

Emerging Regulation for Digital Economy: Challenges and Opportunities for Multilateral Global Governance¹

M. Larionova, A. Shelepov

Marina Larionova – PhD, Head, Centre for International Institutions Research (CIIR), Russian Presidential Academy of National Economy and Public Administration (RANEPA), Professor, Faculty of World Economy and International Affairs, National Research University Higher School of Economics; 11 Prechistsenskaya naberezhnaya, Moscow, 119034, Russian Federation; E-mail: larionova-mv@ranepa.ru

Andrey Shelepov – Candidate of Economic Sciences, Senior Researcher, Centre for International Institutions Research, Russian Presidential Academy of National Economy and Public Administration; 11 Prechistsenskaya naberezhnaya, 119034, Moscow, Russian Federation; E-mail: shelepov-av@ranepa.ru

Abstract

The role of information and communications technology (ICT), high-speed communication infrastructure, digital content and the digital economy as a whole is rapidly growing in the post-pandemic society. Simultaneously, competition for digital technologies and solutions and the contest to influence norms, standards and regulatory mechanisms is escalating. The new regulatory mechanisms and approaches are concurrently being shaped in the key international institutions, including the United Nations (UN), the International Telecommunication Union (ITU), the World Trade Organization (WTO), the Organisation for Economic Co-operation and Development (OECD), the European Union (EU), the Group of 20 (G20) and the BRICS group of Brazil, Russia, India, China and South Africa.

This article presents analysis of the current cooperation on issues of digital economy regulation within the main international institutions. The study aims to assess the influence of the existing and emerging regulatory mechanisms on the balance of power between the key international actors.

This assessment of the emerging mechanisms' impact on the balance of power among international actors indicates that advantages and leverage capabilities accruing from them are distributed unevenly. The advanced members of the OECD and the G20 gain significant advantages, and there is a risk that the new mechanisms will consolidate the balance of power embodied by the Bretton Woods system, which has successfully resisted decades-long endeavours for its reform.

However, regulation of the digital economy is not yet built as an established order. A window of opportunity was opened in 2020, not only to implement the G20's 2008 pledge to reform the international financial and economic architecture, but also to build a new digital economy governance system, ensuring that emerging markets and developing countries have a voice in decision-making commensurate with their weight in the global economy.

The article is structured in three parts. The introduction presents the research questions and objectives and describes the parameters of comparative analysis and influence assessment criteria. The second section reviews the emerging mechanisms and instruments and reflects on their influence on the balance of power. The third section puts forward conclusions and recommendations for enhancing the influence of emerging markets and developing countries on the shaping and functioning of the emerging digital economy's regulatory mechanisms.

Key words: digital economy; regulatory mechanisms; international institutions; factors of influence; G20; OECD; UN; EU; WTO; BRICS

For citation: Larionova M., Shelepov A. (2021). Emerging Regulation for the Digital Economy: Challenges and Opportunities for Multilateral Global Governance. *International Organisations Research Journal*, vol. 16, no 1, pp. 29–63 (in English). DOI: 10.17323/1996-7845-2021-01-02

¹ The article was written on the basis of the RANEPA state assignment research programme.

Introduction

The role of information and communication technology (ICT), high-speed communication infrastructure, digital content and digital economy (DE) as a whole² is rapidly growing in the post-pandemic society [OECD, 2020a; Pilat, 2020]. Simultaneously, competition for digital technologies and solutions is surging, and the contest to influence norms, standards and regulatory mechanisms is escalating. Analysis of cooperation and assessment of the impact of emerging mechanisms on the balance of power between international actors indicates that advantages accruing from the new regulatory instruments and mechanisms are distributed unevenly, as are leverage capabilities. The advanced countries – members of the Organisation for Economic Co-operation and Development (OECD) and the Group of 20 (G20) – gain significant advantages. However, digital economy regulation is not yet built as an established order. How significant are the risks that the new mechanisms will consolidate the balance of power embodied by the Bretton Woods system, which has successfully resisted decades-long endeavours for its reform? Is there a window of opportunity not only to implement the G20's 2008 pledge to reform the international financial and economic architecture, but also to build a new digital economy governance system that ensures emerging markets and developing countries have a voice in decision-making commensurate with their weight in the global economy? What cooperative actions are needed to enhance the ability of developing countries to influence the shaping and functioning of the digital economy's regulatory mechanisms?

This article reviews the existing and emerging mechanisms of digital economy regulation, assesses their influence on the balance of power between the key international actors, evaluates risks and proposes recommendations for collective actions aimed at constructing a balanced system of digital economy governance.

Two methodological problems were addressed: defining the documents' sample and the criteria for a comparative assessment of institutional influence.

Initially, the authors analyzed the entire range of documents produced by the international institutions considered in this article³ which affected the international digital environment and shaped the conditions for the development of both the DE and international cooperation, including recommendations, principles, reports, declarations, analytical reviews, roadmaps, decisions, initiatives, ratings, indices and best practices. However, this initial analysis showed that, despite the influence potential of each of the instruments listed, not all could be considered to be regulatory. Therefore, the sample included the existing and emerging legal instruments for regulating DE, analyzed in terms of the following aspects: legal nature; lobbyists and controversies; validity; openness to accession; main provisions of the documents (goals, objectives, principles); areas of regulation; implementation mechanisms; direct participants (signers); and actors indirectly affected by documents. For each document, a conclusion was made regarding its potential to influence the balance of power between international actors and the risks it poses to sustainable development and increasing the competitiveness of the Russian economy.

² This study does not aim to provide a definition of the DE or determine any parameters of its measurement. Many works are devoted to this issue, such as the fundamental article by R. Bucht and R. Hicks [2017].

³ The study examined the mechanisms of the International Telecommunication Union (ITU), the United Nations (UN), the World Trade Organization (WTO), the OECD, the European Union (EU), the G20, the BRICS group of Brazil, Russia, India, China and South Africa, the Internet Corporation for Assigned Names and Numbers (ICANN) and the Internet Society (ISOC). This article presents an analysis of intergovernmental institutions. The activities and influence of private corporations are discussed in the article by S.A. Vasilkovsky and A.A. Ignatov [2020] in this issue.

The final assessment of each institution's influence takes into account the assessments for the whole sample of its instruments.

Assessments of the influence of international actors typically consider the influence of states and the interactions between them, while research on international institutions largely focuses on efficiency issues rather than influence assessments. V. Lindoso and N. Hall [2016] examined various approaches to assessing the effectiveness of international organizations and identified the limitations of these approaches. R. Lall [2017] used quantitative evidence to support the idea that international organizations' ineffectiveness stems from their use by member countries to advance narrow national interests as opposed to pursuing broader institutional goals. A number of studies examined the sources of international institutional influence. E. Heldt and H. Schmidtke [2017] analyzed interinstitutional differences and time dynamics of three main sources of influence – objectives, responsibility areas and resources – for six international organizations. Recently, much attention has been paid to assessing the legitimacy of international organizations as a source of their influence. The issues of gaining, maintaining and losing legitimacy from this point of view were discussed by J. Tallberg and M. Zürn [2019]. In their fundamental research, O. Costa and K. Jørgensen [2012] analyzed the influence of key international institutions (the World Trade Organization (WTO), the North Atlantic Treaty Organization (NATO) and the United Nations (UN) Security Council) on the European Union (EU). However, they did not propose any methodology to compare the scope of these institutions' influence.

J. Tallberg et al. [2016] proposed a performance-based matrix for institutions that can be used for comparative influence assessments. Within the framework of this study, the proposed approach was modified: six parameters (factors) of influence and their characteristics were identified:

- 1) Dynamics (activeness) of norm-setting – the number of documents and the dynamics of their adoption within the institution's work cycles and in the context of a changing environment.
- 2) Coverage (affected areas) – the number of regulatory spheres within the DE that instruments affect, directly or indirectly, as well as the degree of progress within a specific sphere, which is especially important for specialized institutions.
- 3) Potential of influence on signatories and actors, indirectly affected by the document, stemming from the dominant type of documents – standard-setting, regulatory or norm-setting.
- 4) Degree of binding stemming from the dominant legal nature of the documents – obligatory, recommendatory or declarative.
- 5) Ensuring compliance – the presence and consistency in applying mechanisms for monitoring and assessing compliance with norms or standards contained in the documents.
- 6) Target group – the number of actors and target groups, including members of a particular institution, other countries and international institutions, and non-state actors.

This set of parameters made it possible to carry out a comparative analysis taking into account the specific activities of the institutions, the typology, and the nature of instruments they use. For each parameter, a qualitative assessment was provided based on analysis of the instruments. Then, expert assessment of their quantitative values was made using the following scale: 0 – low, 0.5 – medium, 1 – high. The resulting influence assessment score for each institution was calculated as the arithmetic mean of scores for all six parameters.

The Current State of Cooperation in International Organizations (IOs)

UN

Russia participates in the work of most key IOs and considers the UN to be a priority forum in which the Russian initiative to develop the norms, rules and principles of responsible state behaviour in cyberspace is discussed. Most experts assess the relationship between large-scale cyberattacks and the collapse of critical infrastructure as a key and growing global risk [WEF, 2020]. Issues of international information security (IIS) on the agenda of the UN, as the centre of the international organizations system, have a long and difficult history, beginning in 1998 with the draft General Assembly (GA) Resolution “Developments in the Field of Information and Telecommunications in the Context of International Security” proposed by Russia [UN GA, 1999]. Created in 2004 [UN GA, 2002], the UN Group of Governmental Experts (GGE) on developments in the field of information and telecommunications in the context of international security presented a report on possible measures to address existing and potential threats in the field of information security at the 60th session of the UN GA in 2005. The United States did not support the draft decision on the report due to differences in assessments of IIS threats, including disagreements on whether the use of ICT to achieve military and political goals should be considered as such a threat [UN GA, 2005]. However, despite the contradictions, the number of participants and the range of issues discussed was consistently expanded during the work of the five subsequent GGEs.

By 2016, based on the results of the fourth GGE meeting, approaches were formulated for the development of norms, rules and principles of responsible behaviour of states in cyberspace and confidence building measures. One of the stumbling blocks was the applicability of international law to the use of ICT by states [UN GA, 2015a]. As a result, no consensus was achieved at the fifth GGE (2016–7) [UN GA, 2015b]. The initiative of Russia, China and Cuba to create a fundamentally new set of international rules and norms of behaviour in cyberspace and to establish a special working group within the UN, open to all states and guided by the principles of inclusiveness in decision-making, was interpreted by the United States as an attempt to nullify the progress made by the GGE [Bowcott, 2017]. The United States and its allies take the view that the applicability of existing international law to the use of ICT is full and unconditional. According to the Russian position, this approach risks not taking into account the specifics of the digital sphere (for example, the difficulty of identifying the source of a computer attack, the possibility of using intermediaries, and so on), the arbitrary use of certain international legal norms, including the right to self-defence, and the implementation of countermeasures in the digital sphere that bypass existing mechanisms, including the UN Security Council [Yermakov, 2017].

