensbeschermingseffectbeoordeling' [2019] Arbeidsovereenkomst 20

[188] AH Pool, 'Artikel 35 Gegevensbeschermingseffectbeoordeling' [2019] Arbeidsovereenkomst 20

[189] Article 35(2) GDPR

[190] Article 36(1) GDPR

[191] Article 29 Working Party, '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, 4 April 2017) 19

[192] Article 29 Working Party, '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, 4 April 2017) 19

Chapter 4 – How the DPIA increases accountability

The previous two chapters have described algorithmic accountability and the DPIA. In this chapter, the following sub-question will be answered: *How does a data protection risk assessment increase the accountability of data controllers with respect to algorithmic decision-making?* To determine to what extent the DPIA is effective in increasing accountability, it is necessary to determine the elements of it that are contributing to accountability. The next chapter will then look at the limitations of the DPIA in increasing accountability. This chapter will first look at how the DPIA contributes to transparency and how transparency subsequently contributes to accountability. Then, it will be explained how accountability is supported by the conditions for conducting a DPIA. The choice of legislative instrument will then be discussed. Last, this chapter will demonstrate how the forums function in relation to the DPIA.

4.1 Transparency

The first argument in support of the DPIA increasing accountability, is that it contributes to transparency. This relation is often put forward in the literature as a given; a DPIA contributes to transparency and accountability.[193] This assumption, however, does require examination and explanation.

It is first necessary to explain *what is meant by transparency*. In the literature, transparency is the subject of many articles, but one overarching definition of it misses.[194] In relation to private organizations, transparency has been researched in the context of many different relations – such as business to consumer and business to financer – and definitions range from broad to specific.[195] Common notions in most definitions include openness, insight, and clarity.[196] These notions are used to define transparency in both scientific research and general public discourse.[197]

Additionally, transparency in the literature – particularly in the literature concerning organizational transparency – is often used in relation to the generating and demanding of information.[198] Information is described as an essential component for transparency across the wide variety of definitions in the literature and is described as an important and consistent element of it.[199] For instance, Schnackenberg and Tomlinson define transparency as "the perceived quality of intentionally shared information from a sender"[200] and Rawlins refers to the purposeful communication of "all legally releasable information—whether positive or

---

[193] It governance privacy team and others, EU General Data Protection Regulation (GDPR) - an Implementation and Compliance Guide (4 edn, ITGP 2020) 201; Maranke Wieringa, 'What to account for when accounting for algorithms: a systematic literature review on algorithmic accountability' [2020] FAT* '20: Conference on Fairness, Accountability, and Transparency

[194] Andrew K Schnackenberg and Edward C Tomlinson, 'Organizational Transparency: A New Perspective on Managing Trust in Organization-Stakeholder Relationships' [2014] 42(6) Journal of Management 2

[195] Andrew K Schnackenberg and Edward C Tomlinson, 'Organizational Transparency: A New Perspective on Managing Trust in Organization-Stakeholder Relationships' [2014] 42(6) Journal of Management 3

[196] Lars Thøger Christensen and George Cheney, 'Peering into Transparency: Challenging Ideals, Proxies, and Organizational Practices' [2015] 25(1) Communication Theory 73

[197] Lars Thøger Christensen and George Cheney, 'Peering into Transparency: Challenging Ideals, Proxies, and Organizational Practices' [2015] 25(1) Communication Theory 73

[198] Lars Thøger Christensen and George Cheney, 'Peering into Transparency: Challenging Ideals, Proxies, and Organizational Practices' [2015] 25(1) Communication Theory 73-74

[199] Andrew K Schnackenberg and Edward C Tomlinson, 'Organizational Transparency: A New Perspective on Managing Trust in Organization-Stakeholder Relationships' [2014] 42(6) Journal of Management 5

[200] Andrew K Schnackenberg and Edward C Tomlinson, 'Organizational Transparency: A New Perspective on Managing Trust in Organization-Stakeholder Relationships' [2014] 42(6) Journal of Management 5

negative in nature—in a manner that is accurate, timely, balanced, and unequivocal"[201]. It particularly concerns the exchange of information between affected stakeholders that generates understanding and clarity about, in this case, the algorithm.[202] The more clarity the information provides, the more transparency exists.[203] Similar views on transparency can be observed in the GDPR, since the transparency implementing articles consist of information provision to data subjects (Articles 12 and 13) and the communication of data breaches to supervisory authorities and, in some cases, data subjects (Article 34).[204]

Taken together, transparency can be defined as the generation of visibility and understandability through information.[205] In this definition, transparency is referred to as a process. Central to this process is the creation of openness within the organization and towards outsiders.[206] The process brings to light otherwise unknown aspects of an algorithm.[207] On the other hand, transparency can also be referred to as the outcome of a process. For instance, in the literature, transparency is sometimes referred to as the situation where stakeholders are provided with all accessible and relevant information promptly.[208] A transparent process where a system is made visible and understandable, allows for a transparent outcome where stakeholders are provided with all information.

The purpose of transparency in the context of algorithmic decision-making is to create awareness of what the system is doing by providing visibility.[209] As a consequence of awareness, transparency furthermore allows evaluation of the system.[210] Users of the system can interpret the outputs and decide whether they are, for example, arbitrary or well-reasoned.[211] As will be argued later, transparency is then capable of creating governance of the system through accountability.

Transparency subsequently contributes to accountability by facilitating access to information that allows explaining or justifying the conduct that the DPIA concerns.[212] The data controller is best equipped to evaluate their own data processing activities.[213] This is because the data controller has more knowledge and resources to examine the data processing

---

[201] Brad Rawlins, 'Give the Emperor a Mirror: Toward Developing a Stakeholder Measurement of Organizational Transparency' [2008] 21(1) Journal of Public Relations Research 75

[202] Andrew K Schnackenberg and Edward C Tomlinson, 'Organizational Transparency: A New Perspective on Managing Trust in Organization-Stakeholder Relationships' [2014] 42(6) Journal of Management 5

[203] Andrew K Schnackenberg and Edward C Tomlinson, 'Organizational Transparency: A New Perspective on Managing Trust in Organization-Stakeholder Relationships' [2014] 42(6) Journal of Management 9

[204] Article 29 Working Party, 'Guidelines on transparency under Regulation 2016/679' (WP260, 11 April 2018)

[205] Emilee Rader and others, 'Explanations as Mechanisms for Supporting Algorithmic Transparency' [2018] 103(1) CHI '18: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems 2

[206] Monica Blagescu and others, Pathways to Accountability: The GAP Framework (One World Trust 2005) 30

[207] Emilee Rader and others, 'Explanations as Mechanisms for Supporting Algorithmic Transparency' [2018] 103(1) CHI '18: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems 1

[208] Monica Blagescu and others, Pathways to Accountability: The GAP Framework (One World Trust 2005) 30; Mark Bovens, 'Two Concepts of Accountability: Accountability as a Virtue and as a Mechanism' [2010] 33(5) West European Politics 959; S Berthold and others, 'Crime and Punishment in the Cloud Accountability, Transparency, and Privacy' [2013] 1(1) Political Science 4

[209] Emilee Rader and others, 'Explanations as Mechanisms for Supporting Algorithmic Transparency' [2018] 103(1) CHI '18: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems 3

[210] Emilee Rader and others, 'Explanations as Mechanisms for Supporting Algorithmic Transparency' [2018] 103(1) CHI '18: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems 3

[211] Emilee Rader and others, 'Explanations as Mechanisms for Supporting Algorithmic Transparency' [2018] 103(1) CHI '18: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems 3

[212] Hans Krause Hansen and others, 'Introduction: Logics of transparency in late modernity: Paradoxes, mediation and governance' [2015] 18(2) European Journal of Social Theory 118

[213] Els Kindt, 'Transparency and Accountability Mechanisms for Facial Recognition' (GMFUS, 3 February 2021) <https://www.gmfus.org/news/transparency-and-accountability-mechanisms-facial-recognition> accessed 14 February 2022

activities than, for instance, a governmental supervisory authority.[214] Transparency then is a means to achieve accountability.[215] As has been explained in chapter 2, explanation and justification of conduct constitute elements of accountability.[216] In cases where a company publishes the DPIA or communicates it to the supervisory authority, it allows these parties to pose questions and pass judgment, as will be further explained in paragraph 4.4.[217] The information that the DPIA generates allows the forum to make an informed decision.[218] As has been explained, however, transparency as an outcome is not fully achieved, since disclosure to stakeholders is typically not mandatory. This does have consequences for accountability and will be further discussed in Paragraph 5.1.3.

It should further be noted that transparency in itself is not sufficient to establish accountability. Without a forum capable of assessing the information and passing judgment, transparency brings to light harmful practices without discontinuing them.[219] Transparency in itself can then cause public cynicism and ongoing harm.[220] It is, however, not argued here that transparency itself is sufficient. Accountability consists of multiple elements, including the provision of elements, but additionally a functioning forum and an ability to pass judgment. Transparency contributes to the elements and therefore it is argued that it contributes to accountability as a whole.

Now the concept of transparency and its relation to accountability has been explained, it will now be described *how DPIA increases transparency*. Many authors have stated that a DPIA increases transparency and accountability.[221] For instance, the WP29 has identified transparency as a purpose of the DPIA,[222] and organizations and governments pledge to conduct DPIAs in support of transparency.[223] By conducting a DPIA, aspects of the algorithm are made visible. A data controller can for example discover that certain third parties have access to personal data that it is not required to access for the legitimate aim.[224] The data controller can, on the basis of this information, strengthen its access control mechanisms, such as its access policies.[225] In the situation where the data controller had discovered the

---

[214] Els Kindt, 'Transparency and Accountability Mechanisms for Facial Recognition' (GMFUS, 3 February 2021) <https://www.gmfus.org/news/transparency-and-accountability-mechanisms-facial-recognition> accessed 14 February 2022

[215] Lars Thøger Christensen and George Cheney, 'Peering into Transparency: Challenging Ideals, Proxies, and Organizational Practices' [2015] 25(1) Communication Theory 71

[216] Paragraph 2.2.3

[217] Monica Blagescu and others, Pathways to Accountability: The GAP Framework (One World Trust 2005) 30; Mark Bovens, 'Two Concepts of Accountability: Accountability as a Virtue and as a Mechanism' [2010] 33(5) West European Politics 959; S Berthold and others, 'Crime and Punishment in the Cloud Accountability, Transparency, and Privacy' [2013] Political Science 23

[218] Lars Thøger Christensen and George Cheney, 'Peering into Transparency: Challenging Ideals, Proxies, and Organizational Practices' [2015] 25(1) Communication Theory 71

[219] Mike Ananny and Kate Crawford, 'Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability' [2018] 20(3) New Media & Society 978

[220] Mike Ananny and Kate Crawford, 'Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability' [2018] 20(3) New Media & Society 978

[221] It governance privacy team and others, EU General Data Protection Regulation (GDPR) - an Implementation and Compliance Guide (4 edn, ITGP 2020) 201; Maranke Wieringa, 'What to account for when accounting for algorithms: a systematic literature review on algorithmic accountability' [2020] FAT* '20: Conference on Fairness, Accountability, and Transparency

[222] Article 29 Working Party, '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, 4 April 2017) 19

[223] Lars Thøger Christensen and George Cheney, 'Peering into Transparency: Challenging Ideals, Proxies, and Organizational Practices' [2015] 25(1) Communication Theory 71

[224] NOREA, NOREA Handreiking Data Protection Impact Assessment (2 edn, NOREA 2020) 65-66

[225] Antonello Calabrò and others, 'Integrating Access Control and Business Process for GDPR Compliance: A Preliminary Study' [2019] ITASEC19 - Italian Conference on Cybersecurity

information prior to the data processing, the actor could have implemented the access barriers at an early stage and avoided the compliance breach.[226] The DPIA generates information that consequently brings about access to knowledge and insight.[227] The information that a correctly conducted DPIA brings forth is: a description of the envisaged processing operations and the purposes of the processing, an assessment of the necessity and proportionality of the processing, an assessment of the risks to the rights and freedoms of the data subjects and finally the measures envisaged to address the risks and demonstrate compliance with the GDPR.[228] If the GDPR did not require this information to be generated, the information may not have come to light.

The sole generation of information makes parts of a system visible, but only to whoever has access to the information. The DPIA is limited to generating and organizing information and does not concern with the disclosure of it to stakeholders. As opposed to transparency related provisions such as Article 12 and 13, the DPIA is not concerned with information provision to stakeholders, such as the data subject. It, therefore, does not constitute a process of opening the organization, which is related to transparency as a process. The openness of an organization, is, however, more closely related to the outcome of the process. The generation of information can be seen as the first step towards transparency. A DPIA therefore to that extent constitutes a process that increases transparency.

Transparency is particularly critical for algorithmic accountability, because of the algorithm's black box character. Algorithms, particularly the advanced type, are inherently complex.[229] The opaque character of algorithms hinders accountability, since the forum, for instance, a court, is unable to ask questions and pass judgment due to lacking understandable information.[230] Transparency is particularly important for algorithmic data processing, because of the previously explained proneness to bias and potential to have large impact on people's lives.

