www.jusletter-it.eu

Rolf H. Weber

Transparency on Digital Platforms

The lack of transparency on digital platforms due to insufficient comprehensibility, mandated disclosure rules, information overload, opacity and fragmentation jeopardizes the rights' situation of users. Therefore, transparency alone is not a convincing «disinfectant» for digital platforms; other normative models need increased attention. Consequently, the article analyses alternative regulatory approaches such as accountability, auditability, observability, content moderation and – with regard to the implementation of rules – pleads for a concept of targeted transparency based on elaborated soft law instruments.

Category of articles: Articles
Field of law: E-Commerce

Citation: Rolf H. Weber, Transparency on Digital Platforms, in: Jusletter IT 31 August 2023

ISSN 1664-848X, jusletter-it.weblaw.ch, Weblaw AG, info@weblaw.ch, T +41 31 380 57 77 EDITIONS WEBLAW

Contents

1. Introduction
2. Transparency Challenges
   2.1. Comprehensibility
   2.2. Mandated Disclosure
   2.3. Information Overload
   2.4. Opacity
   2.5. Fragmentation
3. Extensions to New Horizons
   3.1. Accountability
   3.2. Auditability
   3.3. Observability
   3.4. Content Moderation
   3.5. New Legal Approaches
      3.5.1. Regional and National Governmental Regulations
      3.5.2. Soft Law Instruments
4. Outlook

1. Introduction

[1] Digital platforms gained high importance during the last ten years and build a part of daily life. Platforms can be characterized as large-scale infrastructures specialized in facilitating interaction and exchange among independent actors. Platforms play a role in many contexts of society; from a regulatory perspective, two different kinds of platforms must be distinguished:[1]

- Business-oriented platforms offer goods and services to the potential demand side (for example AirBnB, Uber, etc.); relevant legal issues concern competition law (two- or multi-sided markets), consumer law, labor and social security law, etc.
- Communications- and society-oriented platforms host, organize and circulate users' shared content or social interactions; legal issues in this context are content moderation and disinformation.

[2] In the past, most regulatory approaches were attempting to tackle the given challenges by introducing transparency obligations. Already more than 100 years ago (in 1913), Brandeis[2] wanted to make visible the opaque and hidden information, with the objective of creating truth («sunlight») that could enable control and serve as a «disinfectant». After a short description of the transparency notions, strengths and weaknesses of such a regulatory approach are discussed in this contribution.

1 This article is based on a presentation given at the conference «Society of Internet – Platforms II» on 20 June 2023 in Budapest; the text is slightly amended and footnotes have been added. For a good general description of the legal challenges in the context of digital platforms (mainly designed as a human rights-based approach to content moderation [below chapter 3.4]) see Council of Europe, Content Moderation, – Guidance Note (2021), Best practices towards effective legal and procedural frameworks for self-regulatory and co-regulatory mechanisms of moderation (Adopted by the Steering Committee for Media and Information Society – CDMSI), Strasbourg, May 2021, https://edoc.coe.int/en/internet/10198-content-moderation-guidance-note.html.

2 Louis Brandeis, The Other People's Money and How the Bankers Use It, New York 1914, p. 92.

[3] Being defined as «easily seen through or understood», transparency is usually assessed as encompassing characteristics such as clarity, accuracy, accessibility and truthfulness.[3] In so doing, transparency is an important topic in many market and societal segments by among others enabling access to the information necessary for the evaluation of opportunities and costs of operations and exchanges. This understanding of transparency links information disclosure to visibility, insight, and effective regulatory judgement.[4] Furthermore, transparency is relevant for the achievement of other important tenets of regulation, such as independence and accountability of regulators since transparency facilitates compliance, effectiveness and access to data.[5]

[4] Often transparency is differentiated into three main pillars, namely (1) procedural transparency, (2) decision-making transparency and (3) substantive transparency:[6]

1. *Procedural transparency* encompasses rules and procedures in the operation of legal entities that must be clearly stated, have an unambiguous character and are publicly disclosed. The rules should also make the process of governance and lawmaking accessible and comprehensible for the public.
2. *Decision-making transparency* can be seen as reasoned explanations for decisions that, together with public scrutiny, are able to strengthen the institutional credibility and legitimacy of decisions.
3. *Substantive transparency* is directed at the establishment of rules containing the desired substance of revelations, standards and provisions which avoid arbitrary or discriminatory decisions; substantive rules often include requirements of rationality and fairness.

