T20 INDONESIA 2022 THINK

Policy Brief

DEEPFAKES AND SECURITY IN THE INFORMATION ENVIRONMENT: CHALLENGES FOR GOVERNMENTS, SOCIETY, AND BUSINESS

Task Force 2

Meaningful Digital Connectivity, Cyber Security, Empowerment

Andrey G. Ignatyev, Center for Global IT Cooperation, Moscow, Russia
Tatiana A. Kurbatova, Center for Global IT Cooperation, Moscow, Russia

Abstract

This Policy Brief (PB) highlights and examines challenges and impacts of deep manipulated media and texts (known as “deepfakes”, hereinafter referred as DFs) on governments, society, business. Nowadays deepfakes tend to erase the divide between true and false content. Given the nature of Generative-Adversarial Networks (GAN) and other advanced technologies, deepfakes are hardly to be detected. Advances in software and modern digital tools have facilitated the rapid generation, commoditization and proliferation of deepfakes of all types and aims. A priority concern is how to regulate issues related to deepfakes and digital content forgery technology as along with positive aspects, deepfakes can create risks and threats in the financial sphere, social communications, public relations and at the political level as well. PB’s proposal suggests some practical recommendations in three main directions: 1) elaboration of common approaches to development of soft law and regulatory policy instruments to cope with current challenges of deepfakes through launching a global initiative with participation of governments (public institutions), technology companies, digital platforms, and social media, among others. in relation to malicious and harmful deepfakes; 2) intensification of subject matter scientific research, systematization of knowledge and creation of appropriate terminology; and 3) strengthening a dialogue and cooperation with key international organizations.

Challenges

The policy proposal addresses some key challenges.

Combined with the reach and speed of the Internet, a huge number of news channels, social networks and various applications, the creation, distribution, and circulation of deepfakes can reach millions of people relatively quickly. The number of deepfake videos detected up to December 2020 amounts to 85,047 according to Sensity Company Report “The State of Deepfakes 2020: Updates on Statistics and Trends”.

Deepfakes can carry serious risks, the range of which is quite wide. They can pose threats both to an individual or a group of people, and create more serious threats in the information space, affecting national interests. The widespread dissemination of fake and unverified information through online platforms and with manipulation tools, including deepfakes, can be considered as leading to new types of information wars. For instance, there are encrypted chat groups on Telegram that do business. It means that anyone can pay to encrypted chat groups on Telegram to order the creation of custom pornographic deepfakes, including sexualization of children.

Advances in deepfake technology offer many opportunities for a variety of aims both with positive (in art, education, autonomy, medicine, film industry, e-commerce, etc.) or negative consequences. Because of their rapid spread, deepfakes can be used for malicious and criminal aims, for example:

- disinformation;
- distortion and manipulating public opinion;
- political hostility;
- manipulation of election campaigns results;
- violation of intellectual property rights;
- defamation;
- blackmail, hating, bullying;
- harm to childhood: child pornography and other prohibited sexual practices;
- manipulating evidence materials in criminal investigations;
- financial fraud, theft, deception, and many more.

Most of the harm caused by malicious deepfakes relates to various violations and crimes and can be regulated by the legislation in countries, part of the potential harm is not covered by legal acts. Some countries have been taking steps to address the DF threats (e.g., India, China, Singapore, South Korea, USA, UK, Japan, EU). The process of adopting legislative measures in this area by countries is still being implemented rather slowly, this is due to the fact that DF is a multi-level problem and involves many areas, including acute and sensitive issues. In addition, as already noted, possible innovations in legal practice are very difficult to be solved at a technical level.

Deepfakes, as a phenomenon of modern digital opportunities, have become one of today's challenges. To eliminate and minimize today's and tomorrow's risks, "a combination of technology, education, training, and governance is urgently needed".

Below some main threats for governments, business and society are identified:

1. National Security. Deepfake technology can have serious public and national security implications. Deepfake technology allows the public to provide false information in a very credible form, thereby manipulating people's emotions and causing widespread mistrust in society. Political disinformation can also be reinforced and propagated by DFs, and they can be used consciously or unconsciously to generate political dividends, prompting many governments to look for ways to manage such incidents. Deepfakes can have a devastating impact on geopolitics and interstate relations.

Political misinformation threatens the electorate's ability to credibly assess government officials and elect competent leaders. Since the advancement of DF technologies, political elites around the world have been a target of scandals caused by various DFs.