The GDPR does not require the DPIA to be made public or communicated to stakeholders.[231] It is, however, advised to make the DPIA or a summary of it public.[232] Furthermore, the supervisory authority needs to be consulted when there is a residual risk.[233] Since the publication of the DPIA is voluntary and consultation with the supervisory authority is only required when there is a residual risk, it cannot be stated that all stakeholders are provided with all accessible and relevant information promptly. Therefore, transparency as an outcome is not fully accomplished by article 35 GDPR. A fully transparent outcome is, however, more likely to be achieved when a DPIA is conducted. This is because the

---

[226] Antonello Calabrò and others, 'Integrating Access Control and Business Process for GDPR Compliance: A Preliminary Study' [2019] ITASEC19 - Italian Conference on Cybersecurity; Article 32 GDPR

[227] Hans Krause Hansen and others, 'Introduction: Logics of transparency in late modernity: Paradoxes, mediation and governance' [2015] 18(2) European Journal of Social Theory 118

[228] Article 29 Working Party, '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, 4 April 2017) 16

[229] C Adriaansz and E Studer, 'Betekenisvolle transparantie voor algoritmische besluitvorming' [2020] 43(2) Computerrecht 2

[230] C Adriaansz and E Studer, 'Betekenisvolle transparantie voor algoritmische besluitvorming' [2020] 43(2) Computerrecht 3

[231] Article 29 Working Party, '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, 4 April 2017) 18

[232] Article 29 Working Party, '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, 4 April 2017) 18

[233] Article 29 Working Party, '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, 4 April 2017) 18

information that is generated by the DPIA allows for a situation where stakeholders can obtain all relevant information. Private parties can obtain information through legal proceedings and supervisory authorities can obtain access to the DPIA by requesting it.[234] A fully transparent outcome where stakeholders have access to all relevant information, is not possible when the relevant information does not exist. A DPIA, therefore, constitutes transparency as a process and is capable of contributing to transparency as an outcome.

Therefore, a DPIA contributes to transparency that subsequently increases the accountability of data controllers. The generated transparency then leads to an obligation to implement mitigation measures to limit harm.[244] In the next paragraph, the effectiveness of the DPIA in relation to these mitigation measures will be explained.

4.2 The timing of a DPIA

Algorithmic accountability is further supported by conditions under which a DPIA is required. As has been explained in Chapter 3, a DPIA is required at an early stage of the design process. This aligns the requirements of the DPIA with the *data protection by design* duty in article 25 GDPR. Data protection by design requires data controllers to incorporate the data protection principles into the design and development stage of data processing systems.[245] The idea behind this is that the data protection principles can be better implemented in an early stage of the design process.[246] This recognizes the regulatory capacity of the design, which can be more successful than legal regulation.[247] Data protection by design can therefore be explained in line with Lessig's widely excepted four modalities of regulation; law, markets, norms, and architecture.[248] Considering data protection in the early stages of development, allows building data protection into the 'architecture' of the algorithm. Regulation by architecture is particularly effective because it is self-executing, at least to some extent.[249] For example, if an algorithmic decision-making system is not built to ask the subject of the decision-making for their postal address, it simply will not gather this information. No further action is required to protect this personal data. Some examples of regulation by architecture, however, do require some action to comply.[250] For instance, when a user of a program can allow the program to ask for the user's postal address, further action is required to protect the personal data. Therefore regulation by architecture is not consistently fully self-executing, but it is self-executing to some extent. This is desirable, because it does not necessitate enforcement to the extent it is self-executing.[251] Deviation of the norm is simply not possible or limited due to the self-executing character.

To implement the data protection principles into a new system, it is necessary to conduct impact assessments to determine what elements of the system require adjustments to

---

[234] Articles 78 and 79 GDPR; Article 29 Working Party, '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, 4 April 2017) 18

[244] Article 35(7)(d) GDPR

[245] Lee A Bygrave, Article 25 Data protection by design and by default. in , The EU General Data Protection Regulation (GDPR): A Commentary (Oxford University Press 2020) 573

[246] Lee A Bygrave, Article 25 Data protection by design and by default. in , The EU General Data Protection Regulation (GDPR): A Commentary (Oxford University Press 2020) 573

[247] Lee A Bygrave, Article 25 Data protection by design and by default. in , The EU General Data Protection Regulation (GDPR): A Commentary (Oxford University Press 2020) 573

[248] Lawrence Lessig, Code and Other Laws of Cyberspace (Basic Books 1999) 88

[249] Andrew Murray and Colin Scott, 'Controlling the New Media: Hybrid Responses to New Forms of Power' [2002] 65(4) The Modern Law Review 500

[250] Andrew Murray and Colin Scott, 'Controlling the New Media: Hybrid Responses to New Forms of Power' [2002] 65(4) The Modern Law Review 501

[251] Andrew Murray and Colin Scott, 'Controlling the New Media: Hybrid Responses to New Forms of Power' [2002] 65(4) The Modern Law Review 503-504

ensure the implementation of the data protection principles.[252] In short, *a DPIA is capable of pinpointing where privacy can be implemented by design*. This is cost-effective, as it would be more expensive to adjust a design of a system at a later stage.[253] For instance, if data protection concerns that cannot be overcome, arise during the early stages of the design of a system, there will be fewer sunk costs than when the concerns would have arisen during a later stage.[254] It is additionally effective as it is mostly self-executing, as has been explained above.

Privacy by design is an important element of the principle of accountability.[255] For impact assessments to increase accountability, there must be an appropriate *theory of change*.[256] This means that an impact assessment is conducted at a point in time where it is possible to adjust the system according to the outcomes of the assessment.[257] A DPIA that is carried out too late runs the risk of not identifying residual risk and consequently supervisory authorities not being consulted.[258] Privacy by design allows the data controller to be held accountable, as it is capable of changing its conduct and ensuring compliance at a stage where change is still possible. It should be noted, however, that Article 35 requires the DPIA to be conducted before the processing, but not before the design of the system.

Impact assessment is regularly conducted after the main elements of the design have been established.[259] Ideally, the DPIA provokes the development of more privacy-friendly alternatives.[260] In reality, however, firms are unwilling to drastically change the data processing after the main elements of the design have been set, due to high cost and organizational commitment.[261] It is, therefore, necessary to effectively implement privacy by design to conduct the DPIA before setting the main design elements. This has been recognized by the WP29, but is not a requirement in Article 35.[262] The benefits of privacy by design in the DPIA for accountability are therefore conditional on the early conducting – prior to the setting of the main design elements – of the DPIA.

The DPIA is furthermore an *ongoing exercise*, which means that the DPIA requires updating throughout the lifecycle of the system.[263] As explained above, it is important to conduct a DPIA at an early stage of system development. However, it is furthermore essential to also conduct a DPIA in later stages. For instance, a premature impact assessment may not

---

[252] Ann Cavoukian, 'Privacy by Design: The 7 Foundational Principles: Implementation and Mapping of Fair Information Practices' [2006] 1(1) Creation of a Global Privacy Standard 3

[253] David Wright and Paul De Hert, Privacy Impact Assessment (6 edn, Springer 2012) 17

[254] David Wright and Paul De Hert, Privacy Impact Assessment (6 edn, Springer 2012) 17

[255] Christopher Kuner and others, The EU General Data Protection Regulation (GDPR): A Commentary (Oxford University Press 2020) 576

[256] Emanuel Moss and others, 'Assembling Accountability: Algorithmic Impact Assessment for the Public Interest' [2021] 1(1) SSRN Electronic Journal 18-19

[257] Emanuel Moss and others, 'Assembling Accountability: Algorithmic Impact Assessment for the Public Interest' [2021] 1(1) SSRN Electronic Journal 18-19

[258] Emanuel Moss and others, 'Assembling Accountability: Algorithmic Impact Assessment for the Public Interest' [2021] 1(1) SSRN Electronic Journal 18-19

[259] Nigel Waters, Privacy Impact Assessment - Great Potential Not Often Realised. in David Wright and Paul De hert (eds), Privacy Impact Assessment (Springer 2012) 150-151

[260] Nigel Waters, Privacy Impact Assessment - Great Potential Not Often Realised. in David Wright and Paul De hert (eds), Privacy Impact Assessment (Springer 2012) 150-151

[261] Nigel Waters, Privacy Impact Assessment - Great Potential Not Often Realised. in David Wright and Paul De hert (eds), Privacy Impact Assessment (Springer 2012) 150-151

[262] Article 29 Working Party, '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, 4 April 2017) 14

[263] Article 29 Working Party, '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, 4 April 2017) 14

be able to assess important parts of the system that are developed later or identify risks that arise at a later stage.[264] Furthermore, ex-post impact assessments are useful to learn from the past to avoid repeating the same mistake, by, for instance, embedding the same bias into an algorithm.[265] This contributes to transparency, as they bring to light information, which consequently contributes to accountability. By updating the DPIA throughout the entire lifecycle of the system, transparency is increased and consequently increases accountability as well.[266]

Even *when a DPIA is ultimately not conducted*, the documentation of investigating whether a DPIA is required already contributes to accountability by increasing transparency.[267] A DPIA is required when data processing is likely to result in a high risk to the rights and freedoms of natural persons.[268] To determine whether a DPIA is required, data controllers, therefore, need to conduct an assessment of whether the data processing is likely to result in a high risk. Even if the outcome is negative, the documentation allows for visibility that contributes to accountability.

Therefore the timing of the DPIA – starting at an early stage and carried out throughout the lifecycle of the system – contributes to accountability. The effects of privacy by design of the DPIA on accountability are, however, conditional on the data controller conducting the DPIA before setting the main elements of the design. The assessment conducted to decide whether a DPIA is required further contributes to accountability.

4.3 Legislative instrument

Algorithmic accountability is further increased by the DPIA, because of the form of regulation that is used for the DPIA. Meta-regulation, a sub-form of co-regulation, can be defined as a form of regulation where the government holds private parties accountable for their undertakings of self-regulation.[269] As explained by Binns and demonstrated in Table 1, the DPIA can be considered a form of meta-regulation.

Constitutive feature of meta-regulation	Manifestation in the GDPR regime
Requires organizations to take responsibility for their self-regulation efforts	DPIAs require data controllers to assess and mitigate risks themselves (Article 35(1))
Requires organizations to undertake risk-assessment processes	A DPIA should encompass an evaluation of the risks to the rights and freedoms of individuals (Article 35(7c))
Requires organizations to identify risk-mitigation strategies	A DPIA should involve a description of 'the measures envisaged to address the risk' (Article 33(7d))
Does not prescribe specific measures or	No particular measures are prescribed – the

[264] Emanuel Moss and others, 'Assembling Accountability: Algorithmic Impact Assessment for the Public Interest' [2021] 1(1) SSRN Electronic Journal 18-19

[265] Emanuel Moss and others, 'Assembling Accountability: Algorithmic Impact Assessment for the Public Interest' [2021] 1(1) SSRN Electronic Journal 18-19

[266] Ann Cavoukian, 'Privacy by Design: The 7 Foundational Principles: Implementation and Mapping of Fair Information Practices' [2006] 1(1) Creation of a Global Privacy Standard 4-5

[267] Article 29 Working Party, '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, 4 April 2017) 12

[268] Article 29 Working Party, '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, 4 April 2017) 13

[269] Reuben Binns, 'Data protection impact assessments: a meta-regulatory approach' [2017] 7(1) International Data Privacy Law 29

technologies	controller must identify measures by themselves
Holds organizations accountable for adhering to their own policies	Controllers expected to review compliance with the measures set out in their own DPIAs (Article 35(11))
Attempts to leverage corporations' existing management procedures	The GDPR attempts to embed DPIAs in management procedures partly through DPOs (Article 39(1c))
Ensures stakeholders can democratically engage in evaluating organizations' measures and policies	Controller must seek input from data subjects or their representatives when conducting a DPIA (Article 35(9))
Liability to sanctions is related to failure to undertake the process, rather than focusing on the outcome	Undertaking a DPIA, especially if it is referred to the supervisory authority for prior consultation, is likely to significantly reduce any penalties for subsequent infringement due to the circumstances outlined in (Article 83(2))

Table 1: From Reuben Binns, 'Data protection impact assessments: a meta-regulatory approach'[271]

It is a form of regulation that involves the governmental legislative process, but also leaves room for private actors to tailor the DPIA according to the circumstances of the case and the specifics of the industry.[272] The ability of private parties to fill in the obligations of the DPIA provides flexibility for controllers to adopt the DPIA to the specific circumstances of the case.[273] The use of open language in Article 35 provides this flexibility. Aside from providing flexibility and scalability, open language supports the technologically neutral character and consequently sustainability of the regulation.[274] The DPIA can therefore be effectively conducted also when the state of the art inevitably changes.

Legal regulation that does not provide this flexibility and instead provides detailed rules increases the likelihood that controllers will engage in creative compliance.[275] This is a type of compliance that reduces the DPIA to a tick-box exercise and may prevent achieving the objective of the rules.[276] Although there is technical compliance, substantive compliance can be avoided.[277] The DPIA contains open language and therefore limits the possibility for creative compliance. Creative compliance frustrates algorithmic accountability as explained in Chapter 2, as it allows data controllers to conduct a DPIA without achieving the objective of the DPIA to identify and mitigate risks of data processing. A DPIA that is, for instance, communicated to a data protection authority that does not identify risks and lead to mitigation of these risks would avoid accountability for the algorithm.

