HAL open science

Towards a Right not to Be Deceived? An Interdisciplinary Analysis of Media Personalization in the Light of the GDPR

Urbano Reviglio

▶ **To cite this version:**

Urbano Reviglio. Towards a Right not to Be Deceived? An Interdisciplinary Analysis of Media Personalization in the Light of the GDPR. 18th Conference on e-Business, e-Services and e-Society (I3E), Sep 2019, Trondheim, Norway. pp.47-59, 10.1007/978-3-030-39634-3_5 . hal-03759113

HAL Id: hal-03759113

https://inria.hal.science/hal-03759113v1

Submitted on 24 Aug 2022

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution 4.0 International License

This document is the original author manuscript of a paper submitted to an IFIP conference proceedings or other IFIP publication by Springer Nature. As such, there may be some differences in the official published version of the paper. Such differences, if any, are usually due to reformatting during preparation for publication or minor corrections made by the author(s) during final proofreading of the publication manuscript.

Towards a Right Not to Be Deceived? An Interdisciplinary Analysis of Media Personalization in the light of the GDPR

Urbano Reviglio[1]

[1] LAST-JD International Joint Doctorate in Law, Science and Technology, University of Bologna, Bologna, Italy
urbanoreviglio@hotmail.com
http://orcid.org/0000-0001-5948-1476

Abstract. Privacy is a pillar of European law and of the new GDPR. Social and technological developments question its protection and raise the need for more comprehensive legal analysis. Informational and decisional privacy, in particular, prove to be fundamental rights to tackle the pervasiveness of surveillance practices and persuasive technologies. Yet, their protection is uncertain. The paper is a theoretical and interdisciplinary contribution structured as follows. In the first part, it is reviewed the literature on profiling and online personalization in order to provide an overview of the socio-technical landscape, with a special focus on media content and news personalization. In the second part, the consequences of the GDPR on media personalization is analyzed. In the third part, the interplay between data protection, consumer and media law is discussed. In particular, the right to receive information and the value of serendipity are introduced to eventually discuss the idea of a 'right not to be deceived' as a precondition to properly protect privacy and other human rights as well as to preserve trust between users and platforms.

Keywords: Privacy, Profiling, Personalization, GDPR, Data Protection

1 Introduction

Recently, much attention has been given to the assessment of the legal and social outcomes of the new General Data Protection Regulation (GDPR) as well as the E-privacy regulation draft. Despite the introduction of new individual rights and a more compre-hensive understanding of the data protection landscape, many commentators observed the limitations of these regulations. GDPR, for example, lacks a precise language and explicit and well-defined rights and safeguards [1]. There are many doubts on the ex-istence or even efficacy of novel rights such as a right to explanation – which is not explicitly mentioned in the GDPR – the right to transparency and the right to non-discrimination. Thus, many epistemic, technical, and practical challenges must first be overcome.

The article questions how the phenomenon of online personalization – particularly media and news personalization – is currently approached in the European legal frame-work and to what extent privacy is protected. More generally, it questions how the 'personalization paradox' – a trade-off between privacy and personalization quality – and the 'privacy paradox' – the users' inconsistent will to protect their privacy could be tempered. In more detail, the following questions are addressed: how can data subjects exercise their rights if the processing itself is opaque, difficult to understand, and unaware consent is usually given? To what extent does the GDPR ensure that profiling is legal, fair and non-discriminatory with regards to media personalization? And how does the European legislation deals with the risks posed by the employment of increasingly sophisticated techniques of persuasion and engagement that may eventually lead to manipulation?

In this paper, we specifically focus on personalization of media content which raises several social concerns and ethical discussions. In Section 2, we review the literature on emerging issues surrounding profiling and online personalization. In Section 3, an analysis of the new GDPR is done in order to clarify its effectiveness, its ambiguities and its limitations. More generally, we argue that data protection law is insufficient to prevent certain risks posed by media content personalization. Also, the paper advocates for the need to move from a mostly data-centric to a more user-centric view of privacy. Therefore, in Section 4 critical principles and human rights engaged in informational privacy are introduced and discussed and, eventually, conclusions are drawn.