By undermining people's trust in potential and current political figures or state institutions, deepfakes can incite hatred and spread of terrorism.

The range of negative and criminal manifestations of deepfakes is quite wide, and every year new forms and technical possibilities for the development of such practices tend to expand.

2. Judicial system. DF landscape can damage trust in the justice system as evidence in court can be manipulated by DF and affect trial proceedings. The issue of authentication and recognition of digital evidence by prosecutors in judicial practice remains one of the key ones. Problems can arise during cross-examination when one side testifies in the affirmative about the details of a video or other deepfake, while the other side denies its authenticity and content. This may negatively affect court cases due to the additional burden on judges and various experts, in addition, it will require additional financial costs and time to verify evidence. In the context of modern realities associated with the new coronavirus infection Covid-19, many courts have switched to an online format for

hearing cases, which entails additional challenges. Video processing software, including "deepfake" technology, poses problems both for verifying that plaintiffs or witnesses are who they claim to be during a virtual trial, and for parties to claim falsification of any statements and evidence presented in court, including filing various reconsideration claims after the process. Thus, it is very likely that the DF will complicate the work of judges, prosecutors and lawyers, in general, will create overload in legal proceedings.

3. Democracy. DF can be an effective tool for propaganda, various sorts of radicalization of public mood. The use of DF for disinformation poses a threat to democratic mechanisms. Threats of online disinformation, of guarantees for freedom of expression and pluralism in the media, issues of ensuring fair elections take place at an international level. It is necessary to analyze various aspects of the fight against disinformation through content moderation; opinions expressed on a number of challenges related to the spread of disinformation and false information on online platforms and in the global digital ecosystem should also be moderated.

4. *Banking and Financial Systems*. Deepfakes and synthetic media do not pose a serious threat to the stability of the financial system in mature, healthy economies but they can harm individuals, vulnerable businesses and organizations, including government regulators. DF can create certain risks for emerging markets, in some situations and for developed countries experiencing financial crises. Deepfakes can be used to manipulate the market and stocks. For example, a fake video might show to public that the head of a corporation or a bank denies a merger that has occurred or makes claims of financial loss or bankruptcy. The use of video to open accounts remotely for bank customers may be subject to reduced security due to the use of modern DF technologies.

5. Business. Being combined with hacker attacks such as email phishing, deepfakes can be used to cheat companies, which can negatively impact the business climate and negotiations between business partners. DFs can damage the reputation of an enterprise. Also, fraudsters can impersonate high-ranking persons to obtain confidential information or request money.

6. Digital Platforms and Social Media. Social networks have recently started to monitor content to detect possible DF, but they detect only two-thirds of them. Some social media and platforms have officially banned or plan to ban malicious deepfakes on their platforms. These include Facebook, Instagram, Twitter, PornHub, Reddit, Tiktok. Criminals often act anonymously, that makes it difficult for a victim to bring them to justice. That is why platforms can play a crucial role in identifying the perpetrator to help users. In the case of anonymity of users who use malicious DF, it is necessary to consider the possibility of prosecuting a service provider (a site or a platform hosting malicious DFs). Regulation of DFs on large Internet platforms, social networks and other mass resources is needed.

7. *Children and Youth.* Deepfakes can pose a threat to the safety and well-being of children as they intensify cyberbullying and online violence against children on the Internet. Realistic depiction of scenes of aggression, horror, violence, or explicit sexual acts can be harmful to a child's mental health. Deepfake production tools are available to everyone and are quite easy to use. Applications for creating DF are available in smartphones. With the help of such applications, it is possible to carry out destructive actions, both directly involving images of children, and aimed at a children's audience.

For instance, one of the most popular activities for children is to create videos of themselves and post them on various social media. In addition, children are active users of applications that can create a realistic image of a child at an older and mature age from a photo of a child. By uploading their photographs for processing, children provide them to third parties, unconsciously contributing to the creation of vast libraries of content that can be analyzed and used for the production of deepfakes. There have been cases where images of children have been collected and used to create sexualized DFs. The biggest problem with the investigation of such DFs is the difficulty in identifying the children who appear in videos. DFs, as a rule, hide the real face of a child who has been physically abused—without identifying the victim, it is very difficult to identify the perpetrator. There is also a risk that investigators will waste time looking for a child or youth who has not actually been sexually abused.

