

# Global Law in the Face of Datafication and Artificial Intelligence

*Rolf H. Weber*

## I INTRODUCTION

Law is regularly challenged by new societal developments. Therefore, its stabilizing function is at risk in the globalized world if technology moves fast and changes the bases of human interactions. Eventually, law is no longer able to provide support for the reorientation of civil society in the context of a potentially highly dynamic environment. However, in a transnational legal system, such as the international trade regime, the evolution of expectations in world society must be channeled in order to avoid social differences that lead to disruptions.<sup>1</sup> Therefore, law cannot disregard technological developments.<sup>2</sup> This contribution examines challenges to the global legal framework caused by recent (primarily technological) developments. At the outset, the characteristics of the law as a structural system are outlined. Thereafter, potentially changing factors, such as technology-driven datafication (big data, cloud computing) and artificial intelligence (AI), will be briefly addressed. Based on this foundation, the main component of this contribution analyzes a desirable digital governance and the regulatory principles of a data-driven world with regard to the establishment of global legal standards in the international trade context.

## II LEGAL FRAMEWORK AND TECHNOLOGICAL ADVANCES

### *A Law as a Structural System*

Law as a structural system gives guidance about desired behavior, thereby stabilizing normative expectations.<sup>3</sup> In principle, legal concepts can help to support

<sup>1</sup> S-Y Peng, "The Rule of Law in Times of Technological Uncertainty: Is International Economic Law Ready for Emerging Supervisory Trends?" (2019) 22 *Journal of International Economic Law* 1, at 13.

<sup>2</sup> This assessment is not new; twenty years ago, Lawrence Lessig had already pointed to the importance of technical architecture. L. Lessig, *Code and Other Laws of Cyberspace* (New York, Basic Books, 1999).

<sup>3</sup> RH Weber, *Realizing a New Global Cyberspace Framework, Normative Foundations and Guiding Principles* (Zürich, Schulthess Juristische Medien, 2014), at 33.

adequate normative reasoning, since the addressees of legal provisions are supposed to acknowledge the authority of the rule-making body and comply with the law.<sup>4</sup> The functions of law are crystallized in rules and institutions that underpin civil society, facilitate orderly interactions, and resolve disputes and conflicts that arise in spite of such rules.<sup>5</sup> The normative framework allows people and businesses in a community to determine the limits of what can and cannot be done in the collective interest.<sup>6</sup> Therefore, the rule of law helps to achieve a high, discretion-limiting degree of certainty and predictability in social relations and transactions.<sup>7</sup>

Irrespective of the manner in which norms actually influence behavior, law-making bodies must understand the different processes that facilitate legal developments, insofar as law often proves to be path-dependent.<sup>8</sup> This assessment corresponds to the reality that the legal system is linked to other social systems, such as technological advances or ethical relations; that is, law only enjoys relative autonomy and is confronted with technological uncertainty.<sup>9</sup> The structural coupling that occurs between and among the legal system and other systems requires the implementation of mechanisms that allow a change of law called for because of societal needs and circumstances.<sup>10</sup> Only when such mechanisms are institutionalized can the continuous existence of the legal system be secured over time.<sup>11</sup> In other words, even if the law requires predictability and a stable structure, the adaptability of legal rules keeps the law intact in cases of social variation.<sup>12</sup>

Nevertheless, some substantive legal values are so fundamental that their abolition would totally undermine the function of law in society. On the one hand, human rights, such as the freedom of expression or the nondiscrimination principle, represent major (even untouchable) constitutional values. On the other hand, legal order can hardly function without property rights and privacy rights.<sup>13</sup> As a consequence, certain legal pillars may not be “overruled” by technological developments.

These pillars of law as a structural system must be mirrored against the challenges caused by recent technological advances in order to avoid “clashes” that may harm civil society.

<sup>4</sup> Weber, note 3 above, at 34 with further references.

<sup>5</sup> RH Weber, “The Role of Law in Constituting Financial Markets” (2017) 32 *Journal of International Banking Law and Regulation* 253, et seq.

<sup>6</sup> HLA Hart, *The Concept of Law* (2nd ed., Oxford, Oxford University Press, 1997), at 55–57.

<sup>7</sup> RH Weber, *Regulatory Models for the Online World* (Zürich, Kluwer Law International, 2002), at 38.

<sup>8</sup> Weber, note 5 above, at 254.

<sup>9</sup> Weber, note 3 above, at 35; Peng, note 1 above, at 12.

<sup>10</sup> N Luhmann, *Das Recht der Gesellschaft* (Frankfurt, Suhrkamp, 1993), at 93, 283, 441.

<sup>11</sup> Weber, note 5 above, at 254.

<sup>12</sup> Weber, note 3 above, at 34–35.

<sup>13</sup> See also OECD, “Algorithms and Collusion: Background Note by the Secretariat” (2017), <https://perma.cc/5R7T-8JTB>, at 43.

