



## Co-regulating algorithmic disclosure for digital platforms

Fabiana Di Porto & Marialuisa Zuppetta

To cite this article: Fabiana Di Porto & Marialuisa Zuppetta (2020): Co-regulating algorithmic disclosure for digital platforms, Policy and Society, DOI: [10.1080/14494035.2020.1809052](https://doi.org/10.1080/14494035.2020.1809052)

To link to this article: <https://doi.org/10.1080/14494035.2020.1809052>



© 2020 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group.



Published online: 29 Oct 2020.



Submit your article to this journal [↗](#)



Article views: 1076



View related articles [↗](#)



View Crossmark data [↗](#)



Citing articles: 1 View citing articles [↗](#)

## Co-regulating algorithmic disclosure for digital platforms

Fabiana Di Porto  and Marialuisa Zuppetta<sup>†</sup>

### ABSTRACT

With digital platforms gaining dominant intermediating role and exerting regulatory functions vis-à-vis small and medium-sized enterprises (SMEs) through algorithms, EU institutions have started considering to rely on their analytical capacity to regulate the myriads of market transactions occurring within and through them (so-called platform-to-business, or P2B transactions). Most of the time, the EU suggests recurring to light-tough disclosure duties. Hence, the European model falls short in rebalancing information asymmetry and unequal bargaining power plaguing the SMEs. In practice, the EU model consists either in pure delegation of self-regulatory powers (codes of conduct) or non-enforceable co-regulatory schemes (with technical standards established by the platforms themselves). Other models have been suggested that rely on the regulator's access to the platform's data (so called savvy and data-delegated options). These governance models present several limitations, making the platforms' role as regulatory intermediators little credible. In this scenario, the paper purports that a third option should be considered. In particular, to tackle the multifaceted risks associated with algorithmic decisions by digital platforms, while at the same time avoiding stifling innovation, it makes three suggestions: (1) also information disclosures should be done by an algorithm; (2) that is pre-tested in a co-regulatory process, that involves the regulator and stakeholders; and (3) enforced through legal and other empowerment tools, rather than sole fines.

### KEYWORDS

Digital platforms; big data; P2B; SMEs; self-regulation; co-regulation; disclosure; algorithmic co-regulation; terms and conditions; regulatory intermediation; sandbox; knowledge graph

**CONTACT** Fabiana Di Porto  [fabiana.diporto@unisalento.it](mailto:fabiana.diporto@unisalento.it); [fabiana.diporto@mail.huji.ac.il](mailto:fabiana.diporto@mail.huji.ac.il)  University of Salento, Via per Monteroni, Lecce, Italy and Visiting Professor, Faculty of Law, Hebrew University of Jerusalem, Mount Scopus, Israel.

Fabiana Di Porto is Associate Professor of Economic Law and Technology, University of Salento, Lecce. As a Lady Davis Fellow 2019/20, she has been Forchheimer Visiting Professor at the Faculty of Law and Associate at the Federmann Cyber Security Research Center – Cyber Law Program of the Hebrew University, Jerusalem. Marialuisa Zuppetta<sup>†</sup> was Assistant Professor of Public Law at the University of Salento. Previous versions of this paper have been presented at the Workshop on 'Data Economy', organized by the Body for European Regulators for Electronic Communications (Berec) in Brussels on May 14th, 2018, at the Annual Conference of the Italian Society of Law and Economics (ISLE), held in Lecce on December 14<sup>th</sup>, 2018 and at the attendants to the 'EU Regulation of Digital Platforms' seminars held at the Law Faculty of the Hebrew University in November- December 2019; the 15<sup>th</sup> Annual conference of the Academic Society for Competition Law (Ascola), 25-27.6.2020 (available here: [youtu.be/VO9FcZxLVP4](https://youtu.be/VO9FcZxLVP4)). We are thankful to the discussants and the anonymous referees for their very useful comments. All mistakes remain ours. The article has been jointly conceived; however, Marialuisa Zuppetta drafted the Introduction and sect. 2; while Fabiana Di Porto the other sections. This article is dedicated to the beloved memory of co-author Marialuisa, who passed away too early.

<sup>†</sup>We are not dealing with all platforms, but only with 'matchmakers', intended *à la* Evans and Schmalensee (2015): i.e. those connecting suppliers and consumers through algorithms, and reducing search costs for both. This would essentially exclude from the analysis: blogs and platforms such as Facebook, Google's AdSense, Amazon Web Services or PaaS and include e-commerce, price comparison sites and search engines.

© 2020 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group.

This is an Open Access article distributed under the terms of the Creative Commons Attribution-NonCommercial License (<http://creativecommons.org/licenses/by-nc/4.0/>), which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.

## 1. Introduction

Since the past decades, digital platforms (defined à la Evans & Schmalensee, 2016)<sup>1</sup> have become essential intermediaries in the daily lives of individual consumers and the small business (SMEs) alike. These technologies have been enhancing their capabilities to interact, organize, move, buy, purchase. That has been possible thanks to the broadest sharing of data and information among all market participants and their intermediation through powerful Information Technologies (IT). Yet, for long the need to let digital innovation develop made public intervention undesirable to most regulatory institutions at the European level (EC, 2016a Feb. 2<sup>nd</sup>) and the U.S. ones (FTC, 2016; Exec. Order No. 13,859, 2019<sup>2</sup>; Office of Science and Technology Policy, 2020; *contra*: Stigler Group, 2019, calling for regulatory intervention, eg. to react against ‘dark patterns’).<sup>3</sup>

More recently, however, calls for regulation of digital platforms have gained momentum among theoreticians, as well as EU institutions. As platforms in many areas have become ‘superdominant’ or quasi-monopolist and engaging in anticompetitive conduct against their small-business counterparts, competition scholars have started questioning whether antitrust policy ‘should take a tough stance’ against digital ‘ecosystems’ that auto-reinforce their positions in their well-protected ‘walled gardens’ (EC, 2019, p. 16; Evans & Schmalensee, 404; Tirole, 2017; OECD, 2018; Stigler Group, 2019).

For instance, big digital platforms can exploit their informative advantage to self-preference their products against their small business rivals; or degradate the prominence of their competitors’ offers by simply manipulating the algorithms managing rankings, or they may terminate traders’ service contracts without stating any justifications.<sup>4</sup> Moreover, the need to proactively further an EU-wide Digital Single Market (EC, 2015) into a broader European Data Economy, (EC, 2017, 2018) recommend initiatives aimed to tackle the limited bargaining power and lack of information of business users (EC 2020c; operating in and through platforms.<sup>5</sup> This tougher stance is now reflected in the debate surrounding the Digital Services Act Package 2020 (EC, 2020 a, 2020 b), where the Commission is considering ex-ante rules as part of a pro-competition reform debate (EC, 2020d).<sup>6</sup> If implemented, new measures will be adopted to expand existing transparency duties; and increase the number of data sharing agreements being stipulated between the big platforms and their SMEs counterparts. As a default, such agreements will be voluntary; but ex ante access to platforms’ data might be mandated if sector-specific market failures are detected that standard competition rules cannot solve (EC, 2020a, at 3–4; 2020d.)

<sup>2</sup>Exec. Order No. 13,859, *Maintaining American Leadership in Artificial Intelligence*, 84 Fed. Reg. 3967, 11.2.2019.

<sup>3</sup>Note that exceptions to this light-handed approach have always existed: examples of ex ante regulation are the ‘Access to account data rule’ in the Fintech sector (Di Porto & Ghidini, 2020); the mandated exchange of electricity and gas smart metering information (Directives 2019/944/EC and 2009/73/EC); the access to electricity network data rule (Commission Regulation (EU) 2017/1485), and, of course, intelligent transport systems (Directive 2010/40/EU).

<sup>4</sup>Executive summary of the Impact Assessment (SWD (2018) 139 final) accompanying the Proposal for Regulation Regulation 2019/1150, at 2.

<sup>5</sup>See EU Regulation 2019/1150 of the European Parliament and the Council on ‘Promoting fairness and transparency for business users of online intermediation services’, of 20.6.2019, OJEU L-186 of 11.7.2019.

<sup>6</sup>The debate recalls the standard literature on the need to regulating monopolies, whatever the sector: any market player enjoying extensive market power has the potential to exploit it at the detriment of its competitors and clients. Because antitrust rules might not be sufficient for tackling these behaviors, quasi-monopolists are often regulated. Stated otherwise, monopoly or quasi-monopolies are rationales justifying regulation. What is peculiar of digital platforms that enjoy market power (think e.g. to Google search engine in the EU Google case), is the algorithmic means by which they exercise it, as discussed thoroughly in the text. For further details, EC (2019).

In parallel, thanks to thicker knowledge on the possible harm to SME users (and the society more broadly) deriving from decisions led by algorithms and Artificial Intelligence (or AI), (Taeihagh, 2020), a need for protecting the small business beyond the rights entrusted by existing EU legislation, has also been raising (EC, 2020c). Data market power is pernicious because it provides large platforms with wide regulatory powers that go undetected to traditional oversight. For instance, big digital players may ‘set the rules on the platform and unilaterally impose conditions for access and use of data’ over their SMEs counterparts (EC 2020a, p. 8).