As a result of efforts to overcome controversy, two parallel tracks were launched in 2018 – the Open-Ended Working Group (OEWG)⁴ and the Group of Governmental Experts (GGE).⁵

⁴ The OEWG was established in accordance with UN General Assembly Resolution “Developments in the Field of Information and Telecommunications in the Context of International Security” of 5 December 2018 [UN GA, 2018b]. The resolution was promoted by Russia, co-sponsored by 32 countries. The resolution was supported by 119 UN members (mainly BRICS members (except Brazil), the Shanghai Cooperation Organisation (SCO) members and other developing countries), while 46 voted against and 14 abstained.

⁵ The GGE was established in accordance with the UN General Assembly Resolution “Advancing Responsible State Behaviour in Cyberspace in the Context of International Security” of 22 December 2018 [UN GA, 2018a], put forward by the United States together with 35 co-sponsors. It was supported by 139 states, with 11 opposed and 16 abstentions. Supporters included EU states and other developed countries.

The objectives of the OEWG included the development of norms and principles of responsible behaviour of states based on a set of 13 rules⁶ and strategies for their implementation. The GGE was mandated to conduct a study of possible joint measures to address existing and potential threats to information security, norms, rules and principles of responsible behaviour of states, confidence building and capacity building measures, and the applicability of international law to the use of ICT by states. Despite these common objectives, given the competition between Russian and American approaches, there is a high risk of stagnation in the process of developing universal “rules of the game.” Russia participates in the activities of both groups and seeks to ensure the complementary nature of their negotiation processes and a convergence of positions. However, the future document is expected to be based on the principle of the lowest common denominator, limiting the UN’s influence in regulating IIS and strengthening tendencies toward promoting alternative approaches on other platforms [Henriksen, 2019].

ITU

The International Telecommunication Union (ITU) is the UN’s specialized ICT agency, with a uniquely broad membership (193 states, as well as about 900 companies, international and regional organizations, and universities) and the highest degree of international legitimacy among intergovernmental organizations in this field. It produces recommendations that establish technical standards and international norms governing the operation and interoperability of telecommunication networks. ITU recommendations are not binding unless they are adopted at the country level. However, due to their high quality, they are largely integrated into the national legislation of ITU member states. In the telecommunication standardization sector (ITU-T) alone, there are over 4,000 recommendations in more than 20 areas, including: general tariff principles; transmission systems and media, digital systems and networks; protection against interference; construction, installation and protection of cables and other elements of outside plant; data networks, open system communications and security; and global information infrastructure, Internet protocol aspects and next-generation networks.

The International Telecommunication Regulations (ITRs) [ITU, 2012a], adopted at the World Conference on International Telecommunications on 3–14 December 2012 (WCIT-12) in Dubai, are binding for signatories. They replaced the first ITRs adopted in 1988, signed by 178 countries. During the negotiation process, the Russian delegation proposed expanding the ITU’s powers to control the Internet and granting greater control over information flows to national government agencies [ITU, 2013]. Russia’s position was supported by seven countries – China, Saudi Arabia, Algeria, Bahrain, Sudan, Iraq and the United Arab Emirates. This coalition presented its own edition of the ITRs, which envisaged strengthening sovereign control over web addresses, giving states the right to regulate access to sites, and to assign, seize and distribute IP addresses and domain names [ITU, 2012b]. If this proposal had been accepted, the Internet Corporation for Assigned Names and Numbers (ICANN) would have lost its authority to regulate the Internet (it oversees the allocation of domain names and IP addresses in accordance with ITRs-88). The attempt to create an international Internet governance mechanism based on the expansion of the ITU’s mandate under the new ITRs met with stiff resistance from the U.S., Canada, the UK and the EU. U.S. representative Terry Kramer

⁶ They largely reflect the basic Russian approaches to ensuring international information security. They include: the use of ICT exclusively for peaceful purposes; jurisdiction of states over ICT infrastructure located within their borders; applicability of basic international law principles to the use of ICT by states, such as state sovereignty, equality of states and non-interference in the internal affairs of other states; the need to substantiate and prove states’ accusations of organizing and committing illegal actions in the ICT area; and the need for further collective work with the ultimate goal of developing a universal set of “rules of the game” in IIS.

said that the Russian proposal “implies that Internet traffic can be addressed by countries, and the country will be able to decide how to route traffic ... We treat this proposal with concern” [BBC, 2012]. As a result, the United States opposed any mention of the Internet in the ITRs. The inclusion of the phrase “these Regulations recognize the right of access of Member States to international telecommunication services” in the ITRs’ preamble was considered an attempt to extend the ITRs’ scope to regulate the Internet and its contents, and it was used by the U.S., Canada and the UK as a pretext for refusing to ratify. As a result, only 89 countries signed the document that came into force on 31 December 2017.⁷

The likelihood of creating an ITU-based international mechanism for Internet governance is low. The ITU’s regulatory influence in DE is limited to the development of recommendations on technology standards, which are non-binding.⁸ In general, the work on technical instruments (ITU-T recommendations) is more successful than on the ITRs.

WTO

Similar to that of the IIS, the history of the WTO’s negotiation process for the development of digital trade rules and regulations is complicated. The Work Programme on Electronic Commerce (WPEC), launched in 1998 with the adoption of the Declaration on Global Electronic Commerce at the second WTO ministerial conference, aimed to create a set of international rules and regulatory standards for e-commerce that would enhance market transparency and predictability [Azevêdo, 2020]. Disagreements on the main “horizontal” areas quickly became apparent: the classification of the content of electronic data transfer; the relationship between e-commerce and development issues; the fiscal aspects of e-commerce (including levies and duties on e-commerce); and application of the existing WTO rules and norms to electronic commerce. By the 2015 WTO ministerial conference in Nairobi, the WPEC process had become frozen.

Controversial issues relate to both substantive and procedural aspects. There is no consensus on whether electronic products should be considered as goods or services (or mixed), nor, accordingly, on whether digital trade should be regulated in the framework of the General Agreement on Tariffs and Trade (GATT) or the General Agreement on Trade in Service (GATS); there is also no consensus on the moratorium on customs duties in relation to electronic data transfer (the moratorium is updated every two years, while discussions continue on securing its permanent status). The African Group [WTO, 2017d], the Least Developed Countries Group [WTO, 2019c], India, and South Africa [WTO, 2017b] oppose the moratorium, given the potential economic cost of maintaining it for the developing and least developed countries and the negative impact on their emerging digital sectors.⁹ Bangladesh has proposed a differentiated approach according to which duty-free market access would be provided by all developed countries as well as willing developing countries for all goods and services from least developed countries exported using digital platforms [WTO, 2017b].

The U.S. and the EU advocate principles aimed at maximizing the liberalization of information and communication networks and trade in digital services. The United States considers it important to pay attention to new digital products. For example, in 2011, given the growth of the market for mobile applications and cloud computing, the U.S. proposed devel-

⁷ The U.S., Australia, Canada, Japan, India and a number of European countries have not signed the ITRs-12.

⁸ For instance, Recommendation ITU-T Y.2060. Overview of the Internet of Things.

⁹ A joint statement from India and South Africa provides an UN Conference on Trade and Development (UNCTAD) estimate of the potential losses for developing countries from non-application of customs duties on cross-border data transfers – \$10.075 billion in 2017. See WTO [2018b].

oping the rules for international trade in these areas aimed at reducing cross-border barriers [WTO, n. d., a]. The U.S. position on regulating cross-border e-commerce did not change with the appointment of the new presidential administration in 2017. For example, on 12 April 2018, the U.S. made proposals on the basic principles of e-commerce as part of the Joint Statement Initiative on E-Commerce (JSEC) [WTO, 2019b].

The African Group, the Least Developed Countries Group, India, South Africa and Saudi Arabia believe that, given the unresolved issues within the current format, it is impossible to start discussions on new problems in new formats. China also supported preserving the WPEC mechanism and proposed to ensure the parallel and complementary nature of work within the WPEC and the Proponent Group on Electronic Commerce, formed as a result of the 2017 WTO ministerial conference in Buenos Aires [WTO, 2019a]. Brazil's proposals contained a number of concrete initiatives to revitalize the WPEC debate [WTO, 2018a]. In October 2017, Russia presented a draft decision of the WTO ministerial conference providing for the creation of a working group on electronic commerce under the auspices of the general council and for the extension of the moratorium on imposing customs duties on cross-border data transfers [WTO, 2017c]. Australia, Canada, Chile, the EU, Norway, Paraguay and Korea have proposed a similar initiative [WTO, 2017a].

The WTO ministerial conference in Buenos Aires formalized the fragmentation of the WTO dialogue on e-commerce. The proponent group of the WTO members published a joint statement on e-commerce, indicating their intention to carry out preparations to launch a negotiation process outside the WPEC [WTO, 2017e]. In January 2019, 78 WTO members¹⁰ initiated a new and highly dynamic negotiation process on international regulation of e-commerce [WTO, 2019d]. In 2019–20, seven reports on the progress of this proponent group were registered in the WTO database, as well as 60 documents with proposals and positions of states [WTO, n. d., b]. Obviously, this initiative will face confrontation from the African Group, including South Africa, as well as some G20 members (India, Indonesia and Saudi Arabia) and other emerging economies. This opposition stems mainly from linking negotiating positions on e-commerce with a wider range of international development issues, including those of key importance within the Doha round (for example, in the field of agriculture). The negotiation process, including within the framework of the proponent group, is also complicated by differences in approaches to regulating the digital sector between the United States, China and the EU, expressed, first of all, in their views on the necessary degree of state involvement. The general crisis of the multilateral trading system and the WTO remains a significant limiting factor. The fragmentation of regulation and negotiation leads to harmonization of rules in the framework of regional trade agreements¹¹ and other multilateral institutions such as the OECD and G20.¹²

OECD

Analysis shows the OECD's influence in regulating the digital economy is growing. The combined economic power and digital leadership of its members is important but not the only factor of its growing influence. The reputation of the OECD as a unique international expert

¹⁰ The proponent group included, among others, the following G20 members: Australia, Argentina, Canada, Brazil, the EU, China, Japan, Korea, Mexico, Russia, Turkey and the United States.