[5] These different pillars of transparency can be found in the digital platform context and must be reflected in the design of the normative framework. So far, many regulatory approaches have tackled the transparency concept and attempted to create an adequate legal environment that realizes more fairness in platform-relations.

2. Transparency Challenges

[6] The concept of transparency having become an essential regulatory element mainly in financial markets and consumer laws, is increasingly exposed to challenges and critical analyzes. Echoing these voices, transparency is partly seen as policy panacea.[7] The combination of infrastructural capture and algorithmic matching results in forms of socio-technical ordering that makes platforms powerful.[8] Relevant issues in this context are comprehensibility, mandated disclosure, over-information, opacity and fragmentation.

3 Rolf H. Weber, Shaping Internet Governance: Regulatory Challenges, Zurich 2009, p. 121.

4 Mike Ananny/Kate Crawford, Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability, New Media & Society 20 (2018), pp. 973–974, https://doi.org.

5 Bernhard Rieder/Jeanette Hofmann, Towards platform observability, Internet Policy Review 9 (2020), p. 1, p. 5, https://doi.org/10.14763/2020.4.1535.

6 Weber (n. 3), p. 122.

7 Rieder/Hofmann (n. 5), p. 3.

8 Rieder/Hofmann (n. 5), p. 2.

2.1. Comprehensibility

[7] Over the last ten years, regulations in the financial markets and consumer contexts have substantially increased the scope of information duties to be observed by providers of goods and services.[9] As mentioned, Brandeis attributed the characteristics of «sunlight» and «disinfectant» to the transparency principle;[10] however, since information or disclosure often goes too far, the recipient does not anymore understand its key message.[11]

[8] Transparency should address the way how information is delivered in order to optimize the outcome of the informational process.[12] The basic objectives of transparency require robust and general rules; this principle is now enshrined in article 12 para. 1 GDPR; information must be given «in a concise, transparent, intangible and easily accessible form, using clear and plain language».[13] Only clear and intangible pieces of information can optimize the comprehensibility on the side of the addressees. The GDPR requirement is very appropriate, however, the reality in digital relations shows that the chosen information approach often does not comply with the regulatory guideline.

2.2. Mandated Disclosure

[9] In the business-oriented context, the increasing number of information obligations has been mainly criticized by representatives of the law and economics discipline under the heading of «mandated disclosure paradigm».[14] Apart from the hidden costs caused by such kind of disclosure (for example detailed prospectus obligations in case of public offerings), academics argue that the mandated disclosure would exacerbate inequality, impair consumers' decisions and deter lawmakers from adopting better regulations.[15]

[10] Often it appears to be doubtful that the information addressees indeed read and understand the mandatorily provided information.[16] Distributed ledger technologies aggravate the problem: platform users are often not able to understand the «IT language» meaning that for example the disclosure of mathematical formulas constituting a smart contract do not lead to an informed addressee.[17] In addition, from a sociological perspective, the provided information whether individually aggregated or based on advice «will not adequately help the naïves in their dealings

9 Rolf H. Weber, The Disclosure Dream – Towards a New Transparency Concept in EU Consumer Law, EuCML 2023, pp. 67–68.

10 Brandeis (n. 2), p. 92.

11 Rolf H. Weber, From Disclosure to Transparency in Consumer Law, in: K. Mathis/A. Tor (eds.), Consumer Law and Economics, Cham 2021, p. 73, pp. 79–81.

12 Rolf H. Weber/Rainer Baisch, Climate Change Reporting and Human Information Processing – Quo Vadis Transparency?, ex/ante, Special issue 2023, p. 19, p. 27.

13 General Data Protection Regulation (GDPR) 2016/679 of 27 April 2016, OJ 2016 L 119 of 4 May 2016, https://gdpr-info.eu.

14 For a general assessment see Omri Ben-Shahar/Carl E. Schneider, More Than You Wanted to Know: The Failure of Mandated Disclosure, Princeton 2014.

15 Weber (n. 11), p. 75 and p. 77.

16 See below chapter 2.3.

17 Weber (n 11), p. 78.

with the sophisticated».[18] Therefore, a potential way to assist individuals in making better decisions would rather be to direct choices through smart incentives without mandating a certain outcome.[19]

2.3. Information Overload

[11] The transparency principle is also confronted with the issue of information overload. Looking from a societal perspective, too detailed information requirements could have two negative effects:[20]

- The sheer volume and intensity of information leads to a confusion effect since the recipients are not anymore able to cope with all information details and loose the necessary overview in respect of the disclosed data.
- The permanent delivery of (similar) information causes a Kassandra effect; even if the recipients take note of the information, its contents is no longer seen as being serious and reliable.