Hence, the academic quests for explicability, transparency and accountability of AI-led decisions (eg. Ananny & Crawford, 2016; Heemsbergen, 2016; Stohl, Stohl, & Leonardi, 2016), have turned into a policy imperative (Council of Europe, 2019; European Parliament - EP, 2019b; EU High level Expert Group on AI, 2019; OECD, 2019). For instance, the Council of Europe has urged Member States to take measures against illegitimate forms of interference by AI tools.<sup>7</sup> ‘exploit their data’ to. It suggests empowering users by robustly enhancing awareness of how platforms ‘exploit their data’ to train algorithms for commercial purposes.<sup>8</sup>

The European Parliament (EP 2019b) makes a step forward. Like the Council of Europe,, it warns on the ability of algorithms to violate expectations the SMEs fiduciary expectations the SMEs have toward organisations using the same AI systems; on the other,<sup>9</sup> to contain this, it calls for empowerment strategies that are based on AI tools: ‘[I]n the AI era, an effective countervailing power needs to be supported by AI too’.<sup>10</sup> Interestingly, the EP considers AI-led empowerment tools more effective than traditional public regulation and enforcement to reduce AI-led manipulation (such as price discrimination, and over-targeting), suggesting that data mining algorithms could be used in manifold ways to help SMEs, from ‘analysing and summarising massive amounts of reviews, or comparing prices across platforms,’ to ‘detecting discrimination’ or ‘build [ing] supporting tools that could identify pre-judice an unfair treatments’.<sup>11</sup>

\* \* \*

Clearly, the need for regulatory intervention is being gradually established (*why*), as is its addressee (*whom*) – the big digital platforms – and the beneficiaries – the SMEs. The latter are emerging as subjects in need of protection vis-à-vis their platforms’ counterparts on several grounds:

- (i) they suffer from information asymmetry and
- (ii) low bargaining power because they cannot but operate their business through the platforms,  
who, in turn, manage these massive markets through
- (iii) regulatory powers, which they exercise

<sup>7</sup>Council of Europe (2019): ‘Contemporary machine learning tools have the growing capacity not only to predict choices but also to influence emotions and thoughts and alter an anticipated course of action, sometimes subliminally’ (pt. 8). Digital technologies can ‘use personal and non-personal data to sort and micro-target people, to identify individual vulnerabilities and exploit accurate predictive knowledge, and to reconfigure social environments in order to meet specific goals and vested interests’ (pt. 9).

<sup>8</sup>Ibid., pt. 9, lit. e).

<sup>9</sup>EP, 2019, at 5

<sup>10</sup>Ibid., at 7.

<sup>11</sup>Ibid, p. 8.

<sup>12</sup>To make an example, Coglianese and Lehr (2019), at 9 see the ‘fully automated dispute resolution system developed and already used by eBay to settle tens of millions of disputes each year’ as a form of ‘adjudication by algorithms’.

(iv) via algorithmic decisions fed by big data.<sup>12</sup>

And because black box-based, such algorithmic decisions, add a layer of opacity to the platform-to-business (or P2B) relationship, thus worsening the information asymmetry and low bargaining problems of SMEs (i and ii).

If the *why* for regulating and *whom* are more or less clear, there is still little agreement as far as the regulatory governance model to put in place the resulting and the tool/s to employ (*how*). On the one hand, to tackle information asymmetries and resulting low bargaining power plaguing SMEs, the EU institutions propose using traditional disclosure regulation (panacea) to increase transparency and accountability of platforms' business algorithmic decisions. Others contend that because platforms perform a 'visible hand' function (by providing rankings and ratings, match-making and an information intermediation function) traditional disclosure regulation should be dismissed altogether and pure algorithmic self-regulation by the platforms (Ben-Shahar & Schneider, 2011, 2014).

We contend that disclosure regulation could indeed still play a role to empower platforms' business users, but to do so it should be rethought of. Following the EP's suggestions, European institutions should consider designing disclosures through algorithms, and also privilege the involvement of platforms, which enjoy regulatory functions, as credible actors in a data-based co-regulatory governance structure.

This article fills a void in the literature. While a lot has been said about individual consumers' inability to cope with algorithmic decisions affecting their autonomy in online marketplaces, (Gal, 2017; Susser, Roessler, Nissenbaum, 2019; Zuboff 2019) the same does not hold for micro and small-sized enterprises (SMEs). Regarding the latter, the literature mainly focuses on competition analysis, (Evans & Schmalensee, 2015) or the contractual profiles of P2B relationships, (de Streel & Sibony, 2017) while does barely indulge on how to devise disclosures that can work for them, in a digital environment. This contribution links the literature on regulatory intermediation (Abbot, Levi-Faur, & Snidal, 2017) with the legal doctrine on disclosure duties in P2B relations to reach a proposal for the legitimate use of algorithms to produce disclosures in a participated governance.

The article is, therefore, organized as follows. We start by collocating digital platforms in the realm of regulatory intermediators, by sketching how their regulatory functions differ from traditional ones, being them exercised through powerful algorithms trained on massive data collected (also) from the SMEs. Algorithmic regulatory functions of digital platforms are thus classified and analyzed to spot their impact on the life of SMEs operating in and through them. Several criticalities are found that are only marginally tackled by the EU. For this reason, sections 3 and 4 present the two regulatory governance models through which the EU has reacted to the severe information asymmetry and subsequent unequal bargaining power of the SMEs. These are: Disclosure self-regulation enacted through Codes of Conduct (sect. 3); and Disclosure Co-Regulation enacted through light cooperation with digital platforms (sect. 4). As we shall see in sect. 5, both models suffer severe limitations, making big platforms' role as regulatory intermediators little credible. That leads us to discuss new models, where the circulation of data between the platform and the regulator is at the core of intermediation. That provides the theoretical framework for our proposal (sect. 6), where AI tools are used to generate algorithmic disclosures in a participated and experimented fashion. Sect. 7 discusses our model and concludes.

## 2. Regulatory functions of digital platforms. Classifications and issues

Already in 1999, Lessig (1999) recognized that technology could complement or even be a substitute for legal regulation ('code is law'). Scholars from the social sciences have theorized that not only the technology but any actor, private or public, (such as NGOs, certification bodies like Data Protection Officers (Medzini, 2018), or the US Security Council) can play 'major and varied roles in regulation', serving as 'regulatory intermediators' (Abbot, Levi-Faur, & Snidal, 2017).<sup>13</sup> In their view, intermediators add a layer to the dual relationship between the regulator and its targets, by acting 'in conjunction with a regulator to affect the behavior of a target'.<sup>14</sup>

It comes as no surprise that Cohen and Sundararajan (2015) have extended the concept of regulatory intermediators to digital platforms; after all, they had been conceptualized as 'infomediaries' since the Nineties (Gaudeul & Jullien, 2008; Hagel & Rayport, 1997) and later on as 'matchmakers' by Evans & Schmalensee). According to them, in the growing world of peer-to-peer, digital platforms can be accounted as credible parties in the regulatory arena, because they enjoy regulatory functions.

Indeed, when designing its own architecture, a platform defines the rules governing the space where users operate; and in doing so it proceeds from a 'macro-level' down to a 'micro-level', where interactions between platforms and business and among peers are regulated at a very detailed level.<sup>15</sup> That is done through algorithms fed by data produced within the platform.<sup>16</sup> It follows that the kind of regulation produced at the 'micro-level' is not only algorithmic,<sup>17</sup> but also highly 'granular', compared to traditional (i.e. non-algorithmic) legal rules.<sup>18</sup>

For what interests us, the regulatory functions of platforms can easily be grouped into three main functions: (i) setting the architecture design; establishing rules governing (ii) the P2B relationships; and (iii) the interactions between users. Examples of (i) may be: the very design of an algorithm (as is the case with search engines, providing ranking of search results),<sup>19</sup> or the design of rules and institutions that 'shape the functioning of the marketplace' (EC, 2019 at 60). As per (ii), platforms are the ones regulating the way data

<sup>13</sup>Abbot et al. (2017) (contending that regulatory intermediators may give support by 'providing expertise and feedback to facilitating implementation, from monitoring the behavior of regulatory targets to building communities of assurance and trust.', at 19). See also the Special issue of Reg.&Gov (2019).

<sup>14</sup>Abbot et al, previous note, at 19.

<sup>15</sup>Rules produced in these environments tend to have a 'higher degree of granularity without prohibitively high complexity costs': Busch (2019), at 12.

<sup>16</sup>EC (2019), at 60.

<sup>17</sup>Speaking of algorithmic regulation might sound a tautology, given that algorithms are themselves rules. However, one thing is to define rules for using the platform based on free negotiations between SMEs and the said platform. Other thing is that such rules are drafted by the platform using an algorithm that derives the knowledge of the SME's preference from the data it gathers by the SME's usage of the platform. In this case, the information asymmetry is essential, as is the bargaining power of the two counter-parts.

<sup>18</sup>Black (1996), at 27 speaks of 'individualised regulation' to refer to regulation tailored at the single, individual firm. More recently, see: Strahilevitz and Porat (2014); Busch (2016b); and Busch and De Franceschi (2018).

<sup>19</sup>Algorithmic decision-making may also *re-ontologize* the world 'by understanding and conceptualizing it in new, unexpected ways, and triggering and motivating actions based on the insights it generates'. 'The most concrete example is the ways in which artificial agents construct the available action space of online environments, such as *search engines* that make available links to other websites through an algorithmic ranking. Algorithms are, in this regard, part of a process of "reality construction" by including or omitting specific information that, in effect, governs behavior and actions. 'The fact that artificial agents, through the computational generation of knowledge, can constrain, alter and nudge behavior towards a specific goal has also been conceptualized as "algorithmic regulation", "governance by algorithms", of algorithms as "artefacts of governance", and "algorithmic governmentality"' (Gahnberg, 2020, p. 5-6).



generated therein may circulate (e.g. limiting it to the use of application programming interfaces, or APIs); may impose price controls or fix the rating and recommendation policies. Concerning user-to-user relations (iii), it is the platform that typically establishes standard models for presenting commercial offers; decides about delivery and returning policies, and so forth. (EC 2019, at 61).