¹¹ To date, 75 regional trade agreements that include provisions on e-commerce have been concluded [Monteiro, Teh, 2017].

¹² Most G20 members participate in the proponent group. At the same time, the presence of opponents – India, Indonesia and South Africa – significantly weakens the G20's potential. They did not join the “Osaka track” launched at the G20 summit in June 2019.

forum, the quality of its rule-making activities and its intensive engagement with partners (international and regional organizations, partner countries and social partners) are also essential.

The OECD is characterized by high dynamics of norm-setting in DE regulation, prompt response to changes, new risks and challenges, and regular assessment of the relevance of documents and their revision, if necessary. Currently, there are 19 legal instruments in force. Collectively, the documents are comprehensive, directly covering nearly 30 spheres. By the end of 2021, another instrument regulating taxation in the digital economy is expected to be adopted [OECD/G20, 2020], and its influence will be determined not only by the number of OECD¹³ and G20 members supporting it,¹⁴ but also by the scope of economic consequences resulting from revision of taxation laws concerning the cross-border activities of multinational enterprises (MNEs).¹⁵

The OECD has a 40-year history of regulating different aspects of the digital economy. The Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data adopted in 1980 [OECD, 2013a] became the first internationally agreed document in this area and had a significant impact on state policies within the OECD and beyond. The general objectives were confirmed in the 1985 Declaration on Transborder Data Flows [OECD, 1985]. In the context of technology advances and increased risk, in 2013 the OECD council adopted the Revised Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data [OECD, 2013b]. The guidelines set out the basic principles for national application and international cooperation to realize the goal of promoting free data flows yielding economic and social benefits. Considering privacy as a prerequisite for mitigating the risks and barriers to the transborder use of personal data, the guidelines sought to strengthen cooperation between authorities responsible for enforcing privacy-protecting laws. The corresponding recommendation was adopted in 2007 [OECD, 2007a].

Given the growing need for cryptographic technologies to protect the privacy of financial and personal data and to store and transmit them in order to develop national and global information and communication networks and technologies, as well as electronic commerce, the OECD agreed to the 1997 Recommendation Concerning Guidelines for Cryptography Policy [OECD, 1997]. This document was aimed at facilitating common approaches in the cryptographic policy of member countries as well as compatible, interoperable, portable and mobile cryptography methods, practices and procedures. At the same time, the recommendation provided a competitive advantage for OECD-based companies to strengthen their positions in the international open cryptography market.¹⁶ OECD members had an opportunity to promote their methods, procedures and standards as a basis for universal international practices.

Given the critical role broadband plays in the workings of the economy and society, the 2004 Recommendation of the OECD Council on Broadband Development [OECD, 2004] promoted principles and policies to assist the development of broadband markets, facilitate ef-

¹³ There are 137 jurisdictions involved in multilateral negotiations.

¹⁴ The document is expected to be adopted as a common G20-OECD instrument at the Rome summit on 30–31 2021.

¹⁵ The current scenario for revising tax rights is estimated to result in a total increase in global corporate tax revenue of 4% or \$100 billion annually. More than half of this amount will be received from the 100 largest MNEs [OECD, 2020b]. However, this calculation is based on the agreement option that does not rely on the principle of “safe harbour,” which is a condition for the United States’ support of a multilateral solution. See OECD [2020c].

¹⁶ In 2019, the global software market size alone was \$7.5 billion, and it is expected to reach \$16.5 billion by 2024. The main players in this market are U.S. companies. The hardware and technology market size in 2020 was estimated at approximately \$296.4 billion. The demand for crypto products and services will grow with the development of the digital economy. Key growth drivers are digitalization, the development of small and medium-sized enterprises (SMEs) using new products, and data privacy regulation standards.

efficient and innovative supply arrangements and encourage effective use of broadband services to ensure the competitiveness of OECD countries.

With an increase in cross-border data flows, there is a growing need for cooperation in combating spam, which causes significant social and economic damage, and for establishment of an effective relevant international regulatory framework. The 2006 Recommendation of the OECD Council on Cross-Border Co-operation in the Enforcement of Laws Against Spam [OECD, 2006] remains relevant today as the challenges of protecting against spam are aggravated by the growth of the digital economy and the need to secure the Internet.

The 2007 Recommendation of the Council on Electronic Authentication and the Guidance on Electronic Authentication [OECD, 2007b] created a framework for the compatibility of member countries' policies on domestic and cross-border electronic authentication of persons and entities. The OECD has taken the initiative to promote such cooperation at the global level with the engagement of relevant international organizations.

In 2008, Recommendation of the Council for Enhanced Access and More Effective Use of Public Sector Information [OECD, 2008b] was adopted to enhance the use of such information in order to improve productivity and economic efficiency.

The last OECD documents adopted in the 2000s – Declaration for the Future of the Internet Economy (the Seoul Declaration, 2008) [OECD, 2008a], Declaration on the Digital Economy: Innovation, Growth and Social Prosperity (the Cancún Declaration) [OECD, 2016b], which replaced the Seoul Declaration in 2016, and Principles for Internet Policy Making [OECD, 2011] – were aimed at developing compatible approaches to Internet governance based on voluntary codes of conduct and accountability mechanisms, internationally recognized and market-driven security standards, and best online security practices. These documents serve as a basis for building multilateral cooperation to develop globally interoperable technical standards while creating opportunities for the OECD's leading members, primarily the EU and the U.S., and their companies to affect this process and global multilateral Internet governance.

The OECD initiative to design and promote policies to expand the use of green ICTs and “smart” ICT-enabled applications in all sectors and to improve policy coordination in this area between member countries and at the international level resulted in the adoption of the Recommendation of the Council on Information and Communication Technologies and the Environment [OECD, 2010]. The recommendation created advantages for OECD companies producing and applying green technologies in ICT, energy, transport and other sectors. According to the 2017 assessment, the recommendation adopted in 2010 remains relevant.

The OECD considers user confidence and protection to be key conditions for the digital economy's development. Given the rapid changes in the Internet environment, since 2017 the provisions of the 2012 Recommendation of the Council on the Protection of Children Online, aimed at creating effective mechanisms and regulation in this area [OECD, 2012b], have been revised. The 2016 Recommendation on Consumer Protection in E-Commerce [OECD, 2016a] replaced the first OECD document in this sphere, adopted in 1999. The main goal was to create a safe and reliable e-commerce environment by ensuring consumer protection, shaping new governance mechanisms, improving regulation, and strengthening cooperation between consumer protection authorities at the international and regional level based on OECD standards and instruments. The 2012 Recommendation of the Council on International Mobile Roaming Services [OECD, 2012a] was intended to ensure consumer protection, fair prices for mobile roaming services, and effective competition in infrastructure, networks and applications.

Given rapid digitalization and the associated security risks, the OECD revised and updated the documents it had produced in the 2000s. The Recommendation on Digital Security Risk Management for Economic and Social Prosperity [OECD, 2015] was adopted in 2015 to

replace the 2002 Recommendation of the Council Concerning Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security. The document was aimed at ensuring the digital security of economic and social activities through the adoption of national strategies and the creation of compatible digital security management systems in OECD countries. Cooperation is based on common principles, comparable risk metrics, and common methodologies, standards and best practices. The 2019 Recommendation of the OECD Council on Digital Security of Critical Activities [OECD, 2019d], adopted to replace the 2008 Recommendation on the Protection of Critical Information Infrastructure, modernized the key concepts, expanded the scope of application, and took into account the experience of implementing the previous documents. The objectives of the document were to develop optimal national policies and regulations that ensure digital security but do not create barriers that inhibit economic activity, innovation and the digital economy, and also to facilitate regulatory convergence and international cooperation. This cooperation is aimed at ensuring critical infrastructure security in OECD countries, shaping international standards (based on EU and U.S. standards) and fostering the development of a global market for security services and products.

In 2019, two landmark documents were adopted – Recommendation of the Council on Health Data Governance [OECD, 2019e] and Recommendation of the Council on Artificial Intelligence [OECD, 2019c]. The former document focused primarily on the domestic policies of the member states. Its objective was to improve coordination between different frameworks related to the availability of, access to and use of personal health data both within and across national borders, and to ensure security, privacy, interoperability and efficient exchange of data based on common principles, including, where appropriate, codes, standards and the standardization of health data terminology. The OECD Recommendation on Artificial Intelligence, called the first intergovernmental standard on AI, was designed to ensure the necessary regulatory environment and standards in OECD countries and encourage their international promotion.

The OECD recommendations are not legally binding; their implementation is ensured by the political will of the members, as well as compliance monitoring and assessment mechanisms provided for and clearly spelled out in all recommendations and consistently applied in practice for their revision and update. The recommendations create opportunities to consolidate and strengthen the influence of the leading OECD members, primarily the EU and the U.S., both through market mechanisms and agreements with partners and international institutions.

G20

The G20's influence on the regulation of the digital economy is not commensurate with its potential as a premier economic cooperation forum for the world's leading economies. Since 2016, 11 documents have been adopted both at the leaders' level and at the level of ministers responsible for the digital economy. Eighty specific commitments have been made, and their monitoring demonstrates a fairly high level of compliance.

The first four documents were agreed to and adopted at the leaders' level in 2016. The G20 Blueprint on Innovative Growth [G20 Leaders, 2016b], G20 2016 Innovation Action Plan [G20 Leaders, 2016a], G20 New Industrial Revolution Action Plan [G20 Leaders, 2016d], and G20 Digital Economy Development and Cooperation Initiative [G20 Leaders, 2016c] were proposed by the Chinese presidency to stimulate G20 cooperation in the digital economy and innovation as the drivers of economic growth. Given the potential of new technologies to increase productivity and competitiveness, China and other emerging economies are interested in governing these processes, maximizing the benefits of anticipated technological change and industrial transformation, and mitigating their negative impacts. This initiative was an attempt

to integrate developing countries into the governance of these processes, equalize opportunities for influence in the digital economy and bridge the gap between leading industrialized countries and emerging market and developing economies.

The documents set out the fundamental cooperation principles, directions and measures. A G20 task force was established as a mechanism for implementing decisions. Supported by the OECD, this task force should ensure cooperation, continuity and consistency, taking into account the priorities of future G20 presidencies. As a result of a compromise between advanced and developing countries, the provisions of the documents, in fact, provide for the development of a G20 dialogue based on the OECD's principles and approaches, as well as its mechanisms and instruments, which were created by the leading industrial states in accordance with their interests, capacities and goals. Thus, from the very beginning the documents created opportunities to enhance the OECD's influence resulting from the integration of its instruments and mechanisms into G20 cooperation processes.

