From Bilateral to Ecosystemic Transparency: Aligning GDPR's Transparency Obligations with the European Digital Ecosystem of Trust

Kostina Prifti, Joris Krijger, Tamara Thuis and Evert Stamhuis

A. Introduction

Trustworthiness plays a crucial role in the ambition of Europe's digital leadership plans. With its vision for innovation and data technologies such as Artificial Intelligence (AI), the EU seeks to make ethics 'a core pillar' for developing a unique approach to digital innovation. Guidelines and regulatory frameworks of recent years, such as the Ethical Guidelines for Trustworthy AI and the Draft AI Act, are shaped by the ambition to ensure excellence and trust. By enacting the General Data Protection Regulation (GDPR), Europe already introduced the most human centred data protection law in the world, but questions remain about its efficacy[1] and its ability to address all normative data protection concerns in the age of AI.[2] In this chapter we highlight a specific concern related to transparency, one of the core components of human centred AI. More specifically we focus on the relation between the ambition of fostering trustworthiness and the approach to transparency obligations in the GDPR and potentially ensuing AI regulation. As a general characteristic these regulatory frameworks view transparency as a one-dimensional obligation between organizations and data subjects. As such, the functioning and conceptualization of transparency in the GDPR is determined by the overall rationale to "strengthen individuals' fundamental rights in the digital age". This rationale situates transparency obligations in the bilateral relation between individuals and organizations, imposing an implicit duty of care on individuals to safeguard their legal rights and consequently ensure legal compliance of data controllers. Taking recent developments in the fields

1 *S. Mercer*, The Limitations of European Data Protection As A Model for Global Privacy Regulation, AJIL Unbound 2020, 20.

2 *M. Finck*, The Limits of the GDPR in the Personalisation Context. Forthcoming in: U. Kohl, J. Eisler (eds.), Data-Driven Personalisation in Markets, Politics and Law, Cambridge 2021.

of legal, psychological, and organisational science into account, we contest that transparency in its current functioning, with primacy on informing data subjects, placing responsibility on the side of the individual to enforce their rights, results in a realistic and thus fair allocation of responsibilities. As trust correlates with a clear and fair allocation of responsibilities the trustworthiness ambitions of Europe's digital leadership will suffer when the arrangement of obligations remains as incongruent as we will show it is, vis-à-vis the reality in which data driven systems operate.[3]

This chapter provides an exploration, critique, and expansion of the transparency concept in the GDPR by juxtaposing its functioning with the European ambition of becoming a digital ecosystem of trust. We begin with describing the current transparency obligations that are applicable in the case of data science applications, automated individual decision-makings (ADMs) more in particular exposing and abstracting the transparency rationale underlying the GDPR. We chose ADMs as our focal point because these are explicitly specified as data driven practice in the GDPR. ADMs will, despite limitations in Art. 22 of the GDPR, become increasingly more common with the introduction of AI and will, in their current and future appearance, for a considerable proportion fall under the future regulation for AI. In that way our analysis of incumbent regulation also speaks for future regulation. Briefly put, we challenge the positioning of transparency obligations in the bilateral relation between individuals and organizations and the subsequent distribution of responsibilities that is structured around individuals proactively enforcing their rights. We discuss some key issues of the current functioning of transparency obligations in the GDPR and examine the limitations to the underlying rationale in relation to the notion of a trustworthy digital ecosystem. As a result, the chapter advances the claim that the incongruence between the legal notion of transparency and the rationale of fostering trust ought to be reduced by expanding the concept of transparency to a multilateral concept with more actors in an applied manner, thus diversifying and rebalancing the allocation of responsibilities. Transparency as currently conceptualized in the GDPR is insufficient to meet the trustworthiness objectives behind transparency obligations.

Existing literature on transparency in the case of ADMs and other AI powered applications focuses mainly on developing various mechanisms

3 *J. van den Hoven/G. Comandé/S. Ruggieri/J. Domingo-Ferrer/F. Musiani/F. Giannotti/F. Pratesi/M. Stauch/I. Lishchuk* Towards a Digital Ecosystem of Trust: Ethical, Legal and Societal Implications, Opinio Juris In Comparatione 2021, 131.

that contribute to increasing transparency for the individual, facilitating as such the creation of the "informed individual" who then uses the information enabled by transparency to act rationally in defence of their rights.[4] The novelty of the analysis and proposed solution in this chapter is a shift from the direction of improving transparency towards a direction that simultaneously expands and applies the concept of transparency. We suggest that an approach rooted in the digital ecosystem renders an implementation of transparency that better serves the aim to promote trust. Our approach seeks to improve the congruency between the normative allocations of responsibilities and the empirical reality of the actor-relation networks that we call the ecosystem. We first criticize the lack of realism in the currently dominant perception of how it works in the relation between organization and individual. A second line of critique aims at the narrow recognition of relevant relations in current policy developments. In a way, we endorse the plea of Felzmann et al. who worked on transparency in the relation between technology providers and users and we extend their contextualisation effort in the direction of the ecosystem of trust.[5]

B. Current transparency obligations

This section is structured as follows. Owing to the limited technological scope of ADMs when reviewing transparency, the meaning of ADMs is firstly clarified. Secondly, an overview and analysis of legal transparency obligations pertaining to ADMs is provided. Lastly, the section abstracts the legal regulation of transparency for ADMs by exposing the overarching rationale and its main implications. The main takeaway from the transparency rationale in reference to ADMs is that it is positioned in a two-party relation between an organization and an individual, a relation in which or-

4 See for example: *H. Felzmann/E. Fosch-Villaronga/C. Lutz/A. Tamò-Larrieux*, Towards transparency by design for artificial intelligence, Science and Engineering Ethics 2020, 3333; *E. Bayamlıoğlu*, The right to contest automated decisions under the General Data Protection Regulation: Beyond the so-called "right to explanation", Regulation & Governance 2021, available at https://onlinelibrary.wiley.com/doi/full/10.1111/rego.12391 (last access: 05.09.2022); *S. Wachter/B. Mittelstadt/L. Floridi*, Transparent, explainable, and accountable AI for robotics, Science robotics 2017, available at https://www.science.org/doi/10.1126/scirobotics.aan6080 (last access: 05.09.2022).

5 *Ibid*.

ganizations are obliged to provide information intelligibly and individuals are expected to utilise the information to protect their legal interests.