2 Profiling and Data-driven Personalization

Humans constantly categorize, generalize and classify the world around them to reduce complexity. Algorithms can be programmed to automatically process information in similar ways. Profiling practices, thus, create, discover or construct knowledge from large sets of data from a variety of sources that then are used to make or inform decisions [2, 3]. Profiling occurs in a range of contexts and for a variety of purposes. This paper focuses on profiling that makes or informs decisions (presumed preferences) that personalize a user's media environment (e.g. content selection and ordering).

Of course, individuals can be misclassified, misidentified or misjudged, and such errors may disproportionately affect certain groups of people [4]. Profiling technologies, in fact, creates a kind of knowledge that is inherently probabilistic. They cannot produce or detect a sense of self but they can, however, influence a person's sense of self [2, 3]. In the case of media content personalization, individuals may start to want what is recommended to them without even realizing it, in a self-fulfilling prophecy [5]. Algorithms indeed threaten a foundational link in microeconomic theory, that is, preferences' formation [6]. At the same time, mass personalisation can be understood as pursuing the logic of market segmentation until each individual user is reduced to a unique market [7].

Aside from natural human dispositions such as selective exposure, confirmation bias and homophily, personalization of media content - particularly if implicit - can eventually limit information exposure and discovery. As such, filter bubbles [8] and echo chambers [9] are strengthened. In fact, personalization – in particular news personalization – could reduce opportunities to self-determine and negatively affect truth finding by reducing the exposure to alternative points of view and serendipity in the 'marketplace of ideas' [8, 9]. There may be several other consequences on both individual character, mindset and collective moral culture of our societies [7]; from the limitation of personal creativity to a reduction in the ability to build productive social capital. Mass personalization could also weaken media pluralism, solidarity and make people more politically polarized, narcissistic and vulnerable to (self)propaganda [9].

And in a self-reinforcing cycle, this would make people more susceptible to fake news or polarizing messages, help to spread misinformation and, ultimately, erode interpersonal trust. In general, critics argue that these are moral panics, and that personalization might instead foster the cultivation of expert citizens with stronger group identities [10]. It is no more than human nature empowered by the Internet. Yet, another prominent risk remains growing 'epistemic inequality', that is, the richer an individual's social network and the higher the education, the better the benefits of personalization.

In practice, the risks of personalization are very hard to prove and, eventually, to counteract [11]. There is indeed a crisis on the study of algorithms [12]. Their functioning is opaque and 'black-boxed' and their interpretability is not even clear [13]. Also, users consider filtering mechanism as neutral and actually few recognize them or attempt to opt-out [14]. Furthermore, concerns are growing because of the rise of increasingly sophisticated persuasive technologies and the ability of big-data to 'hyper-nudge' individuals and bring them to deception [15] (discussed in Section 4.3). Ultimately, key issues remain unsolved: to what extent personalization is detrimental and whether current legislation is sufficient to address these issues. Before problematizing the interplay between different legal fields, it is necessary to analyze the promises and perils of the current European data protection landscape.

3 European Legislation, GDPR and Its Limits

In the last years, the EU has adopted some provisions that give consumers the power to manage their personal data and not to be subject to automated decision-making such as personalization and algorithmic assistants. The right to data portability[1] envisaged in the new GDPR, as well as the e-Privacy regulation[2], and also the "retrieve them all" provision of the proposed Digital Content Directive, are all tools whereby digital consumers will supposedly have the chance to decide who should use their data to offer them the goods and services that they want [16]. These regulatory interventions bring to the fore a reshaping of the traditional landscape of the consumer protection rules providing a more comprehensive vision of "data consumer law". They in fact grant users several rights, such as the right to transfer data from one controller to another and the right to retrieve any data produced or generated through their use of a platform. They are expected to re-balance the relationship between data subjects and data controllers and to encourage competition between companies. These represent a new paradigm that abandons a purely protective and paternalistic regulation focused only on consumers' weaknesses to experiment with a more proactive approach [16].

Yet, critics suggest that the GDPR – one of the most lobbied piece of EU legislation to date [17] – delivers personalisation to companies on a golden plate [5]. Firstly, by shifting the prerequisite for more expansive (re)uses of personal data from anonymisation to 'pseudonymisation' (which still allows for some form of re-identification). In fact, although anonymised data is effective in protecting privacy, much analytical value of the data is lost through anonymisation (which is relevant for personalisation purposes).

---

[1] - Data portability refers to the ability to move, copy or transfer data easily from one database, storage or IT environment to another. To make an example, move one's Facebook profile to another social network.