While algorithmic production of rules by the platforms can be cost-effective, as it 'suits the scale of peer-to-peer' (EP, 2017 at 23) (flexibility and differentiability), and may generate efficiencies, by allowing transactions that were not possible before such innovations, there are nonetheless issues that need to be tackled.

First, business users cannot know what the parameters used in algorithmic decisions are, nor can they be sufficiently aware of the legal consequences of the decisions taken by the platforms. Often, the data produced through the use of the platform – which is machine-generated data – tend to be treated as belonging to it, and therefore not accessible to the business user. Think for instance to marketing data in marketplace platforms like Amazon: while these data are generated thanks to its users' interaction, they are nonetheless unavailable to them.<sup>21</sup> That puts the latter in a disadvantaged position vis-à-vis the platform, because they may not reuse it to profile their products or service further, and thus ameliorate them.

Moreover, some biases are 'innate' to the use of algorithms and that depends on the datasets, such as overreliance on correlations, which might generate discrimination among users or disadvantaged treatment (think, e.g. to ranking manipulation) (Lim & Taeihagh, 2019).

Furthermore, many business users are still uninformed of the real profit-driven mechanisms governing digital platforms (Whittington & Hoofnagle, 2012, at 1357; Acquisti & Grossklags et al., 2007). Often, digital platforms may take advantage of their users, who cannot understand and benefit from the full value of the data they generate, nor can they understand entirely the rankings practices applied to them. The myriads of micro and SMEs, as we shall see,<sup>22</sup> are not the big business and often behave much like individuals, who have no share in the vast amounts of profit that platforms make out of the personal data they circulate (Grunes, 2013, at 1123; Shelanski, 2013; Argenton & Prüfer, 2012; Vaidhyanathan, 2011; Rust, Kannan, & Peng, 2002).

In the same vein, with online bargains, SMEs' room for negotiation has shirked down, as is their bargaining power; digital platforms enjoy a strong information asymmetry against business users, which they can use to profile them and, accordingly, put themselves in the position to exploit and discriminate among and against them.<sup>23</sup>

The European response to those problems, thus far, has been far from the interventionist, and has relied heavily on traditional informational duties. Although there might be some change in the future,<sup>24</sup> the kind of legislative initiatives the EU has adopted range between delegation of pure self-regulatory powers to the platforms (in the form of codes of conduct), to co-regulation via the setting of EU principles coupled with technical

---

<sup>21</sup>Clearly, unlike those we are dealing with in this article, there are platforms that are likely to be aware of some main parameters, and for which sharing business analytics is a part of the value proposition from the platform (think e.g. of Google Analytics for designing one's own website). Moreover, for platforms of this kind, data sharing is an intrinsic part of the service (think e.g. of a marketing platform).

<sup>22</sup>See sect. 6, below.

<sup>23</sup>EC (2019), at 62.

<sup>24</sup>We refer to EC, 2020a, 2020b and 2020d.

standards established by the platforms themselves. Notwithstanding these differences in the governance structure, however, the kind of disclosure regulation adopted is quite standard (i.e. non-targeted, non-differentiated, and general): it merely suggests employing transparency duties regarding contract terms and conditions, and to release information about data use, or reputation mechanisms. In no way does it encompass or avail of algorithmic tools, as purported by the EP to better empower platform's business users, and their participation to the making of platforms' decisions (e.g. their codes of conduct) is only marginal.

In the following, we will review and discuss the EU model, starting with disclosure self-regulation (sect. 3). Here, recent legal initiatives encouraging platforms to design codes of conduct (or CoC) in the domains of personal data protection and non-personal data circulation will be analyzed.

### **3. The European model: relying on (traditional) disclosure platforms' self-regulation**

Despite the many criticism disclosure regulation has undergone in the last decade (Ben-Shahar & Schneider, 2011, 2014; Craswell, 2006; Easterbrook & Fischer, 1984; Marotta-Wrugler, 2014; Prat, 2005)<sup>25</sup> it is still the preferred mode of intervention by the EU institutions vis-à-vis big digital platforms. The European Model accounts for dozens of novel informational duties that have been introduced despite little evidence of their effectiveness.<sup>26</sup>

#### **3.1. (Traditional) Solicited Codes of Conduct: the GDPR and EU regulation 2018/1807**

Self-regulation by digital platforms is at the core of EU initiatives aimed at the liberalization of non-personal data circulation (Regulation UE 2018/1807).<sup>27</sup> Platforms are 'encouraged' to adopt self-regulatory CoC to provide (also) professional users with 'detailed information and operational requirements for data porting' and the switching of the service provider.<sup>28</sup> The porting of data from one provider to another being fundamental to create the broadest and most competitive data economy, EU institutions consider it essential that professional users are 'aware' of such possibility. Therefore, the CoC should, first of all, establish communication roadmaps to 'raise awareness' about the CoCs themselves (Art. 6(d)). They should furthermore include 'sufficiently detailed, clear

<sup>25</sup>Markets are flooded with too much information, and because many of its drawbacks are irresolvable, disclosure regulation should be dismissed altogether. The advent of the sharing economy could determine the end of information asymmetries without any piece of disclosure regulation, provided that peers exchange their opinions by writing reviews and relying on a network of feedbacks and ratings.

<sup>26</sup>Contra Busch (2016a), 223, (discussing the weaknesses of platforms' reputation systems and suggesting safeguarding measures to fix them). See also Finck (2017), at 14 (contending that although platforms have access to myriads of data that regulators do not possess, which could help to draft proper disclosures, they nonetheless lack the public interest view required to decide what piece of information, at what time, to whom and why should be disclosed).

<sup>27</sup>See Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union. In OJ L 303, 28.11.2018, p. 59–68.

<sup>28</sup>Recital 30, Reg. EU 2018/1807. The codes of conduct should define Guidelines at the EU level on best practices that might 'facilitat[e] the switching of service providers and the porting of data' (Art. 6(a)).



and transparent [technical] information regarding' the switching, that professional users should receive 'before a contract for data processing is concluded' (Art. 6(b)).

Similarly, concerning personal data, the EU GDPR No. 2016/679, foresees several disclosure obligations (Arts. 40 and 41), whereby platforms or their associations (as data controllers and processors) are encouraged to lay down CoCs to 'demonstrate compliance with the Regulation'.<sup>29</sup> In particular, platforms should provide information (amongst others) about the automatic treatment of personal data, including their collection, pseudonymisation, and processing. They should also provide information about the exercise of the rights of data subjects; and to self-assess the risks of data breaches (Article 40(1), *lits.* a-f), h), i)).

In its 2019 Guidelines on Codes of Conduct, the EDPS<sup>30</sup> distinguishes between an industry and nation-wide CoC and a transnational pan-European one.<sup>31</sup> Only the latter would have certifying effects within the whole EU (and to some extent even outside Europe), and thus entail some minimal regulatory powers to the EU Commission<sup>32</sup> (alongside with the National Supervisory Authorities grouped in the EDPS' council). It should be acknowledged, however, that the procedure to have a pan-European CoC approved is overly complicated and demanding.<sup>33</sup>

In the former case – of national CoC – codes containing disclosures would still be adopted by platforms voluntarily<sup>34</sup> as would the establishment of a monitoring body.

### **3.2. Critical assessment of (traditional) disclosure self-regulation (codes of conduct)**

Among the many forms it can take (Black, 1996, 2001), here, disclosure self-regulation would be 'solicited' (i.e. not mandated) by public authorities (the EU), instead of adopted on a purely voluntary basis. That is because platforms are only 'encouraged' to enact

<sup>29</sup>See Recital 13, GDPR. See also EDPS, (2019).

<sup>30</sup>EDPS, (prev. fn)

<sup>31</sup>I.e. a code entailing processing activities in more than one Member State: See Annex 1 to EDPS (2019).

<sup>32</sup>Ibid, pt. 59: 'The Commission may decide by way of an implementing Act that an approved transnational code will have general validity within the Union and shall ensure appropriate publicity if they were to do so.' See Articles 40(9) and 40(10) GDPR.

<sup>33</sup>In a nutshell: a body representing categories of controllers or processors, including micro and SMEs, drafts a CoC which identifies a list of competent Supervisory Authorities (SAs) among EU ones. It indicates the criteria justifying which one, among those, be selected as Supervisory Authority (CompSA), serving as a one-stop-shop authority. It then submits a transnational CoC defining substantial rules and a monitoring body for ensuring compliance. A successful CoC application should demonstrate that: most extensive consultations were carried out before drafting; the draft code is compliant with Member State law(s); the monitoring body meets the independence and accreditation criteria (following Art. 41, GDPR). The CompSA will then notify the CoC to all SAs in search of one or two possible co-reviewers for receiving assistance in the CoC assessment. Within a 'reasonable period of time' (Guidelines, pt 52) the CompSA will submit the CoC to the EDPS' Board for approval (Art. 40(7) GDPR). Here, a further negotiation phase starts, with the Board being allowed to make comments (Art. 64 GDPR) and eventually rejecting approval. Once approved by the Board, the CompSA may still disagree with its Opinion, and therefore with the proposed CoC draft (Art. 40(5) GDPR), or it may finally approve it. Together with the approval of the international CoC, comes (as a *conditio sine qua non*) the accreditation of the monitoring body. The latter works closely with the CompSA (e.g. for complaints handling, monitoring compliance by adopting remedial actions ranging from warnings to the formal exclusion) and its decisions are made publicly available. A CompSA may revoke accreditation if the monitoring body fails to comply with its duties (Art. 41(5) GDPR).

<sup>34</sup>Unlike with international CoCs, the adoption of national ones is less complex: once submitted to the national SA, a preliminary formal control is made, following which – failing any exceptions – a decision on approval is made that is compliant with the national legal timeframe. A second decision on the merit is made by the SA that can either make comments on the draft CoC (and the proponents can accept or re-submit) or definitely approve it. Once approved, the CoC is made publicly available on both the SA's and the EDPS' Board's websites (Arts. 40(6) and 40(11) GDPR).