I. ADMs and profiling; AI powered or not

ADMs were firstly regulated by law in a direct manner in Art. 22 GDPR. This article being positioned between Arts. 12–23 GDPR, the ruling on ADMs seems to be categorised by the legislator as part of rights of data subjects, specifically phrased as a right not to be subjected to a decision based solely on automated processing. Briefly explained, there are a few elements that qualify a decision as an ADM and consequently trigger Art. 22 GDPR. Firstly, the decision must have been made *solely* by automated (what may be termed "autonomous") processing. In other words, the human intervention is missing in the decision-making process. Importantly, this must not be understood as there being no human intervention, as humans are the ones that develop and operate the system. Instead, it means that once the system is designed and composed with the necessary data and logic of processing the data, the system works autonomously, and its results are not reviewed by a human in the loop.[6] Secondly, Art. 22 GDPR takes under its regulative effect only those kinds of autonomous decisions that either produce a legal effect on the individual, or significantly affect them. A legal effect may be losing a job, or being denied healthcare, whereas a significant effect on individuals relates to cases like discrimination. Therefore, a decision falls under the applicability of Art. 22 GDPR if it is autonomous and produces legal effects or similarly affects individuals. As profiling can be done with or without ADM applications, Art. 22 GDPR covers ADM applications with or without profiling. ADMs processing personal data are, in principle, banned – individuals have a right not to be subjected to these kinds of decisions. The techno-empirical reality however is that ADMs are widely used, often based on consent, but also in places where its usage is authorized in the implementing legislation in the member state. Indeed, paragraph 2 of Art. 22 GDPR provides a gateway by outlining three exceptions: when it is necessary for a contract (e.g. in the case of a job opening for which there are 3000 applicants and only 4 HR mem-

6 Article 29 Data Protection Working Party, Guidelines on transparency under Regulation 2016/679, 17/EN WP260.

bers), when it is authorised by member state law, or when it is based on explicit consent.[7]

II. Legal obligations for transparency

To these ADM applications several transparency obligations apply. Transparency is one of the overarching principles in the GDPR, and it is further deduced to several types of obligations, which may be grouped in three categories. The first group of obligations relates to *the right of individuals to get access to information*. Present mainly in Arts. 13–15 GDPR, access to information obligations aim to ensure that individuals are informed about the details of the processing activities, like the identity of controller and processor, the purposes of data processing, its length, data transfers etc. These details are expected to provide the individual with a clear view of the processing activities.

The second group of obligations is concerned with *information about the rights* that individuals have in relation to the processing of their personal data. Individuals' rights about their personal data are outlined in Arts. 15–22 GDPR, and they include the right to erasure, right to accuracy, portability, access, etc. Particularly applicable in cases of ADMs, data controllers must safeguard the individual's rights by enabling the possibility for human intervention, providing the chance for the individual to express their views, as well as to contest the decision when they believe it is inaccurate and/or unfair. In general, data controllers and processors are obliged to inform individuals, pursuant these two groups of obligations, on details of the processing and what rights individuals have in relation to these details.

The first two groups of obligations relate to the "what" dimension of information, namely what information ought to be given to individuals. The third group of obligations relates to the "how" dimension of information, comprising obligations that aim to ensure concise, intelligible, transparent, and easily accessible information. This third group of obligations is also referred to as "intelligibility". Intelligibility is one of the prevailing challenges of ADMs, exacerbated by the non-transparent nature of the decision-making process in machine learning, and particularly deep learning, algorithms.[8] When an ADM is already opaque to experts who developed

7 *Ibid*.

8 *N. Burkart/M. F. Hubner*, A survey on the explainability of supervised machine learning, Journal of Artificial Intelligence Research 2021, 245.

an ADM system, intelligibility to individuals as laypersons is, even more, a considerable challenge.

On a related note, scholars discuss the nature and exact content of a right to an explanation in the GDPR. This Regulation assumes an ex-ante approach to explainability, aiming to ensure that individuals receive an explanation before the processing starts. As a result, individuals, it seems, do not have the right to receive an ex-post explanation, through which the data controller explains the autonomous decision in their particular case.[9] An ex-ante approach to explainability disengages the explanation from contextuality, as the individual may be explained the algorithmic logic in general terms, but would still not know (before, during, and after the ADM) how these general rules of logic apply in their context. For instance, an individual may be explained that the logic of the ADM entails correlating expenditures with the ability to pay back a loan. However, the individual may not be aware, for example, that the loan was rejected because of a gambling addiction in the past, detected by an autonomous data collection and interpretation process. This kind of explanation would only be feasible ex-post. However, data controllers do not have an explicit obligation for ex-post explainability, which means that individuals must challenge and contest the decision before they become aware of what they are contesting specifically.

In summation, there are three kinds of transparency obligations in the GDPR. One kind aims to ensure that individuals are informed on the details of the processing. The second kind aims to ensure that individuals are informed on what their rights are in relation to the details of the processing. The third kind relates to the manner through which the first and second kind of transparency is delivered, usually referred to as explainability.

III. Abstracting the transparency rationale

The objective of the transparency obligations in the GDPR is to provide the necessary information to individuals in an intelligible way, thus empowering individuals to manage their legal rights and legal protection. In

9 *S. Wachter/B. Mittelstadt/L. Floridi*, Why a right to explanation of automated decision-making does not exist in the general data protection regulation, International Data Privacy Law 2017, 76.

this regard, transparency is often viewed as instrumental to due process.[10] The rationale for why individuals must receive information about the processing of their personal information and their rights in an intelligible manner is so that they can exercise their rights, which connects directly with due process. Relating this understanding to the traditional dichotomy found in the law between obligations of conduct and obligations of result, transparency obligations can be perceived as obligations of conduct. As a result, the assessment of whether data controllers have fulfilled their transparency obligations is based on their conduct, not on whether individuals are able to exercise their rights based on the information provided.

Secondly, the transparency obligations as outlined in the previous subsection are positioned mostly in the bilateral relation between organizations and individuals. Data controllers face transparency obligations to the individuals whose data they process, while the involvement of enforcement agencies like national Data Protection Authorities (DPAs) takes a secondary role. Specifically, since DPAs have the duty to monitor and enforce the GDPR, data controllers and processors must be transparent to DPAs about their work. The monitoring notwithstanding, the locus of transparency obligations is clearly the bilateral relation between organizations and individuals. Similar to consumer protection laws, the GDPR puts the weight on individuals to enforce their legal rights, with some support from enforcement agencies.[11]

Lastly, it is worth noting the exoteric conception of transparency that the GDPR advances.[12] The explainability obligations discussed above are guided by the aim of information being intelligible to laypersons. Scholars have evidenced that the GDPR lacks, and may benefit from, an esoteric conception of transparency, where the intricacies of ADMs are made transparent to experts, which would allow scrutiny on a deeper level.[13] The implementation of this idea would require transparency obligations that are different both in shape and form from the obligations that exist to support individuals whose data are being processed.