[2] - Notice that the E-Privacy Regulation should be treated as *lex specialis* in relation to the GDPR. However, the enforcement mechanisms of GDPR and E-privacy Regulation remain the same.

Secondly, the GDPR facilitates personalisation by making the collection and processing/use of personal data essentially a matter of informational self-determination. This emphasis suggests to users that all that is at stake in data protection is their own personal interest whereas also fundamental collective public goods are actually at stake, such as deliberative democracy. Moreover, the GDPR lacks a precise language and explicit and well-defined rights and safeguards [1]. A number of provisions may thus lead to confusion, enforcement gaps or asymmetrical interpretations. This is understandable given that the reform of EU data protection is ongoing and need further guidelines.

The focus of the following analysis is specifically on the most relevant GDPR's articles affecting personalization dependent, above all, on 'profiling' which is a relatively novel concept in European data protection regulation (Art 4(4)). It refers to both the creation and the use of profiles. By virtue of deriving, inferring or predicting information, practices of profiling generate personal and sensitive data. The rights to erasure (Art 17) and restriction of processing (Art 18) are then useful forms of redress in the context of unlawful profiling techniques. Further guidance, however, is needed to clearly set out these Articles' scopes of application. This is also true for highly debated articles that we are going now to briefly analyze, namely Articles 13-15 and Article 22.

3.1 The Right to Transparency

Transparency is often assumed to be an ideal for political discourse in democracies and it is generally defined with respect to "the availability of information, the conditions of accessibility and how the information…may pragmatically or epistemically support the user's decision-making process" [18, p.106]. This is significant regarding decisions – in the case analyzed in this paper, prioritizing personalized media content – that are extremely complex and inevitably black-boxed.

Auditing is one promising mechanism for achieving transparency [19]. For all types of algorithms, auditing is a necessary precondition to verify correct functioning. For platforms that mediate political discourse, auditing can create a procedural record to demonstrate bias against a particular group. Auditing can also help to explain how citizens are profiled and the values prioritized in content displayed to them. It allows for prediction of results from new inputs and explanation of the rationale behind decisions.

Yet, many epistemic, technical, and practical challenges must first be overcome [20]. Firstly, a right to transparency might undermine the privacy of data subjects and the autonomy and competitive advantage of service providers, or even national security. Secondly, the rationale of an algorithm can be epistemically inaccessible, rendering the legitimacy of decisions difficult to challenge. Nevertheless, algorithm auditing may be quickly approaching and the belief that highly complex algorithms are incomprehensible to human observers should not be used as an excuse to surrender high quality political discourse. Developing practical methods for algorithmic auditing is highly needed. For example, Tutt [21] suggests that a regulatory agency for algorithms may be required, and this agency can "classify algorithms into types based on their predictability, explainability, and general intelligence" (p.15) to determine what must be regulated. Actually, GDPR requires data processors to maintain a relationship with data subjects and explain the logic of automated decision making when questioned (Art 13, 14 and 15). The regulation may indeed prove a much-needed impetus for algorithmic auditing.

However, with opacity, implementing transparency and the right to an explanation in a practically useful form for data subjects will be extremely difficult, necessary yet likely insufficient, as will be argued throughout the paper.

3.2 The Right to an Explanation

Especially relevant to profiling, there are the right to be informed (Art 13) and the right of access (Art 14). In particular, Articles 13(2)(f) and 14(2)(g) require data controllers to provide specific information about automated decision-making, based solely on automated processing, including profiling, that produces legal or similarly significant effects, namely: 1) the existence of automated decision-making, including profiling; 2) meaningful information about the logic involved; and 3) the significance and envisaged consequences of such processing for the data subject.

Article 15(1)(h) uses identical language as of the above articles and provides data subjects with a right of access to information about solely automated decision-making, including profiling. However, some key expressions in Articles 13-14, specifically "meaningful information about the logic involved" as well as "the significance and the envisaged consequences" (Art 13(2)(f)), need to be interpreted to provide data subjects with the information necessary to understand and challenge profiling and automated individual decision-making. As a result, the right to explanation has been interpreted in two drastically different ways: as an ex-ante general explanation about system functionality or as an ex-post explanation of a specific decision (Art 15). Yet, in the interest of strong consumer protection, meaningful information must be sufficient to answer questions that the data subject might have before they consent to the processing (notification) and after a decision has been made (right of access).