## B Datafication as a Technological Trend

The term “datafication” was coined by Mayer-Schönberger and Cukier in 2013, primarily with respect to the then-new phenomenon of big data.<sup>14</sup> Datafication, which has become a buzzword in the new IT world, refers to a technological trend that is able to “convert” many aspects of modern life into computerized data.<sup>15</sup> Hereinafter, not only are big data and cloud computing addressed but also new developments in the AI context.

### 1 Big Data and Cloud Computing

Over the past few decades, an immense amount of data has been generated through the (cross-border) flow of information, humans, products, services, and capital. These developments have resulted in data protection concerns, as well as the specific problem of users of online goods and services “paying” for products offered by disclosing data without assessing the nature and value of the data. The recent European Union (EU) Directive on digital content even regulates the payment of online services through the provision of data.<sup>16</sup> Furthermore, data holders are often unaware of how much data is collected and stored about them.

Big data is a term coined for datasets whose size is beyond the ability of commonly used software tools to capture, curate, manage, and process within a tolerable degree of time. The phenomenon of big data analytics is often characterized by four elements, namely volume, variety, velocity, and veracity (the “4 V”). “Volume” refers to the especially large amount of data; “variety” makes it clear that the data is derived from manifold sources and formats; “velocity” mirrors the high speed of the data processing; and “veracity” reflects the reliance on the correctness of the data. A special feature of big data from a legal perspective is the fact that the traditional concept of causation is replaced by the concept of correlation.<sup>17</sup>

For some years, international organizations such as the Organisation for Economic Co-operation and Development (OECD), as well as academic voices, have assumed that big data is potentially a key driver of innovation, productivity growth, and economic competitiveness.<sup>18</sup> The global exchange of data requires unrestricted cross-border data flows in order to realize its merits. In this context, big data analytics is able to improve the outcome of data processing in manifold

<sup>14</sup> V Mayer-Schönberger and K Cukier, *Big Data: A Revolution That Will Transform How We Live, Work and Think* (London, John Murray, 2013), at 73 et seq.

<sup>15</sup> RH Weber, “Digitalisierung und der Kampf ums Recht,” in A Dal Molin-Kränzlin et al. (eds), *Digitalisierung – Gesellschaft – Recht, Analysen und Perspektiven von Assistierenden des Rechtswissenschaftlichen Instituts der Universität Zürich* (Zürich/St. Gallen, Dike, 2019), 3, at 6.

<sup>16</sup> Directive (EU) 2019/770 on certain aspects concerning contracts for the supply of digital content and digital services of 20 May 2019, OJ 2019 L 136 of 22 May 2019, 1 et seq.

<sup>17</sup> Mayer-Schönberger and Cukier, note 14 above, at 50 et seq.

<sup>18</sup> See also RH Weber, “Data Portability and Big Data Analytics, New Competition Policy Challenges,” in *Concorrenza e Mercato* 23/2016, 59, at 61/62.

areas.<sup>19</sup> Examples include the automotive industry, which evaluates ideas submitted through its “virtual innovation agency,” and the health sector, which collects data on larger populations in order to reduce disease, bringing rapidly and accurately identified drugs to the market and providing better healthcare by enabling the application of evidence-based interventions.<sup>20</sup>

A further technical innovation is cloud computing, which facilitates cross-border data flows in order to take advantage of cheaper on-demand computer capacity that can be scaled and paid for as needed. Cloud services encompass software and access to processing, email, storage, and other computer resources. From a business perspective, cloud computing turns a fixed IT cost into a variable operating cost, and from the angle of human resources, cloud computing underpins the capacity of people to work remotely.<sup>21</sup> Major challenges include connectivity and the compliance of cross-border data flows with data protection and data security requirements.<sup>22</sup>

## 2 Artificial Intelligence

Algorithms are able to automate the “production” of goods/services and to facilitate the selection and filtering of information in various ways, thereby attributing relevance to certain data and moderating content. Algorithms are the foundation of AI as a machine-based system that is capable of influencing the environment by making recommendations and predictions without human input.<sup>23</sup> An AI system lifecycle encompasses various phases, such as the design and modeling of data, the verification and validation of data, as well as the deployment, operation, monitoring and storage of data.<sup>24</sup>

AI allows for the implementation of a “regime” of automated decision-making to be conducted in a highly timely and effective manner. Such automation is primarily feasible in situations that do not require a specific human intervention. The new technologies can also transform traditional manufacturing into smart manufacturing, focusing on digitization from early product design through maintenance at the product’s end of life by using advanced sensors and big data analytics.<sup>25</sup> As examples, and only at the very beginning of data-driven innovation potential, the following phenomena can be identified: (i) driverless cars will

<sup>19</sup> Weber, note 3 above, at 6–7.

<sup>20</sup> J Meltzer, “Governing Digital Trade” (2019) 18 *World Trade Review* 23, at 31.

<sup>21</sup> *Ibid.*

<sup>22</sup> For an overview, see DN Staiger, *Data Protection Compliance in the Cloud* (Thesis, Zurich, 2017), at 268 et seq.