[12] The general wisdom that overconsumption of information can have negative effects or even be risky also applies in respect of detailed disclosure requirements:[21] (i) Over-information consumes working and leisure time on both sides of an informational relationship. (ii) Attention is a scarce resource; a person cannot dispose of this resource in an unlimited way. (iii) Over-information increases the risk that messages or data being spread out are considered to be redundant.

[13] Therefore, excessive information provisions are an unsuitable attempt for the realization of an appropriate transparency concept. Moreover, an informative outcome should be achieved on the side of the addressees. But the balancing of interests remains difficult: Incomplete disclosure leaves people ignorant, but complete disclosure creates crushing overload problems;[22] as a consequence, a regulator should recognize that «less is more» even if it cannot be excluded that «less is not enough».[23]

2.4. Opacity

[14] The digitalization of processes and the use of algorithms by digital platforms being large scale technical systems cause manifold severe challenges for assessing their inner workings and social effects.[24] Platforms are marked by opacity and complexity. Opacity is an obvious con-

18 Omri Ben-Shahar/Carl E. Schneider, The Failure of Mandated Disclosure, University of Pennsylvania Law Review 159 (2011), p. 647, p. 748.

19 Weber (n. 9), p. 68; for more details see Richard H. Thaler/Cass R. Sunstein, Nudge: Improving Decisions about Health, Wealth and Happiness, New Haven 2008.

20 Weber (n 11), pp. 79–80.

21 Niklas Luhmann, Die Gesellschaft der Gesellschaft, Frankfurt 1997, p. 1090, p. 1097, pp. 1102 et seq.

22 For more details see Weber (n 11), pp. 79–80.

23 Ben-Shahar/Schneider (n. 18), p. 647.

24 Rieder/Hofmann (n. 5), pp. 6–7.

cern that may stem from secrecy practice, lack of expertise in reading code, and the increasing «mismatch between mathematical optimization in high-dimensionality characteristics of machine learning and the demands of human-scale reasoning».[25] The applicable techniques usually develop decision models inductively and make learn programs from data.

[15] Since many variables come into play, the developed algorithms are not easily «legible», in the same way as more tangible regulatory objects.[26] Consequently, transparency in the sense of reconstructing the procedure of algorithmic decision-making often does not lead to an informative outcome. Even if regulators were given access to data centers and source code, the process of sense-making would not be straightforward in view of complex code designs and involved machine learning.[27] In addition, the existence of different programming languages and execution environments adds further complications.[28]

[16] In a nutshell, analyses on the properties of algorithms and algorithmic systems arrive at the conclusion that the regulatory proposals looking at transparency as solution for platform challenges reflect an insufficient understanding of platform architectures.[29]

2.5. Fragmentation

[17] Furthermore, on the infrastructural side, during the last years the fragmentation of the Internet generally increased due to more extended national security laws protecting sovereignty interests of authoritarian countries.[30] Thereby, cross-border data traffic is becoming more difficult or even impossible, to the detriment of civil society in general and consumers in particular. Geolocation provisions can add a further layer of complexity.

[18] But private enterprises as providers of digital platforms could also have an interest to jeopardize interoperability in order to lock customers / users into the own infrastructure. As an example, lock-in provisions do have a negative impact on the competitive environment.[31] Such kinds of fragmentation could only be overcome by the development of harmonized standards which are imposed on private businesses.

---

25 Jenna Burrell, How the machine «thinks»: Understanding opacity in machine learning algorithms, Big Data & Society 3 (2016), pp. 1–2, https://doi.org/10.1177/2053951715622512.

26 Ansgar Koene/Chris Clifton/ Yohko Hatada/Helena Webb/Rashida Richardson, A governance framework for algorithmic accountability and transparency, European Parliamentary Research Service Study, April 2019, pp. 31–32, https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624262_EN.pdf.

27 Rieder/Hofmann (n. 5), p. 7.

28 Paul Dourish, Algorithms and their others: Algorithmic culture in context, Big Data & Society 3 (2016), p. 1. p. 4, https://doi.org/10.1177/2053951716665128.

29 Rieder/Hofmann (n. 5), p. 9.

30 Generally to the fragmentation issue see Rolf H. Weber, Internet Governance at the Point of No Return, Zürich 2021, pp. 87–89, https://eizpublishing.ch/publikationen/internet-governance-at-the-point-of-no-return/.