A right to explanation is thus not explicitly mentioned in the GDPR. However, relative legal basis have been detected [1]. In particular, Recital 71 states that data subjects have the right 'to obtain an explanation'. Yet, the legal status of recitals is debated as, in general, they only provide guidance to interpret the Articles so they are not considered legally binding. This is a critical gap in transparency and accountability [17].

3.3 The Right to Non-discrimination

Article 22(1) of the GDPR contains additional safeguards against one specific application of profiling, namely the case of automated individual decision-making that fulfils is "based solely on automated processing" and produces "legal effects concerning him or her or similarly significantly affects him or her". Profiling can indeed form the basis of decision-making that is both automated and produces significant effects, in particular discriminatory. A right to non-discrimination is, in fact, deeply embedded in the normative framework that underlies the EU and the use of algorithmic profiling for the allocation of resources is, in a sense, inherently discriminatory [22]. In this sense, Article 22 is set. There are, however, several ambiguities that must be settled.

Firstly, the wording of the "right not to be subject to automated decision-making" can be interpreted as either a prohibition or a right to object. This ambiguity has existed since the Data Protection Directive 1995 [1], but resolving it is nowadays critical [2]. Since profiling and automated decision-making often occur without the awareness of those affected, data subjects may not be able to effectively exercise their right to object. Moreover, Article 22 only applies to decisions that are "based solely" on automated processing, including profiling. Since "based solely" is not further defi-

ned in the regulation, the regulation allows for an interpretation that excludes any human involvement whatsoever. This would render the article inapplicable to many current practices of automated decision-making and there is the risk is that the controller may fabricate human involvement. Finally, paragraph 71 and Article 22(4) specifically address discrimination from profiling that makes use of sensitive data. Goodman and Flaxman [22] broadly questioned the interpretation of the wording 'sensitive data' and argued how significant is its clarification.

In summary, GDPR defines novel rights for data subjects and duties for data controller. Along with the e-Privacy regulation draft, it actually strenghtens 'data consumer protection'. Users can indeed decide whether to enter into a contract, be informed, access the data generated, receive information about the logic involved and not to be subject to automated decision-making based solely on automated processing. The data subject, however, waives some of these rights when entering into a contract for which an automated decision is 'necessary'. As a matter of fact, a user does not have any effective agency towards the logics involved in the personalized news provision. While at first sight data-driven personalization may appear to be only a matter of data protection law, the analysis of automated inferences, predictions or decisions more often lies outside of it [5]. In other words, data protection law focuses on 'inputs' rather than 'outputs', that are mostly out of its scope. Eventually, users will still have a limited (and indirect) control over the outcomes of personalization. In the following chapter, we evaluate the extent to which users may exercise such right and be fruitfully empowered.

4 A Comprehensive Approach to Media Personalization

Data protection law shows some limitations when it comes to the actual consumption of information in the context of media personalization. Yet, the application of consumer protection law to data-related commercial practices can certainly add to the protection offered by data protection law [23].[3] The complex interplay between data protection and consumer law need to be further analyzed in order to understand whether and how they might complement each other so as to be able to prevent the risks of media personalization. There is indeed a fundamental need for interdisciplinary work, not only across academics and practitioners, but also between different legal jurisdictions and across different disciplines. GDPR, for example, does not impose any responsibility on data controllers as regards the information a data subject might consume. Technically, there are two main dimensions that affect an individual's choice – the decision parameters employed by the algorithm and the level of choice which remains at the hands of the user [4] – GDPR focuses only on the former and ignores the latter. This critical point is particularly relevant in concentrated markets in which players refuse traditional editorial responsibility. As such, not only media law but particularly competition law maintain a significant – if not indispensable – role in setting standards and levelling the playing field [24].

[3] - Yet, applying consumer law to deals regarding personal data should never be construed as a justification for using personal data as a commodity as it would conflict with human rights.