[271] Reuben Binns, 'Data protection impact assessments: a meta-regulatory approach' [2017] 7(1) International Data Privacy Law 31
[272] Article 29 Working Party, 'Opinion 3/2010 on the principle of accountability' (WP 173, 13 July 2010), 13
[273] Reuben Binns, 'Data protection impact assessments: a meta-regulatory approach' [2017] 7(1) International Data Privacy Law 29
[274] K Demetzou, 'Data Protection Impact Assessment: A tool for accountability and the unclarified concept of 'high risk' in the General Data Protection Regulation' [2019] 35(6) Computer Law & Security Review 7-8
[275] Claudia Quelle, The Data Protection Impact Assessment: What can it contribute to data protection? (Thesis for the Research Master in Law and the Master's program Law and Technology 2013-2015 2015) 65
[276] Claudia Quelle, The Data Protection Impact Assessment: What can it contribute to data protection? (Thesis for the Research Master in Law and the Master's program Law and Technology 2013-2015 2015) 65
[277] Claudia Quelle, The Data Protection Impact Assessment: What can it contribute to data protection? (Thesis for the Research Master in Law and the Master's program Law and Technology 2013-2015 2015) 65

Furthermore, meta-regulation encourages private parties to put in place organizational structures and practices to comply with the regulation.[278] Likewise, the DPIA obliges data controllers to put in place governance structures and management practices that allow the identification and mitigation of risks. Meta-regulation seeks to regulate while recognizing the complexity of organizations.[279] It takes into consideration the notion that the data controller is best equipped to put in place organizational structures to identify and mitigate risks, because it has internal, and therefore intimate, knowledge of the specifics of the organization and the data processing.[280] Meta-regulation encourages organizations to put in place mechanisms to achieve regulatory goals and simultaneously puts in place techniques to hold the organizations responsible for their efforts to self-regulate.[283] This is done by, for instance, obliging actors to communicate their efforts to authorities. Meta-regulation, therefore, is a more effective way to create accountability as it recognizes organizational complexity.

4.4 The forum

As explained in chapter 2, accountability requires a forum that can pose questions and pass judgment, and an actor that may face consequences. Many different types of forums can exist, as different types of accountability can be identified.[284] For instance, elected representatives and voters can constitute forums in relation to political accountability.[285] For private organizations, the following types of accountability are relevant in relation to the identification of the forums: legal accountability, administrative accountability, professional accountability, and social accountability.[286]

The forum in relation to social accountability can be interest groups, charities, and other stakeholders.[287] This is the public, including the consumers and consumer organizations. Concerning professional accountability, the forum consists of professional peers, such as bodies that lay down codes of standards.[288] Although it is not required to publish the DPIA, it is good practice and additionally beneficial for companies to do so, as it promotes transparency.[289] Another benefit of publishing a DPIA is that it fosters trust among the data subjects in the company.[290] Although research about the extent to which firms publish their DPIAs is missing, firms may not be inclined to publish their DPIAs, as will be explained further in Paragraph 5.1.3.

---

[278] Christina Parker, The Open Corporation: Effective Self-regulation and Democracy (Cambridge University Press 2002) 98, 48

[279] Christina Parker, The Open Corporation: Effective Self-regulation and Democracy (Cambridge University Press 2002) 98, 48

[280] Christina Parker, The Open Corporation: Effective Self-regulation and Democracy (Cambridge University Press 2002) 98, 48, 22-23

[283] Christina Parker, The Open Corporation: Effective Self-regulation and Democracy (Cambridge University Press 2002) 98, 48

[284] Mark Bovens, 'Two Concepts of Accountability: Accountability as a Virtue and as a Mechanism' [2010] 33(5) West European Politics 455-457

[285] Mark Bovens, 'Two Concepts of Accountability: Accountability as a Virtue and as a Mechanism' [2010] 33(5) West European Politics 455

[286] Mark Bovens, 'Two Concepts of Accountability: Accountability as a Virtue and as a Mechanism' [2010] 33(5) West European Politics 455-457

[287] Mark Bovens, 'Two Concepts of Accountability: Accountability as a Virtue and as a Mechanism' [2010] 33(5) West European Politics 457

[288] Mark Bovens, 'Two Concepts of Accountability: Accountability as a Virtue and as a Mechanism' [2010] 33(5) West European Politics 456

[289] Article 29 Working Party, '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, 4 April 2017) 18

[290] Alexandra Duricu, 'Data Protection Impact Assessment (DPIA) and Risk Assessment in the context of the General Data Protection Regulation (GDPR)' [2019] Lulea University of Technology 43

Publication of the DPIA would provide the public with the information that it requires to hold the company accountable for its data processing. The public as a forum can pose questions and pass judgment to contribute to accountability. If the public finds the data processing activities problematic, the company may for instance face lawsuits[291] or boycotts[292]. It is in this case the market that constrains certain behavior.[293] The market is one of the modalities of regulation that are identified and explained by Lessig.[294] The market regulates behavior by placing a price tag on the behavior.[295] Buyers will monitor market behavior and adjust their decisions accordingly.[296] Buyers that disagree with the contents of the DPIA can consequently stop purchasing the related products. Therefore, the company can experience a reduction of trust of data subjects in the company as a negative consequence. As explained in Chapter 2, the possibility that a company faces consequences is one of the factors of accountability. This effect on accountability is, however, conditional on the publication of the DPIA, which will be further researched in Chapter 5.

It is questionable to what extent data protection issues lead to reputational damage that can cause a decline in a company's turnover.[297] Research has shown large data breaches do affect a company's turnover.[298] Public outrage has previously even led to a company's bankruptcy, as was the case of the data protection scandal of Cambridge Analytica.[299] Smaller data breaches did not have such effects.[300] This is because the response of the public depend on the many factors that determine people's attitudes towards privacy.[302] For instance, people tend to find privacy less of an urgent issue when their data is collected by an entity that they have a relationship with.[303] People are furthermore more concerned with privacy issues in general than privacy issues in specific situations where it is weighed against other values.[304] This does not mean the public functions less effectively as a forum. The public as a forum may not pass judgment as strictly as, for instance, the supervisory authorities, but this reflects the balancing of values in the specific context under scrutiny.[305] The passing of judgment by the forum, is, however, conditional on having access to information.

---

[291] Angelique Carson, 'GDPR ushers in civil litigation claims across the EU' (Iapp, 24 March 2020) <https://iapp.org/news/a/gdpr-ushers-in-civil-litigation-claims-across-the-eu/> accessed 14 February 2022

[292] Emily Tan, 'Seven out of ten customers would boycott a brand that mishandled their data' (Campaign, 9 February 2018) <https://www.campaignlive.co.uk/article/seven-ten-customers-boycott-brand-mishandled-data/1456749> accessed 14 February 2022

[293] James Grimmelmann, 'Regulation by Software' [2005] 114(7) Yale Law Journal 1725

[294] Lawrence Lessig, Code and Other Laws of Cyberspace (Basic Books 1999)

[295] James Grimmelmann, 'Regulation by Software' [2005] 114(7) Yale Law Journal 1725

[296] Andrew Murray and Colin Scott, 'Controlling the New Media: Hybrid Responses to New Forms of Power' [2002] 65(4) The Modern Law Review 500

[297] Christos A Makridis, 'Do data breaches damage reputation? Evidence from 45 companies between 2002 and 2018' [2021] 1(8) Journal of Cybersecurity 7

[298] Christos A Makridis, 'Do data breaches damage reputation? Evidence from 45 companies between 2002 and 2018' [2021] 1(8) Journal of Cybersecurity 7

[299] Nicholas Confessore, 'Cambridge Analytica and Facebook: The Scandal and the Fallout So Far' (The New York Times, 4 April 2018) <https://www-nytimes-com.tilburguniversity.idm.oclc.org/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html> accessed 14 February 2022

[300] Christos A Makridis, 'Do data breaches damage reputation? Evidence from 45 companies between 2002 and 2018' [2021] 1(8) Journal of Cybersecurity 7

[302] Daniel J Solove, 'The Myth of the Privacy Paradox' [2021] 89(1) George Washington Law Review 50-51

[303] Stefanie Pötzsch, 'Privacy Awareness: A Means to Solve the Privacy Paradox?' [2008] 298(1) IFIP Advances in Information and Communication Technology 231

[304] Stefanie Pötzsch, 'Privacy Awareness: A Means to Solve the Privacy Paradox?' [2008] 298(1) IFIP Advances in Information and Communication Technology 230

[305] Daniel J Solove, 'The Myth of the Privacy Paradox' [2021] 89(1) George Washington Law Review 50-51; Stefanie Pötzsch, 'Privacy Awareness: A Means to Solve the Privacy Paradox?' [2008] 298(1) IFIP Advances in Information and Communication Technology 230-231

Concerning administrative accountability, the forum consists of auditors, inspectors, and controllers.[306] The GDPR has as an administrative institution, the national supervisory authorities.[307] In case an impact assessment shows residual risk, the data controller should consult the national data protection authority.[308] The authority can consequently monitor compliance.[309] The authority needs to be provided with the DPIA and it can provide advice to the data controller.[310] The DPIA, therefore, allows the authority to function as a forum, as it provides information to pose questions and provide advice. Although the GDPR does not provide the authority with the power to impose instructions on the data controller, the WP29 has expressed that data protection authorities should have this power.[311] Data protection authorities, however, have other enforcement powers that generate consequences for data controllers. The authority can use the information of the DPIA to enforce the GDPR.[312] It can impose fines up to 20 million euros or 4% of the company's global annual turnover of the previous financial year.[313] Therefore the DPIA allows a data protection authority to function as a forum that has the information necessary to pose questions, pass judgment and impose fines.

The final forum is the court in relation to legal accountability. According to article 79 GDPR, data subjects can pursue legal action before the court in the member state where the data controller is situated. The national court may subsequently refer questions to the Court of Justice of the European Union (CJEU).[314] The DPIA may provide the court with information it would otherwise not be able to obtain and is required to pass judgment. Furthermore, data subjects obtain information from the DPIA. If they wish to hold the data controller accountable, data subjects can use the information of the DPIA as the basis of their legal claims.[315]

It should be noted that accountability towards the various forums exist for different topics. Supervisory authorities and the court can hold data controllers accountability only for regulatory obligations. The GDPR's data protection authorities have powers in relation to data protection law.[316] The authorities can for instance investigate and correct when a DPIA is not conducted in accordance with Article 35.[317] The public, on the other hand, can also pass judgment on all topics outside legal obligations. The public can therefore hold the data controllers accountable for a wider range of subjects.

The DPIA can, therefore, provide information to the public, the supervisory authorities, and the court, which can consequently act as a forum and pass judgment.

---

[306] Mark Bovens, 'Two Concepts of Accountability: Accountability as a Virtue and as a Mechanism' [2010] 33(5) West European Politics 456

[307] Mark Bovens, 'Two Concepts of Accountability: Accountability as a Virtue and as a Mechanism' [2010] 33(5) West European Politics 456, Article 54 GDPR

[308] Article 36(1) GDPR

[309] Article 29 Working Party, 'Opinion 3/2010 on the principle of accountability' (WP 173, 13 July 2010), 16

[310] Article 36(1), 36(3)(e)

[311] Article 29 Working Party, 'Opinion 3/2010 on the principle of accountability' (WP 173, 13 July 2010), 17

[312] Article 29 Working Party, 'Opinion 3/2010 on the principle of accountability' (WP 173, 13 July 2010), 16

[313] Article 83(5) GDPR

[314] Christos Giakoumopoulos and others, Handbook on European data protection law (European Union Agency for Fundamental Rights and Council of Europe 2018) 240-242

[315] Angelique Carson, 'GDPR ushers in civil litigation claims across the EU' (Iapp, 24 March 2020) <https://iapp.org/news/a/gdpr-ushers-in-civil-litigation-claims-across-the-eu/> accessed 14 February 2022

[316] Articles 4(16), 51-59 GDPR; Recitals 117-123 GDPR

[317] European commission, 'What are Data Protection Authorities (DPAs)?' (European Commission, 26 April 2022) <https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-are-data-protection-authorities-dpas_en> accessed 26 April 2022

4.5 Conclusion

This chapter answered the third sub-question: *How does a data protection risk assessment increase the accountability of data controllers with respect to algorithmic decision-making?* First, the DPIA contributes to creating transparency, by generating visibility and understandability of an algorithm. Subsequently, transparency contributes to accountability by bringing to light information, such as an assessment of the proportionality of the data processing. Second, the conducting of the DPIA at an early stage allows adjusting of the processing activities. It was then explained that the DPIA is a form of meta-regulation, which is a form of regulation that supports accountability. Finally, this chapter explained how the public, supervisory authorities, and in some cases the court can act as a forum.

Chapter 5 – Limitations of a DPIA in increasing algorithmic accountability

The previous chapters have outlined the concept of algorithmic accountability, the DPIA, and finally how the DPIA can contribute to increasing algorithmic accountability. In this chapter, the fourth and final sub-question will be answered: *What are the limitations of increasing accountability of data controllers with respect to algorithmic decision-making by means of a data protection risk assessment?* To answer this question, it will be first examined how the DPIA itself is limited in increasing algorithmic accountability. Second, it will be examined how accountability is limited due to the nature of algorithms. This chapter will end with a recommendation that addresses the previously demonstrated limitations.

5.1 Limitations related to the DPIA

This thesis will now demonstrate the limitations of the DPIA in increasing algorithmic accountability. First, the DPIA requires the data controllers to make normative decisions, which then, secondly, puts a lot of faith in data controllers to make choices that increase accountability. Finally, there is no adequate independent oversight.