In conclusion, the positioning of transparency obligations in the bilateral relations between individuals and organizations means the individual,

10 *E. Bayamlıoğlu*, The right to contest automated decisions (n. 4).

11 *O. Butler,* Obligations imposed on private parties by the GDPR and UK Data Protection Law: Blurring the public-private divide, European Public Law 2018.

12 *M. Grochowski/A. Jabłonowska/F. Lagioia/G. Sartor*, Algorithmic transparency and explainability for EU consumer protection: unwrapping the regulatory premises, Critical Analysis of Law 2021, 43.

13 *Ibid.*

being privileged with information rights, is implicitly attributed with the main responsibility of ensuring that data controllers and data processors comply with their legal obligations – at least as regards the processing of personal data of that individual. In other words, to individuals *a duty of care* is allocated, expecting them to be informed and act on that information in defence of their legal rights. In this regard, transparency is an enabler of due process, facilitating consent, contestation, and other rights for individuals. However, the practical limitations which disable or hinder the transparency obligations from fulfilling their aim and role as it extends to trust need our attention, now that we have shown how transparency is defined by its rationale. We will display the critique on the transparency regulation for ADMs in the next section.

C. *Empirical, legal and organisational critique*

Transparency obligations for ADMs in the GDPR aim to provide individuals with information that enables them to safeguard their rights in cases when their personal data is processed. This regulatory aim is coherent, insofar as it assumes that rational individuals would take action to safeguard their rights. However, the theoretical rationale for transparency in ADMs must be understood in relation to the empirical context in which it operates. As a result, this section will put forward practical and contextual considerations that challenge the transparency rationale for ADMs in the GDPR. Exposing practical limitations serves as a basis for critique and further development of the concept of transparency and its obligations in the case of ADMs. The section presents and reviews six practical problems that show lack of congruence between the conceptual intentions and the techno-empirical context of operation: information, knowledge, resources, manipulation, enforcement, and public interest problems.

Information problems

Transparency may be understood as an infrastructure for information, enabling access and intelligibility of the latter; information is a central tenet of transparency. However, besides the obligations that the GDPR provides in relation to transparency discussed in the previous section, there are two kinds of information problems that hinder the effectiveness of transparency obligations in the GDPR. These problems relate to cases

when individuals are not aware that a decision about them is made autonomously, which can occur for illegitimate or legitimate reasons.

Data controllers may illegitimately withhold information from individuals when a decision about them is made autonomously.[14] In such cases, the information asymmetry between organizations and individuals is strong considering that the information is entirely in the hands of data controllers who run the ADM. Individuals depend for the information on the organization itself, which may not always have an incentive to comply with the legal obligation to inform individuals.[15]

The legitimate reasons why organizations do not provide the necessary information to individuals as required by law may spring from effective use and competition considerations.[16] Consequently, as scholars point out, the picture in practice is more nuanced than what the GDPR suggests, often involving a balancing exercise.[17] One reason for effective use relates to the integrity of the algorithms behind the ADM. Operating organizations, in the context of their activities, must avoid risks of adversarial learning, referring to cases when users manipulate or circumvent the logic of the ADM.[18] Moreover, data controllers as businesses are weary of competition-related problems that may arise from giving information about the logic of the system. In some cases, that information may be protected under Intellectual Property (IP) rights, in other cases be perceived as a valuable trade secret.[19]

As a result, a closer look at the practical implementation of transparency obligations reveals that the right to access information, while seemingly clear and straightforward in legal doctrine, encounters practical challenges

---

14 *M. Hildebrandt*, Smart technologies and the end (s) of law: novel entanglements of law and technology, Cheltenham 2015.

15 *R. Mancha/D. Nersessian*, From Automation to Autonomy: Legal and Ethical Responsibility Gaps in Artificial Intelligence Innovation, Michigan Technology Law Review 2021, 55.

16 Burell 2016 classifies opaqueness because of manipulation and IP as intentionally opaque: *J. Burrell*, How the machine 'thinks': Understanding opacity in machine learning algorithms, Big Data & Society 2016, available at https://journals.sagepub.com/doi/full/10.1177/2053951715622512 (last access: 14.10.2022)

17 *T. Wischmeyer*, Artificial intelligence and transparency: opening the black box, in: T. Wischmeier/T. Rademacher (eds.), Regulating artificial intelligence, Cham 2020, p. 75.

18 *C. Meek/D. Lowd*, Adversarial learning, in: Proceedings of the eleventh ACM SIGKDD international conference on Knowledge discovery in data mining 2005, p. 641.

19 *E. Bayamlıoğlu*, Tright to contest automated decisions (n. 4).

that may disable the objective and instrumental role of transparency in relation to due process and empowering individuals.

Knowledge problems

The EU regulator adopts an implicit assumption, when regulating ADMs in the GDPR, that an informed individual is always able to safeguard their rights in relation to organizations that control and process their data. As behavioural economics clarifies, the expectation that more information leads to more rational choices is often fallacious and may frequently have the opposite effect.[20] The fallacy arises out of an approach towards information and knowledge as being the same. In other words, the EU regulator assumes that once an individual is informed, they *know how* to utilise the information for their benefit in safeguarding legal rights. Knowledge relates to being able to process information in a way that makes it actionable in a variety of ways, and we could question whether individuals, even after having acquired the information about the processing and their rights, do possess the knowledge to utilise the acquired information to their benefits. The fulfilment of the aim behind transparency obligations requires not informed, but knowledgeable individuals. However, transparency obligations focus only on producing informed individuals, which results in a misalignment between the aim of transparency and its actual obligations.

The literature on consumer attitudes and information points to a combination of this knowledge problem and the previous information problem. Koolen summarizes these as "apathy, attrition and disinterest".[21] Individuals do not give attention to information, are worn out by the frequency and inaccessibility of the information and effectively do not internalize that it is in their personal interest that information is provided. 'Why bother, I have nothing to hide', is the attitude that puts pressure on the whole chain from providing information to acquiring knowledge and dedicating energy to action, which is the next problem.

---

20 *G. Gigerenzer*, Moral satisficing: Rethinking moral behavior as bounded rationality, Topics in cognitive science 2010, 528.