CoC, and no reaction is foreseen in case they fail to do so. One could contend that the industry has a ‘reputational incentive’ to adhere to a CoC (besides the economic one<sup>35</sup>), especially when sensitive questions like the treatment of digital data are at issue. However, as purported by Graef, Gellert, & Husovec (2018), incentives to draw a CoC can sometimes be misaligned to those of the regulator to the point that they can collide with the public goal pursued. That happens, in their view, with Regulation 2018/1807,<sup>36</sup> where an EU-wide CoC disciplining the sharing of non-personal data stemming from digital farming, ends up hindering innovation rather than enhancing the widest data sharing.<sup>37</sup>

On another ground, true that the 2019 Guidelines allow for the broadest differentiation of CoC disciplining the processing of personal data (which have the highest commercial value for business users); however, as highlighted in previous work, such disclosures may not be effective as they do not indulge on the different capabilities of recipients to such information to understand and process the meaning of algorithmic decisions done by platforms and their consequences (Di Porto & Maggolino, 2019, at 2).<sup>38</sup> The only reference one can find is at pt. 28, where code owners are called to demonstrate that *an appropriate level of consultation with the relevant stakeholders*<sup>39</sup> over the draft Code has taken place. However, that does not say much on ‘how’ to assess the understandability and thus the efficacy of CoC.

More generally, there are several limitations on relying on ‘encouraged’ self-regulation, even where CoCs are conceptualized following the best existing practices. First, there is no guarantee that platforms will cooperate in setting or adhering to an industry-wide code, even where the right incentives are set. Second, self-regulation in the digital society faces the limits of territorial oversight: provided (but not demonstrated) that an optimal control system is in place, it would necessarily act at a local (European) level, while platforms operate trans-nationally being their business data-driven. Therefore, as purported by Piffaut, systemic risks, like those that occurred in the 2007 financial crisis, could repeat (Piffaut, 2018, p. 4)

Finally, self-regulatory approaches like those described above, do not put any constraint on the risk that platforms consolidate their economic power vis-à-vis their business counterparts, in particular by using self-regulation to raise regulatory barriers to entry of competitors (Finck, 2017, at 15).

Given these limitations, co-regulation has been suggested as a viable alternative to differently combine the ability of platforms to set micro standards with a higher degree of interference by public institutions.

---

<sup>35</sup>According to Art. 83(2), GDPR and following EDPB (2018b), the adoption of CoC may lead to the application of no fine at all, should the SA consider that the corrective measures applied by the monitoring body are sufficient.

<sup>36</sup>Note 28.

<sup>37</sup>Graef, Gellert, and Husovec (2018) at 12 (stating that somehow contradictorily, on the one hand, the CoC ‘pretends to facilitate the sharing of [non-personal] data by reinforcing the rights of the data originator [i.e. the digital farmer]. On the other hand, however, it provides for more restrictions to the free flow of data than would seemingly apply under the GDPR for personal data.’).

<sup>38</sup>See also Taihigh, Introductory paper, 9: ‘As individuals either lack sufficient technical literacy or are not willing to bear the expected costs of obtaining the required information to interpret these explanations, mandated explanations required by the GDPR are unlikely to effectively inform and empower data subjects’.

<sup>39</sup>And the relevant stakeholders might include the platform’s business users as ‘data subjects or associations/bodies representing them’.

#### 4. (Follows) The European model: Experimenting with (traditional) disclosure co-regulation: *Regulation EU 2019/1150*

A second setting is disclosure co-regulation. Very broadly, co-regulation (Ayres & Braithwaite, 1994; Baldwin, Cave & Lodge, 2012, p. 146)<sup>40</sup> encompasses diverse models, whereby a pool of decision-makers (the State, markets and technology intermediators) interact to produce policy, draft rules (laws, regulations, norms); review and oversee.<sup>41</sup> Differently from self-regulatory schemes described above, here the regulators' involvement serves the function of ensuring the achievement of some public objectives. However, depending on the degree of contribution of platforms as regulatory intermediators, different configurations of co-regulation are possible (Marsden, 2011; de Stree & Sibony 2017, p. 22). In the following, we describe hybrid governance models (Radu this issue, 9–10) that are emerging as a consequence of the adoption of several piece of EU legislation in the field of digital disclosure regulation.

##### 4.1. *EU regulation 2019/1150 on fairness and transparency of P2B relations*

An excellent example of disclosure co-regulation is that provided for in EU Regulation 2019/1150.<sup>42</sup> To enhance transparency in the P2B relationships,<sup>43</sup> the Regulation sets up a co-regulatory regime, where the *regulatory* part consists of 'a set of legally binding transparency obligations on platforms', while the *self-regulatory* one, of 'a non-binding call [to platforms] to establish an independent mediation body' for the out-of-court settlement of complaints.<sup>44</sup> In addition 'an EU observatory for emerging problems, organized around an EU expert group' is set up 'to *monitor* emerging trends and the evolution of problems'.

Turning to the legally binding disclosure obligations, to curb surprise and increase the predictability of platforms' practices, terms and conditions must include information to the business users regarding significant contractual changes in *clear, layman language* and grant them a minimum (15 days) grace period (Art. 3). To prevent accidents like that of 2018, when 'Amazon blocked more than 250,000 seller accounts permanently and over 30,000 accounts temporarily,' (Westerhoff, 2019) platforms must state reasons for restricting, suspending or terminating trader users' services (with 30 days of prior notice)

<sup>40</sup>We use the definitions given by Ayres and Braithwaite (1994) and Baldwin et al. (2012) 146: co-regulation is an 'industry-association self-regulation with some oversight and/or ratification by government.' Note that co-regulation is explicitly referred to in the two Communications by the Commission: EC (2016, February 2<sup>nd</sup>) and EC (2016, May 25<sup>th</sup>).

<sup>41</sup>So called meta-regulation (ie. the involvement of public authorities stands especially on the review/audit side, and external controls by the regulator serve to ensure compliance to internally-crafted rules) (Parker, 2002, 2005; Grabosky, 1995; *contra* Black, 2007; Scott, 2012. Coglianese & Lazer, 2003; Coglianese & Mendelson, 2010).

<sup>42</sup>See, above, note 5.

<sup>43</sup>According to EC, (2019), Regulation 2019/1150 has been adopted in response to various harmful trading practices realized by the platforms, such as: unilateral change of contractual terms and conditions without prior notice; delisting of goods or services; suspension of business users' accounts without a clear statement of reasons. Other practices related to transparency duties include: the setting of unclear conditions for access and use of the data generated and collected by the platform providers; lack of transparency in the ranking of goods and services; and the discriminatory treatment platforms reserve to providers, as compared to their own (competing) services. Finally, the EC contests that most-favoured-nation clauses have been widely used by the online platforms that restrict their counterparts' ability to offer more attractive conditions through other channels.

<sup>44</sup>See the Executive summary of the Impact Assessment (SWD (2018) 139 fin.) accompanying the Proposal, at 2. Besides that, the Proposed Regulation foresees: on the *regulatory side*: 'an obligation to set up internal redress mechanisms, as well as provisions to allow for collective redress for associations representing businesses'.

(Art. 4). Discrimination practices (i.e. platforms favouring their business or related commercial partners) are also subject to disclosure duties (Art. 6); and platforms shall describe rules on access (or non-access) to personal and non-personal data which business users provide to them or which are generated through the platform's use (Art. 7). This does not grant data access or portability to business users<sup>45</sup>; which are the subject of other rights under either the GDPR, the Regulation on the free flow of non-personal data, or other special regimes.

More transparency obligations are addressed to online general search engines, aimed at tackling the economic dependency induced by potentially harmful ranking practices.<sup>46</sup> Search engines are thus subject to a scoped transparency obligation to provide a 'description of the *main ranking parameters* and of the possibilities to influence such rankings against remuneration' (so-called pay-for-ranking results: Art. 5). Such obligations can be viewed as a form of rules that extend the 'explicability duties' (Arts 13 and 14, GDPR) from P2C to P2B relationships. By it, the 'logic' inspiring algorithmic decisions taken by the platforms should be made transparent and therefore accountable to the business. Of course, such an obligation does not imply any duty to disclose algorithms (usually configured as trade secrets).

#### **4.2. Critical assessment: is it really disclosure co-regulation?**

Overall, the strategy envisaged by Regulation 2019/1150 is a classical horizontal, undifferentiated, and light-touch disclosure self-regulatory one, despite the existence of the hard 'regulatory' part, the mechanism for complaint-handling and the collective redress.<sup>47</sup> That is confirmed by the weak enforcement apparatus, where only monitoring tools – the voluntary mediation bodies – are envisaged vis-à-vis the infringement of analyzed disclosures.<sup>48</sup>

If light enforcement might ensure broader cooperation of the platform players, it might, at the same time, spur distrust among the business users.<sup>49</sup> Similarly, the Regulation seeks platforms' cooperation by leveraging on their reputation (e.g. it requires platforms to disclose, on an annual basis, information about the effectiveness of their internal complaint-handling systems). If that obligation can enhance trust among consumers vis-à-vis the most consolidated players, it can nonetheless marginalize start-up platforms whose reputation is still in the making.

Considering the beneficiaries of the information disclosed, micro and SMEs are not the big business: not from an economic point of view, nor a legal one. SMEs tend to be

<sup>45</sup>Graef et al. (note 63), at 11: 'While such obligations are a welcome step in creating transparency about the extent to which access to data is offered to business users, the proposed Regulation does not prescribe a minimum level of data access or ban any unfair practices relating to data access. As such, it does not tackle the interaction of data access with data protection in strategic behaviour that can undermine the level of data innovation to the detriment of both businesses and consumers.'