<sup>23</sup> RH Weber, “Socio-ethical Values and Legal Rules on Automated Platforms: The Quest for a Symbiotic Relationship” (2020) 36 *Computer Law & Security Review* 1 et seq.

<sup>24</sup> See also OECD, “Recommendation of the Council on Artificial Intelligence” (2019), <https://perma.cc/EW3K-FE6R>.

<sup>25</sup> Meltzer, note 20 above, at 29.

become a reality, and (ii) robotics will move forward to become a widespread industry tool based on rapidly advancing AI.

Notwithstanding the fact that AI has many benefits, some risks also cannot be overlooked. Therefore, from a normative concept of civil society, a few questions must be considered in an interdisciplinary manner:<sup>26</sup> (i) Do AI processes comply with fundamental constitutional principles? (ii) Is the AI application based on a sufficient legal foundation? (iii) Do AI processes comply with the applicable requirements of data protection laws? (iv) Who is in charge of monitoring the socially responsible use of AI, and who is liable in case of a failure caused by an algorithm?

These questions merit appropriate answers, even if solid responses that serve the needs of global society are not easy to find. Nevertheless, a reconciliation of AI's chances and risks must be kept in mind if an adequate legal framework for digital governance in global relations, particularly in the international trade regime, is to become a reality.

### III RECONCILING GLOBAL TRADE WITH GLOBAL LAW

#### *A Rule-Making in the Digital World*

##### 1 Globalization and Governance

Globalization is not a clearly defined term; its concrete meaning depends on the given substantive component of societal life.<sup>27</sup> (i) Legal globalization concerns the harmonization of states' normative orders, or the implementation of cross-border legal rules. (ii) Cultural globalization addresses those issues related to manifold social policies. (iii) Commercial globalization reflects the existence of increased transnational businesses and economic activities. Global law as an aspect of legal globalization is confronted with new concepts, examining institutional differentiations and elaborated procedural techniques.<sup>28</sup>

The term "governance," which stems from the Greek word "*kybernetes*" and the Latin word "*gubernator*," means a steersman, and it must be recognized for its importance. Governance can be addressed from the perspective of different disciplines; nevertheless, at whatever level of social organization it may take place, governance refers to the appropriate business conduct of a private or a public body. In this context, some key questions must be asked and answered:<sup>29</sup> (i) Who

<sup>26</sup> Weber, note 23 above, at 1.

<sup>27</sup> See JA Scholte, *Globalization: A Critical Introduction* (New York, St. Martin's Press, 2000); S Caney, *Justice Beyond Borders* (Oxford, Oxford University Press, 2005).

<sup>28</sup> B Kingsbury and L Casini, "Global Administrative Law Dimensions of International Organizations Law" (2009) 6 *International Organizations Law Review* 319 et seq.

<sup>29</sup> RH Weber, *Shaping Internet Governance: Regulatory Challenges* (Zurich, Schulthess Juristische Medien, 2009), at 2.

is entitled to set the rules? (ii) In whose interest are the rules? (iii) By which mechanisms are the rules created? (iv) For which purposes are the rules designed? There is a need to develop overarching networks and negotiation systems between different stakeholders, thus forming a “cooperative approach to governance” that includes the entire society, hence dividing responsibilities between public and private actors.

Based on the described notions of “globalization” and “governance,” the development of a broader rule-making approach encompassing the needs of the international trade regime and of the digital environment of today’s societies appears to be unavoidable and equally justified.

## 2 A Broader and Better-Coordinated Rule-Making Approach

Assessing the dichotomy of regulatory sources and the emergence of new regimes introduced by civil society, adapted transnational concepts must be developed in the global law environment.<sup>30</sup> Institutions can lead states to more cooperative behavior than they otherwise might have adopted, building mutual connections from peripheral points in federative or associate forms.<sup>31</sup> In realizing an appropriate governance framework, civil society involvement should be strengthened. The facilitation of networking opportunities and public support from concerned persons and organizations in the relevant policy field should also be considered; that is, a policy vision must be developed.<sup>32</sup>

In the Internet governance context, a new approach has been developed and applied in part, namely the multistakeholder participation model, which attempts to involve all concerned persons and organizations in the public and private sphere in the discussions and negotiations of the regulatory framework.<sup>33</sup> Practical experience has shown that some basic challenges need to be addressed in order to ensure that the multistakeholder concepts are successful. Four fundamental questions must be tackled:<sup>34</sup> (i) How do governance groups best match challenges with organizations and networks? (ii) How can governing bodies/entities be most able to help develop legitimate, effective, and efficient solutions? (iii) How should the flow of information and knowledge necessary for successful governance be structured? (iv) How can different governance groups approach coordination between available governance networks in order to avoid conflicting interests?

<sup>30</sup> Weber, note 3 above, at 111.

<sup>31</sup> M Senn, *Non-State Regulatory Regimes, Understanding Institutional Transformation* (Heidelberg, Springer, 2011), at 215–216.