31 See Roxana Radu, Negotiating Internet Governance, Oxford 2019, p. 164, p. 167, p. 190.

3. Extensions to New Horizons

[19] Transparency has a long tradition as a «light form» of regulation.[32] The assumption, however, that transparency is able to reveal the truth by reflecting the internal reality of an organization is not fully reflected in reality. As outlined, research on transparency has shown that this principle does more and different things than shedding light on what is hidden. The visibility of an entity and its procedures is not simply a disclosure of pre-existing facts, but a process that implies its own perspective; a potential superficial understanding of transparency in the context of platform regulation risks producing inefficient results.[33]

[20] Therefore, transparency should not be regarded as a state or a «theme» but as the practice of deciding what to make present (i.e. public and transparent) and what to keep confidential.[34] Creating visibility and insights is a specific process which involves choices about what specifically should be exposed and how, what is relevant and what can be neglected, which elements should be shown to whom and how the visible aspects could be interpreted.[35] Potential elements being able to design such a process are accountability, auditability, observability and content moderation.

3.1. Accountability

[21] Accountability encompasses the obligation of one person or legal entity to give account of, explain and justify the undertaken actions or decisions to another person in an appropriate way.[36] Accountability is a pervasive concept, including political, legal, philosophical, and other aspects, each of them casting a different shade on the meaning of the terms. Together with checks and balances, accountability constitutes a prerequisite for legitimacy and a key element of any governance framework that implements a meaningful oversight.

[22] As a fundamental principle, accountability concerns itself with power and power implies responsibility. Therefore, accountability can be framed among three elements,[37] namely (i) the provision of information in a timely manner, (ii) the introduction of standards that hold governing bodies accountable, and (iii) the implementation of mechanisms of sanction. In addition, accountability as a mediated process needs to include the democracy element of global governance if the outcome of the decision-making processes should be acceptable to civil society in general.[38]

[23] Regulatory approaches seeking to create accountability in the digital platform context tackle the relevant issues by «opening the black box» of algorithmic decision-making.[39] However, plat-

32 See also Amitai Etzioni, Is Transparency the Best Disinfectant?, The Journal of Political Philosophy 18 (2010), p. 389, https://doi.org/10.1111/j.1467-9760.2010.00366.

33 See also Council of Europe (n. 1), pp. 42–44 and Jonathan J. Obar, Sunlight alone is not a disinfectant: Consent and the futility of opening Big Data black boxes, Big Data & Society 7 (2015), p. 1, https://doi.org.

34 Rieder/Hofmann (n. 5), p. 5.

35 Weber (n. 9), p. 70.

36 Weber (n. 3), p. 133.

37 Weber (n. 30), p. 70.

38 Rieder/Hofmann (n. 5), p. 6.

39 The black box problem is fundamentally described by Frank Pasquale, The Black Box Society. The Secret Algorithms That Control Money and Information, Cambridge MA 2015.

form accountability should extend beyond oversight of algorithms and platform conduct. In addition, platform behavior cannot be reduced to platform conduct since the socio-technical ordering makes platforms particularly powerful.[40] The tight integration of data collection and targeted «intervention» in form of «surveillance capitalism» (Zuboff)[41] has produced a market form that is unimageable outside the digital *milieu*. As a consequence, the rising power of platforms makes it necessary to assess what kind of accountability must be applied in order to understand the processes and their consequences in more detail.[42]

3.2. Auditability

[24] An improvement of transparency can also be achieved by extended auditability or explainability requirements if the respective provisions overcome an insufficient understanding of algorithms and platform architectures.[43] In order to reach the (theoretical) transparency objective, it would be necessary to develop an institutionalized mechanism for the verification of platform information or platform data. Such attempts in the context of platformization have already been undertaken during the last few years.[44]

[25] Several aspects need to be considered in the implementation of auditability principles:[45] (i) The creation of an intermediary (public or private sector entity) that audits data provided by large online platforms can ensure the accuracy of data. (ii) By bundling the auditing process through centralized auditing intermediaries, the exposure of sensitive private data to as few actors as possible is limited. (iii) By distancing the audit process from the regulator that is asking for data ensures that regulatory action does not overstep its bounds. (iv) By limiting the number of points through which the online platforms need to interact with outside intermediaries lowers potential security risks that could arise from providing access to a wide variety of systems. (v) Having numerous regulators involved in auditing is likely to create unnecessary and redundant processes. (vi) Organizing auditing of transparency data through an external auditing intermediary ensures that even regulators without the capacity to organize audits themselves still may have access to such a system through auditing intermediaries.