5.1.1. The use of open language

A DPIA is required when there is a high risk to a natural person's rights and freedoms. This risk can be physical, material, or non-material[318] and of a social or economic nature[319]. The WP29 provides a list of criteria to decide whether data processing is likely to result in a high risk to a natural person's rights and freedoms.[320] This list is, however, indicative.[321] Data controllers, therefore, need to make normative decisions to determine what constitutes a risk and when to consider it a high enough risk to necessitate a DPIA.[322]

The concept of risk is critical for the obligation of conducting a DPIA and has been discussed extensively in the legal literature.[323] To determine whether a risk is high, the data controllers need to examine the likelihood and severity of the consequences of the event that the risk.[324] This is indicated in Recitals 75 and 76 of the GDPR and repeated by the WP29.[325] A risk that is very likely to occur and that brings about severe consequences constitutes a high risk that subsequently requires a DPIA. On the other hand, a risk that is very unlikely to occur and that brings about minor consequences constitutes a low risk that subsequently does not requires a DPIA. All risks that lie between these two extremes are left to the discretion of the

[318] Recital 75 GDPR
[319] Paul Reuter, The General Data Protection Regulation (GDPR): An EPSU briefing (1 edn, EPSU 2019) 25
[320] Article 29 Working Party, '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, 4 April 2017) 7-9
[321] Article 29 Working Party, '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, 4 April 2017) 12
[322] Claudia Quelle, The Data Protection Impact Assessment: What can it contribute to data protection? (Thesis for the Research Master in Law and the Master's program Law and Technology 2013-2015 2015) 108
[323] K Demetzou, 'Data Protection Impact Assessment: A tool for accountability and the unclarified concept of 'high risk' in the General Data Protection Regulation' [2019] 35(6) Computer Law & Security Review
[324] K Demetzou, 'Data Protection Impact Assessment: A tool for accountability and the unclarified concept of 'high risk' in the General Data Protection Regulation' [2019] 35(6) Computer Law & Security Review 5
[325] Article 29 Working Party, '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, 4 April 2017) 6

data controller.[326] This discretion is broadened by the lack of methodologies provided by either, the GDPR or the WP29 in conducting a DPIA.[327] These provide examples of risk, but situations that are not covered by these example, leave data controllers with little to no guidance.[328] Even situations that are covered by the examples do not provide sufficient guidance, because even the examples indicate a high likelihood of high risk occurring, but no certainty that there is high risk.[329]

Aside from the concept of high risk, Article 35 contains other vague terminology. For instance, it is stated that systematic large-scale data processing is an example of high-risk data processing. It is however unclear what the concepts of 'systematic' and 'large scale' mean.[330] Article 35 further states an assessment of the proportionality and necessity of the data processing is required, which would require further guidance to prevent data controllers from interpreting these terms in completely different manners.[331] The WP29 guidelines failed to clarify many concepts, such as proportionality and necessity.[334] Similarly, it did not adequately clarify the concept of 'high risk', since large discourse in the legal literature on the concept remains.[335]

This use of language in the GDPR is an understandable choice.[336] It provides the data controller with scalability and flexibility to adjust the DPIA to its specific data processing.[337] It is furthermore technologically neutral, which contributes to the sustainability of the regulation.[338] The rules will not require adjustment as technology evolves.[339] However, this comes at the expense of legal certainty.[340] Flexible and scalable rules appear meaningless when the threshold to make the rules applicable is vague to the extent where they could rarely apply. Flexibility and scalability should therefore not come at the expense of legal certainty.

Data controllers are required to make normative decisions to fill in the concept of 'high risk', When data controllers wrongfully find the risks of their data processing not high enough to meet the threshold of Article 35, the DPIA will have minimal effect on the

---

[326] Raphaël Gellert, 'Understanding the notion of risk in the General Data Protection Regulation' [2018] 34(2) Computer Law and Security Review 280

[327] Raphaël Gellert, 'Understanding the notion of risk in the General Data Protection Regulation' [2018] 34(2) Computer Law and Security Review 280

[328] K Demetzou, 'Data Protection Impact Assessment: A tool for accountability and the unclarified concept of 'high risk' in the General Data Protection Regulation' [2019] 35(6) Computer Law & Security Review 7-8

[329] K Demetzou, 'Data Protection Impact Assessment: A tool for accountability and the unclarified concept of 'high risk' in the General Data Protection Regulation' [2019] 35(6) Computer Law & Security Review 7-8

[330] Dariusz Kloza and others, 'Towards a method for data protection impact assessment: Making sense of GDPR requirements' [2019] 1(1) D.pia.lab Policy Brief 2

[331] Dariusz Kloza and others, 'Towards a method for data protection impact assessment: Making sense of GDPR requirements' [2019] 1(1) D.pia.lab Policy Brief 2

[334] Dariusz Kloza and others, 'Towards a method for data protection impact assessment: Making sense of GDPR requirements' [2019] 1(1) D.pia.lab Policy Brief 2

[335] Dariusz Kloza and others, 'Towards a method for data protection impact assessment: Making sense of GDPR requirements' [2019] 1(1) D.pia.lab Policy Brief; K Demetzou, 'Data Protection Impact Assessment: A tool for accountability and the unclarified concept of 'high risk' in the General Data Protection Regulation' [2019] 35(6) Computer Law & Security Review; Shakila-Bu-Pasha, 'The controller's role in determining 'high risk' and data protection impact assessment (DPIA) in developing digital smart city' [2020] 29(3) Information & Communications Technology Law

[336] K Demetzou, 'Data Protection Impact Assessment: A tool for accountability and the unclarified concept of 'high risk' in the General Data Protection Regulation' [2019] 35(6) Computer Law & Security Review 7-8

[337] Article 29 Working Party, 'Opinion 3/2010 on the principle of accountability' (WP 173, 13 July 2010) 14

[338] K Demetzou, 'Data Protection Impact Assessment: A tool for accountability and the unclarified concept of 'high risk' in the General Data Protection Regulation' [2019] 35(6) Computer Law & Security Review 7-8

[339] Recital 18 GDPR

[340] K Demetzou, 'Data Protection Impact Assessment: A tool for accountability and the unclarified concept of 'high risk' in the General Data Protection Regulation' [2019] 35(6) Computer Law & Security Review 7-8

mitigation of the risks.[343] When the data controller determines the threshold is not met, the data controller will not conduct a DPIA. The DPIA will then subsequently not increase accountability in the way described in Chapter 4. Providing additional guidance to establish legal certainty would therefore contribute to algorithmic accountability.

5.1.2. Trust in data controllers

Article 35, therefore, gives a wide margin of appreciation to data controllers. It can be questioned whether accountability increasing measures, such as the DPIA, are as effective when data controllers are given considerable room to interpret the rules as they believe fit.

It can first be wondered whether data controllers have an incentive to invest in the DPIA. Firms have an incentive to make an effort when there is a correct combination of detection and sanctions.[346] Firms will be inclined to avoid sanctions by engaging in compliance-enhancing activities.[347] This is only the case when the possible sanctions are larger than the costs of compliance.[348] The balancing between sanctions and costs of compliance is a case-by-case assessment that further depends on the firm's priorities.[349] Sanctions for non-compliance with Article 35 consist of fines up to 20 million euros or 4% of the company's global annual turnover of the previous financial year.[350] The costs of compliance are less easily calculated. Scientific research on the precise costs of conducting a DPIA and consequently risk mitigation is missing. However, in the legal literature, the DPIA is related to considerable organizational and material costs.[351] This is in relation to the conducting of the DPIA, such as the consultation of stakeholders.[352] The costs are additionally high due to legal uncertainty.[353] When there is legal uncertainty, firms will not know precisely how to behave to comply with the rules and therefore will have to invest more to apply the broad rules to their specific data processing.[354] This can be held against the low enforcement rates of supervisory authorities, which can only examine a very small portion of all data processing.[355] Firms may approach the balancing act differently and accordingly lean towards overcomplying or undercomplying.[356] It is argued here that the costs of compliance are high and the chances of punishment low, thereby increasing the chances of undercompliance.[357] Firms that decide to undercomply, undermine the capacity of the DPIA to increase accountability.

---

[343] Emanuel Moss and others, 'Assembling Accountability: Algorithmic Impact Assessment for the Public Interest' [2021] 1(1) SSRN Electronic Journal 18

[346] Donald C Langevoort, 'Cultures of Compliance' [2017] 54(4) American Criminal Law Review 937

[347] Donald C Langevoort, 'Cultures of Compliance' [2017] 54(4) American Criminal Law Review 937

[348] Donald C Langevoort, 'Cultures of Compliance' [2017] 54(4) American Criminal Law Review 938

[349] Donald C Langevoort, 'Cultures of Compliance' [2017] 54(4) American Criminal Law Review 940

[350] Article 83(5) GDPR

[351] Michael Friedewald and others, 'Data Protection Impact Assessments in Practice' [2021] 13106(1) ESORICS 2021: Computer Security ESORICS 2021 International Workshops 439

[352] Michael Friedewald and others, 'Data Protection Impact Assessments in Practice' [2021] 13106(1) ESORICS 2021: Computer Security ESORICS 2021 International Workshops 439

[353] Donald C Langevoort, 'Cultures of Compliance' [2017] 54(4) American Criminal Law Review 937-938

[354] John E Calfee and Richard Craswell, 'Some Effects of Ucertainty on Compliance with Legal Standards' [1984] 70(5) Virginia Law Review 965

[355] Bert-Jaap Koops, 'The trouble with European data protection law' [2014] 4(4) International Data Privacy Law 253-255

[356] John E Calfee and Richard Craswell, 'Some Effects of Ucertainty on Compliance with Legal Standards' [1984] 70(5) Virginia Law Review 965

[357] Michael Friedewald and others, 'Data Protection Impact Assessments in Practice' [2021] 13106(1) ESORICS 2021: Computer Security ESORICS 2021 International Workshops 439; Donald C Langevoort, 'Cultures of Compliance' [2017] 54(4) American Criminal Law Review 937-938; Bert-Jaap Koops, 'The trouble with European data protection law' [2014] 4(4) International Data Privacy Law 253-255

However, even assuming that data controllers are fully committed to compliance and putting the data principles into practice, the complexity of the law hinders data controllers from doing so. Research has shown that firms in practice grapple with the unclearness of open language.[358] Terminology, such as that of 'risk', is not explained sufficiently to guide firms when they conduct a DPIA or prepare to do so.[359] The DPIA particularly has been criticized to be complex and require extensive expertise to conduct correctly.[360] Firms that are less committed to compliance can pledge by the saying 'ignorance is bliss' and interpret the open norms in a way that is beneficial to the firm, but harmful to data protection.[361] Firms that are fully committed will need to spend considerable time and resources to translate the general open-ended rules into practice.[362] Even then, incorrect application of Article 35 can cause supervisory authorities to fine the firm.[363] In order not to deal with this complexity, firms may reduce compliance to a tick-box exercise.[364] A DPIA would then be conducted in a very limited manner that does not substantively contribute to detecting and reducing risk.[365] The ex-ante character of the DPIA furthermore limits the urgency that consequently makes it more likely that compliance will be reduced to a tick-box exercise.[366] DPIAs will consequently only indicate potential risks and will do little for the identification of all risks and the reduction of them.[367]

It is therefore argued that the trust in data controllers may be misplaced, which leads to not conducting the DPIA or reducing it to a tick-box exercise. This will limit accountability, as it will limit transparency. The conduct of the firm, in that case, is not explained sufficiently for the forum to pass judgment on it.

5.1.3. Inadequate independent oversight

The space given to data controllers is furthermore problematic due to the inadequate independent oversight. This is first of all because public disclosure is not mandated by the regulation.[368] This is an important shortcoming of the DPIA. The public disclosure of a DPIA would allow for public feedback that can trigger changes in the firm at hand and even regulatory changes.[369] By not requiring public disclosure, these mechanisms of feedback are disregarded. Voluntary disclosure cannot lead to real accountability, as the actor can choose

---

[358] Bart-Jaap Koops, 'The Evolution of Privacy Law and Policy in the Netherlands' [2011] 12(2) Journal of Comparative Policy Analysis 165-179

[359] Bert-Jaap Koops, 'The trouble with European data protection law' [2014] 4(4) International Data Privacy Law 253-255

[360] J Sarrat and R Brun, DPIA: How to Carry out One of the Key Principles of Accountability. in , Privacy Technologies and Policy (Springer 2018) 173

[361] Bert-Jaap Koops, 'The trouble with European data protection law' [2014] 4(4) International Data Privacy L aw 253-255

[362] Bert-Jaap Koops, 'The trouble with European data protection law' [2014] 4(4) International Data Privacy Law 253-255

[363] Dariusz Kloza and others, 'Towards a method for data protection impact assessment: Making sense of GDPR requirements' [2019] 1(1) D.pia.lab Policy Brief 1-8.2

[364] Bert-Jaap Koops, 'The trouble with European data protection law' [2014] 4(4) International Dat a Privacy Law 255

[365] Bert-Jaap Koops, 'The trouble with European data protection law' [2014] 4(4) International Data Privacy Law 255

[366] Bert-Jaap Koops, 'The trouble with European data protection law' [2014] 4(4) International Data Privacy Law 255

[367] Nigel Waters, Privacy Impact Assessment - Great Potential Not Often Realised. in Wright David and Paul De hert (eds), Privacy Impact Assessment (Springer 2012) 154

[368] Dariusz Kloza and others, 'Towards a method for data protection impact assessment: Making sense of GDPR requirements' [2019] 1(1) D.pia.lab Policy Brief 4

[369] ME Kaminski and G Malgieri, 'Multi-layered explanations from algorithmic impact assessments in the GDPR' [2020] Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency 75

when it wants to be held accountable.[370] The public can no longer functions as a forum and firms can avoid accountability to the public by not publishing their DPIA. It puts a lot of faith in data controllers, even though it is not beneficial for them to expand on truly problematic data processing, as it could harm their reputation.[371] It may be prone to make assessments public only when it reflects positively on them.[372] Therefore the public cannot provide adequate feedback on the DPIA and it cannot function as a forum.