<sup>32</sup> RH Weber, “Visions of Political Power: Treaty Making and Multistakeholder Understanding,” in R Radu et al. (eds), *The Evolution of Global Internet Governance, Principles and Politics in the Making* (New York, Springer, 2014), 95, at 102 et seq.

<sup>33</sup> Weber, note 3 above, at 126 et seq.

<sup>34</sup> U Gasser et al., “Multistakeholder as Governance Groups: Observations from Case Studies” (2015) Berkman Center for Internet & Society Research Publications No. 2015-1.

Over the last few years, the globalization of the international legal framework, among other fields in international trade law (particularly due to the “outdated” classification regime in the World Trade Organization (WTO) Agreements), and equally in the area of Internet law (due to a stronger emphasis on state sovereignty), has suffered some setbacks. In light of the fact that the legal fragmentation caused by national laws jeopardizes an appropriate design of global law in a network society, coherence between different initiatives should be strengthened in order to overcome trends leading to various forms of fragmentation or distorted regulatory regimes.

The recently developed term “legal interoperability” addresses the process of creating legal rules that cooperate across jurisdictions.<sup>35</sup> This objective can be realized in a matter of degrees, as many options exist between a full harmonization of normative rules and a complete fragmentation of legal systems.<sup>36</sup> As is so often the case in the real world, striking the correct balance is of utmost importance. While an excessively high level of interoperability could cause difficulties in the management of the harmonized rules and fail to acknowledge social and cultural differences, a level too low could present challenges to smooth social interaction.<sup>37</sup>

### B *Regulatory Principles for the Data-Driven World*

In view of these technological innovations, the legal order is confronted with the need to establish an international regulatory framework for the data-driven world that implements the following basic regulatory principles.

#### 1 Transparency

All involved stakeholders should promote a culture of transparency, enshrining the disclosure of data logics and access to the applied algorithms and datasets.<sup>38</sup> Transparency is usually defined as “easily seen through ... evident, obvious, clear.”<sup>39</sup> Transparency means understandable and forward-looking information, appropriate to the context and the state of the art, in order to make stakeholders aware of their interactions (in an *ex ante* or *ex post* data-centered decision-making process).<sup>40</sup>

Transparency requires robust and general rules, not necessarily more regulation; that is, the improvement of transparency does not mean a quantitative increase in

<sup>35</sup> J Palfrey and U Gasser, *Interop: The Promise and Perils of Highly Interconnected Systems* (New York, Basic Books, 2012).

<sup>36</sup> RH Weber, “Legal Interoperability as a Tool for Combatting Fragmentation” (2014) Global Commission on Internet Governance Paper Series No. 4, at 6.

<sup>37</sup> *Ibid.*, at 7–9.

<sup>38</sup> Council of Europe, Report on Artificial Intelligence, T-PD(2018)09Rev, Strasbourg, 3 December 2018, at 11/12.

<sup>39</sup> Oxford English Dictionary Online, 1989.

<sup>40</sup> Weber, note 29 above, at 122/123.

information, but rather “more” in terms of higher information quality.<sup>41</sup> A future-oriented understanding of transparency should observe the following elements:<sup>42</sup> (a) the existence of publicly reliable information; that is, substantive quality standards related to information, supported by an adequate legal framework; (b) the designation of the information recipient as a holder of rights and an essential component for perception and transparency; and (c) the availability of disclosure procedures and observance of the time element; that is, transparency implies constant visibility of information.

Providing information about the type of input data and the expected output, explaining the variables and their weight, and shedding light on analytics architecture usually contribute to transparency with respect to AI algorithms.<sup>43</sup> Nevertheless, a generic statement on the use of AI does not allow for the easy assessment of all challenges and risks; concrete circumstances do play a role, which means that solutions focused on disclosing specific information about the applied algorithms may be the best option.<sup>44</sup>

## 2 Accountability

All stakeholders involved in datafication and AI mechanisms should be accountable for the proper functioning of the systems employed, as well as the integrity of the regulatory environment.<sup>45</sup> Accountability helps to ensure an environment in which individuals and enterprises assume their respective responsibilities. The first legislative attempts to meet this requirement can already be seen: for example, in the field of data protection, the EU General Data Protection Regulation calls upon organizations to apply a “Privacy by Design/Default” approach and – under certain circumstances – to conduct a “Data Protection Impact Assessment.”<sup>46</sup>

Accountability encompasses the obligation of one person to another, according to which the former must give an account of, explain, and justify his/her actions and decisions against criteria of the same kind.<sup>47</sup> Therefore, the proportionality principle, which inspires an adequate and appropriate deployment of big data analytics and AI, should apply.<sup>48</sup> Accountability also relates to good governance, which was previously addressed. The development of respective concepts in public institutions

<sup>41</sup> C Kaufmann and RH Weber, “Transparency of Central Banks’ Policy,” in P Conti-Brown and RN Lastra (eds), *Research Handbook on Central Banking* (Cheltenham, Edward Elgar Publishing, 2018), 518, at 520.

<sup>42</sup> Weber, note 29 above, at 121 et seq., 131.