The G20 Roadmap for Digitalization [G20 Digital Economy Ministers, 2017], adopted at the first G20 digital ministerial meeting, reaffirmed the guiding principles and priorities of the 2016 documents. The main goals included: bridging the digital divide and using the potential of digitalization for inclusive economic growth; providing regulation to promote a competitive environment in order to encourage private sector investment; supporting the development and use of market- and industry-led international standards for technological products and services; and building trust based on effective protection of consumers' and intellectual property rights, transparency and security in the use of ICTs. The 2017 documents consolidated the trend toward strengthening the OECD's influence stemming from the reflection of its priorities and norms in the texts of the G20 Declaration and Roadmap through direct reference to specific instruments, mandates that strengthen the OECD's role, and integration of specific provisions from OECD documents into the texts without direct references.

In the 2018 declaration [G20 Digital Economy Ministers, 2018], issues of the digital economy's regulation are integrated into cooperation priorities aimed at creating the digital infrastructure for development and growth. Further, the G20 Digital Government Principles were adopted. Measures were identified to accelerate the creation of digital infrastructure for development and to bridge the gender digital divide, along with steps to further improve the measurement of the digital economy.

In 2019, Prime Minister Shinzo Abe of Japan made the creation of an international regime for free data flows with trust as a priority of the G20 presidency. One of the objectives in this regard was the launch of the "Osaka track" as a framework to develop international norms for the effective use of data as a source of economic growth, led by the G20. However, this goal was not achieved. Decisions on the digital economy in the G20 Osaka leaders' declaration [G20 Leaders, 2019] are limited to initiating a dialogue on harnessing the potential of data and the digital economy for sustainable growth and supporting the initiative to develop a multilateral agreement on trade-related aspects of e-commerce at the WTO, proposed by the trade ministers of 78 member countries in January 2019. As a result, the document did not change the balance of influence. Dialogue on international norms for the effective use of data as a source of economic growth is carried out within the OECD, whereas the trade aspects of e-commerce are discussed within the WTO. The G20's internal problems prevented bringing the dialogue to a new level and limited the use of the G20's leadership potential to launch Abe's truly ambitious initiative.

The 2019 joint ministerial statement on trade and digital economy identified two key areas of cooperation to achieve the goal of "promoting national experiences and international policies to maximize and share the benefits from digitalization of our economies and societies" [G20 Trade and Digital Ministers, 2019]. The first involved facilitating the free flow of data based on compliance with domestic and international legal frameworks, ensuring their interoperability,

protecting privacy, data and intellectual property, and strengthening consumer and business trust. The second focused on creating conditions for fostering public trust and confidence in artificial intelligence technologies and fully realizing their potential for economic growth and development. The G20 AI Principles, drawn from the OECD Recommendation on AI, were endorsed and the recommendations on national policies and international cooperation for trustworthy AI were taken into account (Section 2 of the G20 AI Principles). Regarding security standards, conditions for free data flow and innovation-friendly policies are in line with the spirit and letter of the OECD documents on digital security governance, privacy protection and transborder data flows in the digital economy.

The G20 digital economy ministerial statement issued in April 2020 sought to harness the potential of digital technologies and solutions to overcome the pandemic and enable economic recovery. The COVID-19 Response [G20 Digital Economy Ministers, 2020] identified six cooperation priorities: communication infrastructure development and network connectivity; exchange of data in a secure manner; research and development of digital technologies for health; use of digital technologies and solutions to enable economic participation during the pandemic; provision of a secure and trusted online environment; and encouragement of a transition by micro, small and medium-sized enterprises (MSMEs) to digitalized production systems, e-commerce and digital business models.

In the G20 Digital Economy Declaration adopted in July 2020, the ministers reaffirmed their commitment to strengthen cooperation in the digital sphere to overcome the pandemic, ensure recovery, and support sustainable and inclusive economic growth. In contrast to the 2019 declaration, the ministers endorsed Section 2 of the AI Principles and made a commitment to advance them in accordance with national priorities. The progress on free data flows with trust and cross-border data flows was less significant but areas for future work were agreed to, primarily the exchange of experience and good practices, including interoperability and transfer mechanisms and privacy enhancing technologies (PETs). The approval of the G20 Roadmap Toward a Common Framework for Measuring the Digital Economy and a three-tiered definitional framework became the basis for further movement toward interoperability and common standards. In the security sphere, acknowledging that cooperation to advance security in the DE can ensure strong, sustainable and inclusive economic growth was an achievement. The transformation of the digital economy task force into working group confirmed the G20's increased attention to DE issues and their inclusion in the long-term cooperation agenda.

However, despite a wide range of priorities, G20 cooperation in the digital sphere has not become a pillar for achieving the goal of strong, sustainable, balanced and inclusive growth. The objective of integrating developing countries into shaping DE regulation was not achieved. The engagement with international organizations in the digital economy task force has so far created additional opportunities for these institutions themselves, rather than strengthening the potential for G20 influence. The Japanese presidency's priority of launching the discussion on international norms for the effective use of data as a source of economic growth, in which the G20 would play a leading role, was not realized. Parameters of G20 cooperation tend to be based on OECD principles and approaches. Of course, their use cannot be a priori considered as contradicting the interests of developing and emerging market economies. However, through G20 cooperation on the development and use of market- and industry-led international standards for technology products and services that are consistent with international rules and contribute to increased interoperability and security in the use of ICTs, the OECD creates advantages for promoting technology companies, products, services and developments of its own leading member countries. At the same time, the integration of DE regulation issues into the G20 agenda creates potential opportunities for developing countries' influence on future DE regulation, which they cannot otherwise use in the OECD.

BRICS

Digitalization as a separate cooperation area appeared for the first time on the BRICS agenda during the 2015 Russian presidency. Russia proposed to hold the first communications ministers meeting and establish a special working group. By 2020, BRICS members had made 37 commitments on ICT development and digitalization. Overall, six BRICS documents address the digitalization sphere.

The ICT Development Agenda and Action Plan [BRICS Working Group on ICT Cooperation, 2016] adopted in 2016 represented an attempt to create a digital partnership and develop a roadmap for interaction within BRICS to bridge the digital divide. The document identified the key cooperation areas and priorities. However, it was not followed by any systemic implementation measures.

The Framework for BRICS E-Commerce Cooperation [Russia/China, 2015] and the BRICS E-Commerce Cooperation Initiative [BRICS CGETI, 2017], aimed at deepening BRICS cooperation in this area, did not set the objective of shaping a collective BRICS position on relevant issues. Nevertheless, the implementation of some practical steps envisaged by the framework could facilitate BRICS' coordination and promotion of common positions, for instance, in the G20 and the WTO.

The BRICS Action Plan for Innovation Cooperation (2017–20) [BRICS STI Ministers, 2017] approved the long-term BRICS priorities, including in the digital technologies area. Its implementation, along with the BRICS Science, Technology and Innovation Work Plan for 2019–22 [BRICS STI Ministers, 2019], should help accelerate the development and implementation of innovative solutions in the advanced industries of the five countries to ensure sustainable economic development and bridge the digital divide.

The Work Plan for the BRICS Partnership on New Industrial Revolution (PartNIR) adopted in 2019 [PartNIR, 2019] included a wide range of measures to promote the digital economy's development, including the creation of new engines of growth and infrastructure development to meet the needs of the new industrial revolution to ensure the industrial transformation of BRICS countries. Filling the initiative with specific innovative projects and large investments and establishing a powerful platform for innovative development could provide significant support for strengthening cooperation on the digital economy between the five countries and bridging the digital divide in terms of innovation performance and practical implementation of digital technologies for long-term growth. As of 2020, BRICS countries agreed on the terms of reference for the Partnership Advisory Group and updated its work plan, but so far, these decisions have not been implemented.

Currently, issues related to DE regulation are not explicitly included in the BRICS agenda, as there are no documents containing the decisions and/or collective positions of the five. Obviously, this reflects contradictions between the members on the issues of security in the use of ICT¹⁷ and electronic commerce.¹⁸ It is also obvious that in order to ensure that new DE regulation is in line with the interests of BRICS and other developing countries and emerging market economies, it will be necessary to consolidate the political will to overcome contradictions and act collectively.

¹⁷ They manifest themselves in the dialogue on IIS within the UN. In the framework of the BRICS Working Group on Security in the Use of ICTs, there is also no consensus on approaches to creating a legal framework for intra-BRICS cooperation on security in the use of ICT. The Russian Federation proposes the development of an intergovernmental agreement between all BRICS countries, whereas Brazil advocates the development of bilateral agreements between the countries.

¹⁸ They manifest themselves in the WTO (Work Programme on Electronic Commerce and Joint Statement Initiative on E-Commerce).

EU

The EU is strengthening its influence in international DE regulation. In 2020, it adopted a new digital strategy. One of its four goals is to secure the EU's status as a global digital economy leader by developing and promoting digital standards and regulation using the full set of regulatory, diplomatic and technological means, external financing and development assistance instruments, as well as the authority and status of the EU and its members in international organizations and agreements [EC, 2020].

The first Digital Single Market Strategy [EC, n. d.] of 2015 included three pillars: better consumer access to digital goods and services across Europe; creating conditions for digital networks and innovative services to flourish; and maximizing the growth potential of the digital economy. Since 2015, more than 30 regulations, directives and decisions have been approved, mostly focused on internal regulation. However, many of them have implications for external actors, as they actually set the entry and conduct rules for the EU market. Regulation covers the areas of taxation, facilitating and strengthening connectivity, e-commerce, consumer protection, data protection and processing, media and copyright, and cybersecurity. The full review requires a separate study but the following examples are illustrative.

The Proposal for a Council Directive Laying Down Rules Relating to the Corporate Taxation of a Significant Digital Presence [EC, 2018a] aimed to ensure that profits are registered and taxed in states where businesses have significant digital interactions with users. The document defines the rules for establishing the tax base for digital companies that operate cross-border without having any physical presence in a jurisdiction, "significant digital presence" indicators,¹⁹ and principles for determining taxable profits in EU states. The new regulation applies not only to corporate taxpayers established in the EU but also to businesses that are registered or incorporated in any non-Union jurisdiction that does not have a double taxation treaty with a member, where the taxpayer has a significant digital presence.