8. Loss of trust in information. Machine manipulated content can produce an effect of so-called Liar's Dividends. It implies that people can successfully deny the authenticity and express doubts about content that is not actually deepfakes, that is, to doubt, for example, completely realistic videos, images, or texts. It is assumed that the effect of "Liar's Dividend" will continue to arise and progress with the expansion of the scale of proliferation of deepfakes. It is important to note that the spread of deepfakes creates an additional phenomenon that seems to be a serious threat—people have doubts about the authenticity of real videos and thus they would stop trusting any content, assuming that any media can be a deepfake.

Proposals for G20

Legislative measures in this area goes rather slowly, this is due to the fact that DFs is a multi-level problem and involves many areas, including acute and sensitive ones.

The development of machine learning and a synthesis of modern AI techniques are certainly facilitated by the process of rapid improvement of software and hardware. Given the nature of deepfakes, a development of regulation of deepfake technology should be based on research and careful analysis of the relevant processes.

In response to the challenges listed above, we would propose the following policy recommendations and solutions that could support the G20's efforts on developing solutions to reduce cyber security risks and threats caused by the digital era.

All steps on development of approaches to regulatory measures on DFs in T20 initiatives should be based on:

- equal and fair representation of countries in the relevant working international expert group on DFs;
- initiatives should not violate the sovereignty of countries and take into account their national legislative practices, cultural characteristics and traditional values;
- T20 initiatives and possible tools, as well as political decisions on DFs should ensure the interests of all nations, the positions of all actors with the decisive role of state institutions;
- initiatives and decisions should be based on scientific analysis and evidence base, verified statistics and case studies.

The recommendations proposed below do not imply any direct and mandatory regulatory measures or regulatory provisions that should be developed after comprehensive international studies.

Recommendation 1: Development of soft law and regulatory policy instruments

It is necessary to call countries to share their best regulatory practices on DF technologies and contribute to international best practices and instruments to identify reasonable approaches for further policy on deepfakes.

Proposed Solution: The G20 could launch a global initiative with participation of state representatives (public institutions), technology companies, digital platforms, social media, leading experts and other actors and stakeholders with the following goals to:

- monitor and review effective national policies and good practices of digital platforms and social media on DFs;
- develop general approaches to regulation in the area of DFs;
- consider setting up and maintenance an international *DF Register on malicious DFs*;
- provide effective forms of exchange of practices on DF detection;
- consider the possibility to label DFs (where appropriate).

To implement the solution proposed it is necessary to launch a *DF task force (DFTF)* or a *DF Collaborative Network* (with equal representation of all G20 member-countries) to coordinate the initiative proposed. To promote the initiative proposed, the establishment of a *G20 DF Observatory* could be considered. An observatory may also contain useful links to scientific articles and publications in the field of DF.

The modalities and objectives of such a body (group) should be carefully thought through and agreed at a G20 country level. Doing so, the G20 should instruct a proposed task force to monitor the implementation of this initiative to promote international awareness of the proposed task force with a view of raise in awareness of deepfakes and their impact on individuals and society, to informing, advising and encouraging non-members to participate in the G20's work in the field of cooperative investigation and reduction of risks related to deepfakes.

1. At the governance and political levels. The G20 should instruct the task force to develop procedures for the notification and exchange of information among countries on malicious deepfakes to prevent or reduce risks posed by deepfakes for election campaigns, other governance and political processes, among others.

2. At the business level. Effective mechanisms should be put in place to identify harmful deepfakes that can have a financial impact on markets or the performance of exchanges and trading platforms, as well as create a negative environment for business development. Deepfakes should not be used to compete unfairly and suppress competitors in markets. Deepfakes are providing cybercriminals with new sophisticated capabilities to fraud. There is an acute question about the need to provide for strict obligations to use such products strictly for lawful purposes.

3. At the society level. The public should be widely informed about the modern possibilities of using DFs to promote false and misleading information. The citizens' critical thinking should be developed in all possible ways to evaluate different information objectively. Various training programs and tools should be developed to enhance the capacity and skills to distinguish DFs from real and truthful information.

Developers of face-swapping apps and tools should be held accountable for misuse of their products. The safety of children, especially the sexualization of minors, should be in focus of their policies. In order to reduce risks for data privacy and advocate digital skills the G20 should call global platforms and social media to labeling, where appropriate, products in which DFs are used (paying particular attention to DFs, which can be used to manipulate the behavior of users or platform participants).