A similar problem arises for administrative accountability to supervisory authorities, who only need to be consulted when the DPIA demonstrates residual risk.[373] As demonstrated above, data controllers can bend the open-ended rules to avoid needing to consult the supervisory authority or they may not have the organizational capacity to correctly conduct the DPIA to find residual risk. In many cases, therefore, the supervisory authority will not be able to function as a forum. In cases where the supervisory authority is contacted, the authority may not be resourced well enough to be able to give adequate feedback.[374] As the 2021 ICL report shows, supervisory authorities deal with decreasing budgets, an enormous number of cases to process, and little specialist knowledge.[375] This prevents authorities from critically assessing a DPIA that is conducted by an often much better-equipped data controller.[376] This is further intensified by the algorithm's opacity due to corporate secrecy, the technical skills required to assess an algorithm.[377] This will be explained in depth in paragraph 5.2.1. Supervisory authorities do therefore not effectively function as a forum, because it is often not required to consult them and when they are consulted, they are not well-equipped to provide feedback.

The last forum that can provide feedback and pass judgment is the court. According to articles 78 and 79 respectively, data subjects have the right to an effective judicial remedy against a supervisory authority and a controller or processor. It can be questioned, however, how likely it is that data subjects will make use of this rise. An elaborate survey of the 2015 Eurobarometer has shown that EU citizens do consider online privacy an urgent issue.[378] However, the same survey showed that EU citizens do not take simple action to prevent their data from being collected.[379] This example illustrates the "privacy paradox", which means that people think of privacy as important, but are willing to trade it for anything else.[380] It is therefore more likely most people will accept a data breach than that they invest in going to a

---

[370] Emanuel Moss and others, 'Assembling Accountability: Algorithmic Impact Assessment for the Public Interest' [2021] 1(1) SSRN Electronic Journal 9

[371] Emanuel Moss and others, 'Assembling Accountability: Algorithmic Impact Assessment for the Public Interest' [2021] 1(1) SSRN Electronic Journal 9

[372] Emanuel Moss and others, 'Assembling Accountability: Algorithmic Impact Assessment for the Public Interest' [2021] 1(1) SSRN Electronic Journal 21

[373] Article 29 Working Party, '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, 4 April 2017) 18

[374] ME Kaminski and G Malgieri, 'Multi-layered explanations from algorithmic impact assessments in the GDPR' [2020] Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency 75

[375] Johnny Ryan and Alex Toner, 'Europe's enforcement paralysis: ICCL's 2021 report on the enforcement capacity of data protection authorities' [2021] Irish Council for Civil Liberties 4

[376] ME Kaminski and G Malgieri, 'Multi-layered explanations from algorithmic impact assessments in the GDPR' [2020] Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency 75

[377] Paul B. De Laat, 'Algorithmic Decision-Making Based on Machine Learning from Big Data: Can Transparency Restore Accountability?' [2018] 31(1) Philosophy & Technology 536

[378] Maciej Sobolewski and others, 'GDPR: A Step Towards a User-centric Internet?' [2017] 52(4) Intereconomics 211-212

[379] Maciej Sobolewski and others, 'GDPR: A Step Towards a User-centric Internet?' [2017] 52(4) Intereconomics 211-212

[380] Frantz Rowe, 'Contact tracing apps and values dilemmas: A privacy paradox in a neo-liberal world' [2020] 55(1) International Journal of Information Management 2

court. Furthermore, since the DPIA does not need to be disclosed to data subjects, they are not made aware of issues that would trigger them to go to court. If a case does not go to court, the firm will not be held accountable by the court.

Therefore the public does not function effectively as a forum, because public disclosure of the DPIA is not required. Supervisory authorities also do not function effectively as a forum, because they are often not consulted and they are not well-equipped to provide adequate feedback. Finally, the court is not an effective forum, because a case is rarely brought to court. After all, the DPIA is not disclosed to data subjects and due to the privacy paradox. As demonstrated in Chapter 2, accountability requires a forum that can ask questions and pass judgment. Since an effective forum for the DPIA does not exist, accountability is limited.

5.2. Limitations related to algorithms

The limitation in relation to the requirements for the DPIA is explained above. Now, this chapter will turn to the limitations in relation to algorithms. First, it will be explained in what ways algorithms are opaque and how this forms a limitation for accountability. Then, it will be explained how the risks that algorithmic accountability seeks to reduce are broader than data protection issues.

5.2.1. The opacity of algorithms

Conducting a DPIA is not a simple task when it concerns an algorithm. Whereas simple algorithms can be relatively clear-cut and easily understandable, more complex algorithms – such as the machine learning type that is the topic of this thesis – are considered opaque. Burrell's framework provides insight in the various types of the opacity of algorithms.[381] This framework accounts for three forms of opacity: corporate secrecy, the incapacity of people that are not technically savvy, and finally, the black box character of machine learning algorithms.[382]

The first type of opacity is corporate secrecy. Firms that have developed algorithms can view it as their intellectual property.[383] By keeping the algorithm a trade secret, the firm preserves a competitive advantage over firms with comparable algorithms.[384] It is additionally possible to prevent competing firms from free-riding on the firm's efforts to develop an algorithm by patenting the algorithm.[385] Trade secrecy is however more beneficial, since there is continuous innovation in the field of machine learning that could lead to going around the patent.[386] It can be argued that firms also benefit from open-source innovation that would lift the veil of corporate secrecy. In practice, however, competing through trade secrecy is still the standard and open-source innovation is more an exception than the standard.[387] Another reason to keep an algorithm secret is to prevent the subject of the algorithmic decision-making

[381] Jenna Burrell, 'How the machine 'thinks': Understanding opacity in machine learning algorithms' [2016] 3(1) Big Data & Society
[382] Jenna Burrell, 'How the machine 'thinks': Understanding opacity in machine learning algorithms' [2016] 3(1) Big Data & Society 3-5
[383] Paul B. De Laat, 'Algorithmic Decision-Making Based on Machine Learning from Big Data: Can Transparency Restore Accountability?' [2018] 31(1) Philosophy & Technology 536
[384] Paul B. De Laat, 'Algorithmic Decision-Making Based on Machine Learning from Big Data: Can Transparency Restore Accountability?' [2018] 31(1) Philosophy & Technology 536
[385] Paul B. De Laat, 'Algorithmic Decision-Making Based on Machine Learning from Big Data: Can Transparency Restore Accountability?' [2018] 31(1) Philosophy & Technology 536
[386] Paul B. De Laat, 'Algorithmic Decision-Making Based on Machine Learning from Big Data: Can Transparency Restore Accountability?' [2018] 31(1) Philosophy & Technology 536
[387] Paul B. De Laat, 'Algorithmic Decision-Making Based on Machine Learning from Big Data: Can Transparency Restore Accountability?' [2018] 31(1) Philosophy & Technology 536

from gaming the system.[388] For instance, if a subject of algorithmic-decision making is aware that by making known they own a car above a certain value, they would not qualify for a loan, they may avoid admitting to having such a car.

Second, algorithms are opaque due to the technical illiteracy of most people. This type of opacity is based on the possibility to reverse engineer an algorithm and subsequently understand its decisions and bias.[389] Reverse engineering, however, requires learning specialized skills such as reading program language.[390] It is further necessary to study computational thinking and programming.[391] A large number of resources are necessary to give computer scientists the level of education required for reverse engineering.[392] Journalists that could be essential in clearing the opacity of algorithms for the public are therefore limited in doing so.[393] The public is, therefore, unable to understand algorithms, since they are not educated well enough to explain their working.

Finally, algorithms are opaque due to their complexity. This complexity does not only exist for people that lack technical skills, but also for computer scientists and even the creators of the algorithm.[394] Algorithms operate on a large scale at high speed and often independently.[395] For instance, an algorithm can be created to detect traffic signs on pictures. This algorithm may be eventually able to do so, while the creators of the algorithm are unable to understand or explain how it works.[396] Algorithms are furthermore linked to datasets that continually change, thereby complicating the context within which algorithms function.[397] Even though the creators evidently do not lack access or knowledge, they, therefore, are unable to understand the algorithms or, consequently, indicate how problems, such as bias, arise.[398] The algorithm then operates as a black box: it provides output without justifying or explaining the output.[399]

This type of opacity is particularly present in machine learning algorithms that operate on a particularly large scale and with high complexity.[400] Machine learning algorithms are especially useful when they are complex.[401] The more complex relations it analyzes, the more

---

[388] Paul B. De Laat, 'Algorithmic Decision-Making Based on Machine Learning from Big Data: Can Transparency Restore Accountability?' [2018] 31(1) Philosophy & Technology 534

[389] Nicholas Diakopoulos, 'Algorithmic accountability reporting: On the investigation of black boxes' [2014] 3(3) Digital journalism 13

[390] Jenna Burrell, 'How the machine 'thinks': Understanding opacity in machine learning algorithms' [2016] 3(1) Big Data & Society 4

[391] Nicholas Diakopoulos, 'Algorithmic accountability reporting: On the investigation of black boxes' [2014] 3(3) Digital journalism 26

[392] Nicholas Diakopoulos, 'Algorithmic accountability reporting: On the investigation of black boxes' [2014] 3(3) Digital journalism 26

[393] Jenna Burrell, 'How the machine 'thinks': Understanding opacity in machine learning algorithms' [2016] 3(1) Big Data & Society 4

[394] Mike Ananny and Kate Crawford, 'Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability' [2018] 20(3) New Media & Society 981

[395] Mike Ananny and Kate Crawford, 'Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability' [2018] 20(3) New Media & Society 981

[396] Mike Ananny and Kate Crawford, 'Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability' [2018] 20(3) New Media & Society 981

[397] R van den Hoven van Genderen, 'Algoritmen en AI: distopische black box of glazen bol? Is een wettelijk kader voor transparantie van algoritmen mogelijk en wenselijk?' [2020] 5(1) Computerrecht 2

[398] Mike Ananny and Kate Crawford, 'Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability' [2018] 20(3) New Media & Society 981

[399] W Nicholson Price, 'Big Data and Black-Box Medical Algorithms' [2018] 10(471) Science Translational Medicine 1

[400] Jenna Burrell, 'How the machine 'thinks': Understanding opacity in machine learning algorithms' [2016] 3(1) Big Data & Society 4-5

[401] Jenna Burrell, 'How the machine 'thinks': Understanding opacity in machine learning algorithms' [2016] 3(1) Big Data & Society 4-5

accurately it could generate output.[402] However, it is then simultaneously less explainable. They especially suffer from the 'curse of dimensionality'.[403] The training data on basis of which the algorithms learn is multi-dimensional in the sense that it processes a large number of properties of data.[404] For instance, an algorithm that does not only search for words in books, but additionally looks at the book titles and background information. The code is consequently more complex and opaque.[405]

Algorithms are therefore opaque. This is problematic when a data controller is conducting in DPIA in relation to an algorithm. The opacity prevents complete and accurate mapping of risks.[406] It may not be easy to determine whether a machine learning algorithm is presenting discriminatory behavior, when it is not possible to explain how it behaves.[407] This can make the DPIA a challenging exercise. The DPIA furthermore needs to be conducted prior to the data processing. Since a machine learning algorithm evidently 'learns' as it is in action, it may not be possible to identify risks before it is deployed.[408] Identifying residual risk would then become a guessing exercise, as the outcomes of the algorithm cannot be predicted.[409]

Algorithms, particularly of the machine learning type, therefore are opaque due to corporate secrecy, technical illiteracy of the public, and the algorithm's black box character. This prevents identification of risks when conducting a DPIA. Accountability is subsequently limited to both the public as a forum and the supervisory authorities. DPIAs are not communicated to the public to maintain corporate secrecy. Even if it were communicated or if the public attempted reverse engineering, transparency would be difficult to create due to technical illiteracy. Secondly, the supervisory authority needs to be notified when the DPIA demonstrates residual risks. Since the DPIA is conducted prior to the deployment of the algorithm, it may not be possible to identify residual risk. Furthermore, creators may not be aware of residual risk that develops or presents itself at a later stage, since machine learning algorithms change overtime. This causes the supervisory authority not to be notified. Finally, a problem with all types of accountability is the black box character of algorithms. When even the creators of an algorithm are unable to understand and explain its output, the supervisory authorities will not be able to pass judgment as it is not provided with adequate information. The algorithm's opacity, therefore, limits algorithmic accountability.

5.2.2. Algorithmic issues extending beyond data protection issues

Algorithmic accountability has been explained to be important to counter an algorithm's bias and defects with potentially large effects. The concerns that are raised

---

[402] Jenna Burrell, 'How the machine 'thinks': Understanding opacity in machine learning algorithms' [2016] 3(1) Big Data & Society 4-5

[403] P Domingos, 'A few useful things to know about machine learning' [2012] 55(10) Communications of the ACM 78

[404] Jenna Burrell, 'How the machine 'thinks': Understanding opacity in machine learning algorithms' [2016] 3(1) Big Data & Society 4-5

[405] Jenna Burrell, 'How the machine 'thinks': Understanding opacity in machine learning algorithms' [2016] 3(1) Big Data & Society 5

[406] Anton Vedder and Laurens Naudt, 'Accountability for the use of algorithms in a big data environment' [2017] 31(2) International Review of Law, Computers & Technology 215-216

[407] Anton Vedder and Laurens Naudt, 'Accountability for the use of algorithms in a big data environment' [2017] 31(2) International Review of Law, Computers & Technology 216

[408] Anton Vedder and Laurens Naudt, 'Accountability for the use of algorithms in a big data environment' [2017] 31(2) International Review of Law, Computers & Technology 216

[409] Anton Vedder and Laurens Naudt, 'Accountability for the use of algorithms in a big data environment' [2017] 31(2) International Review of Law, Computers & Technology 216

include ethical concerns that are related to human norms and values.[410] As has been explained in Chapter 2, algorithms are cultural objects that simultaneously shape and are shaped by society.[411] As society changes, the algorithm changes too.[412] For instance, when the data that influences the algorithm represent increasingly black people, the algorithm will make decisions differently. Simultaneously, an algorithm influences society.[413] For instance, an algorithm that is biased to grant loans to people only with common last names can consequently change society to where people with uncommon last names are less wealthy. Bias and other risks of algorithms are therefore complex and extend beyond data protection matters. The DPIA provides a useful opportunity to look into the risks of algorithms, but it is currently limited to data protection issues. Extending the scope of the impact assessment to risk for all human rights would allow looking at an algorithm more holistically.[414] This would increase chances of identifying and consequently mitigating all risks.[415]

It needs to be noted that data controllers need to establish whether the data processing has a high risk on the rights and freedoms of natural persons, in order to establish whether conducting a DPIA is required.[416] This suggests a holistic assessment as suggested above is already required prior to conducting a DPIA. It suggests a dual assessment: an assessment of the risks of the data processing on the rights and freedoms of a natural person and an assessment of the data protection risks. It can be wondered to what extent the second assessment should be part of the first assessment, since natural persons have the right to privacy according to 8(1) of the Charter of Fundamental Rights of the European Union. However, only the assessment of the data protection risks needs to be documented and possibly communicated to the supervisory authorities. The lack of a forum means such assessment does not increase accountability in relation to these issues.