21 *C. Koolen*, Transparency and Consent in Data-Driven Smart Environments, European Data Protection Law Review 2021, 174 with further references.

Resources problems

It is challenging to ensure that individuals are informed, and even more challenging to ensure that they are knowledgeable in how to safeguard their legal rights in the context of ADMs. Another practical challenge concerns the resources required for an individual to utilise the information provided because of transparency obligations to safeguard their legal rights. Limitations of resources may be financial, particularly worrying in cases of poorer and vulnerable groups. Contesting an ADM may require the hiring of professional legal services, which is affordable by only a few. Furthermore, limitations of resources may also be time related. To be informed, individuals are expected to spend time reading lengthy texts written in legalese language, sometimes even simply to accept or reject cookies, let alone in cases of complex ADM. When it comes to contesting, too, time constraints are significant as it may take years for a case to be finalised.

The problem of resources is challenging even in contexts where individuals are exposed to an ADM rarely, perhaps once or twice in their lifetime such as having applied for a loan or for a high-end job position. The advent of autonomous technologies like personal intelligent assistants, care robots, autonomous vehicles, and more, expand these challenges even further. With autonomous technologies, which operate without constant human supervision, an individual may be exposed to tens or hundreds of automated decisions in a single day.[22] The regulatory expectation that individuals would have resources to contest ADMs in such quantities would be simply unrealistic.

The resources problem challenges consent, too, considering that paragraph 2 of Art. 22 requires individuals to give explicit consent (as one of the bases) before an autonomous decision is taken about them. While this obligation may work in cases when individuals are rarely exposed to ADMs, although even then with many limitations,[23] it is severely challenged in cases where individuals are exposed to a large quantity of automated decisions. Individuals would not have the time, assuming they would have the desire and the ability, to engage in giving consent multiple times du-

22 *B. Liu*, Recent advancements in autonomous robots and their technical analysis, Mathematical Problems in Engineering 2021, available at https://www.hindawi.com/journals/mpe/2021/6634773/ (last access: 05.09.2022).

23 *E. Kosta*, Peeking into the cookie jar: the European approach towards the regulation of cookies. *International journal of law and information technology* 2021, 380; *Koolen*, Transparency and Consent (n. 21).

ring the days. It is also not an acceptable solution for consent to be given in an overarching "blanket" manner, as that does not fit the notion of consent that the GDPR advances.

The quantitative increase of ADMs, particularly in autonomous technologies, poses challenges also in the work of national DPAs. As the institution responsible for the enforcement of the GDPR and the competent authority to handle complaints against data controllers, DPAs are notoriously struggling to handle all complaints and requests within due and reasonable time.[24] These challenges arise as a combination of a lack of resources, funding, and staff members, and a quantitative increase in data processing activities, particularly ADMs. The rational model of due process that transparency supports, namely that informed individuals would complain to relevant authorities when their rights are infringed, is challenged not only from the individual perspective, who may not be informed, knowledgeable, or have the resources, but also from the institutional perspective.

Manipulation problems

Besides information, knowledge, and resource related problems, individuals may be manipulated in making choices in the context of ADMs, which might not necessarily align with their data processing preferences. Consent for data processing is to a great extent self-management by individuals. However, privacy protection based on privacy self-management frameworks (consent and contest) fails to protect individual privacy and misses the collective dimension of privacy.[25] The implication of privacy self-management is that individuals make their own decisions whether to accept or reject the conditions presented to them by a data processor. Important to consider is that in making choices, outcomes are, besides rational deliberation, influenced by the design of the choice environment.[26] Consequently, the way the choice is presented by the data processor may

24 *B. Daigle/M. Khan*, The EU general data protection regulation: an analysis of enforcement trends by EU data protection authorities, Journal of International Commerce and Economics 2020, available at https://www.usitc.gov/staff_publications/jice/eu_general_data_protection_regulation_analysis (last access: 05.09.2022).

25 *L. Baruh/M. Popescu*, Big data analytics and the limits of privacy self-management, New Media & Society 2017, 579.

26 *M. Weinmann/C. Schneider/J. vom Brocke*, Digital Nudging, Business & Information Systems Engineering 2016, 433.

influence to a great extent how an individual chooses to reject or accept terms and conditions.[27]

One way to influence decisions through choice architecture is through making use of nudging techniques. According to Thaler and Sunstein,[28] a nudge is "any aspect of the choice architecture that alters people's behaviour in a predictable way without forbidding any options or significantly changing their economic incentives". Nudging in the context of consent for data processing can include altering the provision of information, correcting misapprehensions about social norms, altering profiles of different choices, or implementing default options.[29] In a digital environment, such as websites or mobile applications, nudging implies the use of design-elements in the user interface to alter the behaviour and thus choices of data subjects.[30] Examples of digital nudges in the realm of cookie consent is for instance the use of different colours or the two-step cookie design, presenting the accept option as more attractive choice.

Transparency objectives are, therefore, hindered by manipulation problems such as the case of nudging, where organizations may abide by the legal obligations of transparency while still nudging individuals to make certain choices that suits the organizations' cost-benefit considerations.

Enforcement problems

Mercer notes that, despite the advanced and established status of the GDPR, its efficacy can be questioned as, so far, there have been only few notable enforcement actions.[31] We see at least three causes that can be discerned for this lack of enforcement, that come on top of the resources problem we mentioned above. The first relates to the discrepancy between attitudes towards privacy and actual behaviour. This discrepancy is known as the 'privacy paradox': although users value privacy they take very little

27 *E. J. Johnson/S. B. Shu/B. G. C. Dellaert/C. Fox/D. G. Goldstein/G. Häubl/R. P. Larrick/J. W. Payne/E. Peters/D. Schkade/B. Wansink/E. U. Weber*, Beyond nudges: Tools of a choice architecture, Marketing Letters 2021, 487.

28 *C. R. Sunstein/R. H. Thaler*, Nudge: Improving decisions about health, wealth, and happiness, New Haven 2008.

29 *Y. Lin/M. Osman/R. Ashcroft.*, Nudge: Concept, Effectiveness, and Ethics, Basic and Applied Social Psychology 2017, 293.

30 *Weinmann/Schneider/vom Brocke*, Digital Nudging (n. 26).