To begin with, we acknowledge that informational and decisional privacy are fundamental for criticizing emerging means of opinion formation and behavioral change arising from personalization [25]. The latter is complementary with the former, and it is broadly intended as the right against unwanted access such as unwanted interference in our decisions and actions.[4] In addition, the right to freedom of expression is also significantly involved, especially because individual privacy has not been traditionally justified in terms of public good or interest of groups [5]. Thus, a reconceptualization of the right to be informed as a 'right to receive information' in order to increase control over data-driven personalization is discussed [26]. Related to this, it is introduced the the value of serendipity as a design principle [27]. These, however, may not even be sufficient to tackle the risks that personalization brings to privacy and freedom of expression, especially considering emerging techniques of behavioral modification [14, 15, 28]. In this light, the idea of a 'right not to be deceived' is introduced, as a conceptualization that could enact more effectively other fundamental human rights.

4.1 The Right to Receive Information

The news consumers' fundamental rights to receive information guaranteed by Article 10 ECHR may prove an important point of departure to realize democratic values in the personalized media landscape [26]. Information consumption is indeed deeply changed and needs to be reconceived. Given the vast amount of information produced and consumed, to some extent users are necessarily passive actors who have to delegate information filtering to algorithms and, therefore, to platforms. Thus, the right to information is, in effect, a right to receive information. How this would eventually translate is difficult to argue. Article 10 may nonetheless entail positive obligations for the state, such as ensuring that media users receive balanced news. Yet, it is an under-theorized right, lacking a framework to understand the rights of news consumers or the obligations of states regarding news recipients.

Media (and in particular news) personalization invites us to reconsider subjective rights to receive information. In traditional one-to-many media, people have a subjective right to receive information that others are willing to impart, but they do not have a right to receive information that the media is not willing to impart. In fact, the media would lose its editorial freedom if people could demand specific news stories and distribute these to them and, at the same time, if these were conflicting, it would be difficult to decide whose right to receive information should prevail. By enabling one-to-one communication, personalization technologies could, in theory, resolve conflicts between subjective rights to receive information and the media's or other parties' freedom of expression. Such a type of subjective right to receive information could help to establish what news consumers legitimately may expect from the news media with respect to the diversity or relevance of personalized recommendations.

Actually, media personalization may enable or hinder the exercise of this largely institutionally protected right. There are many different values and interests at stake especially with news personalization, which may lead to conflicts (prominently truth

[4] - Even if decisional privacy does not feature as a concept in the European legal tradition, art.8 of the ECHR does ackowledge the function of privacy as a right to personal development and autonomy as its underlying value.

finding versus social cohesion) that are not likely to end up in court but must be discussed in public. There is a need to discuss what the right to receive information should mean nowadays, how it relates to data protection, and to empirically study how people's information seeking strategies and privacy attitudes influence the exercise of this right.

Harambam et al [10] identifies four ways in which people so far can actually influence the algorithmically curated information they encounter, and these are: 1) Alternation, that is, switching between different news outlets and media forms, and also by using multiple or different recommenders. Yet, it requires effort, skills, and it does little to work around hidden biases in algorithmic curation. Then, 2) awareness, that is, being aware of algorithms functioning. In this respect, the GDPR, which raises the bar on transparency and user control over personal data processing, may have a positive impact.[5] 3) Adjustment, that is, adjust algorithms according to personal interests and wishes. Most news outlets, however, have not developed formal ways to influence their curating algorithms. And finally, 4) Obfuscation, that is, mobilizing against the data-driven processes through the deliberate addition of ambiguous, confusing, or misleading information to interfere with data collection. Yet, this may run against some of the goals and benefits of personalization.

The above techniques are not particularly effective as well as are difficult to pursue for the average user.[6] Yet, what forms of intervention at the level of data inputs and processing can be achieved in the context of algorithmic news recommenders to guarantee this right must be discussed further. This leads to a related issue which might help to better define strategies to tackle the current limitations of data protection law previously outlined.

4.2 The Value of Serendipity

Personalization also affects media law and threatens basic democratic principles such as diversity and pluralism. Generally speaking, media pluralism is achieved when users autonomously enjoy a diverse media diet. Even if media diversity online is shown to be more than in traditional media, such exposure does not always end up in an actual experience of diversity. Cognitive and affective factors that drive Internet users must also be considered [30]. This requires employing a user-centric perspective and extending beyond the assumption that supply diversity equals experience of diversity, and that diversity of sources equals diversity of content. Also, pluralism as a normative principle remains vague and under-theorized, and it is not a reliable indicator of a society's level of freedom, since it may create only the illusion of content diversity [31] In the digital age, it is indeed becoming less clear in which sense it is meaningful to speak of media pluralism if the consumption is characterized by limitless choice [32].