The Proposal for a Council Directive on the Common System of a Digital Services Tax on Revenues Resulting From the Provision of Certain Digital Services [EC, 2018b] should extend the tax regime to those digital activities of companies that are not yet taxable but are profitable for agents carrying them out.²⁰ Many EU states are either in the process of adopting taxes on digital services or have already adopted them, including Austria (5%, December 2019), France (3%, October 2019), Hungary (7.5%, June 2019), Italy (3%, January 2020) and Slovakia (limited list of digital services, 5%, March 2018) [KPMG, 2019]. This gives the Commission an argument for adopting a unified approach at the EU level in order to ensure uniform taxation of digital services across the Union, prevent fragmentation of the digital single market and eliminate the potential for unfair competition between jurisdictions.

No consensus has yet been reached on these initiatives. Large countries, primarily Germany, France and Spain, advocate the adoption of both legislative initiatives. Countries (for example, Ireland) that have specially adjusted their tax regime in order to attract large corporations to their jurisdictions oppose a common European tax and advocate the need to work in this area within the OECD. In March 2019, the Economic and Financial Council decided to

¹⁹ A "significant digital presence" is considered to exist in a member in a tax period if the business carried on through it consists wholly or partly of the supply of digital services through a digital interface and one or more of the following conditions is met: total revenues obtained in that tax period and resulting from the supply of those digital services to users located in that member state exceed 7 million euros; the number of users of one or more of those digital services exceeds 100,000; or the number of business contracts for the supply of any such digital service exceeds 3,000.

²⁰ Mainly digital interface services with the total amount of taxable revenues obtained by the entity within the Union during that financial year exceeding 50 million euros.

continue its work toward an agreement at the OECD level. As no agreement was reached by the end of 2020, the EU continues preparations for reform of its tax rules. The digital tax will contribute revenue to the EU's resources by the end of 2023. Members will be able to collect a value-added tax (VAT) from companies generating profits in their jurisdictions, which now enjoy the advantage of being registered in jurisdictions with more favourable tax regimes. The Commission's coordinating role in the tax area will also increase. This measure will affect large businesses (American and Chinese digital and Internet giants, including Facebook, Google, Amazon, Ali-Baba) and will not put an additional burden on small businesses.

Other examples of the influence of the EU's regulation outside the Union include Regulation (EU) 2019/1150 on Promoting Fairness and Transparency for Business Users of Online Intermediation Services,²¹ Regulation (EU) 2016/679 on the Protection of Natural Persons With Regard to the Processing of Personal Data and on the Free Movement of Such Data,²² and Directive (EU) 2018/1808 Amending Directive 2010/13/EU on the Coordination of Certain Provisions Laid Down by Law, Regulation or Administrative Action in Member States Concerning the Provision of Audiovisual Media Services.²³

Although the EU is not the leader in terms of the number of high-tech companies, it consolidates regulatory leadership and the ability to enhance its influence on other actors based on other factors. The attractiveness of the EU consumer market determines the need to follow its rules. The advantages of the EU also include: a well-developed bureaucratic system that can pass regulatory documents quite effectively; a very strong and comprehensive legal system, ensuring law enforcement; a kind of moral leadership that allows EU requirements to be promoted as a priori correct; and the significant role of the EU in international organizations.

Conclusions and Recommendations

The analysis indicates that advanced countries – members of the OECD, the EU and the G20 – have significant advantages for strengthening their influence through the existing and emerging mechanisms of digital economy regulation (Table 1).

The risks of deadlock in the negotiations on international information security are high due to the competing approaches of the U.S. and Russia in the Group of Governmental Experts and the Open-Ended Working Group, respectively. Problems stemming from these risks include obstruction of the UN's influence in regulating IIS and strengthening trends to promote alternative approaches on other platforms. A number of factors can be used to ensure progress. Working in both groups Russia could prioritize forging a consensus on the rules, norms and principles of responsible behaviour of states, deferring the issue of a new treaty on cybersecurity. This approach conforms to Russia's principled position on the central role of the UN, its

²¹ Any online platform or search engine willing to enter the European market and work with European consumers and businesses must comply with the requirements set out in the Regulation [European Parliament and Council, 2019].

²² The Regulation sets out the rules regarding the protection of individuals in relation to the processing and free movement of personal data. It applies to any actors (state and non-state) who in any way process any data of EU citizens or collect it on EU territory. Companies based outside the EU must apply the same rules when offering services and goods or tracking people's behaviour within the EU. In addition, the regulation sets out rules for the EU's provision of data to other countries and international organizations, which explicitly contain requirements for the protection of human rights and the rule of law. Given the possible contradictions and the obvious political aspect of this issue, the EU may refuse some actors (states and their companies) that do not comply with the EU's requirements to process the data of its citizens [European Parliament and Council, 2016].

²³ The requirements set out in the directive apply to all audiovisual content entering the EU [European Parliament and Council, 2018].

universal norms of international law and the UN Charter [Ministry of Foreign Affairs of Russia, 2019]. It will help preserve influence, facilitate the process within the UN, and support the de-securitization of cooperation on digital economy, concentrating security issues in the UN and economic issues in other fora, such as the G20.

Table 1. Assessment of the Influence of IIS on Digital Economy Regulation

Institution	Dynamics of the norm-setting	Scope of the spheres directly and indirectly impacted by the regulation	Influence potential stemming from the dominant type of the documents	Degree of binding by the dominant legal character of the documents	Compliance-ensuring mechanisms	Target group	Average
UN	0.5	1	0	0.5	0	0.5	0.42
ITU	0.5	1	1	0.5	0	0.5	0.58
WTO	0.5	1	1	1	0.5	1	0.83
OECD	1	1	1	0.5	1	1	0.92
G20	1	1	0	0	0.5	1	0.58
BRICS	0.5	0.5	0	0	0.5	1	0.42
EU	1	1	1	1	1	1	1

Source: Compiled by the authors.

The probability of an agreement on the new International Telecommunication Regulations might have been higher if the proposal had been limited to the expansion of the ITU's competencies to Internet governance with a division of competencies between the ITU and ICANN. However, the proposal on the members' sovereign right to establish and implement public policy, including international policy, on matters of Internet governance and to regulate the national Internet segment catalyzed opposition. As a result, only 88 members joined the new regulations, whereas 188 countries had signed the previous version in 1988. However, the impact of ITU recommendations on technology standards is still high. In this regard, cooperation in the ITU on developing recommendations on new technologies such as the Internet of Things and the fifth generation of mobile technologies (5G, or IMI-2020) is more productive and should be enhanced.

Substantive deliverables on e-commerce two-track negotiations at the WTO's 12th ministerial conference in Nur-Sultan in June 2021 [WTO, 2020] will require significant endeavours. Russia could contribute to shared rules, promoting the complementarity of the two negotiating processes, as well as transparency and openness of the JSEC initiative for all WTO members. It could use the proximity of approaches on substantive and procedural issues to facilitate dialogue with the EU and China in the WPEC and JSEC. The cooperation would also be useful for EU-Russia relations. With Russia's mediation, BRICS could become an important platform for bridging the positions with India and South Africa. Simultaneously, cooperation on e-commerce regulation should be promoted in the Eurasian Economic Union (EAEU).

OECD recommendations are positioned as regulatory, normative and value reference points, form common standards for members, and are promoted in international practice through cooperation with non-members within multilateral, regional and bilateral, as well as market mechanisms. Influencing international regulation, the OECD members, primarily the U.S. and the EU, build the global market for goods and services conforming to their own stand-

ards. This creates advantages for the OECD members' companies and technologies, which are positioned as complying with the best standards, norms and principles. The main risks for non-members stem from the absence of opportunities for participation in, and influence on, the new regulatory instruments and mechanisms.

The EU is enhancing its influence on digital economy regulation both within and beyond the Union. The EU digital strategy adopted in 2020 includes actions aimed at developing the digital single market and promoting the EU's digital standards and regulations globally. Given the EU's role as one of the key economic partners, it is vital that Russia monitors and assesses the impact of the EU's legal initiatives undertaken in implementation of the strategy on EU-Russia trade and economic cooperation. It is especially important in the context of Russia's goal to expand digital products exports. Given the EU's influence in international institutions, consolidation of efforts would be consequential wherever it meets Russia's interests. For instance, European and Russian interests coincide on the digital economy taxation rules negotiated in the OECD. Taxation of large corporations with significant digital presence generating revenue in the Russian market would increase budget incomes without exacerbating the tax load for national companies. As one of the EU's priorities is the promotion of its standards and regulation in the Commonwealth of Independent States (CIS), including the members of the EAEU, its agenda should include the development of digital economy regulation in the EAEU with due account of the best EU and OECD practices, as well as building cooperation between the EAEU and the EU, thus balancing influence and creating conditions for the EAEU-EU cooperation in other spheres.

The G20's influence on digital economy regulation is not commensurate with its role as a premier economic forum for cooperation among the world's largest economies. The arguments in favour of strengthening G20 cooperation on the digital economy are manifold. Most importantly, the G20 had a successful experience related to the reform of global financial regulation, and digital economy development is mandatory for attaining the G20's goal of strong, sustainable, balanced and inclusive growth.

The post-pandemic recovery will need an established foundation for cooperation and the G20's decisions in 2020 have created a window of opportunity for upgrading cooperation and enhancing the G20's role in shaping digital economy governance. This is important in view of the minimal scope for developing and emerging market economies' influence in the OECD, difficulties experienced in the UN and WTO negotiation processes and absence of BRICS decisions on digital security, Internet governance, digital infrastructure development and other digital economy regulation priorities.

Integration of DE regulation issues into the G20 agenda would create opportunities to enhance the developing and emerging market economies' influence on the fledgling regulation framework. Even if the initiatives are deliberated based on existing or evolving OECD documents, as might be the case with critical infrastructure security, artificial intelligence principles or recommendations on consumer protection, there will be more room for consideration of the interests of the developing countries in the G20. In the context of anti-pandemic measures and bolstering health systems, there is a need for strengthening data governance.²⁴ In this regard, and given the importance and role of data for the DE,²⁵ as a first step the G20 initiative on

²⁴ The identified cooperation areas include agreeing on principles to ensure privacy, trust, accessibility and exchange of data, improving national policies, and building capacity to use and share data across sectors and countries [OECD, 2019a].

²⁵ Progress in the digital transformation of the economy and society largely depends on the quality and accessibility of data. According to OECD estimates, data access and exchange can provide an economic growth increase of 0.1% to 1.5% of GDP in case of public sector data, and of 1% to 2.5% of GDP if private sector data are considered [OECD, 2019b].

data governance could be put forward with the aim of developing common approaches to data governance at the national and international levels, including issues of availability, accessibility, integrity, use and security.