31 *S. Mercer*, The Limitations of European Data Protection (n. 1).

action to protect their personal data or enforce their privacy rights.[32] A second reason for the relatively small number of enforcement actions concerns the nature of risks and harms that, from a traditional regulatory perspective, are not significant enough to warrant enforcement action. Compared with other chapters and articles in the Charter of Fundamental Rights of the European Union, such as freedom of expression or right to integrity of the person, the harms resulting from a violation of privacy regulation seem relatively small, especially when they are addressed on an individual level. The third concerns the 'enforceability' of these privacy regulations. As Finck remarks,[33] advanced algorithms are trained on training data, which is often personal data, before being deployed. This way of training raises the question of how data subjects' rights that involve the modification or deletion of data can be reconciled with the nature of these technologies. She stresses that this might make it difficult, if not impossible, to implement their rightful request to have their data removed. Given the time and costs of retraining models, enforcing GDPR rights comes close to removing the entire model that has been fed with their data.

Public interest problems

The GDPR relies on consent as a notion of individual self-determination. As discussed above there is good reason to question the understanding individuals have to the digital ecosystem they operate in, rendering the basis of their consent problematic. However, there is another problem with this focus on individual rights and consent, as this "fails to capture communal repercussions and the impact of individual consent on the public interest".[34] Fairfield and Engel therefore proposed to view privacy not as a private good, but as a public good since 'an individual who is careless with data exposes not only extensive information about herself, but about others as well'.[35] By focusing on grounds for making data available on an individual level, such as consent for data collection or processing, the GDPR misses the repercussions this consent can have on a public level. An individual decision about data sharing can, through storing, aggregating, or combining data sets, affect others in ways they never consented to. In

32 *A. Acquisti/J. Grossklags*, Privacy and rationality in individual decision making, Security & Privacy 2005, 26.
33 *Finck*, The Limits of the GDPR in the Personalisation Context (n. 2).
34 *Ibid.*, p.1.
35 *C. Engel/J. A.T. Fairfield*, Privacy as a Public Good, Duke Law Journal 2015, 385.

a transparency framework tailored to informed proactive individuals this public aspect is overlooked.

D. Trust and Transparency

The shortcomings and limitations discussed above raise the question as to what extent transparency obligations in the GDPR serve the ecosystem of trust the European Union seeks to establish. To align the functioning of transparency with the notion of a European trustworthy digital ecosystem we propose a focus on redefining the notion of transparency from bilateral to ecosystemic, recognizing the empirical reality of the individual and the context of deployment of advanced technologies that warrant approaching the relevant relations more broadly. Before further fleshing out this complementary conceptualization of transparency we will first analyse in more detail how the current functioning of transparency, and subsequent distribution of responsibilities centred on proactive individual enforcement of rights, relates to an ecosystem of trust.

In its Data Governance Act the European Union describes a 'trustworthy environment' as something that "requires instruments able to ensure that data from the public sector, industry and citizens is available for use in the most effective and responsible manner, while citizens retain a reasonable degree of control over the processing of data they generate, and businesses can rely on adequate protection of their investments in data economy".[36]

Trust, however, is a complex concept that needs to be outlined somewhat more to pinpoint how GDPR's shortcomings might impact this ecosystem of trust. Trust, as a psychological state, is a subjective attitude where one accepts a vulnerability based on positive expectations of the intentions or behaviour of another.[37] It has often been remarked that trust functions as an important prerequisite of technology acceptance and adoption.[38] Trust, in the context of AI, is often related to trust in machines and transparency, then, is regarded as a method to enhance trust in

36 Data Gouvernance Act, Explanatory Memorandum.

37 *D. M. Rousseau/ S. B. Sitkin/R. S. Burt/C. Camerer*, Introduction to Special Topic Forum: Not so Different after All: A Cross-Discipline View of Trust, The Academy of Management Review 1998, 393.

38 E.g. *V. Venkatesh/J. Y. L. Thong/X. Xu*, Unified Theory of Acceptance and Use of Technology: A Synthesis and the Road Ahead, Journal of the Association for Information Systems 2016, 328; *K. Siau/W. Wang*, Trust is hard to come by.

technological artefacts. For example, the positive effect on trust when AI assistants provide a transparent reasoning for choosing one solution over a set of alternatives.[39] However, trust in the digital economy requires something else than trust in AI as a technology. When it comes to the digital economy and the role of AI in it, it is much more relevant to assess data infrastructures, institutions and mechanisms. To relate this notion of trust to a digital ecosystem of trust we will use van den Hoven et al. definition of a digital ecosystem of trust.[40] They define a digital ecosystem of trust as "a system of interacting organisms and their environment, in which appropriate norms are clear to parties, and responsibilities are well defined and adequately and fairly allocated to actors and agents. Trust needs to be horizontal between citizens and parties and vertical between citizens and governments".[41]

Our main criticism of transparency as it functions in the GDPR is its strong but problematic emphasis on the proactive individual who shoulders the majority of the responsibility in making sure her rights are upheld and if necessary enforced. As the adequate and fair allocation of responsibilities is an important part of a digital ecosystem of trust, there emerges an incongruence between the current functioning of transparency and the role it could, or should, play in the broader digital ecosystem of trust.

We argue that the current conceptualization of transparency could or maybe even should be complemented with a functioning of transparency that addresses two aspects: a congruent representation of individuals' behaviour and of the relation-network in which the data driven technology operates. It is generally held that transparency, and transparency assessments, matter because access to relevant information is vital for maintaining accountability. Indeed, "transparency is thus a highly valued instrumental good, since it is an input into a process of monitoring that increases the odds that voters or consumers get what they want from institutional actors".[42] This is an important starting point for a different perspective on the role and function of transparency in the governance of

---

Building Trust in Artificial Intelligence, Machine Learning, and Robotics, Cutter Business Technology Journal 2018, 47.

39 *F. Biessmann et al.*, Transparency and trust in artificial intelligence systems, Journal of Decision Systems 2020. DOI: 10.1080/12460125.2020.1819094.

40 *van den Hoven/Comandé/Ruggieri/Domingo-Ferrer/Musiani/Giannotti/Pratesi/Stauch/Lishchuk*, Towards a Digital Ecosystem of Trust (n. 3).

41 *Ibid*, p. 134.