[26] The most important question about an auditing intermediary concerns the decision of whether such an intermediary would be public, private or somewhere in between.[46] Such an institution could be created within the context of the recently adopted EU Digital Services Act (DSA).[47] A further challenge raised by the proposal of auditing intermediaries is how much access

40 Rieder/Hofmann (n. 5), p. 2.

41 Shoshanna Zuboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power, New York 2019, p. 15.

42 To the autonomy and power elements in the accountability context see also Weber (n. 30), p. 71.

43 See also Ananny/Crawford (n. 4), p. 975; Jef Ausloos/Paddy Leerssen/Pim ten Thije, Operationalizing Research Access in Platform Governance, Algorithm Watch, Report, June 2020, pp. 18–20, https://www.ivir.nl/publicaties/download/GoverningPlatforms_IViR_study_June2020-AlgorithmWatch-2020-06-24.pdf.

44 See Ben Wagner/Lubos Kuklis, Establishing Auditing Intermediaries to Verify Platform Data, in: M. Moore/D. Tambini (eds.), Regulating Big Tech, Oxford 2021, pp. 169 et seq.

45 Wagner/Kuklis (n. 44), pp.172–173.

46 Wagner/Kuklis (n. 44), p. 174.

47 Digital Services Act (DSA), Regulation 2022/2065 of 19 October 2022 on a Single Market for Digital Services, OJ 277 L 1 of 27 October 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022R2065.

to data these intermediaries would actually need. In particular, it must be avoided that auditing intermediaries are misused by authoritarian countries for strategic national interests.[48]

3.3. Observability

[27] A further approach proposes to realize a concept of observability as a pragmatic way of thinking about the means and strategies necessary to hold platforms accountable.[49] Unlike transparency being normally described as a state that may exist or not, observability emphases the conditions for the practice of observing in a given domain.[50] While observability incorporates similar regulatory goals as transparency, it also partly deviates, most importantly by understanding accountability as a complex, dynamic «social relation».[51] Observability should be a mechanism that can overcome the lack of sensitivity for fundamental power imbalances, strategic occlusions, and false binaries between secrecy and openness. Insofar, observability could create a meaningful understanding that serves as an effective check on platform power.[52]

[28] The challenges raised by platforms as regulatory structures need to be addressed more broadly, beginning with the question of how large-scale, transnational environments that heavily rely on technology as a mode of governance can be assessed.[53] The concept of observability seeks to develop concrete actions in respect of (i) how people need to be treated on large online platforms, (ii) how connections between participants are made and structured, and (iii) which outcomes should be achievable.[54] Some concrete strategies may come out of self-regulation efforts; however, a co-regulatory framework appears to be appropriate for the realization of effective and robust observability principles.

[29] In the academic literature, the concept of observability starts with the recognition of a growing information asymmetry between platform companies, a few data brokers and everyone else. The resulting data monopoly deprives society of a crucial resource for producing knowledge about itself.[55] The deep political and social repercussions reflect the need to implement broader forms of social accountability. The concept of observability could be based on public interest as a normative horizon for assessing and regulating the societal challenges of platformization.[56] In the context of the public sphere, public interest encompasses the protection of human rights such as the freedom of expression and the freedom of information, fostering cultural and political diversity throughout the whole society.[57]

---

48 Wagner/Kuklis (n. 44), pp.174–175.

49 For further details to the observability concept see Rieder/Hofmann (n. 5), pp. 9–18; Vincent August/Fran Osrecki, Transparency Imperatives: Results and Frontiers of Social Science Research, in: V. Augustin/F. Osrecki (Eds.), Der Transparenz-Imperativ: Normen – Praktiken – Strukturen, Wiesbaden 2019, pp. 1–34, https://link.springer.com/chapter/10.1007/978-3-658-22294-9_1.

50 Rieder/Hofmann (n. 5), p. 3.

51 See Mark Bovens, Analysing and Assessing Accountability: A Conceptual Framework, European Law Journal 13 (2007), p. 447, p. 450, https://doi.org/10.1111/j.1468-0386.2007.00378.

52 This approach has been developed in detail by Rieder/Hofmann (n. 5), p. 6.

53 Rieder/Hofmann (n. 5), pp. 9–10.

54 See also José van Dijck/Thomas Poell/Martin de Waal, The Values in a Connective World, Oxford 2018, p. 158.

55 Rieder/Hofmann (n. 5), p. 11.

56 Rieder/Hofmann (n. 5), p. 12.

57 José van Dijck, Governing digital societies: Private platforms, public values, Computer Law & Security Review 36 (2020), 1, 3, https://doi.org/10.1016/j.clsr.2019.105377.