In the search for approaches to regulating DFs, modern social engineering technologies that are increasing in scale and sophistication should be taken into account. In this context, it could be advisable to focus on three areas:

- social profiling at scale;
- deep voice mimicry;
- deep fake video mimicry (with special mention of “Mouth Mapping” technology).

Recommendation 2: Scientific research, systematization of knowledge and public awareness

Given the impact on governments, society and business, international studies on deepfakes should be an important direction in scientific discourse and a meaningful aspect to which attention should be paid in the development of AI technology in general. In this context the G20 could contribute to better global understanding on deepfakes phenomena and focus on systemizing knowledge on DFs.

In particular, it is advisable to develop and agree for the purposes of the initiative proposed: i) a basic definition of DF; ii) a general classification of deepfakes; iii) other necessary terms and definitions.

Proposed Solution: the 20 should encourage a proposed task force on DFs (DFTF) to:

- develop useful studies, research, articles and scientific publications in a field relevant to DFs;
- strengthen contacts and interaction with national research and development institutions;
- raise the awareness of citizens in the area of deepfakes, promote knowledge and accurate information about the various forms and modalities of DFs in the modern information environment (placing such information in various materials distributed under the auspices of the G20);

- study risks and threats and to identify current challenges related to DFs; to develop a *DF risk map (G20 DFRM)* that is helpful for member states.

Recommendation 3: Dialogue and cooperation with key international organizations

The G20 could give more importance to the international dialogue on DF issues. To that end, it is advisable to recommend including some specific provisions on DFs into various practical instruments of international organizations (in the field of Cybersecurity, Digitalization, AI Development, AI Ethics) in the agendas of international events and meetings.

Proposed Solution: A task force (DFTF) or a collaborative network on DFs should launch a series of consultations with relevant international organizations/forums (UN, OECD, ITU etc.). Such consultations should contribute to the coordination of DF policies and the harmonization of balanced approaches to the issues addressed.

RELEVANCE TO THE G20

Indonesia's G20 presidency focuses its agenda on key pillars among which digital transformation is one of such pillars. Under this pillar, one of the objectives is to strengthen the capacity for nations to prosper. The issue of deepfakes is very relevant and important in the overall context of security in the information environment in 2022.

CONCLUSION

Deepfakes can be considered as one of the most dangerous uses of Artificial Intelligence. They can promote spread of misinformation and be a trigger of new schemes of crime, information wars as they tend to erase the divide between true and false content. With the development of technology and related applications, DF creation becomes available to a wide range of people, including perpetrators, abusers and criminals as well. The key problem is that given the nature of GANs and other digital content forgery technologies, DFs are hardly detected. Now we have not been able to fully recognize and realize all threats that the DF can pose in the future so far.

The G20 is best positioned to assume a leadership role in coordinating efforts among multiple stakeholders to promote greater awareness in need to elaborate common approaches to development of soft law and regulatory policy instruments to cope with current challenges of deepfakes through launching a global initiative with participation of

governments (public institutions), technology companies, digital platforms, and social media, among others. The efforts of the G20 could be directed to three main areas: collection of statistics on DFs, enriching the scientific knowledge, drawing up a risk map and rise in public awareness; creation of detection tools; regulation at any stage of DF creation and use.

The G20 should call countries to develop a more globally coordinated and holistic approach to DFs within the context of their increase in accessibility and widespread deployment in recent years and DFs impact on crime (e.g., put up barriers to spread of DFs related to sexual abuse and exploitation of children on the Internet and to other forms of sexualization of children). As one of priority steps the G20 could take measures in relation to malicious and harmful deepfakes to intensify subject matter scientific research and useful publications, systematize knowledge and creation of evidence base and appropriate terminology; and to strengthen a dialogue and cooperation with key international organizations. Based on these measures, the G20 in cooperation with other international actors could move toward a step-by-step development of balanced and effective DF-regulatory tools for the benefit of all nations and ethnic groups, for protection and prosperity of all people around the world.