<sup>43</sup> Council of Europe, note 38 above, at 12; for further details see Weber, note 23 above, at 6–7.

<sup>44</sup> See also OECD, note 24 above, at no. 1.3.

<sup>45</sup> Weber, note 3 above, at 78 et seq.

<sup>46</sup> The details are contained in article 25 and article 35 of the General Data Protection Regulation (GDPR).

<sup>47</sup> For further details see Weber, note 23 above, at 7.

<sup>48</sup> Weber, note 29 above, at 137 et seq. with further references.



and private enterprises requires publicly assessable accounts as a precondition for a sustainable society.<sup>49</sup>

The obligation to be accountable encompasses the task of disclosing information about the actual AI processes. To improve respective foreseeability, standards should be developed and introduced that moderate the behavioral requirements in a concise manner. Furthermore, the responsibility of the accountable person to ensure that concerned individuals are protected from damages when having suffered a detriment is to be legally developed in a precise way.<sup>50</sup>

### 3 Safety and Robustness

Technological innovations must be safe and robust throughout their entire lifecycle so that data-driven communications and transactions can overcome adverse conditions or foreseeable potential misuse. Safety and robustness also extend to the terms of security and resilience. Therefore, the traceability of the datasets, processes, and decisions must be secured. Furthermore, the risks with respect to safety and robustness should be managed throughout the entire process of hardware or software applications. Consequently, the execution of impact assessments with respect to technological risks is necessary.<sup>51</sup>

International instruments already state that the likely impact of AI on civil society must be adequately taken into account in order to safeguard fundamental rights. For example, the Recommendation of the OECD Council on Artificial Intelligence refers in part 1.4 to robustness, security, and safety as follows:<sup>52</sup>

AI systems should be robust, secure and safe throughout their entire lifecycle so that, in conditions of normal use, foreseeable use or misuse, or other adverse conditions, they function appropriately and do not pose unreasonable safety risk. To this end, AI actors should ensure traceability, including in relation to datasets, processes and decisions made during the AI system lifecycle, to enable analysis of the AI system's outcomes and responses to inquiry, appropriate to the context and consistent with the state of art.

Furthermore, the use of AI through modern data-processing techniques and the trend toward implementation of data-intensive processes require a more advanced understanding of risk assessment by individuals, businesses, and public organizations, since possible adverse outcomes stemming from data processes cannot be excluded.<sup>53</sup>

<sup>49</sup> See C Kaufmann and RH Weber, "The Role of Transparency in Financial Regulation" (2010) 13 *Journal of International Economic Law* 779, at 789.

<sup>50</sup> Weber, note 29 above, at 147.

<sup>51</sup> For a comprehensive discussion of new forms of impact assessments, see A Mantelero, "AI and Big Data: A Blueprint for Human Rights, Social and Ethical Impact Assessment" (2018) 34 *Computer Law & Security Review* 754 et seq.

<sup>52</sup> OECD, note 24 above, at no. 1.4; for further details see Weber, note 23 above, at 7–8.

<sup>53</sup> Council of Europe, note 38 above, at 13.

Risks and compliance assessments are not only justified by collective social and ethical values, as well as the nature of fundamental rights and treatments affected by AI application. They also represent an opportunity to better foster public trust as a key objective of the information society.<sup>54</sup>

#### 4 Interim Assessment

As stated earlier, the use of modern data-processing techniques and the trend toward implementation of information-intensive data analytics require a more advanced understanding of risk assessment. In particular, the fact that automated decision-making may have an impact on fundamental rights (including the nondiscrimination principle), as well as collective social and ethical values, must be addressed.<sup>55</sup> AI programs can affect various human rights, i.e. the right to human dignity, the principle of nondiscrimination, privacy rights, and the guarantee of self-determination.<sup>56</sup>

Furthermore, risks and compliance assessments are not only justified by the nature of the rights and freedoms potentially affected by datafication (or big data analytics), as well as AI applications. In a participatory environment such assessment can contribute to an increased level of trust.<sup>57</sup> As the most recent political developments in the political arena have shown, trust plays an important role in the context of the international trade regime. Trust can even be seen as a central pillar of the globalized governance, as previously discussed.

#### C Combatting Distortive Interferences

In the digital society and economy, the factual possession and control of data is key. New technologies, such as datafication and AI, lead to situations in which the data control function is primarily assumed by large private enterprises and by governments. The use of big data results and the application of algorithms give these entities information power,<sup>58</sup> which can be exercised in either a good or bad way. Improvement in healthcare or the strengthening of measures to protect cybersecurity undoubtedly have a positive effect. However, the misuse of data is also possible, for example with the objective of spreading inaccurate, embarrassing, or misleading information or controlling the data exchange for one's exclusive benefit, insofar as

<sup>54</sup> O'Neill, *Justice, Trust and Accountability* (Cambridge, Cambridge University Press, 2005).

<sup>55</sup> See also RH Weber, "Ethics in the Internet Environment" (2016) Global Commission on Internet Governance Paper Series No. 39, at 7.