[30] Furthermore, the principle of observability reflects the acknowledgment that the volatility of platforms requires continuous observation. If terms of service contracts would be made available as machine-readable documents, the ongoing observation and interpretation of platform activities could be facilitated.[58] Another factor concerns the availability of interfaces that provide continuous access to relevant data. Thereby, questions of how data and analytical capacities are made available, to whom, and for what purpose need to be tackled.[59]

[31] Observability requires a critical audience. But the capacity for critique must be broader than «only» a critical attitude. Moreover, frameworks for data access should be linked to a cultivation of a robust civil society. Therefore, observability as a social relation makes scrutiny of realized transparency by a specific forum necessary.[60]

[32] Regulating digital platforms with the objective of increasing observability does mean working towards structured information interfaces between platforms and society. Such kind of regulation requires engaging with the specific properties of algorithmic systems and the co-produced nature of platform behavior.[61] The complex interactions between technical design, terms of service, and often large numbers of both users and «items/issues» have the consequence that the processes on large-scale platforms are conceptually insufficient.[62] Therefore, only a broadly understood concept of public interest as a normative benchmark could reasonably regulate platform behavior and realize targeted transparency.

3.4. Content Moderation

[33] Content moderation is an important element in the context of the communications- and society-oriented platforms. In the social environment, the uncertain or complex character of algorithms on the one side and the enormous generative and performative power of algorithmic systems on the other, require the realization of concepts, strategies and concrete tools that help to comprehend their logics and to establish effective political oversight.[63]

[34] Platforms steering the algorithms are silently interfering into the informational flows, governing data production, organizing platforms' news feeds, and pushing advertisements. Thereby, users are exposed to specific types of harmful content, political ads and propaganda, misinformation and disinformation. As a consequence, users' safety and the well-functioning of democracies are impacted; in addition, the platform-orientation towards fundamental rights is undermined.[64]

---

58 Rieder/Hofmann (n. 5), pp. 13–14.

59 van Dijck (n. 57), p. 3.

60 See also Bovens (n. 51), p. 450.

61 Rieder/Hofmann (n. 5), p. 13 and p. 22.

62 For a more detailed analysis see Philip M. Napoli, Social media and the public interest: Governance of new platforms in the realm of individual and algorithmic gatekeepers, Telecommunications Policy 39 (2015), pp. 751 et seq., https://doi.org/10.1016/j.telpol.2014.12.003.

63 See Urs Saxer, Von den Medien zu den Plattformen, Tübingen 2023, pp. 21 et seq.;
Nicolas P. Suzor/Sara Myers West/Andrew Quodling/Jillian York, What Do We Mean When We Talk About Transparency? Toward Meaningful Transparency in Commercial Content Moderation, Int'l J. of Communication 13 (2019), pp. 1526–1543.

64 For a general overview see Luca Belli/Yasmin Curzi/Clara Almeida/Natália Couto/Roxana Radu/Rolf H. Weber/Ian Brown, Towards Meaningful and Interoperable Transparency for Digital Platforms, UN IGF 2022, pp. 3 et seq., https://www.intgovforum.org/en/filedepot_download/57/23886; see also Saxer (n. 63). pp. 9 et seq., pp. 125 et seq., pp. 129 et seq.

Platform practices can also endanger freedom of expression due to a lack of transparency;[65] this is the case if social media platforms are compelled to share API's or «middleware» acting as common content-curation services ascribing users control over the information they see on various platforms.[66]

[35] Therefore, the debate on platform regulation needs to be reflexive with regard to the specific materiality of the regulatory field and the constitutive effect implied by it. Such reflexivity must be expressed in a procedural framework that encompasses the whole variety of concerned stakeholders.[67] The development of rules for appropriate content moderation should be influenced not only by the platform providers but also by members of civil society being the affected individuals; the framework needs to have a co-regulatory design.

[36] A particular problem occurs if platforms are in a position to assume a quasi-judicial power or even a quasi-legislative power.[68] Such development is particularly problematic if the rules (for example in respect of take-downs as in case of Meta) are set by private enterprises. In order to hinder such kind of appearances, decision-making processes based on guaranteed fundamental rights and democracy principles need to be conducted by way of establishment of moderation policies and rules that avoid unjustified actions against users' content or account interests and that provide for remedies in case of illegitimate interventions into the social network environment.[69] Standardization by way of self-regulation or co-regulation is a viable tool, but the respective regulations must be developed by extending the discussions to all interested stakeholders including members of civil society.[70]

3.5. New Legal Approaches

[37] In the past, legislators have more often released rules governing business-oriented platforms than communications- and society-oriented platforms. In the context of digital services, some rules exist in respect of flagging content or taking it down, as a combination of manual reviews and artificial intelligence tools, even if it cannot be overlooked that the mechanisms often remain opaque to the users.