<sup>46</sup>Legal standing is awarded to organizations representing platforms' business counterparts (that can act on behalf of their members): see Executive summary of the Impact Assessment, cit., 2.

<sup>47</sup>See Annex to the IA, at 20 specifying that the costs for setting up the internal mechanism for complaint-handling and collective redress (following Arts. 9 and 12) towards platforms' business users should be '*minute*' (Ibid, at 142).

<sup>48</sup>According to Art. 10, platforms are subject to a *non-binding* obligation to set up independent mediation bodies for out of court settlement; while monitoring is under the responsibility of an EU Observatory on the Online Platform Economy (which merely 'monitors' the impacts of the Regulation and its regulatory and self-regulatory components on the platforms economy).

<sup>49</sup>Even though there might be some spillover effects, as business users may utilize the legal provisions in court or antitrust proceedings (e.g. to help demonstrate discriminatory behavior by dominant platforms). See Annexes to the IA, at 144.

‘economically dependent’ by the platforms and search engines they operate through; and that explains why in some jurisdictions, like Germany, concurrent norms like abuse of economic dependence (or relative market power) apply along with Regulation 2019/1150 (Di Porto & Posdzun, 2018). Similarly, both Directives on Unfair Commercial Practices (UCP) and Unfair Terms and Conditions (UCT) continue to apply to SMEs operating in platforms (e.g. preventing information manipulation)<sup>50</sup> even though they are not *stricto sensu* final consumers.

Finally, what the Regulation fails to recognize is that SMEs and especially micro-business behave much like individuals, and therefore may suffer the same cognitive bias. It instead accounts for a relatively typological, notional idea of SME, in support of which it offers the ‘informational panacea’. Once again, when it comes to ‘how’ to draft information for the business users, the Regulation relies on ‘codes of conduct’ that the Commission shall ‘encourage’ platforms and search engines to draw up, without any further guidance (Art. 13). Requirements of simplification of information (and possibly salience) would be much welcome, such as those foreseen in Article 5 (description of ranking parameters).

However, fostering high levels of informational ‘visibility’ in the digital markets does not lead to increased transparency: quite the opposite, it conduces to decreased transparency and increased opacity (it is the so-called ‘transparency paradox’) (Stohl et al., 2016, p. 131).

In an aim to fill the design gap as far as the disclosures are concerned, other models of disclosure co-regulation in the P2B relations have been suggested that make greater use of the algorithmic decisional capabilities of platforms and their regulatory powers.

## 5. New governance models: Data-based (or savvy) self- and co-regulation

Including digital platforms’ intermediation in the regulatory governance conundrum is the real advancement of more recent proposals. They dispose of mass regulatory and oversight capabilities that lack modern regulators for producing and implementing disclosures (Westerhoff, P. 2019).

Piffault suggests that platforms be subject to a ‘form of data-based regulation, where public policy objectives are attributed to them, and their achievement validated through data analysis’. (Piffault, at 2) In his view, some form of smart regulation, that he terms ‘savvy regulation’, should be put in place starting from the consideration that digital platforms are foremost ‘run on the basis of and produce data’. Therefore, they can perform better than traditional regulators, provided that they possess the infrastructure and data needed to both draft differentiated rules and oversee their implementation at a very granular level. They also have an incentive to do so, given that the more effective their oversight, the higher their reputation. That would put platforms in the best position to also address negative issues showing some public interest like, for instance, tax evasion or green rules compliance in flat renting.<sup>51</sup>

---

<sup>50</sup>To mention an example, in Italy Facebook has been condemned for providing misleading information under the UCP regime, and the Competition Authority (which is responsible for applying such set of rules), applied a €10 Mio administrative fine.

On that basis, the author suggests putting an obligation onto platforms to provide the regulator with ‘access to data and to allow simulations to satisfy compliance with some predetermined [public interest] standards’ (Piffault at 6). In particular, once the pursuit of a public objective is assigned to a platform (e.g. avoiding discrimination between hosts in an accommodation application), data feeding the algorithms used by the platforms should be made accessible to the regulator and the wider public to allow testing and ensure compliance with some pre-determined standards.

The proposal points to a fairly open access regime, where the public interest issue at stake is openly discussed, and the data generated by the platform are made publicly accessible to allow third parties (the academia included) ‘to test ideas and adaptations, conduct experiments and use the collective intelligence instead of sticking to proprietary private data’.<sup>52</sup> Obviously, one can expect fierce opposition by the platforms to the sharing of ‘large quantities of behaviour-revealing data with public authorities’ (Finck, 2017, at 13).

At the other side of the (ideal) spectrum stands Sundararajan, (EP, 2017) who purports a ‘data-driven delegation’ model. Here, ‘data is instead left inside the platform’s systems while allowing [its] use for regulation by delegating regulatory responsibility to the platform.’

Concerning controls, audits that are needed to check for compliance would be supplemented by an API; the latter, however, ‘would not provide access to raw data, as in Piffault’s model, but could allow a government to run “queries” to verify compliance.’<sup>53</sup> For instance, APIs could randomly check for compliance of tax collection by platforms.

The core of Sundararajan’s proposal is that platforms are the only ones to own the data and the capacity to run analytics over big datasets that are relevant for regulatory purposes. Also, they are in the best position to check for discrimination, biases and other undesired consequences of (their own) algorithmic decisions. Therefore, ‘rather than tasking the government with the development of such methods on data provided by platforms, it is better to allow, or perhaps even require, the platforms to develop these methods themselves and apply these to the data that remains within the platforms. After all, they have access to some of the world’s best computer scientists.’<sup>54</sup>

Although it is undeniable that governments do not possess the technical capabilities to duly oversee platforms’ algorithmic regulatory powers, the proposal completely dismisses the quests made by the Council of Europe and the EP – which happens to be the same editor as that of Sundararajan’s proposal.<sup>55</sup> It is worth reminding that the latter have been calling for the activation of empowerment strategies, ‘supported by AI tools’,<sup>56</sup> to countervail the manipulative potential of AI-led decisions.

---

<sup>51</sup>As reported by the EP (2017), at 24, the City of Lisbon delegates the hotel occupancy tax collection to AirBnB. In the same vein, a Municipality could delegate AirBnB with the implementation of environmental rules on differentiated home waste collection, e.g. by nudging homeowners through higher ranking positions.

<sup>52</sup>Ibid. at 7.

<sup>53</sup>Ibid.

<sup>54</sup>Ibid. at 25.

<sup>55</sup>See above, the Introduction.

<sup>56</sup>EP (2019 Jan.) at 7.



## 6. Algorithmic disclosure co-regulation for platforms' business users

In view to empower small business users through AI tools and also strengthening the accountability of platforms' decision-making as far as disclosures are concerned, we suggest endorsing algorithmic disclosure co-regulation. Building on previous work,<sup>57</sup> we will articulate on how this model also answers the quest for increased participation<sup>58</sup> of business users in algorithmic decisions that affect their economic lives, without having to receive the disclosures passively. Our model provides a cost-effective way to carry on frequent assessment on datasets to produce well-functioning algorithmic disclosures on a collaborative fashion, instead of delegating this task completely to the platforms.

Our model is based on three propositions and starts from a set of observations. The propositions are: (1) that disclosures targeted at business users should be done by algorithms (as suggested by the EP); (2) should be pre-tested in a co-regulatory process that involves the regulator (possibly the European Commission, the Bercé or an ad hoc EU authority enjoying enforcing powers), the platforms, the business users and the consumers (using regulatory sandboxes); and (3) enforced through legal and other empowerment tools, rather than sole fines.

As far as the observations are concerned, our starting point is the EDPB's important statement (2018a), according to which: algorithms are subject to bias and 'can result in assessments based on imprecise projections'. (p. 27) Therefore, it is crucial to 'carry out frequent assessments on the data sets ... to check for any bias, and develop ways to address any prejudicial elements, including overreliance on correlations'. Those checks and audits require 'regular reviews of the accuracy and relevance of automated decision-making, including profiling ... not only at the design stage but also continuously' (p. 28). This affects algorithms used by platforms, which are subject to frequent changes to provide for the best products and services. And makes EU legislative duty to disclose the 'main parameters' of algorithmic rankings<sup>59</sup> of little value for business users, because such parameters can become rapidly obsolescent, making their disclosure not timely, or the chosen format outdated or its content meaningless. Therefore, instead of requesting the platforms to provide for access to their data or their algorithms, we suggest instead that the disclosure duties to which they are subject (which may regard ranking parameters but also other contractual clauses), be drafted in a completely different fashion.

For any disclosure targeted at business users in platforms to be tailored at their informational needs, meaningful and dynamic (i.e. changing over time according to their preferences), we propose to set up an agile group for the ex-ante testing of algorithmic disclosures in the course of a co-regulatory process.<sup>60</sup> That is, in fact, not entirely new to the regulatory landscape, as 'regulatory sandboxes' already exist in the Fintech industry, where new rules are experimented in controlled environments (thanks to simulations run over big data) before being implemented at large scale.<sup>61</sup>

---

<sup>57</sup>Di Porto & Maggiolino (2019).

<sup>58</sup>EP (2019 Apr)

<sup>59</sup>See Recitals 26–28 and art. 5, Regulation EU 1150/2019 requiring search engines to disclose the 'description of the *main parameters* determining the ranking of all indexed websites and their relative importance'.

<sup>60</sup>(Gahnberg, , pp. 9–10).

<sup>61</sup>Regulatory sandboxes are aimed at fostering collaboration between regulators and the financial industry to test new regulations in controlled environments (check their potential impacts on consumers and the market) before implementation. That, in turn, helps to foster innovation in the Fintech industry. See: ESMA, EBA and EIOPA (2019); Piri (2019); Amer et al. (2016), Mattli (2018); Picht and Loderer (2018).