<sup>56</sup> FA Raso et al., "Artificial Intelligence and Human Rights: Opportunities and Risks" (2018) Berkman Klein Center for Internet & Society at Harvard University Research Publication No. 2018-6, at 14 et seq.

<sup>57</sup> See O'Neill, note 54 above, at 61 et seq.

<sup>58</sup> On the phenomenon of information power, see D Kuehl, *Defining Information Power*, 1997 (June, No. 115) Strategic Forum, at 1 et seq. More recently, the initiatives introduced by political bodies and particularly by antitrust authorities against the US giants (GAFA: Alphabet (Google), Amazon, Facebook, and Apple) clearly show the sensitivity of the problem.

the holder of data can become a “data demagogue,”<sup>59</sup> contradicting the basic principles of an appropriate international trade regime.<sup>60</sup>

### 1 Anticompetitive Behavior

From the perspective of competition law, different issues are at stake. An initial aspect concerns the changed market parameters. Digital markets, as well as the exchange of communications in a digital society, should increase the possibilities for participation among all interested individuals and organizations/businesses. However, the markets tend to be dominated by a few firms (Alphabet (Google), Amazon, Facebook, and Apple (GAFA)). Similar experiences are found in East Asia (Alibaba, Tencent).

The overwhelming dominance of a few players in digital markets causes anticompetitive concerns, which are primarily due to the risk that a market-dominant position has been misused.<sup>61</sup> The oligopolistic market structure is now challenged by competition authorities (for example, the Directorate Competition of the EU), as well as political bodies in the United States and Europe. The outcome of these interventions is unresolved for the time being.

Other behavioral problems are also on the horizon – for example, the tacit collusion by big firms through the use of parallel algorithms.<sup>62</sup> For good reasons, primarily the OECD, as one of the most important international organizations in the economic field, is thoroughly analyzing the respective challenges.<sup>63</sup> So far, competition law does not appear to be fully fit to tackle these problems. The lack of general competition law principles in the WTO framework must be seen as another disadvantage for the international trade regime.<sup>64</sup> Furthermore, the lack of coherent competition policies among jurisdictions leads to the disadvantage that national competition authorities are ill equipped to effectively address the anticompetitive data practices; the need for more streamlined standards between antitrust regimes is obvious.

<sup>59</sup> RS Neeraj, “Trade Rules for Digital Economy: Charting New Waters at the WTO” (2019) 18 *World Trade Review* 121, at 129.

<sup>60</sup> This subchapter uses the title “distortive interference,” not “data demagogues,” in order to avoid any preliminary assessment, particularly because the remarks must remain relatively short.

<sup>61</sup> Neeraj, note 59 above, at 129.

<sup>62</sup> RH Weber, “Disruptive Technologies and Competition Law,” in K Mathis and A Tor (eds), *New Developments in Competition Law and Economics* (Cham, Springer International Publishing, 2019), 223, at 232 et seq.

<sup>63</sup> See for example OECD, “Algorithms and Collusion, Competition Policy in the Digital Age” (2017), <https://perma.cc/WZR9-7M4T>; OECD, “Rethinking Antitrust Tools for Multi-sided Platforms” (2018), <https://perma.cc/V7VD-7X2E>.

<sup>64</sup> RH Weber, “Unfinished Business: Competition Law and the WTO,” in J Chaisse and T-Y Lin (eds), *International Economic Law and Governance, Essays in Honour of Mitsuo Matsushita* (Oxford, Oxford University Press, 2016), at 201–215.

## 2 Denial of Network Neutrality

A second issue is network neutrality: all market participants (providers of goods and services, as well as consumers) should have unfettered access to the digital infrastructure.<sup>65</sup> The preferential treatment of some businesses or individuals results in the risk of competition distortion. Therefore, discrimination toward certain market participants must be considered unjustified.

In some countries (for example, in the EU), network neutrality provisions do exist.<sup>66</sup> The national implementation of the neutrality principle, however, does not always cover existing needs. In the United States, the trend has moved away from regulatory intervention because of the existing political climate. Obviously, rules cannot replace the market. However, illegitimate discrimination does have a substantial negative effect on the international trade framework.<sup>67</sup>

## 3 Data Localization

A third challenge, more due to efforts of governments than private enterprises, concerns data localization requirements. Around the globe, such requirements are implemented in a variety of forms.<sup>68</sup> Information and communications technology companies may be obligated to host all subscriber and consumer data locally within the country; in some instances, only information covering certain substantive areas (for example, health) must be stored in the country.

Data localization reduces access to data and digital technologies and may also be counterproductive. Requiring data localization in relation to cybersecurity increases data vulnerability in a single jurisdiction, making it easier to target and possibly preventing data backups in globally distributed data centers.<sup>69</sup> Obviously, such provisions raise the costs of access to, and use of, data, thereby reducing gains from digital trade.

## 4 Interim Assessment

As the aforementioned deliberations demonstrate, global law is exposed to “data demagogues” who strive to interfere with cross-border data flows. Various forms of

<sup>65</sup> Neeraj, note 59 above, at 138.