42 *N. Bowles/J. T. Hamilton/D. A. L. Levy* (Eds.), Transparency in Politics and the Media: Accountability and Open Government, Bloomsbury Publishing 2013, p. 15.

data driven systems. As we have shown, such a perspective goes beyond the bilateral individual and rights-oriented approach and requires a reconceptualization of transparency that is centred around its techno-empirical dimension. This approach complements the focus on possibilities for redress with an interpretation of transparency based on promoting trust in the data ecosystem and its accompanying accountability mechanisms. Where in the GDPR transparency may function as a normative limit to the power of organizations vis-à-vis individuals, we should focus on how the tool of transparency can also function to tailor power and responsibility to the more complex concrete context.[43]

Developing a transparency framework that redistributes responsibilities among multiple parties involved in the processing of data bears certain implications on the nature of transparency obligations in various spheres. To provide an impetus for the expansion of transparency from bilateral to ecosystemic, affecting multiple agents and actors rather than just an individual and an organisation, we will discuss three of these considerations such a framework should account for.

E. Expanding transparency obligations to foster trust; an exploration

As shown above, there is a clear need to broaden the conceptual domain of transparency obligations towards ecosystemic relationships. This requires redefining the bilateral individual-organization relationship and expand to, what *Brodie et al.*[44] describe as "network relationships among versatile actors in […] ecosystems". To facilitate the development of this revised transparency notion, this section exploratively analyses the second leg of that revision: the expansion of transparency obligations in ADMs to a broader relation network. Expanding transparency obligations to foster trust in a digital ecosystem requires the consideration of multilateral relations between all actors in the ecosystem. Following *Li et al.*[45] we take digital ecosystems to be "complex and interdependent systems and their underlying infrastructures by which all constituents interact and exhibit

43 *S. Gutwirth/P. Hert*, Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power, Privacy and Criminal Law 2006, 18.

44 *R. J. Brodie/J. A. Fehrer/E. Jaakkola/J. Conduit*, Actor Engagement in Networks: Defining the Conceptual Domain, Journal of Service Research 2019, 173.

45 *W. Li/Y. Badr/F.Biennier*, Digital ecosystems: challenges and prospects in: Proceedings of the International Conference on Management of Emergent Digital EcoSystems (MEDES '12), New York 2012, p. 117.

as a whole self-organizing, scalable and sustainable behaviors." Digital and business ecosystems are metaphorical to the biological ecosystem in which the interdependencies of all actors, coevolving in their capabilities in the environment, are highlighted.[46] Relating this field to technology and innovation one could say that a social innovation environment is about a set of actors from different societal sectors and their environment with legal and cultural norms, supportive infrastructures and many other elements that enable or inhibit the development of social innovations.[47]

Rather than situating transparency obligations solely in the information exchange between the individual and the organisation operating the technology, we seek to tailor transparency obligations to the specifics of the various relations that are part of a digital ecosystem. In the context of ADM applications, we distinguish, beyond the transparency interaction between individuals and organizations, transparency as related to the interactions within organizations, between organizations, between the organization and institutional bodies, between institutional bodies and individuals, either impacted by the technology or intermediary user/operator, between society/general public and organizations and society/general public and institutions. We will address a selection of these in the following section where we exploratively analyse some of the aspects of transparency obligations that require further alignment with the extent and complexity of interactions in the ecosystem in which advanced algorithms operate.

I. Experts, Oversight Institutions and Organizations

The positioning of transparency obligations beyond the bilateral relations between individuals and organizations bears certain implications on the nature of transparency obligations for other actors in the ecosystem. Specifically, since information must be made transparent to laypersons who are assumed to have little information and knowledge on the workings of AI, the "how" of transparency is guided towards simplicity. By being simple and concise, the information made transparent is intelligible to non-experts. As a result, an opportunity so far neglected is the relevance

46 *J.F. Moore*, The Death of Competition: Leadership and Strategy in the Age of Business Ecosystems, New York 1996.

47 *F. Sgaragli*, Enabling Social Innovation Ecosystems for Community-led Territorial Development, Rome 2014.

and utility of making information about ADMs transparent to experts.[48] Experts are involved in numerous capacities in the digital ecosystem, as representative of a professional user category or of a supervising mechanism, to name but a few. The duty to explain to experts bears some implications. Firstly, an inclusion of experts as beneficiaries of transparency obligations necessitates a change in the nature of transparency obligations, specifically because the information made transparent may be not only more technical and complicated but also more complete and thus more transparent. An expert-based level of scrutiny is higher than non-expert scrutiny. Therefore, the first change relates to the nature of the information that must be made transparent.

A second implication relates to the fact that an inclusion of experts creates the possibility for institutional oversight over the use of ADMs as regulated by the GDPR, a kind of oversight so far neglected by the regulatory framework. In this regard, expert-based institutional oversight may be categorised as: input, output, and throughput oversight.[49] Input oversight bears an ex-ante nature, relating to the involvement of institutional expertise before the ADM system is placed in the market. The proposed AI legislation by the European Commission may be understood closely to this type of oversight, insofar as AI powered ADM systems must pass a certification process before being placed in the market. However, the proposed legislation relies on market-based solutions since the ex-ante certification process is performed by licensed private actors,[50] so there is a possibility to expand the involvement of institutional expertise in an ex-ante manner. In principle, such expert-based oversight would ensure that only ADM systems that comply with legal requirements are made available to consumers.

Output-based oversight becomes necessary considering that, due to the unpredictable nature of AI powered ADMs, complying with ex-ante requirements does not guarantee that ADMs will not infringe individual's rights. In this regard, institutional expertise of the output-based type would benefit from transparent information to assess the impact of ADMs

48 *Grochowski/Jabłonowska/Lagioia/Sartor*, Algorithmic transparency and explainability for EU consumer protection (n. 12).

49 *B. Haggart/C. I. Keller*, Democratic legitimacy in global platform governance, Telecommunications Policy 2021, 1.

50 Article 19, Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts {SEC(2021) 167 final} – {SWD(2021) 84 final} – {SWD(2021) 85 final}.

on individuals. National DPAs have some minor output-based oversight competences according to the GDPR; for instance, they have the right to conduct ex officio investigations.[51] However, the resources problems identified in the previous section hinder them from effectively exercising these competences on a large scale. Lastly, throughput type of oversight relates to overseeing the process of using ADMs between their ex-ante approval and their ex-post assessment. Throughput oversight allows institutions to be informed and have some form of control over the process of using ADMs, which is relevant considering that process-related problems may not be evident before or after the use of ADMs, but only in the course of their use.