The envisaged small experimental group would include the regulator (that takes the initiative, like in innovation hubs), the final consumers and individuals representing the platforms and the SMEs. The actual individuals representing the SMEs would of course vary depending on the topic of algorithmic disclosures (for instance, if layouts to be tested in the sandbox through algorithms pertain to how to share data in the short-term rental sector, then participants in the sandbox would be digital platforms operating in there, flat owners, consumers, data scientist technicians, and the regulator).<sup>62</sup>

Goal of the group would be to train the selected algorithm for designing the disclosures. So for instance, when drafting different disclosure formats of ‘the main parameters determining the ranking of all indexed websites and their relative importance’, Art. 5 Regulation EU 1150/2019 requires that search engines allow corporate website users to ‘obtain an adequate understanding’ of ‘whether, and how and to what extent, certain design characteristics of the[ir] website. is taken into account’ by the algorithm in its ranking. Hence, pre-testing in a controlled environment the best format such information might have, that is also produced automatically through an algorithm and fairly accommodates the interests of all stakeholders is a desirable outcome.

The testing would also allow to comply with a further legal requirement, namely: to ‘ensure predictability for corporate website users’, not of the parameters though, but of the disclosures; while also ensuring that ‘the description. be kept up to date, including the possibility that any changes to the main parameters should be made easily identifiable.’ (Art. 5). In our proposal, diverse algorithmic techniques<sup>63</sup> would be used to develop disclosures that are differentiated and targeted at various groups of SMEs depending on their willingness to receive a more simplified or granular (detailed) disclosure format (e.g. three groups may be identified while running the tests: (i) simple, (ii) intermediate, and (iii) sophisticate recipient).<sup>64</sup> Every choice they make will be tracked during the test, and data will feed the algorithm, providing it with information on how to produce the best disclosures, meaning those that fail the least to be read, understood and give a due course of action.

Technically speaking, we suggest using a knowledge graph to realize the differentiated targeted disclosures. The process should start with three libraries: two of which are textual (the disclosure duties established by EU laws and regulation; and the platforms’ disclaimers implementing them), and one would consist of the behavioural data coming from the sandbox. In conceptualizing the sandbox, we should elaborate on the concepts that are typical of one sector. To do so, we need to create relationships with a natural language sandbox: that serves to allow humans to participate in the sandbox to either confirm or reject such concepts. On that basis, we should produce them to all the stakeholders in the sandbox (because we are in a co-regulatory regime). By saying that they are ‘satisfied’ (i.e. by ‘confirming’ the layouts), they will feed into the sandbox.

We should reproduce that test for several formats and several times (sessions) until we get to the point where all participants are mostly satisfied and least dissatisfied. We

---

<sup>62</sup>It is especially important to select these stakeholders in a way that the interests of the business users are well represented before those of the platforms and enough receptive of those of final consumers.

<sup>63</sup>Several algorithmic techniques exist (think of Natural Language Processing – NLP – or Generation – NLG) that allow for text mining and simplification, but also the graphic rendering of text (super or hyper-simplification).

<sup>64</sup>Based on data, ‘clustered’ disclosures can be produced that meet the needs of the recipients, while adapting to the changing of their preference over time. For instance, over-simplified information about the ranking parameters could be provided, that are clustered (i.e. based on a group of users with similar characteristics).

should repeat this with the clauses of each disclosure per each of the 3 or  $n$  formats we want to target the cluster SMEs.

In the knowledge graph, both the texts and behavioral data would be integrated employing SMEs' user experience.<sup>65</sup> Behavioral data coming from the regulatory sandbox would be used to confirm or contradict the links described by the graph.<sup>66</sup>

The human presence, as said, is essential to monitor if errors occur in the building of the knowledge graph: technicians supervising in the sandbox may intervene to eventually deactivate any error that may occur in the algorithm. That implies that we need technicians to participate in the sandbox, besides regulators, firms (platforms and SMEs), and consumers.

It is important to stress that there would be no need for the platform to disclose any of its own algorithms (which might easily remain secret) to other stakeholders participating in the trials.<sup>67</sup> That is because the kinds of algorithms that are needed to get to targeted algorithmic disclosures are either available on an open access basis,<sup>68</sup> or because it could be provided by the regulator itself (Di Porto 2020). The consumers and SMEs contribute with their behavioral data to feed the algorithm: for instance, in case of disclosures of standard form contracts (typically the fine print one finds online and hardly reads), the experimental phase would consist of the stakeholders testing different formats of ToCs.<sup>69</sup>

Testing is also relevant to implement rapid amendments to the algorithmic disclosures, should any major risks associated with AI-led decisions emerge during the training (such as algorithmic biases in rankings, overreliance on correlation or discrimination).

Following the best practice identified by the Art. 29 WG, such modifications would feedback into the algorithm to ameliorate it and, consequently, the disclosures.

Indeed, the pre-testing phase also allows detecting with some precision what are the informational needs and understanding capabilities of the business users. In this sense, algorithmic disclosures would produce useful information, by dynamically adapting its content and format to what the recipient needs at the time she needs. Also, as articulated elsewhere, because co-regulated algorithmic disclosures would necessarily be targeted at

---

<sup>65</sup>To make a parallel, this operation resembles the way Google search engine operates (through domains and supra-domains). More specifically, when Google users are shown a picture and are asked to 'confirm' that what they see is a cat, they can confirm or not. If they do, they reinforce a node of the graph (that the picture shown is a cat and not, say, a muffin). Similarly, human stakeholders in the sandbox provide behavioral data that confirm a proposed clause or text, thus reinforcing nodes, and gradually strengthening the links in our knowledge graph.

<sup>66</sup>The ontology serves to link all the pieces with concepts of the domain, supra-domain, and vertical (i.e. sector-specific) domain. For instance, imagine we aim to link the term 'fintech' (domain) to the normative goal (supra-domain) to a sector-specific term, like 'transparency in financial fintech' (vertical domain). However, because most of the time, norms do not speak in such a detail, we need to use a meta-level to provide further instructions. For instance, very often norms in the financial domain do not require retailers of financial products to disclaim full detailed composition of their products, but would instead require for general transparency. Therefore, we would need to provide a meta-level whereby to instruct the algorithm this way: 'When using the word 'norms', link it to the concept 'transparency', then link it to 'disclaimer'.

<sup>67</sup>Notoriously, algorithms are covered by IPRs (and are usually qualified as trade secrets). Legally speaking, under EU law firms are not entitled any general right to be informed about the overall system used to make automatic decisions, nor can they demand the full disclosure of the algorithm: see Recital 27 and Art 5(6) Regulation EU 1150/2019.

<sup>68</sup>Just to make an example, think to the very ambitious publicly-funded Lynx project (<http://lynx-project.eu/> (accessed 05.06.2020)), providing for an ontology of linked legal sources aimed at making compliance easy to firms (especially SMEs) in three legal domains (business law, labor law and energy law). For more details, see Montiel-Ponsoda & Rodríguez-Doncel (2018)

<sup>69</sup>Notoriously, algorithms are covered by IPRs (and are usually qualified as trade secrets). Legally speaking, under EU law, firms are not entitled to any general right to be informed about the overall system used to make automatic decisions, nor can they demand the full disclosure of the algorithm: see Recital 27 and Art 5(6) Regulation EU 1150/2019.

the different informational needs of the recipients, they would comply with the principle of proportionality (Di Porto & Maggiolino 2019).

Once sufficient data is gathered that the tested algorithm can produce well-functioning disclosures, intended as those that are informative to the identified groups and bias-free (i.e. or not conducive to self-serving information manipulation), are algorithmic disclosures implemented on large scale.

The same is for any modification to the algorithmic disclosures that the participants to the sandbox accept – and the regulator certifies: they become implementable by the platforms on a large scale.

Also, they could be given a special legal effect: for instance, all pre-tested modifications could automatically be implemented and produce a direct effect among the counterparties. So for instance, an amendment to the Terms of Contract of a certain service in a given sector, which is agreed upon in the sandbox, and implemented in the algorithmic disclosure, could become immediately effective.

With algorithmic disclosure co-regulation, enforcement of disclosures becomes somehow less problematic. Codes of conduct would no longer be a fictional substitute for compliance, as the effectiveness of disclosures to really inform recipients would be tested in advance.

## 7. Discussion and conclusion

In this paper, we reviewed different models that include digital platforms as regulatory intermediators, alongside the public authorities (at the EU level) and the markets. In this journey, we explored which one was best suited to build disclosure regulation for the platform economy, between ‘solicited’ or ‘encouraged’ self-regulation (based on codes of conduct) and co-regulation. In this latter case, we explored how technology, and AI algorithms, especially, could contribute to the shaping of a well-functioning co-regulatory system.

We concluded that none of the two ‘extreme’ proposals reviewed was suitable: not the fully open ‘savvy option’, mandating platforms to share the data feeding their algorithms with the wider public, because it would stifle innovation. Nor the ‘data-delegated regulation’ option, because it would not solve the problem of possible algorithmic manipulation by platform, identified as a significant concern by both the Council of Europe and European Parliament.

On our side, we proposed a regulatory sandbox model where stakeholders come together to develop and train an algorithm that could provide disclosures about the platform’s operations to the business-users.

We suggest that disclosures (still the core of EU legislation of digital platforms) be conceived and drafted through algorithms (algorithmic disclosures). That would necessarily imply a collaboration between the platforms and the regulator (as the other proposals) but would imply wider participation, by allowing also individuals representing final consumers and the SMEs to contribute in the design of disclosure. Algorithmic disclosures are thus pre-tested (by running analytics) in small groups representing all the mentioned stakeholders (like in regulatory sandboxes); freed of biases and risks of manipulations, through repeated testing and feedbacks and then implemented on a large scale.