5.3 Conclusion

This Chapter discussed the limitations of the DPIA in increasing algorithmic accountability. First, it was explained that data controllers are required to make normative decisions prior to and during conducting a DPIA. This puts a lot of faith in data controllers to make decisions to identify and mitigate risks, even though they may not have the resources or the incentive to adequately do so. This decreases transparency and therefore accountability. There additionally is no adequate independent oversight or also called forum, which further decreases accountability. Furthermore, algorithms are opaque, because of corporate secrecy, technical illiteracy, and finally, technical opacity. Transparency is therefore only possible in a limited matter and accountability is further decreased.

---

[410] David Danks and Alex John London, 'Algorithmic Bias in Autonomous Systems' [2017] 1(1) Conference: Twenty-Sixth International Joint Conference on Artificial Intelligence 5

[411] Nick Seaver, 'Algorithms as culture: Some tactics for the ethnography of algorithmic systems' [2017] 4(2) Big Data & Society 2-5

[412] Nick Seaver, 'Algorithms as culture: Some tactics for the ethnography of algorithmic systems' [2017] 4(2) Big Data & Society 2-5

[413] Nick Seaver, 'Algorithms as culture: Some tactics for the ethnography of algorithmic systems' [2017] 4(2) Big Data & Society 2-5

[414] The Ada Lovelace Institute and Datakind UK, 'Examining the Black Box: Tools for assessing algorithmic systems' (Ada Lovelace Institute, 29th April) <https://www.adalovelaceinstitute.org/report/examining-the-black-box-tools-for-assessing-algorithmic-systems/> accessed 9 March 2022

[415] David Danks and Alex John London, 'Algorithmic Bias in Autonomous Systems' [2017] 1(1) Conference: Twenty-Sixth International Joint Conference on Artificial Intelligence 5

[416] Article 35 General Data Protection Regulation

Chapter 6 - A balancing of arguments

The past chapters have answered the subquestions. This chapter will now answer the main research question: *To what extent does a data protection impact assessment, as required under article 35 GDPR, contribute to the accountability of data controllers in the private sector to data subjects with respect to machine learning algorithms that make decisions?* In order to do this, arguments of the past Chapters will be revisited and analyzed. Based on these findings, a recommendation will be given, followed by a conclusion.

6.1 The extent to which the DPIA contributes to accountability

To assess whether the DPIA contributes to accountability, the concept of accountability needed to be explained. The following elements of accountability were identified by Bovens[417]

"1. there is a relationship between an actor and a forum
2. in which the actor is obliged
3. to explain and justify
4. his conduct;
5. the forum can pose questions;
6. pass judgement;
7. and the actor may face consequences"

The DPIA in various ways does and does not contribute to these elements, for instance by providing ways for the actor to explain his conduct and the forum to pass its judgments.

The DPIA brings to light information, such as the objective of the data processing, and thereby contributes to transparency.[418] Transparency facilitates information provision to stakeholders, which contributes to accountability.[419] It serves as an explanation of the data controller's conduct. However, this explanation can only exist to the extent it is possible to explain the machine learning algorithm. Algorithmic opacity limits the complete and accurate mapping of risks and therefore the ability of the DPIA to contribute to transparency.[420] It should further be noted that a fully transparent outcome requires a situation where all stakeholders are provided with all relevant information. The DPIA does not necessarily lead to a fully transparent outcome, particularly due to a less effective forum.

The privacy by design aspect that is related to the DPIA further contributes to accountability, by identifying and passing judgment on data protection risks at a moment in time where a change to the conduct of the data controller is still possible.[421] The DPIA is furthermore an ongoing exercise, which allows the identification of risks related to parts of the system that develop in a later stage.[422] Also when the DPIA is ultimately not conducted, but an assessment of whether the DPIA is required on the other hand is conducted,

---

[417] Mark Bovens, 'Analysing and Assessing Accountability: A Conceptual Framework' [2007] 13(4) European Law Journal 452

[418] Hans Krause Hansen and others, 'Introduction: Logics of transparency in late modernity: Paradoxes, mediation and governance' [2015] 18(2) European Journal of Social Theory 118

[419] Hans Krause Hansen and others, 'Introduction: Logics of transparency in late modernity: Paradoxes, mediation and governance' [2015] 18(2) European Journal of Social Theory 118

[420] Anton Vedder and Laurens Naudt, 'Accountability for the use of algorithms in a big data environment' [2017] 31(2) International Review of Law, Computers & Technology 215-216

[421] Emanuel Moss and others, 'Assembling Accountability: Algorithmic Impact Assessment for the Public Interest' [2021] 1(1) SSRN Electronic Journal 18-19

[422] Emanuel Moss and others, 'Assembling Accountability: Algorithmic Impact Assessment for the Public Interest' [2021] 1(1) SSRN Electronic Journal 18-19

accountability is increased by the generation of information.[423] This contributes to transparency. The limitations of transparency as explained above, however, remain.

The regulatory form of meta-regulation that is used for the DPIA is thirdly an aspect of the DPIA that contributes to accountability. Meta-regulation provides flexibility that allows data controllers to put in place the mechanisms they consider fit to achieve regulatory goals.[424] This flexibility is, for instance, provided by the use of open language. The use of open language, however, generates legal uncertainty.[425] If it is highly uncertain when the DPIA needs to be conducted, it is possible data controllers will persistently argue they do not need to conduct a DPIA, rendering the rules meaningless.

Finally, several forums are capable of passing judgment on basis of the DPIA. First, the public can boycott the data controller or bring its case to court.[426] Public disclosure is, however, not required.[427] This is deeply problematic as it discontinues the accountability relationship between the public and the data controller. Second, national supervisory authorities have enforcement powers and need to be consulted when there is a residual risk. Although they are therefore consulted more regularly than the public, it is still in a limited number of cases. Furthermore, the issue of open language and trust in data controllers arises, since data controllers may quickly decide there is no residual risk due to the lack of explanation of risk and risk identification.[428] Lastly, the court can function as a forum. The public, however, that needs to bring the case to court, may regularly avoid doing so, because of the high costs of going to court against an abstract data breach.[429]

As these findings demonstrate, the DPIA, therefore, contains mechanisms that increase accountability. However, these mechanisms are regularly not triggered due to unclear or missing rules. First, transparency cannot be achieved when the opaque character of algorithms prevents the generation of relevant information. Second, Article 35 does not make clear when a DPIA needs to be conducted, which additionally hinders its ability to generate transparency. Third, it is not required to publish the DPIA, which means the public as a forum cannot pass judgment. Article 35, therefore, lacks or fails to clarify thresholds for the accountability mechanisms. The DPIA contributes to the accountability of data controllers in the private sector to data subjects with respect to machine learning algorithms that make decisions, only to the extent the accountability mechanisms are triggered.

Lastly, it has been stated that algorithmic issues extend beyond data protection issues. The identified shortcomings lead to the following recommendation.

---

[423] Article 29 Working Party, '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, 4 April 2017) 12

[424] Christina Parker, The Open Corporation: Effective Self-regulation and Democracy (Cambridge University Press 2002) 98, 48

[425] K Demetzou, 'Data Protection Impact Assessment: A tool for accountability and the unclarified concept of 'high risk' in the General Data Protection Regulation' [2019] 35(6) Computer Law & Security Review 7-8

[426] Emily Tan, 'Seven out of ten customers would boycott a brand that mishandled their data' (Campaign, 9 February 2018) <https://www.campaignlive.co.uk/article/seven-ten-customers-boycott-brand-mishandled-data/1456749> accessed 14 February 2022

[427] Dariusz Kloza and others, 'Towards a method for data protection impact assessment: Making sense of GDPR requirements' [2019] 1(1) D.pia.lab Policy Brief 4

[428] K Demetzou, 'Data Protection Impact Assessment: A tool for accountability and the unclarified concept of 'high risk' in the General Data Protection Regulation' [2019] 35(6) Computer Law & Security Review 7-8

[429] Maciej Sobolewski and others, 'GDPR: A Step Towards a User-centric Internet?' [2017] 52(4) Intereconomics 211-212

6.2 Recommendation

It is recommended to make the assessment of the risks to rights and freedoms of a natural person part of the required assessment. Such holistic impact assessment has previously been proposed in the US through the praised Algorithmic Accountability Act.[430] The algorithmic assessment has been found valuable in the literature.[431] It has been found beneficial to extend beyond privacy issues to broader issues in relation to society.[432] An assessment of human rights may be outside the scope of the GDPR.[433] The GDPR is concerned with the processing of personal data and the DPIA is likewise concerned with data protection.[434] A holistic assessment is therefore misplaced under the GDPR.

Such an assessment may be better suited to the proposed Regulation laying down harmonized rules on artificial intelligence.[435] The regulation was proposed by the European Commission in April 2021 and seeks to address the risks of artificial intelligence of all kinds and not limited to, for example, data protection risks.[436] Its subject matter is artificial intelligence systems, which include machine learning algorithms.[437] The proposal prohibits specified AI systems, and provides rules for high-risk AI systems and AI systems with a transparency risk.[438] High-risk AI systems are systems that present risk, considering probability and severity, for health and safety or the fundamentals rights of persons.[439] This is similar to how data controllers are expected to determine high risk.[440] In the proposal for the Artificial Intelligence Act, however, it is not the task of the designer or user of the algorithm to determine whether it is high risk. Whereas the GDPR leaves the explaining of 'high risk' to data controllers, the proposal for the Artificial Intelligence Act provides a list of AI systems that are considered high risk.[441] By requiring an impact assessment for high-risk AI systems under the proposed Artificial Intelligence Act, the issue of uncertainty around the term 'high risk' is avoided.

To address the mentioned shortcomings, it is important to ensure the mechanisms of accountability are regularly triggered. The wording of an article requiring such impact assessment would need to find the right balance between legal certainty and technological neutrality. Legal certainty about when the assessment is required is, as previously argued, preferred to ensure data controllers cannot avoid an impact assessment by interpreting the meaning of high risk in a limited manner. Consequently, due to more legal certainty, accountability is less reliant on the motivation and capacity of the data controller.

---

[430] Mark Maccarthy, 'An Examination of the Algorithmic Accountability Act of 2019' [2019] 1(1) Transatlantic High Level Working Group on Content Moderation Online and Freedom of Expression 7-8

[431] Mark Maccarthy, 'An Examination of the Algorithmic Accountability Act of 2019' [2019] 1(1) Transatlantic High Level Working Group on Content Moderation Online and Freedom of Expression 7-8

[432] The Ada Lovelace Institute and Datakind UK, 'Examining the Black Box: Tools for assessing algorithmic systems' (Ada Lovelace Institute, 29th April) <https://www.adalovelaceinstitute.org/report/examining-the-black-box-tools-for-assessing-algorithmic-systems/> accessed 9 March 2022 16

[433] Article 2 General Data Protection Regulation

[434] Article 2 General Data Protection Regulation; Article 35 General Data Protection Regulation

[435] Commission, 'Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts' COM(2021) 206 final

[436] Commission, 'Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts' COM(2021) 206 final

[437] Article 2 Proposal for an Artificial Intelligence Act; Annex I (a) Proposal for an Artificial Intelligence Act

[438] Article 5-52 Proposal for an Artificial Intelligence Act

[439] Cons 32 Proposal for an Artificial Intelligence Act

[440] Article 29 Working Party, '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, 4 April 2017) 6

[441] Article 6 Proposal for an Artificial Intelligence Act

Furthermore, mandatory publication of the impact assessment would be beneficial to ensure adequate independent oversight. The publication could be limited to parts of the impact assessment that does not contain information that reveals trade secrets or leads to security risks. As proposed by the WP29, a summary of the DPIA's finding would contribute to transparency.[442]

A holistic impact assessment does not solve the problem of the algorithm's opacity. More research is therefore required to overcome this issue. It can further be wondered whether it is desirable to deploy an algorithm that is opaque to the extent where it is not understandable to the designer or user of the system, in high-risk situations such as in hiring or insurance.[443] The research to what extent this is the case is a complex task that is outside the scope of this thesis.

It is therefore recommended to include a holistic impact assessment in the AI Act. This would provide the transparency that increases accountability, while avoiding leaving the definition of 'high risk' to data controllers. Such an article can further be formulated to allow the benefits of meta-regulation, while ensuring adequate independent oversight by, for instance, obligating publication of the impact assessment. Thereby, the impact assessment is designed to preserve the elements that increase accountability and discard elements that limit accountability.