Moreover, as extensively discussed in recent years [Dominioni, 2019], regulation of digital platforms should be considered by the G20 in view of its influence on the economy and society. The problem of digital platform regulation cannot be resolved at the national level, though such proposals have been elaborated.²⁶ There is also relevant experience [European Parliament and Council 2019], plans [Government of France, 2020] and proposals [Strowel, Vergote, 2016] at the EU level. The OECD is currently studying the economic and social impact of platforms [OECD, 2019a] and discussing approaches to their regulation, primarily in terms of taxation [OECD, 2019f, p. 12, 2020d].

The establishment of a new institution responsible for the development, coordination and monitoring of DE regulation with the participation of key international organizations and invited countries could reduce the risks of legitimizing the norms and standards formed by the OECD through the G20. In analogy with the Financial Stability Board, it could be called the Digital Stability Board [Fay, 2019]. Such a cooperation mechanism may help avoid crises caused by a weakness of the DE regulatory system, just as the 2008 crisis was rooted in problems related to systemic financial regulation. Simultaneously, it would enable major developing and emerging market economies to participate in shaping global governance and regulation of the digital economy.

References

- Azevêdo R. (2020). *Speech: Joint Statement on E-Commerce*. Davos, 24 January. World Trade Organization. Available at: https://www.wto.org/english/news_e/spra_e/spra300_e.htm (accessed 15 June 2020).
- BBC (2012). *Russia Backtracks on Internet Governance Proposals*. 11 December. Available at: <https://www.bbc.com/news/20676293> (accessed 15 July 2020).
- Bowcott O. (2017). Dispute Along Cold War Lines Led to Collapse of UN Cyberwarfare Talks. *The Guardian*, 23 August. Available at: <https://www.theguardian.com/world/2017/aug/23/un-cyberwarfare-negotiations-collapsed-in-june-it-emerges> (accessed 15 July 2020).
- BRICS Contact Group on Economic and Trade Issues (CGETI) (2017). BRICS E-Commerce Cooperation Initiative. Available at: [https://www.ranepa.ru/images/media/brics/china2016/BRICS%20E-commerce%20Cooperation%20Initiative_final%20\(2\).pdf](https://www.ranepa.ru/images/media/brics/china2016/BRICS%20E-commerce%20Cooperation%20Initiative_final%20(2).pdf) (accessed 15 July 2020).
- BRICS Science, Technology and Innovation (STI) Ministers (2017). BRICS Action Plan for Innovation Cooperation (2017–2020). Available at: <https://www.ranepa.ru/images/media/brics/china2016/BRICS%20Action%20Plan%20for%20Innovation%20Cooperation.pdf> (accessed 15 July 2020).
- BRICS Science, Technology and Innovation (STI) Ministers (2019). BRICS Science, Technology and Innovation Work Plan 2019–2022. Available at: https://www.ranepa.ru/images/News_ciir/Project/BRICS_new_downloadings/2019/STI_WORKING_PLAN_2019-2022.pdf (accessed 15 July 2020).
- BRICS Working Group on ICT Cooperation (2016). ICT Development Agenda and Action Plan. Available at: <https://www.ranepa.ru/images/media/brics/indianpresidency2/11-11-2016%20BRICS%20ICT%20Development%20Agenda%20&%20Action%20plan.pdf> (accessed 15 July 2020).
- Bucht R., Hicks R. (2018). Opredeleniye, kontseptsiya i izmereniye tsifrovoy ekonomiki [Definition, Concept and Measurement of the Digital Economy]. *Vestnik mezhdunarodnykh organizatsiy*, vol 13, no 2, pp. 143–72. Available at: <http://doi.org/10.17323/1996-7845-2018-02-07> (in Russian).

²⁶ For instance, for the U.S. proposals see Feld, [2019], Kimmelman [2019] and Stigler Center/Chicago Booth [2019]. For the UK proposals see Digital Competition Expert Panel [2019].

Costa O., Jørgensen K. (2012). The Influence of International Institutions on the EU: A Framework for Analysis. *The Influence of International Institutions on the EU* (O. Costa, K. Jørgensen (eds)). London: Palgrave Macmillan. Available at: http://www.doi.org/10.1057/9780230369894_1.

Digital Competition Expert Panel (2019). Unlocking Digital Competition: Report. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf (accessed 15 July 2020).

Dominioni S. (2019). Digital Economic Powers and Digital Political Rulers. Commentary, 17 October. Italian Institute for International Studies. Available at: <https://www.ispionline.it/en/publicazione/digital-economic-powers-and-digital-political-rulers-24187> (accessed 15 July 2020).

Ermakova V.I. (2017). Vystupleniye predstavatelya Rossiyskoy Federatsii v Pervom komitete 72-y sessii General'noy Assamblei OON V.I. Yermakova v ramkakh diskussii po razdelu "Drugiye mery razoruzheniya i mezhdunarodnaya bezopasnost". Rezhim dostupa [Speech by the Representative of the Russian Federation in the First Committee of the 72nd session of the UN General Assembly V.I. Ermakova in the Framework of the Discussion on the Section "Other Measures of Disarmament and International Security"]. 23 October. Available at: https://russiaun.ru/ru/news/1com_intsec2310 (accessed 15 June 2020) (in Russian).

European Commission (EC) (2018a). Proposal for a Council Directive Laying Down Rules Relating to the Corporate Taxation of a Significant Digital Presence. COM (2018) 147 Final. Available at: https://ec.europa.eu/taxation_customs/sites/taxation/files/proposal_significant_digital_presence_21032018_en.pdf (accessed 15 July 2020).

European Commission (EC) (2018b). Proposal for a Council Directive on the Common System of a Digital Services Tax on Revenues Resulting From the Provision of Certain Digital Services. COM (2018) 148 Final. Available at: https://ec.europa.eu/taxation_customs/sites/taxation/files/proposal_common_system_digital_services_tax_21032018_en.pdf (accessed 15 July 2020).

European Commission (EC) (2020). Shaping Europe's Digital Future. Available at: https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_en_4.pdf (accessed 15 July 2020).

European Commission (EC) (n. d.). Shaping the Digital Single Market. Available at: <https://ec.europa.eu/digital-single-market/en/shaping-digital-single-market#Moredocuments> (accessed 15 June 2020).

European Parliament and Council (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons With Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation). Available at: <https://eur-lex.europa.eu/eli/reg/2016/679/oj> (accessed 15 July 2020).

European Parliament and Council (2018). Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 Amending Directive 2010/13/EU on the Coordination of Certain Provisions Laid Down by Law, Regulation or Administrative Action in Member States Concerning the Provision of Audiovisual Media Services (Audiovisual Media Services Directive) in View of Changing Market Realities. Available at: <https://eur-lex.europa.eu/eli/dir/2018/1808/oj> (accessed 15 July 2020).

European Parliament and Council (2019). Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on Promoting Fairness and Transparency for Business Users of Online Intermediation Services. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019R1150> (accessed 15 July 2020).

Fay R. (2019). Digital Platforms Require a Global Governance Framework. Centre for International Governance and Innovation. Available at: <https://www.cigionline.org/articles/digital-platforms-require-global-governance-framework> (accessed 15 July 2020).

Feld H. (2019). The Case for the Digital Platform Act: Market Structure and Regulation of Digital Platforms. Roosevelt Institute/Public Knowledge. Available at: https://www.publicknowledge.org/assets/uploads/documents/Case_for_the_Digital_Platform_Act_Harold_Feld_2019.pdf (accessed 15 July 2020).

Government of France (2020). Regulation of Digital Platforms: Launch of a European Working Group. 25 February. Available at: <https://www.gouvernement.fr/en/regulation-of-digital-platforms-launch-of-a-european-working-group> (accessed 15 June 2020). Group of 20 (G20) Digital Economy Ministers (2017) G20 Digital Economy Ministerial Conference. Düsseldorf, 6–7 April. Available at: <https://www.ranepa.ru/images/media/g20/2017hamburg/g20-digital-economy-ministerial-declaration-english-version.pdf> (accessed 15 July 2020).

- Group of 20 (G20) Digital Economy Ministers (2018). G20 Digital Economy Ministerial Declaration. Salta, 24 August. Available at: https://www.ranepa.ru/images/media/g20/2018buenosaires/g20_detf_ministerial_declaration_salta.pdf (accessed 15 July 2020).
- Group of 20 (G20) Digital Economy Ministers (2020). Extraordinary G20 Digital Economy Ministerial Meeting: COVID-19 Response Statement. Virtual Meeting, 30 April. Available at: <http://www.g20.utoronto.ca/2020/2020-g20-digital-0430.html> (accessed 15 July 2020).
- Group of 20 (G20) Leaders (2016). Plan deystviy “Gruppy dvadtsati” po innovatsiyam 2016 goda [2016 G20 Innovation Action Plan]. Available at: <https://www.ranepa.ru/images/media/g20/2016Hangzhou/План%20действий%20инновации.pdf> (accessed 15 July 2020) (in Russian).
- Group of 20 (G20) Leaders (2016b). Kontury innovatsionnogo rosta “Gruppy dvadtsati” [Contours of G20 Innovative Growth]. Available at: <https://www.ranepa.ru/images/media/g20/2016Hangzhou/Контурьы.pdf> (accessed 15 July 2020) (in Russian).
- Group of 20 (G20) Leaders (2016c). Plan deystviy “Gruppy dvadtsati” v svyazi s novoy industrial'noy revolyutsiyey [G20 Action Plan for the New Industrial Revolution]. Available at: <https://www.ranepa.ru/images/media/g20/2016Hangzhou/План%20действий%20индустриал.pdf> (accessed 15 July 2020) (in Russian).
- Group of 20 (G20) Leaders (2016a). Initsiativa “Gruppy dvadtsati” po razvitiyu i sotrudnichestvu v oblasti tsifrovoy ekonomiki [G20 Digital Economy Development and Cooperation Initiative]. Available at: <https://www.ranepa.ru/images/media/g20/2016Hangzhou/Инициатива%20цифр.pdf> (accessed 15 July 2020) (in Russian).
- Group of 20 (G20) Leaders (2019). Osakskaya deklaratsiya po voprosam tsifrovoy ekonomiki [Osaka Declaration on the Digital Economy]. Osaka, 29 June. Available at: https://www.ranepa.ru/images/News_ciir/Project/G20_new_downloadings/OSAKA_DECLARATION_ON_DIGITAL_ECONOMY_rus.pdf (accessed 15 July 2020) (in Russian).
- Group of 20 (G20) Leaders (2020). Ekstrennyy sammit liderov “Gruppy dvadtsati”. Zayavleniye po novoy koronavirusnoy infektsii COVID-19 [Emergency G20 Leaders' Summit: Statement on the Novel Coronavirus Infection COVID-19]. Virtual Meeting, 26 March. Available at: https://www.ranepa.ru/ciir/saudovskoe-predsedatelstvo-2020/G20_Extraordinary%20G20%20Leaders%20Summit_Statement_RUS.pdf (accessed 15 July 2020) (in Russian).
- Group of 20 (G20) Trade and Digital Ministers (2019). G20 Ministerial Statement on Trade and Digital Economy. Tsukuba City, 8–9 June. Available at: https://www.ranepa.ru/images/News_ciir/Project/Ministerial_Statement_on_Trade_and_Digital_Economy.pdf (accessed 15 July 2020).
- Heldt E., Schmidtke H. (2017). Measuring the Empowerment of International Organizations: The Evolution of Financial and Staff Capabilities. *Global Policy*, vol. 8, supplement 5, pp. 51–61. Available at: <https://onlinelibrary.wiley.com/doi/epdf/10.1111/1758-5899.12449> (accessed 15 July 2020).
- Henriksen A. (2019) The End of the Road for the UN GGE Process: The Future Regulation of Cyberspace. *Journal of Cybersecurity*, vol. 5, no 1, Tyy009. Available at: <https://doi.org/10.1093/cybsec/tyy009>.
- International Telecommunication Union (ITU) (2012a). Final Acts: World Conference on International Telecommunications. Dubai, 3–4 December. Available at: <https://www.itu.int/en/wcit-12/Documents/final-acts-wcit-12.pdf> (accessed 15 July 2020).
- International Telecommunication Union (ITU) (2012b). Proposals for the Work of the Conference. ITU-SG WCIT12 Contribution 47. Available at: <https://www.itu.int/md/S12-WCIT12-C-0047/en> (accessed 15 June 2020).
- International Telecommunication Union (ITU) (2013). Proposals for the Work of the Conference. ITU-SG WCIT12 Contribution 27. Available at: <https://www.itu.int/md/S12-WCIT12-C-0027/en> (accessed 15 June 2020).
- Kimmelman G. (2019). The Right Way to Regulate Digital Platforms. 18 September. Shorenstein Center on Media, Politics and Public Policy. Available at: <https://shorensteincenter.org/the-right-way-to-regulate-digital-platforms/> (accessed 6 March 2021).