We contended that not only do ex-ante design, testing and amendments of algorithmic disclosures increase participation of SMEs in the rule-making process, but they do also provide for greater empowerment to the business users. On this last point, lacking empirical evidence, one can only speculate that by actively receiving targeted and personalized disclosures, a business user will be better empowered than through undifferentiated, detailed, untimely information about, say, the ‘main parameters determining the ranking’ of its services.

One of the main problems is to ensure collaboration in the sandbox. Why should the platforms share their (private) algorithmic regulatory power with the public rule-maker and the addressees? And also, why would the digital firms want to participate in the regulatory sandbox instead of producing their own disclosures? In the end, anything that happens in the sandbox implies some disclosure of trade strategies to the regulator, competitors, and SMEs and final consumers. Information is an asset, and even in the little margins left by the disclosure duties, platforms might not want to share the way to convey it to their clients.

Setting the right incentives is pivotal to gain participation. First, there is a reputational advantage for the platforms, which are seen as engaging in pro-small business activities. Second, the automatic production of rules saves the costs for producing the disclosures and updating them. Third, the direct effect of modifications of disclosures agreed in the sandbox does also save costs to the platforms. As per the incentives for SMEs and consumers, they will have voice and representation in the rule-making process by feeding the algorithm with their behavioral data.

Such disclosures would save costs on platforms and search engines for not having to continually update their disclosures (like their terms and conditions on rankings) and to notify these changes to all their counterparts. As said, all disclosures and changes that are agreed upon in the sandbox will be directly implemented through the algorithm and would most probably generate less litigation in court. In this sense, algorithmic disclosures may save some costs of private enforcement, at least for the pre-tested issues, provided that they have been thoroughly discussed and accepted within the pre-trial, and certified by the regulator.

One should mention that not all domains are suitable for algorithmic disclosures. For instance, in some areas retailers might not use (or not use yet) algorithms or big data technologies, and cannot, therefore, take advantage of this new mode of disclosure.

Given that they would empower micro and SMEs, algorithmic disclosures may potentially help saving time for the scaling-up process of European digital companies. Finally, the co-regulatory process entailed in such disclosures would maintain a leading role for the Commission, the Bercé or a new EU-wide authority for algorithms. The EU, however, would still need to cooperate internationally to ensure that algorithmic disclosures might have a legal effect also outside its borders.

## **Disclosure statement**

No potential conflict of interest was reported by the authors.

## Funding

This work was supported by the Lady Davis Fund and the Ministero dell'Istruzione, dell'Università e della Ricerca PRIN Project, 2017 Prot. 2017BAPSXF.

## Notes on contributors

*Fabiana Di Porto*, Associate Professor of Economic Law and Innovation, University of Salento; Forchheimer Visiting Professor, Faculty of Law (Lady Davis Fund 2019/20), Hebrew University of Jerusalem, Israel.

*Marialuisa Zuppetta*†, Assistant Professor of Public Law, University of Salento.

## ORCID

Fabiana Di Porto  <http://orcid.org/0000-0002-4420-9741>

## References

- Abbot, K. W., Levi-Faur, D., & Snidal, D. (2017). Theorizing regulatory intermediaries. *The ANNALS of the American Academy of Political and Social Science*, 670(1), 14.
- Acquisti, A., Grossklags, J., (2007). What can behavioral economics teach us about privacy? In A. Acquisti, S. Gritzalis, C. Lambiroudakis, S. de Capitani di Vimercati (Eds.), *Digital privacy: Theory, technologies and practices*. Auerbach Publications, 363.
- Ananny, M., & Crawford, K. (2016). Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability. *New Media & Society*, 20(3), 973–989.
- Argenton, C., & Prüfer, J. (2012). Search engine competition with network externalities. *Journal of Competition Law and Economics*, 8(1), 73.
- Arner, D. W., Barberis J.N., Buckley, R.P. (2016). Fintech, RegTech, and the reconceptualization of financial regulation. *NW. Journal of International Law & Bus*, 37, 371.
- Ayres, I., & Braithwaite, J. (1994). *Responsive regulation*. Oxford University Press, Oxford.
- Baldwin, R., Cave, M., & Lodge, M. (2012). *Understanding regulation*. Oxford University Press, Oxford.
- Ben-Shahar, O., & Schneider, C. E. (2011). The failure of mandated disclosure. *University of Pennsylvania Law Review*, 159, 647.
- Ben-Shahar, O., & Schneider, C. E. (2014). *More than you wanted to know: The failure of mandated disclosure*. Princeton University Press, Princeton.
- Black, J. (1996). Constitutionalising self-regulation. *The Modern Law Review*, 59(1), 24.
- Black, J. (2001). Decentring regulation: Understanding the role of regulation and self-regulation in a “post-regulatory” world. *Current Legal Problems*, 54(1), 103.
- Black, J. (2007). Tensions in the Regulatory State. *Public Law*, Spring, 58.
- Busch, C. (2016a). Crowdsourcing, consumer confidence: How to regulate online rating and review systems in the. In C. Economy & A. De Franceschi (Eds.), *European contract law and the digital single market: The implications of the digital revolution* (p. 223). Intersentia, Uitgevers.
- Busch, C. (2016b). The future of pre-contractual information duties: Personalization of disclosures with big data. In Twigg-Flesner (Ed.), *Research handbook on EU consumer and contract law* (p. 221). Edward Elgar, Cheltenham. Retrieved from [ssrn.com/abstract=2728315](https://ssrn.com/abstract=2728315).
- Busch, C., & De Franceschi, A. (2018). Granular legal norms: Big data and the personalization of private law. In V. Mak, E. Tjong Tjin, & T. A. Berlee (Eds.), *Research handbook on data science and law* (p. 408). Edward Elgar, Cheltenham. Retrieved from: [ssrn.com/abstract=3181914](https://ssrn.com/abstract=3181914).
- Busch, C. (2019). Self-regulation and regulatory intermediation in the platform economy. In M. Cantero Gamito & H. W. Micklitz (Eds.), *The role of EU in transnational legal ordering*:

- standards, contracts, codes.* (p. 115) Edward Elgar, Cheltenham. Retrieved from [ssrn.com/abstract=3309293](https://ssrn.com/abstract=3309293)
- Coglianese, C., & Mendelson, E. (2010). Meta-regulation and self-regulation. In R. Baldwin, M. Cave, & M. Lodge (Eds.), *The Oxford handbook of regulation* (p. 146). Oxford University Press, Oxford.
- Coglianese, C., & Lazer, D. (2003). Management based regulation: Prescribing private management to achieve public goals. *Law Society Review*, 37(4), 691.
- Coglianese, C., & Lehr, D. (2019). Transparency and algorithmic governance. *Additional District Magistrate (LR)*, 71, 1.
- Cohen, M., & Sundararajan, A. (2015). Self-regulation and innovation in the peer-to-peer sharing economy. *The University of Chicago Law Review*, 82, 116–131.
- Council of Europe. (2019). *Declaration by the committee of ministers on the manipulative capabilities of algorithmic processes*. Decl(13/02/2019)1, 13.2.2019.
- Craswell, R. (2006). Taking information seriously: Misrepresentation and nondisclosure in contract law and elsewhere. *Virginia Law Review*, 92, 565.
- de Streel, A., & Sibony, A.-L. (2017, October). Towards smarter consumer protection rules for the digital society. *CERRE Project Report*.
- Di Porto, F., & Ghidini, G. (2020). I access your data, you access mine. *Requiring Data Reciprocity in Payment Services. IIC*, 51, 307–329.
- Di Porto, F., & Maggiolino, M. (2019). Algorithmic information disclosure by regulators and competition authorities. *Global Jurist*, 19(2), 1–17. Retrieved from: [ssrn.com/abstract=3363169](https://ssrn.com/abstract=3363169).
- Di Porto, F., & Posdzun, R. (Eds.). (2018). *Abusive practices in competition law*. Ascola series, Edward Elgar, Cheltenham.
- Di Porto, F. (2020). From BADs to BEDs. Algorithmic Disclosure Regulation. Theoretical aspects for empirical application. Hebrew University of Jerusalem Legal Research Paper 20-18. Retrieved from: <https://ssrn.com/abstract=3633847> or <http://dx.doi.org/10.2139/ssrn.3633847>
- Easterbrook, F. H., & Fischer, D. R. (1984). Mandatory disclosure and the protection of investor. *Virginia Law Review*, 70(4), 669.
- EC. (2016a, February 2nd). *Communication ‘A European agenda for the collaborative economy’*, COM(2016)0356 final.
- EC. (2016b, May 25th) *Communication ‘online platforms and the digital single market’*, COM (2016) 288 final.
- EC. (2017). *Communication ‘building a European data economy’*, COM(2017)9 fin., 10. 1.2017.
- EC. (2018). *Communication ‘towards a common European data space’*, COM(2018)232 final.
- EC. (2019). *Competition policy for the digital era*. Report by J. Crémer, Y.-A. de Montjoye, H. Schweitzer, 16.
- EC. (2020a). *Communication on ‘A European strategy for data’* (COM(2020) 66 final). <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1601713734544&uri=CELEX:52020DC0066>
- EC. (2020b). *Shaping Europe’s digital future*. (COM(2020) 67 final). <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1601713734544&uri=CELEX:52020DC0067>
- EC. (2020c). *White paper on AI*. (COM(2020) 65 final). <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1601713734544&uri=CELEX:52020DC0065>
- EC. (2020d) *Digital Services Act package: Ex ante regulatory instrument for large online platforms with significant network effects acting as gate-keepers in the European Union’s internal market, Inception impact assessment*, Ares(2020)2877647, 4 June.
- EDPB - European Data Protection Board. (2018a). *Guidelines on automated individual decision-making and profiling*, 6 February
- EDPS - European Data Protection Supervisor. (2019). *Guidelines 1/2019 on codes of conduct and monitoring bodies under regulation 2016/679*, 12 February
- ESMA, EBA and EIOPA. (2019). *FinTech: Regulatory sandboxes and innovation hubs*, JC 2018 74.
- European Commission. (2015). *Communication ‘A digital single market strategy for Europe’*. COM (2015)192 fin., 6. 5.2015.
- EU High level Expert on AI. (2019, April 8). *Ethics guidelines for trustworthy AI*.