6.3 Conclusion

The DPIA, therefore, contains mechanisms for accountability, but these are regularly not triggered due to unclear or non-existent thresholds. Algorithmic issues furthermore extend beyond data protection issues. A holistic algorithmic impact assessment with clear thresholds for the mechanisms of accountability is therefore recommended. The main research question has therefore been answered in this Chapter. The next Chapter will conclude the thesis.

[442] Article 29 Working Party, '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, 4 April 2017) 17

[443] Cons 36, 37 and 46 Proposal for an Artificial Intelligence Act

Chapter 7 – Conclusion

Machine learning algorithms increasingly make high-impact decisions. At the same time, the algorithms are highly opaque and prone to bias and other defects that can harm particularly vulnerable groups of people. Accountability is a mechanism to correct bias. It is therefore important to study tools that intend to strengthen accountability. The GDPR's DPIA is intended to strengthen accountability. It is one of the accountability tools of the GDPR that has received less attention in the legal literature. As the GDPR is an influential regulation, it is important to study its triumphs and defeats for future regulation.

Therefore, the following research question was formulated: *To what extent does a data protection impact assessment, as required in article 35 GDPR, contribute under the accountability of data controllers in the private sector to data subjects with respect to machine learning algorithms that make decisions?*

The conducted research on basis of literature has generated the following findings. **First**, the DPIA is capable of contributing to transparency by facilitating the generation of and access of stakeholders to information that may have otherwise remained hidden. This is only to the extent the algorithm that is the topic of the DPIA, is not opaque. Opaque algorithms hinder the accurate completion of the DPIA and consequently its contribution to transparency and accountability.

Second, the DPIA is conducted at a time when it is still possible to adjust the system according to the outcomes of the assessment. It is additionally an ongoing exercise that allows mapping of risks that show in a later stage of development. This contributes to transparency, although the demonstrated limitations of transparency remain. The assessment to determine whether a DPIA is required likewise contributes to transparency.

The form of regulation that is used for the DPIA, meta-regulation, **thirdly** contributes to accountability. This form of regulation provides flexibility to data controllers to implement regulatory goals effectively. It contributes to accountability by avoiding the DPIA from developing into a tick-box exercise and by recognizing organizational complexity. This flexibility, however, requires open language, which generates legal uncertainty. Particularly legal uncertainty around the concept of 'high risk' may render the DPIA useless due to the freedom of data controllers to decide when it is required. This trust in data controllers may be misplaced, as they may lack the incentive to invest in the DPIA or the material and organizational capacity to conduct it correctly.

Fourth, there are various forums for the DPIA that contribute to accountability; the public, supervisory authorities, and the court. Publication of the DPIA is, however, not required. The public is therefore typically unable to function as a forum and consequently also not bring any issues to court. National supervisory authorities are similarly not always made aware of the DPIA, since consultation is only required when there is a residual risk.

These findings show that although the DPIA contains mechanisms for accountability. For instance, it provides information to supervisory authorities that can consequently use its enforcement powers. Rules to trigger these mechanisms are, however, unclear or missing. For instance, since it is unclear when a DPIA is required due to uncertainty around the concept of 'high risk', the ability of DPIA to generate transparency is hindered.

A final limitation that was found is that DPIAs a limited to data protection issues, while algorithms are complex constructs of society that contain issues that extend far beyond data protection issues. A holistic approach would benefit the identification and mitigation of these issues. Based on this limitation and the previously explained finding, it is recommended to include a holistic impact assessment in the proposed AI Act.

Accountability allows the exercising of control over the conduct of private entities. This can allow at least some public control over biased algorithms that make important decisions, such as the granting of a loan and the selection of job applicants. As a consequence,

functioning mechanisms for accountability are desirable. It was found that the DPIA contributes to accountability only to the extent it applies. The rules for this are either absent or unclear. The DPIA thereby shows a crucial shortcoming as a mechanism for accountability in relation to machine learning algorithms.

It should be noted that an answer to the research question depends on practice. For instance, it has been argued that data controllers are likely to lack the incentive to invest in the DPIA, particularly when it contains open language, due to high cost and low enforcement rates. However, data controllers in practice may choose differently based on their priorities. If their priorities are, for instance, avoiding high fines or maintaining public trust, the results may differ. The findings, therefore, reflect a theory-based likely scenario that may differ from practice. Future research can therefore look into the extent to which data controllers prioritize compliance and how they conduct their cost-benefit analysis.

As has been explained, however, it can be wondered to what extent the DPIA is suitable as a mechanism for accountability in relation to machine learning algorithms, due to algorithm-related issues extending beyond data protection. Such impact assessment may be better placed under a more holistic regulation for algorithms, such as the AI Act. Although a recommendation has been given, further research is necessary to review such an approach and consider other possibilities. Further research is additionally required to address the issue of opacity. The literature has not yet identified a solution for risk identification and mitigation for opaque machine learning algorithms, which cannot be fully understood and explained by even its creators.

Impact assessments have little impact when the firm that conducts them is unable to understand and consequently gather information about the workings of its algorithms. Accountability is likewise hindered by the algorithm's opacity. It can be wondered whether algorithms that are opaque to the extent their risks cannot be identified and mitigated, should be making important decisions for natural persons. The proposal for the AI act already seeks to prohibit certain artificial intelligence practices with unacceptable risk. [444] The question then is: is an algorithm whose risk level cannot be determined, unacceptably risky?

[444] Consideration 27 Proposal for an Artificial Intelligence Act; Article 5 Proposal for an Artificial Intelligence Act

Bibliography

Legislation

Article 29 Working Party, '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, 4 April 2017)

Article 29 Working Party, 'Guidelines on transparency under Regulation 2016/679' (WP260, 11 April 2018)

Article 29 Working Party, 'Opinion 3/2010 on the principle of accountability' (WP 173, 13 July 2010

Directive (EU) 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/31

Directive (EU) 2011/92/EU of 13 December 2011 on the assessment of the effects of certain public and private projects on the environment [2011] OJ L 26/1

Proposal for a Regulation (EU)

Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard tot he 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

Books and papers

Adriaansz C and Studer E, 'Betekenisvolle transparantie voor algoritmische besluitvorming' [2020] 43(2) Computerrecht

Akter S and others, 'Algorithmic bias in data-driven innovation in the age of AI' [2021] 60(1) International Journal of Information Management

Al-qizwini M and others, 'Deep learning algorithm for autonomous driving using GoogLeNet' [2017] 2017 IEEE Intelligent Vehicles Symposium

Alikhademi K and others, 'A review of predictive policing from the perspective of fairness' [2022] 30(1) Artificial Intelligence and Law

Ananny M and Crawford K, 'Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability' [2018] 20(3) New Media & Society

Angwin J and others, 'Machine Bias: Risk assessments in criminal sentencing' [2016] ProPublica <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing> accessed 6 September 2021

Berthold S and others, 'Crime and Punishment in the Cloud Accountability, Transparency, and Privacy' [2013] 1(1) Political Science

Bieker F and others, 'A Process for Data Protection Impact Assessment under the European General Data Protection Regulation' [2016] 1(1) Conference: 4th Annual Privacy Forum

Binns R, 'Algorithmic Accountability and Public Reason' [2018] 31(4) Philosophy & Technology

Binns R, 'Data protection impact assessments: a meta-regulatory approach' [2017] 7(1) International Data Privacy Law 29

Blagescu M and others, Pathways to Accountability: The GAP Framework (One World Trust 2005)

Bovens M, 'Analysing and Assessing Accountability: A Conceptual Framework' [2007] 13(4) European Law Journal

Bovens M, 'Two Concepts of Accountability: Accountability as a Virtue and as a Mechanism' [2010] 33(5) West European Politics

Brand D, 'Algorithmic Decision-making and the Law' [2020] 12(1) EJournal of eDemocracy and Open Government

Brkan M, 'Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond' [2019] 27(2) International Journal of Law and Information Technology

Brown A and others, 'Toward Algorithmic Accountability in Public Services: A Qualitative Study of Affected Community Perspectives on Algorithmic Decision-making in Child Welfare Services' [2019] 1(1) CHI '19: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems

Bu-Pasha S, 'The controller's role in determining 'high risk' and data protection impact assessment (DPIA) in developing digital smart city' [2020] 29(3) Information & Communications Technology Law

Burrell J, 'How the machine 'thinks': Understanding opacity in machine learning algorithms' [2016] 3(1) Big Data & Society

Bygrave LA, Article 25 Data protection by design and by default. in , The EU General Data Protection Regulation (GDPR): A Commentary (Oxford University Press 2020)

Calabrò A and others, 'Integrating Access Control and Business Process for GDPR Compliance: A Preliminary Study' [2019] ITASEC19 - Italian Conference on Cybersecurity

Calfee JE and Craswell R, 'Some Effects of Ucertainty on Compliance with Legal Standards' [1984] 70(5) Virginia Law Review

Caplan R and others, 'Algorithmic Accountability: A Primer' [2018] 1(1) Tech Algorithm Briefing: How Algorithms Perpetuate Racial Bias and Inequality

Carson A, 'GDPR ushers in civil litigation claims across the EU' (Iapp, 24 March 2020) <https://iapp.org/news/a/gdpr-ushers-in-civil-litigation-claims-across-the-eu/> accessed 14 February 2022

Casey B, Farhangi A and Vogl R, 'Rethinking Explainable Machines: The GDPR's 'Right to Explanation' Debate and the Rise of Algorithmic Audits in Enterprise' [2019] 34 Berkeley Technology Law Journal

Cavoukian A, 'Privacy by Design: The 7 Foundational Principles: Implementation and Mapping of Fair Information Practices' [2006] 1(1) Creation of a Global Privacy Standard

Christensen LT and Cheney G, 'Peering into Transparency: Challenging Ideals, Proxies, and Organizational Practices' [2015] 25(1) Communication Theory 73

Cilliers D and others, 'The perceived benefits of EIA for government: a regulator perspective' [2020] 38(5) Impact Assessment and Project Appraisal 358-367

Commission, 'Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts' COM(2021) 206 final

Confessore N, 'Cambridge Analytica and Facebook: The Scandal and the Fallout So Far' (The New York Times, 4 April 2018) <https://www-nytimes-com.tilburguniversity.idm.oclc.org/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html> accessed 14 February 2022

Cooper P, 'How the Facebook Algorithm Works in 2021 and How to Make it Work for You' (Hootsuite, 10th February) <https://blog.hootsuite.com/facebook-algorithm/> accessed 18 April 2021

Danks D and London AJ, 'Algorithmic Bias in Autonomous Systems' [2017] 1(1) Proceedings of the 26th International Joint Conference on Artificial Intelligence

De Laat PB, 'Algorithmic Decision-Making Based on Machine Learning from Big Data: Can Transparency Restore Accountability?' [2018] 31(1) Philosophy & Technology

Demetzou K, 'Data Protection Impact Assessment: A tool for accountability and the unclarified concept of 'high risk' in the General Data Protection Regulation' [2019] 35(6) Computer Law & Security Review

Diakopoulos N, 'Accountability in Algorithmic Decision Making' [2016] 59(2) Communications of the ACM

Diakopoulos N, 'Algorithmic accountability reporting: On the investigation of black boxes' [2014] 3(3) Digital journalism

Domingos P, 'A few useful things to know about machine learning' [2012] 55(10) Communications of the ACM

Doshi-velez F and others, 'Accountability of AI Under the Law: The Role of Explanation' [2017] SSRN Electronic Journal <DOI:10.2139/ssrn.3064761> accessed 16 May 2021

Duricu A, 'Data Protection Impact Assessment (DPIA) and Risk Assessment in the context of the General Data Protection Regulation (GDPR)' [2019] Lulea University of Technology

European commission, 'What are Data Protection Authorities (DPAs)?' (European Commission, 26 April 2022) <https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-are-data-protection-authorities-dpas_en> accessed 26 April 2022

European data protection board, 'Article 29 Working Party' (EDPB Europa) <https://edpb.europa.eu/about-edpb/more-about-edpb/article-29-working-party_en> accessed 8 September 2021

European data protection supervisor (EDPS), 'The History of the General Data Protection Regulation' (EDPS Europe, 2021) <https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en> accessed 8 September 2021

Fazlioglu M, 'What's Subject to a DPIA under the GDPR? EDPB on Draft Lists of 22 Supervisory Authorities' [2018] IAPP

Fink K, 'Opening the government's black boxes: freedom of information and algorithmic accountability' [2017] 21(1) Information Communication and Society

Franklin S, History, motivations, and core themes. in Keith Frankish (ed), The Cambridge handbook for artificial intelligence (Cambridge University Press 2014)

Friedewald M and others, 'Data Protection Impact Assessments in Practice' [2021] 13106(1) ESORICS 2021: Computer Security ESORICS 2021 International Workshops

Fuller M, Software Studies: A Lexicon (1 edn, MIT Press 2008)

Garcia M, 'Racist in the Machine: The Disturbing Implications of Algorithmic Bias' [2016/2017] 33(4) World Policy Journal

Garcia-gathright J and others, 'Assessing and Addressing Algorithmic Bias - But Before We Get There' [2018] ArXiv

Gellert R, 'Understanding the notion of risk in the General Data Protection Regulation' [2018] 34(2) Computer Law and Security Review

Gerbrandy A and Custers B, 'Algoritmische besluitvorming en het kartelverbod' [2018] 21(3) Markt en Mededinging

Giakoumopoulos C and others, Handbook on European data protection law (European Union Agency for Fundamental Rights and Council of Europe 2018)