<sup>66</sup> See for example Article 3(3) of the Telecom Single Market Regulation (EU) 2015/2120; for further information on the EU regulations on network neutrality see <https://perma.cc/P7SF-CS4K>.

<sup>67</sup> A full review of the literature on network neutrality cannot be done in this chapter; for the EU see note 66; for the US, see T Wu, “Network Neutrality, Broadband Discrimination” (2003) 2 *Journal on Telecommunications and High Technology Law* 141 et seq.; more recently CS Yoo, “Wireless Network Neutrality: Technological Challenges and Policy Implications” (2017) 31/2 *Berkeley Technology Law Journal* 1409 et seq.

<sup>68</sup> Meltzer, note 20 above, at 25, 36; Neeraj, note 59 above, at 138–139; A Chander, “The Internet of Things: Both Goods and Services” (2019) 18 *World Trade Review* 14 et seq.

<sup>69</sup> Meltzer, note 20 above, at 25.

unjustified market interventions, such as anticompetitive behavior, denial of network neutrality, and data localization provisions, can have a competition distortion effect. Such an outcome must be avoided or, at the very least, mitigated by the regulator.

In addition, legal uncertainty, caused by technological advances, leads to discretionary power that is not always consistent with the rule of law.<sup>70</sup> This fact primarily concerns governments and other regulatory bodies. However, private enterprises can also have power in factual forms. A balance between differing interests is often difficult to find, but efforts to reconcile such interests appear to be unavoidable.<sup>71</sup>

## D *New Digital Trade Regime*

### 1 Outdated Goods and Service Classifications

So far, a commonly agreed-upon definition of what represents digital trade does not exist. The WTO has addressed the “production, distribution, marketing, sale, or delivery of goods and services by electronic means” as part of digital trade in its Work Programme on Electronic Commerce of 1998.<sup>72</sup> Cross-border data flows enabling digital trade have not played a major role in the previous discussions, notwithstanding the fact that their appearance is important.

Legal scholars of WTO law have been tackling the distinction between goods (General Agreement on Tariffs and Trade, GATT) and services (General Agreement on Trade in Services, GATS) for many years, since it is not clear which “product category” and consequently which Agreement would be suitable in addressing digital assets.<sup>73</sup> The differentiation is practically important, since the GATT offers less room for maneuvering to member states that are unwilling to liberalize digital markets than the GATS.<sup>74</sup>

The WTO itself is well aware of the existing problems, and efforts have been initiated to remedy the situation. In the context of the 11th Ministerial Conference (December 2017, Buenos Aires), a short “Joint Statement on Electronic Commerce” was adopted, inviting participating member states to undertake further work on digital trade.<sup>75</sup> Most developed countries have agreed to this Joint Statement; China did it almost at the last minute. However, no concrete outcome can be

<sup>70</sup> Peng, note 1 above, at 13–14.

<sup>71</sup> *Ibid.*, at 14–15.

<sup>72</sup> World Trade Organization, Work Programme on Electronic Commerce, adopted by the General Council on 25 September 1998, Geneva.

<sup>73</sup> See RH Weber, “Digital Trade and E-commerce: Challenges and Opportunities of the Asia-Pacific Regionalism” (2015) 10 *Asian Journal of WTO & International Health Law and Policy* 321 et seq.

<sup>74</sup> *Ibid.*, at 332; for further details see RH Weber, “A New International Trade Framework for Digital Assets” in M Kolsky Lewis et al. (eds), *A Post-WTO International Legal Order* (Cham/Switzerland, Springer, 2020), 277, at 280 et seq.

<sup>75</sup> WTO, WT/MIN(17)/60 of 13 December 2017.

seen for the time being, even though several proposals have been submitted and discussed in the WTO forum. The World Trade Report 2018 of the WTO also intensively addressed digital trade, pointing to the further transformation of the global trade regime. As a result of these investigations, the WTO has pleaded for a technology-induced reshaping of the regulatory environment.<sup>76</sup> Nevertheless, a solution to the existing problems may not surface in the near future.

## 2 New Data-Oriented Regulatory Approaches in World Trade Organization Law

An important component of the regulatory challenges concerns cross-border data flows. Foundational principles of data regulation in international trade law must be developed.<sup>77</sup> The elements encompass fostering digital trust and ensuring interoperability and transparency, in support of the free flow of information. Therefore, a hybrid regulatory approach based on a polycentric governance model<sup>78</sup> appears to be suitable.

New business models must become part of the trade rule framework. For example, digital platforms should be able to overcome barriers that have prevented small companies from participating in international trade, and from facilitating the building of trust in global transactions.<sup>79</sup> In summary, regulatory support for the implementation of digital platforms that are stable and trustworthy is an objective that must be pursued.

The WTO rules typically do not refer to private standards, industry best practices, or multistakeholder institutions.<sup>80</sup> However, these models are commonplace in the digital world and therefore must also be incorporated in international trade law. Self-regulation and – possibly – coregulation do have important merits; therefore, it appears to be worthwhile for WTO bodies to cooperate with international organizations and associations that are involved in the development of international trade standards.