---

65 See Luca Belli, Structural Power as a Critical Element of Digital Platforms' Private Sovereignty, in: E. Celeste/A. Heldt/C. Iglesias Keller (eds.), Constitutionalising Social Media, New York/Dublin 2022, pp. 81–100; Blayne Haggart/Clara Iglesias Keller, Democratic legitimacy in global platform governance, Telecommunications Policy 45 (2021), pp. 1 et seq., https://doi.org/10.1016/j.telpol.2021.102152; Tarleton Gillespie, Custodians of the Internet, New Haven 2019.

66 Belli et al. (n. 64), p. 5.

67 For more details to the multistakeholder approach see Weber (n. 30), pp. 44–60.

68 Belli et al. (n. 64), p. 3; see also Jean-Marie Chenou/Roxana Radu, The «Right to be Forgotten»: Negotiating Public and Private Ordering in the European Union, Business & Society 58 (2019), pp. 74–102, https://doi.org.

69 See also Giovanni De Gregorio/Roxana Radu, Digital constitutionalism in the new era of Internet governance, Int. J. of Law and Information Technology 30 (2022), pp. 68 et seq., https://doi.org/10.1093/ijlit/eaac004.

70 For further details to the notions of «self-regulation» and «co-regulation» see Rolf H. Weber, in: L. Belli/N. Zingales/Y. Curzi (eds.), Glossary of Platform Law and Policy Terms, IGF Katowice, December 2021, pp. 83–84, pp. 291–293, https://www.intgovforum.org/en/filedepot_download/45/20436.

3.5.1. Regional and National Governmental Regulations

[38] In the European Union the objective of the Digital Services Act (DSA) is to contribute to the proper functioning of the internal market for intermediary services by setting out harmonized rules for a safe, predictable and trusted online environment (Art. 1 DSA).[71] Specific information requirements are to be observed in connection with the terms and conditions for business transactions on digital platforms (Art. 14 DSA). The respective data shall include information on any policies, procedures, measures and tools used for the purpose of content moderation, including algorithmic decision-making software. The information shall be set out in clear, plain, intelligible, user-friendly and unambiguous language, and shall be publicly available in an easily accessible and machine-readable format.

[39] The Regulation on Platform-to-Business Relations (P2B)[72] of 2019, in force since July 2020, introduces significant constraints to the contractual freedom of relevant online intermediaries, such as online platforms and search engines. Service providers need to ensure compliance in several areas, for example regarding information duties and contract terms. In particular, the applicable data access policies must be described.

[40] In Japan, the Act on Improving Transparency and Fairness of Digital Platforms (TFDPA)[73] is aiming to improve the transparency and fairness of digital platforms; the TFDPA provides for requirements of digital platform providers to disclose terms and conditions and other information to platform users, intends to secure fairness in operating digital platforms and obliges the providers to submit a yearly report on the current situation of business operation based on self-assessments. The philosophy relies on voluntary and proactive initiatives by digital platform providers, with government involvement or other regulations; thereby, digital platform providers should be able to adequately exercise their originality and ingenuity. The TFDPA contains notification obligations in respect of contract terms and conditions as well as prior notification of contract amendments. Administrative measures consist in recommendations and public announcements if a notification is not complied with.

[41] In other countries, more general laws include some provisions having an impact on digital platform transparency. For example, the Indian IT Act and the Chinese algorithmic regulations aim at dissecting potential complexities, particularly in respect of the effects on freedom of expression, privacy, and other human rights.

[42] The existing regional and national governmental regulations appear to underestimate certain aspects being important for the normative environment of digital platforms:

- Forward-looking lawmakers should recognize that often «less is more» and «quality is more important than quantity»;[74] thereby, an optimization of transparency can more likely be achieved.
- Regulations should include complaints-handling and mediation procedures, as for example foreseen in Articles 20 and 21 of the EU DSA.[75]

---

71 See above n. 47.

72 Regulation 2019/1150 of 20 June 2019, OJ 186 L 57.

73 Act on Improving Transparency and Fairness of Digital Platforms, 27 May 2020, https://www.meti.go.jp/english/policy/mono_info_service/information_economy/digital_platforms/index.html.