Given such limitations, current debates center on whether designing for more 'serendipity' might sustain diversity and represent an innovative design and ethical principle for information environments [27]. Extensive accounts on how to research serendipity and cultivate it in digital environments provide ground for novel studies. Yet, serendipity is an elusive and nuanced phenomenon; in this context, it is intended

[5] - This is the case with Facebook which is implementing a feature "why I am seeing this" to provide users a better understanding of the reasons why a post has been recommended [29].

[6] - Recently, it is even questioned whether the actual 'horizontal approach' based on the notion of 'average consumers' is fit to protect all consumers in a highly personalized digital environment [27].

as the attempt to design for unexpected and meaningful information encountering that are indeed statistically less likely, thus less accurate, and that intersect users' profiles. As such, it has the potential to prevent the threats of filter bubbles, echo chambers and 'over-personalization'. In practice, it implies a diversification of information and more interactive control over the algorithmic outputs. Sunstein [9] advocated an "architecture of serendipity" as it would sustain 'chance encounters and shared experiences' that he regards as preconditions for well-functioning democracies. Therefore, taking into consideration serendipity in the design process can fruitfully inform designers, users and eventually policy-makers to stimulate what Harambam et al. [10] defined as alternation, awareness, adjustment and obfuscation.

4.3 Towards a "Right Not to Be Deceived"?

Human behavior can be manipulated by priming and conditioning, using rewards and punishments. Algorithms can autonomously explore manipulative strategies that can be detrimental to users [13, 25]. Basically, they exploit human biases and vulerabilities to affect self-control, self-esteem and personal beliefs.[7] Therefore, autonomy and democracies are indeed seriously threatened [6, 28, 33, 36].

Such Big Data-driven nudging is defined by Yeung [15] as a technique of "hyper-nudging", that is, a "nimble, unobtrusive and highly potent, providing the data subject with a highly personalised choice environment". Hyper-nudging operates through the technique of 'priming', dynamically configuring the user's informational choice context to influence their decisions. Thus, it concerns the entire design process, not only algorithmic decision-making [36]. This introduces a new form of power, a new 'invisible hand' in which power is identified with ownership of behavioral modification (i.e. artificial emotional intelligence) [37]. In this sense, social media already act as addictive machines [33]. As such, users are tempted to give up their rights to benefit from such hyper-nudging personalization. In theory, using such techniques goes against the 'fairness' and 'transparency' provisions of the GDPR [28]. In this sense, GDPR proves to be a necessary yet insufficient step. In fact, as smart environments will permeate societies, users (especially young people [6]) will be automatically plugged in and guided through life along algorithmically determined pathways, and the boundary between legitimate persuasion and deception will become increasingly blurred.

The right most clearly implicated by big data-driven hyper-nudging is the right to informational privacy. As such, data controllers are obliged to follow the principle of data protection by design and by default. This might go beyond the individual to focus a priori on the creation of better algorithms [17]. For example, privacy might be fundamental also to enable what Hildebrandt [3] defines as 'agonistic machine learning', that is, demanding companies or governments that base decisions on machine learning to 'explore and enable alternative ways of datafying and modelling the same event, person or action'. In this sense, the value of serendipity is also understood.

---

[7] - For example, Facebook is especially committed to maintain friends' relationships. Its "NewsFeed" is thus moderated by homophily [41] which is, however, the primary driver of content diffusion, especially misinformation and conspiracy theories, with a frequent result of homogeneous, polarized clusters that tend to lead to emotionally charged and divisive content [39].

Of course, also consumer law could actually help to protect consumers against unfair profiling and persuasion practices [23]. However, the extensive uncertainty and context dependence imply that people cannot be counted on to navigate the complex trade-offs involving terms of services and privacy self-management [38]. There is overwhelming evidence that most people neither read nor understand online privacy policies. According to behavioral sciences as well, existing notice and consent model cannot be relied upon to protect the right to informational privacy [15].