KPMG (2019) Taxation of the Digitalized Economy: Developments Summary. Available at: <https://tax.kpmg.us/content/dam/tax/en/pdfs/2019/digitalized-economy-taxation-developments-summary.pdf> (accessed 15 July 2020).

Lall R. (2017). Beyond Institutional Design: Explaining the Performance of International Organizations. *International Organization*, vol. 71, no 2, pp. 245–80. Available at: <https://doi.org/10.1017/S0020818317000066>.

Lindoso V., Hall N. (2016). Assessing the Effectiveness of Multilateral Organizations. BSG Working Paper Series WP-2016/013, Blavatnik School of Government. Available at: https://www.bsg.ox.ac.uk/sites/default/files/2018-05/2016-04_Hall_Lindoso-Multilateral_Effectiveness.pdf (accessed 15 July 2020).

Ministry of Foreign Affairs of the Russian Federation (2020). Vneshnepoliticheskaya i diplomaticheskaya deyatel'nost' Rossiyskoy Federatsii v 2019 godu [Foreign Policy and Diplomatic Activity of the Russian Federation in 2019]. Available at: <https://www.mid.ru/documents/10180/4105169/%D0%9E%D0%91%D0%97%D0%9E%D0%A0+2019.docx/5ea5f13c-881a-45a8-9f61-831241e70e93> (accessed 15 July 2020) (in Russian).

Monteiro J.-A., Teh R. (2017). Provisions on Electronic Commerce in Regional Trade Agreements. Working Paper No ERSD-2017-11, World Trade Organization. Available at: https://www.wto.org/english/res_e/reser_e/ersd201711_e.htm (accessed 15 July 2020).

Organisation for Economic Co-Operation and Development (OECD) (1985). Declaration on Transborder Data Flows. Available at: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0216> (accessed 15 July 2020).

Organisation for Economic Co-Operation and Development (OECD) (1997). Recommendation of the Council Concerning Guidelines for Cryptography Policy. Available at: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0289> (accessed 15 July 2020).

Organisation for Economic Co-Operation and Development (OECD) (2004). Recommendation of the Council on Broadband Connectivity. Available at: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0322> (accessed 15 July 2020).

Organisation for Economic Co-Operation and Development (OECD) (2006). Recommendation of the Council on Cross-Border Co-Operation in the Enforcement of Laws Against Spam. Available at: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0344> (accessed 15 July 2020).

Organisation for Economic Co-Operation and Development (OECD) (2007a). Recommendation of the Council on Cross-Border Co-Operation in the Enforcement of Laws Protecting Privacy. Available at: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0352> (accessed 15 July 2020).

Organisation for Economic Co-Operation and Development (OECD) (2007b). Recommendation of the Council on Electronic Authentication. Available at: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0353> (accessed 15 July 2020).

Organisation for Economic Co-Operation and Development (OECD) (2008a). Declaration for the Future of the Internet Economy (Seoul Declaration). Available at: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0366> (accessed 15 July 2020).

Organisation for Economic Co-Operation and Development (OECD) (2008b). Recommendation of the Council for Enhanced Access and More Effective Use of Public Sector Information. Available at: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0362> (accessed 15 July 2020).

Organisation for Economic Co-Operation and Development (OECD) (2010). Recommendation of the Council on Information and Communication Technologies and the Environment. Available at: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0380> (accessed 15 July 2020).

Organisation for Economic Co-Operation and Development (OECD) (2011). Recommendation of the Council on Principles for Internet Policy Making. Available at: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0387> (accessed 15 July 2020).

Organisation for Economic Co-Operation and Development (OECD) (2012a). Recommendation of the Council on International Mobile Roaming Services. Available at: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0388> (accessed 15 July 2020).

Organisation for Economic Co-Operation and Development (OECD) (2012b). Recommendation of the Council on the Protection of Children Online. Available at: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0389> (accessed 15 July 2020).

Organisation for Economic Co-Operation and Development (OECD) (2013a). Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data. Available at: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188> (accessed 15 July 2020).

Organisation for Economic Co-Operation and Development (OECD) (2013b). The OECD Privacy Framework. Available at: https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf (accessed 15 July 2020).

Organisation for Economic Co-Operation and Development (OECD) (2015). Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity. Available at: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0415> (accessed 15 July 2020).

Organisation for Economic Co-Operation and Development (OECD) (2016a). Consumer Protection in E-Commerce: OECD Recommendation. Available at: <https://www.oecd.org/sti/consumer/ECommerce-Recommendation-2016.pdf> (accessed 15 July 2020).

Organisation for Economic Co-Operation and Development (OECD) (2016b). Declaration on the Digital Economy: Innovation, Growth and Social Prosperity (Cancún Declaration). Available at: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0426> (accessed 15 July 2020).

Organisation for Economic Co-Operation and Development (OECD) (2019a). An Introduction to Online Platforms and Their Role in the Digital Transformation. Available at: https://www.oecd-ilibrary.org/science-and-technology/an-introduction-to-online-platforms-and-their-role-in-the-digital-transformation_53e5f593-en;jsessionid=XNP36WHdzLdM2vJO0c2M6jYa.ip-10-240-5-42 (accessed 15 July 2020).

Organisation for Economic Co-Operation and Development (OECD) (2019b). Enhancing Access to and Sharing of Data. Available at: <https://www.oecd.org/going-digital/enhancing-access-to-and-sharing-of-data.pdf> (accessed 15 July 2020).

Organisation for Economic Co-Operation and Development (OECD) (2019c). Recommendation of the Council on Artificial Intelligence. Available at: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449> (accessed 15 July 2020).

Organisation for Economic Co-Operation and Development (OECD) (2019d). Recommendation of the Council on Digital Security of Critical Activities. Available at: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0456> (accessed 15 July 2020).

Organisation for Economic Co-Operation and Development (OECD) (2019e). Recommendation of the Council on Health Data Governance. Available at: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0433> (accessed 15 July 2020).

Organisation for Economic Co-Operation and Development (OECD) (2019f). The Role of Digital Platforms in the Collection of VAT/GST on Online Sales. Available at: <https://doi.org/10.1787/e0e2dd2d-en> (accessed 15 July 2020).

Organisation for Economic Co-Operation and Development (OECD) (2020a). Policy Options to Support Digitalization of Business Models During COVID-19: Annex. Available at: <http://www.oecd.org/sti/policy-options-to-support-digitalization-of-business-models-during-covid-19-annex.pdf> (accessed 15.09.2020).

Organisation for Economic Co-Operation and Development (OECD) (2020b). Tax Challenges Arising From the Digitalisation of the Economy: Update on the Economic Analysis & Impact Assessment. Webcast, 13 February. Available at: <https://www.oecd.org/tax/beps/presentation-economic-analysis-impact-assessment-webcast-february-2020.pdf> (accessed 15 July 2020).

Organisation for Economic Co-Operation and Development (OECD) (2020c). International Community Renews Commitment to Multilateral Efforts to Address Tax Challenges From Digitalisation of the Economy. 31 January. Available at: <http://www.oecd.org/tax/beps/international-community-renews-commitment-to-multilateral-efforts-to-address-tax-challenges-from-digitalisation-of-the-economy.htm> (accessed 15 June 2020).

Organisation for Economic Co-Operation and Development (OECD) (2020d). Public Comments Received on the Draft Model Rules for Reporting for Platform Operators With Respect to Sellers in the Sharing and Gig Economy. 15 April. Available at: <http://www.oecd.org/tax/exchange-of-tax-information/public-comments->

received-on-the-draft-model-rules-for-reporting-for-platform-operators-with-respect-to-sellers-in-the-sharing-and-gig-economy.htm (accessed 15 June 2020).

Organisation for Economic Co-Operation and Development (OECD) / Group of 20 (G20) (2020). Statement by the OECD/G20 Inclusive Framework on BEPS on the Two-Pillar Approach to Address the Tax Challenges Arising From the Digitalisation of the Economy. Available at: <http://www.oecd.org/tax/beps/statement-by-the-oecd-g20-inclusive-framework-on-beps-january-2020.pdf> (accessed 15 July 2020).