References

Lesher, M., H. Pawelec and A. Desai , "Disentangling untruths online: Creators, spreaders and how to stop them", Going Digital Toolkit Note, No. 23, p. 8, footnote 3, 2022, https://goingdigital.oecd.org/data/notes/No23_ToolkitNote_UntruthsOnline.pdf

Thanh Thi Nguyen, Cuong M. Nguyen, Dung Tien Nguyen, Thanh Nguyen and Saeid Nahavandi, Survey: Deep Learning for Deepfakes Creation and Detection, School of Information Technology, Deakin University, Victoria, Australia, School of Engineering, Deakin University, Victoria, Australia, Institute for Intelligent Systems Research and Innovation, Deakin University, Australia, 2020, https://www.academia.edu/40447359/Deep_Learning_for_Deepfakes_Creation_and_Detection_A_Survey

Danielle K. Citron & Robert Chesney, Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security, 107 California Law Review 1753, 2019, https://scholarship.law.bu.edu/faculty_scholarship/640

Sensity Company, Report: The State of Deepfakes 2020: Updates on Statistics and Trends, 2021, https://sensity.ai/reports/

Delloitte, Future of risk in the digital era. Transformative change. Disruptive risk, us-rfa-future-of-risk-in-the-digital-era-report.pdf

Stamatis Karnouskos, Artificial Intelligence in Digital Media: The Era of Deepfakes, IEEE Transactions on Technology and Society, Vol. 1, No. 3, September 2020, p.138

Danielle K. Citron & Robert Chesney, Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security, 107 California Law Review 1753, 2019, https://scholarship.law.bu.edu/faculty_scholarship/640

Matt Reynolds, Courts and lawyers struggle with growing prevalence of deepfakes, 2020, https://www.abajournal.com/web/article/courts-and-lawyers-struggle-with-growing-prevalence-of-deepfakes

Will Knight, Deepfakes Aren't Very Good. Nor Are the Tools to Detect Them, 2020, https://www.wired.com/story/deepfakes-not-very-good-nor-tools-detect/

Nick Statt, Thieves are now using AI deepfakes to trick companies into sending them money. So AI crimes are a thing now, 2019, https://www.theverge.com/2019/9/5/20851248/deepfakes-ai-fake-audio-phone-calls-thieves-trick-companies-stealing-money

Mika Westerlund, The Emergence of Deepfake Technology, Technology Innovation Management Review, 2019, https://www.proquest.com/docview/2329154005

Will Knight, Deepfakes Aren't Very Good. Nor Are the Tools to Detect Them, 2020, https://www.wired.com/story/deepfakes-not-very-good-nor-tools-detect/

Jon Bateman, Deepfakes and Synthetic Media in the Financial System: Assessing Threat Scenarios, Carnegie Endowment, 2020,

https://carnegieendowment.org/2020/07/08/deepfakes-and-synthetic-media-in-financial-system-assessing-threat-scenarios-pub-82237

Eelmaa, Simone, Sexualization of Children in Deepfakes and Hentai: Examining Reddit User Views, 2021, https://osf.io/preprints/socarxiv/6wuhj/

Cristian Vaccari, Andrew Chadwick, Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News, Social Media + Society, 2020, https://journals.sagepub.com/doi/pdf/10.1177/2056305120903408

Eelmaa, Simone, Sexualization of Children in Deepfakes and Hentai: Examining Reddit User Views, 2021, https://osf.io/preprints/socarxiv/6wuhj

Claire Wardle, This Video May Not Be Real, 2019, https://www.nytimes.com/2019/08/14/opinion/deepfakes-adele-disinformation.html

Emily Czachor, Congressional Candidate's Tweet Calling Floyd's Death a 'Deepfake' Removed, 2020, https://www.newsweek.com/congressional-candidates-tweet-calling-floyds-death-deepfake-removed-1512916

Darren Thomson, Social Engineering Blurring reality and fake: A guide for the insurance professional, CyberCube, 2020, https://insights.cybcube.com/social-engineering-cybercube-report

Indonesia's G20 Presidency: Priority issues, https://g20.org/g20-presidency-of-indonesia/

International Telecommunication Union: Members, https://www.itu.int/en/ITU-D/MembersPartners/Pages/Members/members.aspx?Type=U

Youth Russian Internet Governance Forum, https://youth.rigf.ru/en#conf

BIBLIOGRAPHY

Edson C. Tandoc Jr., Zheng Wei Lim and Richard Ling, DEFINING "FAKE NEWS", Digital Journalism, 2017, https://www.tandfonline.com/doi/full/10.1080/21670811.2017.1360143

Ibrahim Mammadzada "Deepfakes and freedom of expression: European perspective", Tallinn University of Technology School of Business and Governance