II. Choice Architecture, Developers and Stakeholders

The conceptualization of transparency mainly or solely in the bilateral relations between individuals and organizations also bears some challenges and implications from a more organizational perspective. Transparency obligations to provide information in a concise, intelligible, transparent, and easily accessible way are – as previously mentioned – limitedly enforced and allow for manipulation of the individual's choice. That results in an undesirable level of uncertainty. Organizations currently have no directions on the way in which cookie consent notices should be designed and presented to individuals. As shown in a study by *Bauer et al.*,[52] the way the choice architecture is designed in terms of salience, effort, and framing impacts the decision-making process of the individual. Transparency obligations in the design of the choice environment would not only enable individuals to make an unmanipulated choice but potentially increase awareness about these choices in society at large. These obligations could imply for instance the same level of salience and effort in the choice options presented to individuals to decrease the level of manipulation by data processors. Considering the concept of nudging previously mentioned, organizations can self-nudge to behave in a way that is more socially

51 Article 57, GDPR.

52 *J. M. Bauer/R. Bergstrøm/R. Foss-Madsen*, Are you sure, you want a cookie? – The effects of choice architecture on users' decisions about sharing private online data, Computers in Human Behavior 2021, 120.

preferable,[53] and enhances trust in the digital ecosystem in which they operate.

Besides the environment in which organizations and individuals interact, the current transparency obligation limitedly addressed the complex organizational structures in which ADMs are operating and interacting with individuals and their data. Instead of perceiving algorithms as constrained and procedural formulas, Seaver stresses the importance of understanding algorithms as "heterogenous and diffuse sociotechnical systems".[54] This understanding of algorithms includes the embedding of the algorithm in the specific organizational context in which it is developed and/or used. ADMs are designed, developed and deployed by different types of actors over time, and hence a holistic overview and understanding of all processes including interdependencies by these actors are often impossible.[55] Within organizations, users and developers may know how the technology works on a certain level of abstraction, but rarely know everything about the technology and the chain of actions and processes connected to it.[56] There are different knowledge levels to what they know about the technique they use, as for instance managers responsible for an AI system do not understand the details of what data scientists develop. Consequently, the traceability as to who decided on what at which point in time about how the data is collected and processed could be compromised.[57] This limited traceability of the decision-making process may not only affect the type of information the organizations can provide but also how responsibilities are attributed in cases of disparate impact or negati-

53 *L. Floridi/J. Cowls/M. Beltrametti/R. Chatila/P. Chazerand/V. Dignum/C. Luetge/R. Madelin/U. Pagallo/F. Rossi/B. Schafer/P. Valcke/E. Vayena*, AI4People — An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations, Minds and Machines 2018, 689.

54 *N. Seaver*, Algorithms as culture: Some tactics for the ethnography of algorithmic systems, Big Data & Society 2017, available at https://journals.sagepub.com/doi/full/10.1177/2053951717738104 (last access: 06.09.2022).

55 *L. Floridi/J. Cowls/M. Beltrametti/R. Chatila/P. Chazerand/V. Dignum/C. Luetge/R. Madelin/U. Pagallo/F. Rossi/B. Schafer/P. Valcke/E. Vayena*, Auditing algorithms: Research methods for detecting discrimination on internet platforms, Data and Discrimination: Converting Critical Concerns into Productive Inquiry 2014, available at https://link.springer.com/article/10.1007/s11023-018-9482-5 (last access: 14.10.2022).

56 *M. Coeckelbergh*, Artificial Intelligence, Responsibility Attribution, and a Relational Justification of Explainability, Science and Engineering Ethics 2020, 2051.

57 *B. D. Mittelstadt/P. Allo/M. Taddeo/S. Wachter/L. Floridi*, The ethics of algorithms: Mapping the debate, Big Data & Society 2016 available at https://journals.sagepub.com/doi/full/10.1177/2053951716679679 (last access: 14.10.2022).

ve outcomes of ADM. With advanced algorithms becoming opaque for experts in the organizations, they influence how roles and responsibilities are delegated in the ADM processes.[58]

So, in the operations of the organization, users and even experts are often unaware of the unintended consequences or moral significance of the ADM system that they are using.[59] Moreover, professionals on a more managerial level seem to be increasingly aware and concerned about using algorithms responsibly, yet do not perceive it as their personal responsibility to act upon this concern.[60] While this gap in organizational responsibility can be partly explained by the uncertain nature and unpredictability of the long-term societal impact of innovation processes,[61] regulatory transparency obligations that account for the organizational structures surrounding ADMs could result in a fairer and clearer allocation of responsibilities, both inside and outside the organizations. Multilateral transparency obligations from an organizational perspective imply a reflection on the different tasks and roles of actors in the ADM process. If systems are designed in a non-transparent way, transparency should challenge the people involved in the process to take responsibility for its outcomes. Therefore, both regulations, as well as institutions such as a DPA and the organization itself, should consider who is to be held accountable for the ADM's implications, and thus define what level of transparency is required. As it is important to address unanticipated issues with the ADM, the system's design should allow for the possibility to reverse actions and make its behaviour visible so it can be grasped by the stakeholders involved.[62]

One development that receives much attention in the past years, is the use of Explainable AI (XAI) methods and techniques to provide a post-hoc explanation of the system's output. But we do not assess these as the panacea for the incongruency we deal with in this chapter. While these methods provide experts with additional insights and information about the algorithms that are developing and deploying, there is little understan-

58 *K. Martin*, Ethical Implications and Accountability of Algorithms, Journal of Business Ethics 2019, 835.

59 *M. Coeckelbergh*, Artificial Intelligence (n. 56); *A. Matthias*, The responsibility gap: Ascribing responsibility for the actions of learning automata, Ethics and Information Technology 2004, 175.

60 *Mancha/Nersessian*, From Automation to Autonomy (n. 15).

61 *M. Sand/I. van de Poel*, Varieties of responsibility: Two problems of responsible innovation, Synthese 2018, 4769.

62 *Mancha/Nersessian*, From Automation to Autonomy (n. 15), p. 136.

ding of how organizations use XAI methods in practice.[63] Additionally, most of these methods are deployed for the purposes of developers and machine learning engineers to debug models, and they limitedly address the needs of users or individuals as specified in the GDPR. Mittelstadt et al.[64] question for instance to what extent the methods, making use of local approximations, could be considered reliable and useful for non-experts. Another concern is that the use of explainable AI in the ADM context could even lead to unfair allocations of responsibility as individuals are given the perception that they have control over their data and how it is processed by providing them a post-hoc explanation.[65] In this way, designers of the system processing the data may distance themselves from the responsibility for the ADM's behaviour.