PartNIR (2019). Work Plan for the BRICS Partnership on New Industrial Revolution. Available at: https://www.ranepa.ru/ciir/sfery-issledovaniy/briks/dokumenty-briks/briks-brazilskoe-predsedatelstvo-2019/20190917_PARTNIR_WORK_PLAN.pdf (accessed 15 July 2020).

Pilat D. (2020). How G20 Countries are Accelerating Digital Transformation During the COVID-19 Crisis. OECD Innovation Blog, 7 August. Available at: <https://oecd-innovation-blog.com/2020/08/07/g20-covid-19-digital-transformation-business-policy/> (accessed 15 September 2020).

Russia/China (2015). Framework for BRICS E-Commerce Cooperation. Available at: <https://www.ranepa.ru/ciir/sfery-issledovaniy/briks/dokumenty-briks/Ecommerce-cooperation.pdf> (accessed 15 July 2020).

Stigler Center for the Study of the Economy and the State (Stigler Center) / The University of Chicago Booth School of Business (Booth School) (2019). Committee for the Study of Digital Platforms, Market Structure and Antitrust Subcommittee. Draft Report of 15 May. Available at: <https://research.chicagobooth.edu/-/media/research/stigler/pdfs/market-structure---report-as-of-15-may-2019.pdf?la=en&hash=B2F11FB118904F2AD701B78FA24F08CFF1C0F58F> (accessed 15 July 2020).

Strowel A., Wouter V. (2016). Digital Platforms: To Regulate or Not to Regulate? Available at: https://ec.europa.eu/information_society/newsroom/image/document/2016-7/uclouvain_et_universit_saint_louis_14044.pdf (accessed 15 July 2020).

Tallberg J., Sommerer T., Squatrito T., Lundgren M. (2016). The Performance of International Organizations: A Policy Output Approach. *Journal of European Public Policy*, vol. 23, no 7, pp. 1077–96. Available at: <http://doi.org/10.1080/13501763.2016.1162834>.

Tallberg J., Zürn M. (2019). The Legitimacy and Legitimation of International Organizations: Introduction and Framework. *Review of International Organizations*, no 14, pp. 581–606. Available at: <https://doi.org/10.1007/s11558-018-9330-7>. United Nations (UN) (1999) Dostizheniya v sfere informatizatsii i telekommunikatsii v kontekste mezhdunarodnoy bezopasnosti [Developments in the Field of Information and Telecommunications in the Context of International Security]. UN General Assembly Resolution A/Res/53/70. Available at: <https://undocs.org/ru/A/RES/53/70> (accessed 15 July 2020) (in Russian).

United Nations (UN) (2002). Dostizheniya v sfere informatizatsii i telekommunikatsii v kontekste mezhdunarodnoy bezopasnosti [Developments in the Field of Information and Telecommunications in the Context of International Security]. UN General Assembly Resolution A/RES/56/19. Available at: <https://undocs.org/ru/A/RES/56/19> (accessed 15 July 2020) (in Russian).

United Nations (UN) (2005). Gruppya pravitel'stvennykh ekspertov po dostizheniyam v sfere informatizatsii i telekommunikatsiy v kontekste mezhdunarodnoy bezopasnosti. Doklad General'nogo sekretarya [Group of Governmental Experts on Advances in Informatization and Telecommunications in the Context of International Security. Report of the Secretary-General]. Available at: <https://undocs.org/pdf?symbol=ru/A/60/202> (accessed 15 July 2020) (in Russian).

United Nations (UN) (2015b). Dostizheniya v sfere informatizatsii i telekommunikatsii v kontekste mezhdunarodnoy bezopasnosti [Developments in the Field of Information and Telecommunications in the Context of International Security]. UN General Assembly Resolution A/Res/70/237. Available at: <https://undocs.org/ru/A/RES/70/237> (accessed 15 July 2020) (in Russian).

United Nations (UN) (2015a). Gruppya pravitel'stvennykh ekspertov po dostizheniyam v sfere informatizatsii i telekommunikatsiy v kontekste mezhdunarodnoy bezopasnosti. Zapiska General'nogo sekretarya [Group of Governmental Experts on Advances in Informatization and Telecommunications in the Context of International Security. Note by the Secretary-General]. Available at: <https://undocs.org/ru/A/70/174> (accessed 15 July 2020) (in Russian).

United Nations (UN) (2018b). Dostizheniya v sfere informatizatsii i telekommunikatsii v kontekste mezhdunarodnoy bezopasnosti [Developments in the Field of Information and Telecommunications in the Context of

International Security]. UN General Assembly Resolution A/Res/73/27. Available at: http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/73/27&Lang=R (accessed 15 July 2020) (in Russian).

United Nations (UN) (2018a). Pooshchreniye otvetstvennogo povedeniya gosudarstv v kiberprostranstve v kontekste mezhdunarodnoy bezopasnosti [Advancing Responsible State Behaviour in Cyberspace in the Context of International Security]. UN General Assembly Resolution A/Res/73/266. Available at: <https://undocs.org/ru/A/RES/73/266> (accessed 15 July 2020) (in Russian).

Vasilkovsky S.A., Ignatov A.A. (2020). Kontseptsiya tsifrovogo suvereniteta i rol' negosudarstvennykh institutov v sisteme regulirovaniya Interneta [The Concept of Digital Sovereignty and the Role of Non-State Institutions in the Internet Regulation System]. *Vestnik mezhdunarodnykh organizatsiy*, vol. 15, no 4, pp. 196–203. Available at <http://doi.org/10.17323/1996-7845-2020-04-10> (in Russian).

World Economic Forum (WEF) (2020). Burning Planet: Climate Fires and Political Flame Wars Rage. News Release, 15 January. Available at: <https://www.weforum.org/press/2020/01/burning-planet-climate-fires-and-political-flame-wars-rage> (accessed 15 July 2020).

World Trade Organization (WTO) (2017a). Work Programme on E-Commerce: Communication From Australia, Canada, Chile, the European Union, the Republic of Korea, Norway and Paraguay. Available at: https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S009-DP.aspx?language=E&CatalogueIdList=239579,239541,239472,239464,239336,239275,239266,239269,239278,238899&CurrentCatalogueIdIndex=3&FullTextHash=&HasEnglishRecord=True&HasFrenchRecord=True&HasSpanishRecord=true (accessed 15 July 2020).

World Trade Organization (WTO) (2017b). Work Programme on Electronic Commerce: Communication From Bangladesh, Panama and Singapore. Available at: https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S009-HTML.aspx?Id=240761&BoxNumber=3&DocumentPartNumber=1&Language=E&HasEnglishRecord=True&HasFrenchRecord=True&HasSpanishRecord=True&Window=L&PreviewContext=DP&FullTextHash=371857150# (accessed 15 July 2020).

World Trade Organization (WTO) (2017c). Work Programme on E-Commerce: Communication From the Russian Federation. Available at: https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S009-DP.aspx?language=E&CatalogueIdList=239336,239275,239266,239269,239278,238899,238906&CurrentCatalogueIdIndex=3&FullTextHash=371857150&HasEnglishRecord=True&HasFrenchRecord=True&HasSpanishRecord=True (accessed 15 July 2020).

World Trade Organization (WTO) (2017d). The Work Programme on Electronic Commerce: Statement by the African Group. Available at: https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S009-DP.aspx?language=E&CatalogueIdList=239609,239579,239541,239472,239464,239336,239275,239266,239269,239278&CurrentCatalogueIdIndex=0&FullTextHash=&HasEnglishRecord=True&HasFrenchRecord=False&HasSpanishRecord=False (accessed 15 July 2020).

World Trade Organization (WTO) (2017e). New Initiatives on Electronic Commerce, Investment Facilitation and MSMEs. 13 December. Available at: https://www.wto.org/english/news_e/news17_e/minis_13dec17_e.htm (accessed 15 June 2020).

World Trade Organization (WTO) (2018a). Exploratory Work on Electronic Commerce: Non-Paper From Brazil. Available at: <https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/Jobs/GC/176.pdf&Open=True> (accessed 15 July 2020).

World Trade Organization (WTO) (2018b). Work Programme on Electronic Commerce: Moratorium on Customs Duties on Electronic Transmissions: Need for a Re-Think. Communication From India and South Africa. Available at: <https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/WT/GC/W747.pdf&Open=True> (accessed 15 July 2020).

World Trade Organization (WTO) (2019a). Joint Statement on Electronic Commerce: Communication From China. Available at: <https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/INF/ECOM/19.pdf&Open=True> (accessed 15 July 2020).

World Trade Organization (WTO) (2019b). Joint Statement on Electronic Commerce Initiative: Communication From the United States. Available at: <https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/INF/ECOM/5.pdf&Open=True> (accessed 15 July 2020).

World Trade Organization (WTO) (2019c). Work Programme and Moratorium on Electronic Commerce: Communication From Chad on Behalf of the LDC Group. Available at: <https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/WT/GC/W787.pdf> (accessed 15 July 2020).

World Trade Organization (WTO) (2019d). DG Azevêdo Meets Ministers in Davos: Discussions Focus on Reform; Progress on E-Commerce. 25 January. Available at: https://www.wto.org/english/news_e/news19_e/dgra_25jan19_e.htm (accessed 15 June 2020).

World Trade Organization (WTO) (2020). WTO Members Discuss Kazakhstan's Offer to Host 12th Ministerial Conference in June 2021. 29 May. Available at: https://www.wto.org/english/news_e/news20_e/gc_29may20_e.htm (accessed 15 June 2020).

World Trade Organization (WTO) (n. d., a). Briefing Note: Electronic Commerce. Available at: https://www.wto.org/english/thewto_e/minist_e/min11_e/brief_ecom_e.htm (accessed 15 June 2020).

World Trade Organization (WTO) (n. d., b). Trade Topics: Joint Initiatives. Available at: https://docs.wto.org/dol2fe/Pages/FE_Browse/FE_B_009.aspx?TopLevel=10785#/ (accessed 15 June 2020).

Yermakov V.I. (2017) Vystupleniye predstavatelya Rossiyskoy Federatsii v Pervom komitete 72-y sessii General'noy Assamblei OON V.I. Yermakova v ramkakh diskussii po razdelu "Drugiye mery razoruzheniya i mezhdunarodnaya bezopasnost". [Speech by the Representative of the Russian Federation in the First Committee of the 72nd session of the UN General Assembly V.I. Yermakov in the Framework of the Discussion on the Section "Other Measures of Disarmament and International Security". 23 October. Available at: https://russiaun.ru/ru/news/1com_intsec2310 (accessed 15 June 2020) (in Russian).