Jan Kietzmann, Deepfakes: Trick or Treat?, Gustavson School of Business University of Victoria, Canada, https://core.ac.uk/download/pdf/250590695.pdf

Johannes Tammekänd, John Thomas, and Kristjan Peterson, Deepfakes 2020: The Tipping Point, Sentinel, 2020, https://thesentinel.ai/media/Deepfakes%202020:%20The%20Tipping%20Point,%20Sentinel.pdf

John Wojewidka, The deepfake threat to face biometrics, Biometric Technology Today, vol. 2020, no. 2, pp. 5-7., https://www.researchgate.net/publication/339321149_The_deepfake_threat_to_face_biometrics

Kertysova, Katerina, Artificial Intelligence and Disinformation: How AI changes the way disinformation is produced, disseminated, and can be countered, Security and Human Rights in Monitor, p. 11., 2019, https://www.shrmonitor.org/assets/uploads/2019/11/SHRM-Kertysova.pdf

Lyu, S., Detecting 'deepfake' videos in the blink of an eye, The Conversation, 2018, http://theconversation.com/detecting-deepfake-videos-in-the-blink-of-an-eye-101072

Paul G. Allen, Defending Against Neural Fake News, School of Computer Science and Engineering, University of Washington, Allen Institute for Artificial Intelligence, 2019, https://proceedings.neurips.cc/paper/2019/file/3e9f0fc9b2f89e043bc6233994dfcf76-Paper.pdf

Rashid, Md Mamunur, Lee, Suk-Hwan, Kwon, Ki-Ryong, Blockchain Technology for Combating Deepfake and Protect Video/Image Integrity, Journal of Korea Multimedia Society Vol. 24, No. 8, p. 1044-1058, 2021, https://doi.org/10.9717/kmms.2021.24.8.1044

Shadrack Awah Buo, The Emerging Threats of Deepfake Attacks and Countermeasures, Department of Computing & Informatics Bournemouth University, UK, 2020, https://arxiv.org/ftp/arxiv/papers/2012/2012.07989.pdf

Tim Hwang, Deepfakes: A Grounded Threat Assessment, 2020, https://cset.georgetown.edu/publication/deepfakes-a-grounded-threat-assessment/

References

ANO «Center for Global IT-Cooperation» (CGITC) was created in 2020 for the international expert study of global cooperation between Russia and the international community in the field of information technology (IT), as well as the promotion of new approaches to multilateral Internet governance.

CGITC is a member of the Telecommunication Development Sector (ITU-D) of the International Telecommunication Union. Moreover, it is a participant of the international Internet Governance Forum (IGF), co-organizer of the annual Russian Internet Governance Forum and a key organizer of the annual Youth Russian Internet Governance Forum.

The Center works with a pool of Russian and international experts to develop new approaches in the field of global IT-cooperation, conduct research and implement projects in the field of digital literacy, popularize scientific and technological cooperation, develop the international legal framework for the international Internet governance, as well as through the received contacts and with the assistance of all interested experts in Russia and abroad to conduct a number of scientific and expert round tables, conferences and webinars.

In December 2021, ANO «Center for Global IT-Cooperation» (https://cgitc.ru/en/) conducted the analytical research “Deepfakes in the Digital Environment: Main International Approaches”.

About the Authors

Andrey G. Ignatyev, Center for Global IT Cooperation (CGITC), Moscow (Russia), email: andrey.ignatyev@cgitc.ru

Andrey G. Ignatyev worked on trade and economic issues in Russia and abroad, since 2010 he was involved in international cooperation in the field of digital economy at the Russian Ministry of Economic Development. He is currently Head of Analytics at CGITC, member of AIGO expert group (OECD), expert in ISO/IEC JTC 1/SC 42 Artificial Intelligence, member of National Technical Committee 164 «Artificial Intelligence», researcher in AI Master's degree at MGIMO University, author of publications on regulation and ethics in the field of AI.

Tatiana A. Kurbatova, Center for Global IT Cooperation (CGITC), Moscow (Russia), email: tatiana.kurbatova@cgitc.ru

Tatiana A. Kurbatova, a senior analyst at CGITC, worked on trade and economic issues at the Russian Ministry of Economic Development, Russian Federal Antimonopoly Service. Since 2015, involved in international cooperation in the field of digital economy at the Ministry of Economic Development. She is a researcher on international cooperation and a co-author of publications on international organizations and institutions.