74 See above chapter 2.3.

75 Art. 20 and 21 DSA (n. 47).

- The proactive screening of critical material is important, even if not frequently requested in legal acts.

[43] Nevertheless, the existing governmental regulations do not suffice; therefore, soft law instruments need to be considered.

3.5.2. Soft Law Instruments

[44] Apart from governmental regulations, self-regulatory or co-regulatory mechanisms should also be considered. Soft law is playing an increasingly important role in the digitized world.[76] Soft law has the advantage of being usually developed in a multistakeholder environment and of having a cross-border reach without restrictions of national boundaries.[77]

[45] As an example, the UN IGF Coalition on Platform Responsibility has presented a «Model Framework for Meaningful and Interoperable Transparency for Digital Platforms» at the occasion of the Internet Governance Forum in December 2022.[78] Relevant aspects would be to make sure that quantitative data can be assessed from a qualitative perspective; therefore, digital platforms should make available data sets including qualitative information on (i) which content was reported, (ii) which measures were taken by the platform, (iii) which procedures were adopted (maintenance, removal, depriorization, etc.), (iv) to what extent due process requirements were applied and (v) what the consequence of user appeal has been.

[46] The «Model Framework» proposes standardized and shared rules:[79] From a substantive perspective, platforms should share detailed and intelligible information on (i) their content moderation rules, (ii) the functioning of automated algorithmic moderation systems, and (iii) due process procedures. From a methodological perspective, platforms should (i) collectively standardize the information provision, (ii) make data continuously available in an interoperable, understandable and machine-readable format as audited by third parties, (iii) publish their initiatives regarding the identification and prevention of biases in their algorithms and the content moderation procedures and (iv) support an adequate and interoperable content moderation.

[47] In addition, the implementation of complaints-handling processes is imperative. An independent body of experts must be established being capable of assessing the different potential kinds of complaints raised by the concerned persons.[80] Only if a reliable and trustfulness complaints-handling is available and is seriously acting in practice, market players are incentivized to comply with the regulatory framework.

4. Outlook

[48] The ongoing discussions about transparency on digital platforms show that at first instance major emphasis should be put on the quality of information and not on the extension of the

76 For more details see Rolf H. Weber, Sectoral Self-Regulation as Viable Tool, in: K. Mathis/A. Tor (eds.), Law and Economics of Regulation, Cham 2021, p. 25, pp. 26–27.

77 See Weber (n. 76), pp. 27–28 with further references; Council of Europe (n. 1), pp. 39–40.

78 Belli et al. (n. 64), p. 7.

79 Belli et al. (n. 64), p. 7.

80 See text to n. 75 above.

quantity of information, as partly done in national regulations. Only a meaningful understanding of transparency can serve as an effective check on platform power. Not more information is needed, but a better structured disclosure of data becomes imperative.[81] Therefore, a broader concept of public interest as a normative benchmark for assessing platform behavior is needed.[82]

[49] A three-dimensional concept of transparency merits to be implemented: The first dimension should refer to institutional aspects, i.e. procedures and decision-making. The second dimension of transparency could constitute the substantive backbone of the regulations. The third dimension is the accountability of actors for rebuilding confidence in the market system.[83] Thereby, meaningful transparency means that platform providers undertake (i) to enable observability, including increased data accuracy, in respect of transparency measures and (ii) to create interoperable standards on transparency.[84]

[50] Furthermore, a concept of targeted transparency should be developed. Information contents must be designed in view of the potential addressees and lead to their improved empowerment:[85] (i) Individual users of the platforms should be informed about how (personal) information will be used and organized by the platform and how removal decisions of content are taken. (ii) Civil society or the general public needs information about the functioning and the algorithmic instruments of the digital platform. (iii) Regulatory bodies, public supervisors and other auditing bodies are to be informed about the implementation of protection measures and the compliance with existing regulations.

[51] The way to transparency on digital platforms might be long and cumbersome, however, improved transparency instruments would be available and it appears to be worthwhile to implement better behavioral rules in the interest of businesses and civil society.

Prof. Dr. Rolf H. Weber, Professor for International Business and Economic Law at the University of Zurich and Attorney-at-law in Zurich (Bratschi Ltd.). All Internet sources have last been checked on August 3, 2023.

81 See chapters 2.2 and 2.3 above.

82 Rieder/Hofmann (n. 5), p. 23.

83 For further details see Weber (n. 3), pp. 140–143 and p. 147.

84 Belli et al. (n. 64), p. 7.

85 Belli et al. (n. 64), p. 6.