In addition to privacy, online digital users could have a separate and distinct right not to be deceived, rooted in a moral agent's basic right to be treated with dignity and respect given that deception violates the autonomy of the person deceived, involving the control of another without that person's consent. Appropriate information and specific consent to the use of techniques of deception ought to be given. Unfolding the preconditions of such a right may help tech companies to regain and preserve trust. Online platforms should in fact routinely disclose to its users and the public any experiment that the users were subjected to with the purpose of promoting engagement. Yet, given the complexity and subtleness of online deception the choice may not even be sufficiently informed and conscious even with consent. Independent and external review boards need to be established to review and approve experiments in advance. The current massive power asymmetry between global digital service providers and individual users in fact cannot be ignored [24, 37]. As it is currently set, the EU legal framework seem to be insufficient to prevent users' potential deception.

5 Conclusions

GDPR defines novel rights for data subjects and duties for data controllers. However, GDPR's rights to an explanation, transparency and non-discrimination may actually prove ineffective in practice when users consume information filtered by proprietary algorithms, and even nurture a new kind of "transparency fallacy". Developments in personalization can actually narrow privacy conceptions and make data protection insufficient to protect fundamental human rights. Data protection actually relies too much on individual rights for what are too often group harms. There is indeed high need for user-centric as well as group-centric approaches to critically govern emerging issues of data-driven media personalization. Also, users cannot be fully relied to manage all the complexities of data protection. On the contrary, personalized persuasive techniques are likely to be employed on a mass scale and, therefore, contrary to recent trends in policy, it is also advocated a more paternalistic approach.

Even if conceptualizing alternative privacy strategies for the online media context has proven to be difficult, two intertwined human rights have been introduced to enrich discussion on privacy in relation to profiling and media personalization. Firstly, we argued that data protection law should complement with media and consumer law in order to guarantee individuals a right to receive information. In general, such right could empower users to bypass and adjust algorithmic filters and receive more serendipitous information outside one's predetermined algorithmic path. Secondly, given the increasingly sophisticated techniques of behavioral modification and the characteristics of personalized persuasive technologies, a right not to be deceived in the online context has been introduced. Above all, any experiment that the users may be subjected to with the purpose of promoting engagement ought to be disclosed by platforms and approved by an independent agency. By discussing the above perspectives, the article provided a more comprehensive legal understanding on personalized online services in the light of the GDPR and offered an argumentative basis for further contextualisation and reflection.

References

1. Wachter, S., Mittelstadt, B., & Floridi, L.: Why a right to explanation of automated decision-making does not exist in the general data protection regulation. *International Data Privacy Law*, 7(2), 76-99 (2017)

2. Kaltheuner, F., & Bietti, E.: Data is power: Towards additional guidance on profiling and automated decision-making in the GDPR. *Journal of Information Rights, Policy and Practice*, 2(2) (2018)

3. Hildebrandt, M.: Privacy as protection of the incomputable self: From agnostic to agonistic machine learning. Forthcoming in *Theoretical Inquiries of Law*, 19(1) (2019)

4. Rannenberg, K., Royer, D., & Deuker, A. (Eds.).: *The future of identity in the information society: Challenges and opportunities.* Springer Science & Business Media (2009)

5. Kohl, U., Davey, J., & Eisler, J.: Data-driven personalisation and the law-a primer: collective interests engaged by personalisation in markets, politics and law (2019)

6. Gal, M. S.: Algorithmic Challenges to Autonomous Choice. *Michigan Telecommunications and Technology Law Review* (2017)

7. Yeung, K.: Five Fears About Mass Predictive Personalisation in an Age of Surveillance Capitalism. *International Data Privacy Law*, forthcoming (2018)

8. Pariser, E.: *The filter bubble: How the new personalized web is changing what we read and how we think*. Penguin, New York (2011)

9. Sunstein, C. R.: *# Republic: Divided Democracy in the Age of Social Media.* Princeton University Press (2017)

10. Harambam, J., Helberger, N., & van Hoboken, J.: Democratizing algorithmic news recommenders: how to materialize voice in a technologically saturated media ecosystem. *Phil. Trans. R. Soc. A*, 376(2133) (2018)

11. Zuiderveen Borgesius, F. J., Trilling, D., Moeller, J., Bodó, B., De Vreese, C. H., & Helberger, N.: Should We Worry About Filter Bubbles?. *Internet Policy Review. Journal on Internet Regulation*, 5(1) (2016)

12. Bodo, B., Helberger, N., Irion, K., Zuiderveen Borgesius, F., Moller, J., van de Velde, B., ... & de Vreese, C.: Tackling the Algorithmic Control Crisis - The Technical, Legal, and Ethical Challenges of Research into Algorithmic Agents. *Yale JL & Tech.*, 19, 133 (2017)