Gillespie T, Algorithm. in Benjamin Peters (ed), Digital Keywords: a vocabulary of information society and culture (Princeton University Press 2016)

Gillespie T, The Relevance of Algorithms. in Gillespie and others (eds), Media Technologies: Essays on Communication, Materiality, and Society (MIT Press 2014)

Goodman B, 'A Step Towards Accountable Algorithms? Algorithmic Discrimination and the European Union General Data Protection' [2016] 29th Conference on Neural Information Processing Systems

Grimmelmann J, 'Regulation by Software' [2005] 114(7) Yale Law Journal

Guo Y and others, 'An Interactive Personalized Recommendation System Using the Hybrid Algorithm Model' [2017] 9(10) Symmetry

Gupta R and Pal SK, Introduction to Algorithmic Government (1 edn, Palgrave Macmillan 2021)

Ha vo N and others, 'The NL2KR Platform for building Natural Language Translation Systems' [2015] 1(1) ACL <DOI:10.3115/v1/P15-1087> accessed 16 May 2021

Hansen HK and others, 'Introduction: Logics of transparency in late modernity: Paradoxes, mediation and governance' [2015] 18(2) European Journal of Social Theory

Hasan KM and others, 'Path planning algorithm development for autonomous vacuum cleaner robots' [2014] 1(1) Conference: 2014 International Conference on Informatics, Electronics & Vision (ICIEV) <DOI:10.1109/ICIEV.2014.6850799> accessed 16 May 2021

Huang C and others, 'Credit scoring with a data mining approach based on support vector machines' [2007] 33(4) Expert Systems with Applications

It governance privacy team and others, EU General Data Protection Regulation (GDPR) - an Implementation and Compliance Guide (4 edn, ITGP 2020)

Jackson JR and Marabelli M, 'Algorithmic Bias' [2018] 15(4) Accountability & Ethics

Jay S and others, 'Environmental impact assessment: Retrospect and prospect' [2007] 27(4) Environmental Impact Assessment Review

Johnson DG and Nissenbaum H, Computers, ethics & social values (Prentice Hall 1995)

Kaminski ME, 'The Right to Explanation, Explained' [2019] 34(1) Berkeley Technology Law Journal

Kaminski ME and Malgieri G, 'Multi-layered explanations from algorithmic impact assessments in the GDPR' [2020] Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency

Kemper J and Kolkman D, 'Transparent to whom? No algorithmic accountability without a critical audience' [2019] 22(14) Information, Communication & Society

Kindt E, 'Transparency and Accountability Mechanisms for Facial Recognition' (GMFUS, 3 February 2021) <https://www.gmfus.org/news/transparency-and-accountability-mechanisms-facial-recognition> accessed 14 February 2022

Kloza D and others, 'Towards a method for data protection impact assessment: Making sense of GDPR requirements' [2019] 1(1) D.pia.lab Policy Brief

Köchling A and Wehner MC, 'Discriminated by an algorithm: a systematic review of discrimination and fairness by algorithmic decision-making in the context of HR recruitment and HR development' [2020] 13(3) Business Research

Koops B, 'The trouble with European data protection law' [2014] 4(4) International Data Privacy Law

Kosta E, Data protection impact assessment. in , The EU General Data Protection Regulation (GDPR): A Commentary (Oxford University Press 2020)

Krafft TD and others, 'How to regulate algorithmic decision-making: A framework of regulatory requirements for different applications' [2022] 16(1) Regulation & Governance

Kroll J and others, 'Accountable Algorithms' [2016] 165(1) University of Pennsylvania Law Review

Kuner C and others, The EU General Data Protection Regulation (GDPR): A Commentary (Oxford University Press 2020)

Langevoort DC, 'Cultures of Compliance' [2017] 54(4) American Criminal Law Review 937

Lawrence DP, Environmental Impact Assessment: Practical Solutions to Recurrent Problems (1 edn, John Wiley & Sons, Inc 2003) 165

Lee NT, 'Detecting racial bias in algorithms and machine learning' [2018] 16(3) Journal of Information, Communication and Ethics in Society

Lepri B and others, ' "Fair, Transparent, and Accountable Algorithmic Decision-Making Processes' [2018] 31(4) Philosophy & Technology

Lessig L, Code and Other Laws of Cyberspace (Basic Books 1999)

Library of congress, 'Brown v Board at Fifty: "With an Even Hand"' (Library of Congress) <http:/loc.gov> accessed 16 May 2022; Library of congress, 'The Civil Rights Act of 1964: A Long Struggle for Freedom' (Library of Congress) <http:/loc.gov> accessed 16 May 2022

Nahmias Y and Perel M, 'The Oversight of Content Moderation by AI: Impact Assessments and Their Limitations' [2021] 58(1) Harvard Journal on Legislation

Maccarthy M, 'An Examination of the Algorithmic Accountability Act of 2019' [2019] 1(1) Transatlantic High Level Working Group on Content Moderation Online and Freedom of Expression

Maggiolino M, 'EU Trade Secrets Law and Algorithmic Transparency' [2019] 1(1) Bocconi Legal Studies Research Paper No 3363178

Makridis CA, 'Do data breaches damage reputation? Evidence from 45 companies between 2002 and 2018' [2021] 1(8) Journal of Cybersecurity

Martin K, 'Ethical Implications and Accountability of Algorithms' [2019] 160(1) Journal of Business Ethics

Metawa N, Elhoseny M, Hassan MK and Hassanien AE, 'Loan Portfolio Optimization using Genetic Algorithm: A case of credit constraints' [2016] 12th International Computer Engineering Conference

Morgan R, 'Environmental impact assessment: The state of the art' [2012] 30(1) Impact Assessment and Project Appraisal

Moss E and others, 'Assembling Accountability: Algorithmic Impact Assessment for the Public Interest' [2021] 1(1) SSRN Electronic Journal

Murray A and Scott C, 'Controlling the New Media: Hybrid Responses to New Forms of Power' [2002] 65(4) The Modern Law Review

New J and Castro D, How Policymakers can foster Algorithmic Accoutability (Center for Data Innovation 2018)Newell S and Marabelli M, 'Strategic opportunities (and challenges) of algorithmic decision-making: A call for action on the long-term societal effects of 'datification'' [2015] 24(1) Journal of Strategic Information Systems

Neyland D, 'Bearing Account-able Witness to the Ethical Algorithmic System' [2016] 41(1) Science, Technology, & Human Values

NOREA, NOREA Handreiking Data Protection Impact Assessment (2 edn, NOREA 2020)

Nos, 'De verzekering is bij huisnummer 186A duurder dan bij 186' (NOS, 26-08-2015) <https://nos.nl/artikel/2054035-de-verzekering-is-bij-huisnummer-186a-duurder-dan-bij-186> accessed 9 September 2021

Ortolano L and Shepherd A, 'Environmental impact assessment: challenges and opportunities' [1995] 13(1) Impact Assessment

Pan S, Larson K, Bradshaw J and Law E, 'Dynamic task allocation algorithm for hiring workers that learn' [2016] Proceedings of the Twenty-Fifth International Joint Conference on Artificial Intelligence

Parker C, The Open Corporation: Effective Self-regulation and Democracy (Cambridge University Press 2002)

Politou E and others, 'Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions' [2018] 4 J Cybersecur

Pool AH, 'Artikel 35 Gegevensbeschermingseffectbeoordeling' [2019] Arbeidsovereenkomst

Pötzsch S, 'Privacy Awareness: A Means to Solve the Privacy Paradox?' [2008] 298(1) IFIP Advances in Information and Communication Technology

Price WN, 'Big Data and Black-Box Medical Algorithms' [2018] 10(471) Science Translational Medicine

Quelle C, The Data Protection Impact Assessment: What can it contribute to data protection? (Thesis for the Research Master in Law and the Master's program Law and Technology 2013-2015 2015)

Rader E and others, 'Explanations as Mechanisms for Supporting Algorithmic Transparency' [2018] 103(1) CHI '18: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems

Rainie L and Anderson J, 'Code-Dependent: Pros and Cons of the Algorithm Age' [2017] Pew Research Center

Rawlins B, 'Give the Emperor a Mirror: Toward Developing a Stakeholder Measurement of Organizational Transparency' [2008] 21(1) Journal of Public Relations Research

Reuter P, The General Data Protection Regulation (GDPR): An EPSU briefing (1 edn, EPSU 2019)

Rosenblat A, Kneese T and Boyd D, 'Algorithmic Accountability' [2014] The Social, Cultural & Ethical Dimensions of "Big Data" OSF Preprints

Rowe F, 'Contact tracing apps and values dilemmas: A privacy paradox in a neo-liberal world' [2020] 55(1) International Journal of Information Management

Rücker D and Kugler T, New European General Data Protection Regulation: A Practitioner's Guide (1 edn, Hart Publishing 2017) 1

Ryan J and Toner A, 'Europe's enforcement paralysis: ICCL's 2021 report on the enforcement capacity of data protection authorities' [2021] Irish Council for Civil Liberties

Sanchez-rola I and others, 'Can I Opt Out Yet?: GDPR and the Global Illusion of Cookie Control' [2019] 1(1) In Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security (Asia CCS '19)

Sander B, 'Freedom of Expression in the Age of Online Platforms: The Promise and Pitfalls of a Human Rights-Based Approach to Content Moderation' [2020] 43(4) Fordham International Law Journal

Sarrat J and Brun R, DPIA: How to Carry out One of the Key Principles of Accountability. in, Privacy Technologies and Policy (Springer 2018) 173

Schermer BW and others, Handleiding Algemene verordening gegevensbescherming (Ministerie van Justitie en Veiligheid 2018)

Schnackenberg AK and Tomlinson AC, 'Organizational Transparency: A New Perspective on Managing Trust in Organization-Stakeholder Relationships' [2014] 42(6) Journal of Management

Scott C, 'Accountability in the Regulatory State' [2000] 27(1) Journal of Law and Society

Shah H, 'Algorithmic accountability' [2018] 376(1) Philosophical Transactions of The Royal Society A Mathematical Physical and Engineering Sciences

Seaver N, 'Algorithms as culture: Some tactics for the ethnography of algorithmic systems' [2017] 4(2) Big Data & Society

Shapiro A, 'Reform predictive policing' [2017] 541(7638) Nature <http://dx.doi.org/10.1038/541458a> accessed 16 May 2021

Sobolewski M and others, 'GDPR: A Step Towards a User-centric Internet?' [2017] 52(4) Intereconomics

Solove DJ, 'The Myth of the Privacy Paradox' [2021] 89(1) George Washington Law Review

Tan E, 'Seven out of ten customers would boycott a brand that mishandled their data' (Campaign, 9 February 2018) <https://www.campaignlive.co.uk/article/seven-ten-customers-boycott-brand-mishandled-data/1456749> accessed 14 February 2022

The Ada Lovelace Institute and Datakind UK, 'Examining the Black Box: Tools for assessing algorithmic systems' (Ada Lovelace Institute, 29th April) <https://www.adalovelaceinstitute.org/report/examining-the-black-box-tools-for-assessing-algorithmic-systems/> accessed 9 March 2022

UN Human Rights Committee (HRC) 'CCPR General Comment No. 18: Non-discrimination' (10 November 1989)

University of Hawaii Cancer Center. "Algorithm to find precise cancer treatments." ScienceDaily. ScienceDaily, 9 August 2016. <www.sciencedaily.com/releases/2016/08/160809185854.htm>.

Van den Hoven van Genderen R, 'Algoritmen en AI: distopische black box of glazen bol? Is een wettelijk kader voor transparantie van algoritmen mogelijk en wenselijk?' [2020] 5(1) Computerrecht

Veale M and others, 'Algorithms that remember: model inversion attacks and data protection law' [2018] 376(1) Philosophical Transactions of the Royal Society A

Veale M and others, 'Fairness and Accountability Design Needs for Algorithmic Support in High-Stakes Public Sector Decision-Making' [2018] Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI'18)

Vedder A and Naudt L, 'Accountability for the use of algorithms in a big data environment' [2017] 31(2) International Review of Law, Computers & Technology

Vyravene R and Rabbanee FK, 'Corporate negative publicity – the role of cause related marketing' [2016] 24(4) Australasian Marketing Journal

Wachter S, Mittelstadt B and Floridi L, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' [2017] (2) Harvard Journal of Law & Technology

Wang R and others, 'Factors Influencing Perceived Fairness in Algorithmic Decision-Making: Algorithm Outcomes, Development Procedures, and Individual Differences' [2020] 1(1) Conference: CHI '20: CHI Conference on Human Factors in Computing Systems

Waters N, Privacy Impact Assessment - Great Potential Not Often Realised. in David Wright and Paul De hert (eds), Privacy Impact Assessment (Springer 2012)

Weber RH and Studer E, 'Cybersecurity in the Internet of Things: Legal aspects' [2016] 32(5) Computer Law and Security Review

Wieringa M, 'What to account for when accounting for algorithms: a systematic literature review on algorithmic accountability' [2020] FAT* '20: Conference on Fairness, Accountability, and Transparency

Woollven C, '7 Key Stages of the Data Protection Impact Assessment (DPIA)' [2021] IT Governance (4 September 2019) <https://www.itgovernance.co.uk/blog/gdpr-six-key-stages-of-the-data-protection-impact-assessment-dpia> accessed 3 May 2021.

Wright D and De Hert P, Privacy Impact Assessment (6 edn, Springer 2012)

Yu H and others, 'Building Ethics into Artificial Intelligence' [2018] IJCAI

Zarsky T, 'Incompatible: The GDPR in the Age of Big Data' [2017] 4(2) Seton Hall Law Review

Zhou J and Chen F, Human and Machine Learning (Springer International Publishing 2018)