- European Parliament (EP). (2017). *The collaborative economy: Socioeconomic, regulatory and policy issues*. (by A. Sundararajan), PE 595.360 EN, IP/A/IMCO/2016-12, February.
- European Parliament (EP). (2019b). *A governance for algorithmic accountability and transparency*, PE624.262, April.
- European Parliament (EP). (2019a). *Artificial intelligence: Challenges for EU citizens and consumers*, PE631.043, January.
- Evans, D. S., & Schmalensee, R. (2015). The antitrust analysis of multisided platform businesses. In R. D. Blair & D. D. Sokol (Eds.), *The Oxford handbook of international antitrust economics* (p. 404). Oxford University Press, Oxford.
- Evans, D. S., & Schmalensee, R. (2016). *Matchmakers: The new economics of multisided platforms*. Harvard Business Review Press, Boston.
- Finck, M. (2017). Digital regulation. *LSE Law, Society and Economy Working Paper 15/2017*.
- Gal, M. S. (2017). Algorithmic Challenges to Autonomous Choice. *Michigan Telecommunication and Technology Law Review*, 25, 59–104.
- Gahnberg, C. (2020). The governance of artificial agency. *Policy & Society*, this issue.
- Gaudeul, A., & Jullien, B. (2008). E-commerce, two-sided markets and info-mediation. In E. Brousseau & N. Curien (Eds.), *Internet and digital economics* (p. 268). Cambridge University Press, Cambridge.
- Grabosky, P. N. (1995). Using non-governmental resources to foster regulatory compliance. *Governance*, 8(4), 527.
- Graef, I., Gellert, R., & Husovec, M. (2018). Towards a holistic regulatory approach for the European data economy: Why the illusive notion of non-personal data is counterproductive to data innovation. *DP 2018-028 TILEC Discussion Paper*. Retrieved from [ssrn.com/abstract=3256189](https://ssrn.com/abstract=3256189)
- Grunes, A. P. (2013). Another look at privacy. *The George Mason Law Review*, 20, 1107.
- Hagel, J., & Rayport, J. F. (1997). The coming battle for customer information. *Harvard Business Review*, 53–61.
- Heemsbergen, L. (2016). From radical transparency to radical disclosure: Reconfiguring (in) voluntary transparency through the management of visibilities. *International Journal of Communication*, 10, 138–151.
- Lessig, L. (1999). *Code and other laws of cyberspace*. Basic Books, New York.
- Lim, H. S. M., & Taeihagh, A. (2019). Algorithmic decision-making in AVs: Understanding ethical and technical concerns for smart cities. *Sustainability*, 11(20), 5791.
- Marotta-Wrugler, F. (2014). Even more than you wanted to know about the failures of disclosure. *NYU L. and Econ. Working Papers, Paper n. 394*. Retrieved from [lsr.nellco.org/nyu\\_lewp/394](https://lsr.nellco.org/nyu_lewp/394)
- Marsden, C. (2011). *Internet co-regulation*. Cambridge University Press, Cambridge.
- Mattli, W. (ed.). (2018). *Global algorithmic capital markets: High-frequency trading, dark pools, and regulatory challenges*. Oxford University Press, Oxford.
- Medzini, R. (2018). *Regulatory Intermediaries in the European privacy regime: How, why and to what effect?* Retrieved from <https://csrcl.huji.ac.il/event/rotem-medzini>
- Montiel-Ponsoda, E., & Rodríguez-Doncel, V. (2018, May 12). Lynx: Building the legal knowledge graph for smart compliance services in multilingual Europe. In G. Rehm, V. Rodríguez-Doncel, & J. Moreno-Schneider (Eds.), *Proceedings of the 1st workshop on LREC (language resources and technologies for the legal knowledge graph) workshop* (pp. 19–22). Retrieved from <https://delicias.dia.fi.upm.es/members/vrodriguez/pdf/2018.legalkg.pdf>
- OECD. (2018) *Rethinking antitrust tools for multi-sided platforms*. Retrieved from [www.oecd.org/competition/rethinking-antitrust-tools-for-multi-sided-platforms.htm](http://www.oecd.org/competition/rethinking-antitrust-tools-for-multi-sided-platforms.htm)
- OECD. (2019). *Recommendation on AI*. Paris, May 25th
- Parker, C. (2002). *The open corporation: Effective self-regulation and democracy*. Cambridge University Press, Cambridge.
- Parker, C. (2005). Regulator-required corporate compliance program audits. *Law Policy*, 25(3), 221.



- Picht, P. G., & Loderer, G. T. (2018). Framing algorithms – competition law and (other) regulatory tools. *MPI Research Paper* No. 18-24. Retrieved from [ssrn.com/abstract=3275198](https://ssrn.com/abstract=3275198)
- Piffaut, H. (2018, May). Platforms, A call for data-based regulation. *CPI Antitrust Chronicle*, 4.
- Piri, M. M. (2019). The changing landscapes of fintech and regtech: Why the United States should create a federal regulatory sandbox. *Business and Finance Law Review*, 2, 233–254.
- Prat, A. (2005). The wrong kind of transparency. *American Economic Review*, 95(3), 862.
- Radu, R. (2020). AI governance: National, hybrid, ambiguous. *Policy & Society*. this issue.
- Rust, R. T., Kannan, P. K., & Peng, N. (2002). The customer economics of internet privacy. *Journal of the Academy of Marketing Science*, 30(4), 455.
- Scott, C. (2012). Regulating everything: From mega- to meta-regulation. *Administration*, 60, 57.
- Shelanski, H. A. (2013). Information, innovation, and competition policy for the internet. *University of Pennsylvania Law Review*, 161, 1663.
- Special issue of Reg.&Gov. (2019). *Exploring the formal and informal roles of regulatory intermediaries in transnational multi stakeholder regulation* (pp. 125–298).
- Stohl, C., Stohl, M., & Leonardi, P. M. (2016). Managing opacity: Information visibility and the paradox of transparency in the digital age. *International Journal of Communication*, 10, 123–137.
- Strahilevitz, L., & Porat, A. (2014). Personalizing default rules and disclosures with big data. *Michigan Law Review*, 112, 1417.
- Susser, D., Roessler, B., & Nissenbaum, H. (2019). Technology, autonomy, and manipulation. *Internet Policy Review*, 8, 2–3.
- Taeihagh, A. (2020). The governance of artificial intelligence and robotics. *Policy & Society*, this issue.
- Tan, S., & Taeihagh, A. (2020). Governing the adoption of robotics and autonomous systems in long-term care in Singapore. *Policy & Society*, 1–21. this issue. doi:10.1080/14494035.2020.1782627
- The Stigler Center Group at Chicago Booth. (2019). *Report by the committee for the study of digital platforms, privacy and data protection subcommittee*. Retrieved from <https://research.chicagobooth.edu/-/media/research/stigler/pdfs/data-report.pdf?la=en&hash=54ABA86A7A50C926458B5D44FBAAB83D673DB412>
- Tirole, J. (2017). *Economics for the common good*. Oxford, Oxford University Press.
- U.S. Federal Trade Commission (FTC). (2016, November). *The sharing economy, FTC staff report*. Retrieved from [www.ftc.gov/system/files/documents/reports/sharing-economy-issues-facing-platforms-participants-regulators-federal-trade-commission-staff/p151200\\_ftc\\_staff\\_report\\_on\\_the\\_sharing\\_economy.pdf](http://www.ftc.gov/system/files/documents/reports/sharing-economy-issues-facing-platforms-participants-regulators-federal-trade-commission-staff/p151200_ftc_staff_report_on_the_sharing_economy.pdf)
- U.S. Office of Science and Technology. (2020, January). Draft memorandum for the heads of executive departments and agencies. *Guidance for Regulation of Artificial Intelligence Applications*. Retrieved from [www.whitehouse.gov/wp-content/uploads/2020/01/Draft-OMB-Memo-on-Regulation-of-AI-1-7-19.pdf](http://www.whitehouse.gov/wp-content/uploads/2020/01/Draft-OMB-Memo-on-Regulation-of-AI-1-7-19.pdf)
- Vaidhyanathan, S. (2011). *The googlization of everything (and why we should worry)*. Los Angeles: Univ. of California Press.
- Westerhoff, P. (2019). The German Amazon marketplace agreement case: A landmark settlement with global reach or more hype than substance?, 20. 11.2019. Retrieved from: [www.hausfeld.com/news-press/the-german-amazon-marketplace-agreement-case-a-landmark-settlement-with-global-reach-or-more-hype-than-substance](http://www.hausfeld.com/news-press/the-german-amazon-marketplace-agreement-case-a-landmark-settlement-with-global-reach-or-more-hype-than-substance)
- Whittington, J., & Hoofnagle, C. J. (2012). Social networks and the law: Unpacking privacy’s price. *North Carolina Law Review*, 90, 1327.
- Zuboff, D. (2019). *The age of surveillance capitalism: The fight for the future at the new frontier of power*. New York: Public Affairs.