13. Albanie, S., Shakespeare, H., & Gunter, T.: Unknowable Manipulators: Social Network Curator Algorithms. *arXiv preprint arXiv:1701.04895* (2017)

14. Gillespie, T.: The relevance of algorithms. *Media technologies: Essays on communication, materiality, and society*, 167 (2014)

15. Yeung, K.: 'Hypernudge': Big Data as a mode of regulation by design. *Information, Communication & Society*, 20(1), 118-136 (2017)

16. Colangelo, G., & Maggiolino, M.: From fragile to smart consumers: Shifting paradigm for the digital era. *Computer Law & Security Review* (2019)

17. Edwards, L., & Veale, M.: Slave to the algorithm: Why a right to an explanation is probably not the remedy you are looking for. *Duke L. & Tech. Rev.*, 16, 18 (2017)
18. Turilli, M., & Floridi, L.: The ethics of information transparency. *Ethics and Information Technology*, 11(2), 105-112 (2009)
19. Mittelstadt, B.: Automation, Algorithms, and Politics| Auditing for Transparency in Content Personalization Systems. *International Journal of Communication*, 10, 12 (2016)
20. Burrell, J.: How the machine 'thinks': Understanding opacity in machine learning algorithms. *Big Data & Society*, 3(1) (2016)
21. Tutt, A.: An FDA for algorithms. *Social Science Research Network* (2016)
22. Goodman, B., & Flaxman, S.: European Union regulations on algorithmic decision-making and a "right to explanation". *arXiv preprint arXiv:1606.08813* (2016)
23. Helberger, N., Borgesius, F. Z., & Reyna, A.: The perfect match? A closer look at the relationship between EU consumer law and data protection law. *Common Market Law Review*, 54(5), 1427-1465 (2017)
24. Lynskey, O.: Grappling with "Data Power": Normative Nudges from Data Protection and Privacy. *Theoretical Inquiries in Law*, 20(1) (2019)
25. Lanzing, M.: "Strongly Recommended" Revisiting Decisional Privacy to Judge Hypernudging in Self-Tracking Technologies. *Philosophy & Technology*, 1-20 (2018)
26. Eskens, S., Helberger, N., & Moeller, J.: Challenged by news personalisation: five perspectives on the right to receive information. *Journal of Media Law*, 9(2), 259-284 (2017)
27. Reviglio, U.: Serendipity as an Emerging Design Principle of the Infosphere: Challenges and Opportunities. In *Ethics and Information Technology*. Springer (2019)
28. Zarsky, T. Z.: Privacy and Manipulation in the Digital Age. *Theoretical Inquiries in Law*, 20(1) (2019)
29. Facebook Newsroom, https://newsroom.fb.com/news/2019/03/why-am-i-seeing-this/, last accessed 07/06/2019
30. Hoffmann, C. P., Lutz, C., Meckel, M., & Ranzini, G.: Diversity by choice: Applying a social cognitive perspective to the role of public service media in the digital age. *International Journal of Communication*, 9(1), 1360-1381 (2015)
31. Karppinen, K.: Media and the paradoxes of pluralism. *The media and social theory*, 27-42 (2008)
32. Helberger, N., Karppinen, K., & D'Acunto, L.: Exposure diversity as a design principle for recommender systems. *Information, Communication & Society*, 1-17 (2016)
33. Deibert, R. J.: The Road to Digital Unfreedom: Three Painful Truths About Social Media. *Journal of Democracy*, 30(1), 25-39 (2019)
34. Calo, R.: Digital market manipulation. *Geo. Wash. L. Rev*., 82, 995 (2013)
35. Kidron, B., Evans, A., Afia, J., Adler, J. R., Bowden-Jones, H., Hackett, L., ... & Scot, Y.: *Disrupted childhood: the cost of persuasive design*, London: 5rights (2018)
36. Fogg, B. J., Lee, E., & Marshall, J.: *Interactive technology and persuasion. The Handbook of Persuasion: Theory and Practice.* Thousand Oaks, CA: Sage (2002)
37. Zuboff, S.: Big other: surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, 30(1), 75-89 (2015)
38. Acquisti, A., Brandimarte, L., & Loewenstein, G.: Privacy and human behavior in the age of information. *Science*, 347(6221), 509-514 (2015)