Lastly, conceptualizing transparency multilaterally fostering trust in the ADM's digital ecosystem, requires transparency obligations that effectuate a shift in focus from the relation between the data processor and the individual to a format in which organization also relate to groups of individuals, institutional bodies, other organizations, e.g.in a value chain. For instance, business organizations hire data processors, third-party vendors, to implement an algorithmic application within their business processes. With the involvement of third-party vendors, an organization is not a single actor, but part of a chain of actors that have a potential obligation to share information with individuals.

III. Public

While current transparency obligations are focused on protecting individual rights, this focus might conflict with a fair allocation of responsibility

63 *U. Bhatt/A. Xiang/S. Sharma/A. Weller/A. Taly/Y. Jia/J. Ghosh/R. Puri/J. M. F. Moura/P. Eckersley*, Explainable machine learning in deployment, Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency – FAT* '20, p. 648, available at https://dl.acm.org/doi/abs/10.1145/3351095.3375624 (last access: 06.09.2022).

64 *B. Mittelstadt/C. Russell/S. Wachter*, Explaining Explanations in AI, Proceedings of the Conference on Fairness, Accountability, and Transparency – FAT* '19, p. 279 available at https://dl.acm.org/doi/10.1145/3287560.3287574 (last access: 06.09.2022).

65 *G. Lima/N. Grgić-Hlača/J. Keun Jeong/M. Cha*, The Conflict Between Explainable and Accountable Decision-Making Algorithms, 2022 ACM Conference on Fairness, Accountability, and Transparency, p. 2103, available at https://arxiv.org/abs/2205.05306 (last access: 06.09.2022).

and the transparency objectives from the general public, society at large. From a more societal perspective, individuals could benefit from other data subjects sharing their data with data processing organizations to improve the accuracy and trustworthiness of the ADM process and outcomes. However, from an individual perspective, it might be worthwhile protecting one's own privacy and restrict organizations from collecting and processing personal data. One of the ways of balancing both interests is the involvement of stakeholders from multiple perspectives and invite them to co-design and co-own solutions,[66] hence cooperate with citizens and customers to create cohesion and collaboration in the ways transparency obligations are executed. An important element here is to make use of participatory mechanisms that help to assess to which extent tasks and decision-making should be delegated to ADMs in a way that is aligned with values and understanding of society.[67] A transparency obligation towards society at large could be compared to the current ESG related disclosure obligations of organizations to report on non-financial performance. Not only is this information useful to investors, it also fosters trust in an organization from a broader societal perspective when an organization is transparent about its policies and results.

In this way, transparency as a multilateral concept allows for dialogue between stakeholders in society varying from businesses, governmental institutions, and citizens, eventually collaborating to promote trust in the digital ecosystem as a whole.

F. Conclusion and further research

In this chapter we have developed the following point: Transparency obligations in the GDPR, in their current form – and to some extent the Draft AI Act – might have adverse effects on the 'envisioned digital ecosystem of trust' ambitions of the European Union, due to the unrealistic allocation of responsibility vis-à-vis individuals, as citizens, consumers or otherwise impacted persons. Our objections against the current conceptualisation can be summarized as: (a) it does not effectively help the data subject, (b) it does not provide guidance to the organization who operates the technology on what satisfactory transparency is, (c) it does not match the

66 *Floridi/Cowls/Beltrametti/Chatila/Chazerand/Dignum/Luetge/Madelin/Pagallo/Rossi/Schafer/Valcke/Vayena*, AI4People (n. 53).

67 *Ibid*.

complex ecosystem these technologies are part of, (d) it does not include the public interest as an accountable consideration.

A more just distribution of responsibilities, and therefore a more trustworthy ecosystem, might arise when transparency obligations are revised by (i) incorporating a realistic perception of what individuals can and will do and (ii) by extending transparency towards various other relations in the ecosystem, beyond the bilateral relation between individual and operating organization. We have highlighted several of these relations and provided suggestions for how transparency can have a role in them. How that plays out needs further attention in follow-up work.

A next step would be to define the actor-relation network around a concrete ADM use case, be it AI powered or not, and flesh out how in that network the transparency expectations exist, first in the normative perspective of law and ethics. It would certainly help the contextualisation of the outcome when the co-existence or interaction with incumbent transparency obligations is analysed more in-depth. With those we mean: transparency obligations that exist in a concrete use case but have nothing to do with GDPR or AI Act. It may be that incumbent obligations easily absorb the new ones, but more research is warranted. Examples of such situations are the disclosure between health care provider and patient, or the openness that is required for public administration bodies vis-à-vis citizens, the elected representatives, and the public at large.

Another line of research could follow-up on this and try to assess empirically what individual recipients appreciate as satisfactory information sharing in case of an ADM, both in process and in content, and under which conditions information sharing results in actionable knowledge. This would certainly move beyond the current research into algorithm appreciation,[68] as it takes algorithmic decision-making as a given and focuses more on contextual aspects. In that empirical project we would include

68 *G. Yalcin/E. Themeli/E. Stamhuis/S. Philipsen/S. Puntoni*, Perception of Justice by Algorithms, Artificial Intelligence and Law 2022, available at https://doi.org/10.1007/s10506-022-09312-z (last access: 06.09.2022); *N. Helbergera/T. Araujob/C. H. de Vreeseb*, Who is the fairest of them all? Public attitudes and expectations regarding automated decision-making, Computer Law & Security Review 2020, available at https://www.sciencedirect.com/science/article/abs/pii/S0267364920300613 (last access: 06.09.2022); *J. Gonçalves/I. Weber/G. M. Masullo/M. Torres da Silva/J. Hofhuis*, Common sense or censorship: How algorithmic moderators and message type influence perceptions of online content deletion, New Media & Society 2021, available at https://journals.sagepub.com/doi/10.1177/14614448211032310 (last access: 06.09.2022).

the perceptions and practices of professionals that try to live up to the standards of transparency they are confronted with.

The impact that our revision of transparency might have on costs of compliance in organizations is another line of research that we have not pursued at all.[69] We may hypothesize that a better fit to the ecosystem increases satisfaction and therefore has a beneficial effect on cost-benefit ratios in the long run but whether this is the case is open for debate.

We can conclude by stating that, to live up to the promises of excellence and trust, the EU should start to conceptualize transparency broader than it currently does. It should move from bilateral to ecosystemic transparency if it wants trust in digital technologies to prevail as this will allow it to arrive at a fairer distribution of risks and responsibilities that will befit its value driven approach.

69 *C. Tikkinen-Piri/A. Rohunen/J. Markkula*, EU General Data Protection Regulation: Changes and implications for personal data collecting companies, Computer Law & Security Review 2018, 134.