Another issue concerns ongoing discussions about digital trade barriers.<sup>81</sup> The respective objectives are often at least partly founded in sound policy or social reasoning. Examples include cross-border cooperation on cybersecurity issues, the

<sup>76</sup> World Trade Organization, “World Trade Report 2018: The Future of World Trade: How Digital Technologies Are Transforming Global Commerce” (2018), <https://perma.cc/NKD3-BT7E>, at 130 et seq.

<sup>77</sup> Weber, note 74 above, 285 et seq.; AD Mitchell and N Mishra, “Regulating Cross-Border Data Flows in a Data-Driven World: How WTO-Law Can Contribute” (2019) 22 *Journal of International Economic Law* 389 et seq.

<sup>78</sup> See Weber, note 3 above, at 92 et seq.

<sup>79</sup> Meltzer, note 20 above, at 33.

<sup>80</sup> Mitchell and Mishra, note 77 above, at 404–405; see generally J Pauwelyn, “Rule-Based Trade 2.0? The Rise of Informal Rules and Standards and How They May Outcompete WTO Treaties” (2014) 17 *Journal of International Economic Law* 739 et seq.

<sup>81</sup> Meltzer, note 20 above, at 35–36.

implementation of an appropriate privacy framework, and the integration of consumer trust-enhancing measures.<sup>82</sup>

Finally, legal scholars are generally of the opinion that the WTO framework should be expanded in the light of smart goods and smart services, constituting the Internet of Things.<sup>83</sup> Apart from horizontal obligations on cross-border data flows and data localization,<sup>84</sup> efforts must be undertaken to amend the international trade regime by way of new provisions that enable digital innovation and promote business trust.<sup>85</sup> For example, technical standards for digital services that are consistent with internationally recognized standards should be adopted.

### E *International Regulatory Cooperation*

Cross-border data flows and digital trade are in the process of transforming the global legal framework. In contrast, experience over the last five years has shown that many governments have become less inclined to agree on new, internationally accepted rules and are increasingly restricting cross-border data flows.<sup>86</sup> The discussed data localization requirements can be seen as a new form of digital protectionism that extends beyond justified objectives, such as protection of privacy, law enforcement needs, and cybersecurity concerns. Fragmentation of the Internet is another widely discussed topic.<sup>87</sup>

The developments identified herein are leading us in the wrong direction. Rather, efforts should be undertaken to strengthen international regulatory cooperation. Therefore, the interplay between global needs and national interests should be better analyzed, and should also lead to an appropriate design of such cooperation.<sup>88</sup> Legal interoperability (for example, through mutual recognition understandings) must become a regulatory objective,<sup>89</sup> and a convergence toward principles and standards in areas such as privacy and cybersecurity is desirable.<sup>90</sup> Such developments can only be successful if international regulatory cooperation between actively public and private cross-border organizations is improved (in the form of interagency coordination and compliance management measures).

In the light of growing nationalism and deepened sovereignty interests in many large and small states around the globe, international regulatory cooperation represents a difficult stand. Nevertheless, from an academic and political perspective,

<sup>82</sup> For further details see Mitchell and Mishra, note 77 above, at 407 et seq.

<sup>83</sup> Weber, note 74 above, at 288; Neeraj, note 59 above, at 127–128.

<sup>84</sup> Mitchell and Mishra, note 77 above, at 6–7.

<sup>85</sup> *Ibid.*, at 3; see also M Burri and R Polanco, “Digital Trade Provisions in Preferential Trade Agreements: Introducing a New Dataset” (2020) 23 *Journal of International Economic Law* 187 et seq.

<sup>86</sup> Meltzer, note 20 above, at 25/26.

<sup>87</sup> M Mueller, *Will the Internet Fragment? Sovereignty, Globalization and Cyberspace* (Cambridge, Polity Press, 2017).

<sup>88</sup> See Palfrey and Gasser, note 35 above, at 178 et seq.

<sup>89</sup> Weber, note 36 above, at 6 et seq.

<sup>90</sup> Meltzer, note 20 above, at 47.

coordination is always better than confrontation. This assessment should motivate policymakers to place more emphasis on the harmonization of international bodies' activities.

#### IV OUTLOOK

Overarching key elements of global law in the context of the international trade regime are transparency, trust, and traceability. An optimal design for a balanced policy environment in the global trade ecosystem must consider aspects including risk assessment and ethical considerations, thereby strengthening the trust of all involved stakeholders in the global legal framework.

Regulation should become an enabler of digital innovation and should not limit business activities in an undue way. Interoperability, with respect to technical standards, data models, and AI processes, may help in the design of an appropriate normative framework. Governance measures that avoid further fragmentation may also help to realize a globally accepted legal environment. The difficulties ahead are remarkable, but not insurmountable. However, a new way of thinking is needed, setting traditional sovereignty considerations aside and moving toward new intellectual concepts.