ISSN 2949-2483

Volume 2 Number 4

JOURNAL OF DIGITAL TECHNOLOGIES AND LAW

2024

ELECTRONIC SCIENTIFIC AND PRACTICAL JOURNAL

JOURNAL OF DIGITAL TECHNOLOGIES AND LAW
Volume 2, No. 4
2024
DOI: 10.21202/2949-2483.2024.4
ELECTRONIC SCIENTIFIC AND PRACTICAL JOURNAL
eISSN 2949-2483
Published since 2023, frequency – 4 issues a year. DOI: 10.21202/2949-2483

Editorial Board

Chief editor

Ildar R. Begishev – Dr. Sci. (Law), Associate Professor, Honored Lawyer of the Republic of Tatarstan, Chief Researcher of the Institute of Digital Technologies and Law, Professor, Department of Criminal Law and Procedure, Kazan Innovative University named after V. G. Timiryasov (Kazan, Russian Federation)

Editor-in-chief

Anna K. Zharova – Dr. Sci. (Law), Associate Professor, Director of the Center for Cyberspace Research, Associate member of the International scientific-educational Center "UNESCO Chair on Copyright, Neighboring, Cultural and Information Rights", National Research University Higher School of Economics, Senior Researcher of the Institute of State and Law, Russian Academy of Sciences (Moscow, Russian Federation)

Deputy editors-in-chief

Elizaveta A. Gromova – Dr. Sci. (Law), Associate Professor, Deputy Director of the Law Institute on international activity, Associate Professor, Department of Entrepreneurial, Competition and Environmental Law, South Ural State University (national research university) (Chelyabinsk, Russian Federation)

Maksim V. Zaloilo – Cand. Sci. (Law), Leading Researcher, Department of the Theory of Law and Interdisciplinary Research of Legislation, Institute of Legislation and Comparative Law under the Government of the Russian Federation (Moscow, Russian Federation)

Irina A. Filipova – Cand. Sci. (Law), Associate Professor, Associate Professor, Department of Labor Law and Environmental Law, National Research Lobachevsky State University of Nizhny Novgorod (Nizhniy Novgorod, Russian Federation)

Albina A. Shutova – Cand. Sci. (Law), Senior Researcher of the Institute of Digital Technologies and Law, Associate Professor, Department of Criminal Law and Procedure, Kazan Innovative University named after V. G. Timiryasov (Kazan, Russian Federation)

Editorial

Head of the editorial office – Gulnaz Ya. Darchinova
Executive editor – Oksana A. Aymurzaeva
Executive secretary – Svetlana Z. Valiullina
Editor – Gulnara A. Tarasova
Technical editor – Svetlana A. Karimova
Designer – Gulnara I. Zagretdinova
Translator – Elena N. Belyaeva, Cand. Sci. (Pedagogy), member of the Guild of Translators and Interpreters of the Republic of Tatarstan
Specialist in the promotion of the journal on the internet – Polina S. Gulyaeva

Address: 42 Moskovskaya Str., 420111 Kazan, Russian Federation
Tel.: +7 (843) 231-92-90
Fax: +7 (843) 292-61-59
E-mail: lawjournal@ieml.ru
Website: https://www.lawjournal.digital
Telegram: https://t.me/JournalDTL_world
VKontakte: https://vk.com/JournalDTL
Yandex.Dzen: https://dzen.ru/JournalDTL
Odnoklassniki: https://ok.ru/JournalDTL

Founder and publisher of the Journal

Kazan Innovative University named after V. G. Timiryasov. Address: 42 Moskovskaya Str., 420111 Kazan, Republic of Tatarstan, Russian Federation. Tel.: +7 (843) 231-92-90. Fax: +7 (843) 292-61-59. E-mail: info@ieml.ru. Website: https://ieml.ru

© Kazan Innovative University named after V. G. Timiryasov, compilation and formatting, 2024.

Certificate on registering a mass medium: EL no. FS 77-84090 of 21.10.2022, issued by Roskomnadzor.
Territory of distribution: Russian Federation, foreign countries.

The articles are Open Access, distributed under the terms of the Creative Commons Attribution license 4.0 International (CC BY 4.0) (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted re-use, distribution and reproduction, provided the original article is properly cited.

When citing any materials of the Journal, reference is mandatory. The authors are responsible for the verity of the facts stated in articles. The opinions expressed in the articles may not be shared by the Editorial Board and do not impose any obligations on it.

Age classification: Information products for persons over 16 y.o.

Date of signing the issue for publication: 2024, December 13. Hosted on the website https://www.lawjournal.digital: 2024, December 20.

International editors

Daniel Brantes Ferreira – PhD, Professor, AMBRA University (USA), CEO, Brazilian Centre for Mediation and Arbitration (Rio de Janeiro, Brazil)

Chiara Gallese Nobile – PhD, post-doc, Department of Mathematics and Earth Sciences, University of Trieste (Trieste, Italy)

Mohd Hazmi Mohd Rusli – PhD, Associate Professor, Faculty of Shariah and Law, International Islamic University Malaysia (Kuala-Lumpur, Malaysia)

Karuppannan Jaishankar – PhD, Founding Principal Director and Professor of Crime Sciences, International Institute of Crime and Security Sciences (IICSS), (Bengaluru, India)

Jose Antonio Castillo Parilla – PhD in Digital Law (University of Bologna) and PhD in Civil law (University of Granada); Master in New Technologies and Law (University Pablo de Olavide, Seville); Degree in Law (University of Granada), Juan de la Cierva Research Fellow at University of Granada (Spain)

Members of the editorial board

Aleksey A. Efremov – Dr. Sci. (Law), Associate Professor, Professor of the Department of International and Eurasian Law, Voronezh State University (Voronezh, Russian Federation)

Aleksey V. Minbaleyev – Dr. Sci. (Law), Associate Professor, Head of the Department of Informational Law and Digital Technologies, Kutafin Moscow State Law University (Moscow, Russian Federation)

Anatoliy A. Streltsov – Dr. Sci. (Law), Doctor of Engineering, Professor, Honored Researcher of the Russian Federation, Corresponding member of the Academy for Cryptography of the Russian Federation, Leading Researcher of the Center for the Informational Security Issues, Lomonosov Moscow State University (Moscow, Russian Federation)

Anna A. Chebotareva – Dr. Sci. (Law), Associate Professor, Head of the Department of Legal Provision of State Governance and Economy, Russian University of Transport (Moscow, Russian Federation)

Armen Zh. Stepanyan – Cand. Sci. (Law), Associate Professor, Department of Integrational and European Law, Kutafin Moscow State Law University (Moscow, Russian Federation)

Diana D. Bersey – Cand. Sci. (Law), Associate Professor, Associate Professor, Department of Criminal Law and Procedure, North Caucasus Federal University (Stavropol, Russian Federation)

Dmitriy V. Bakhteev – Dr. Sci. (Law), Associate Professor, Department of Criminology, Ural State Law University named after V. F. Yakovlev, Head of CrimLib.info projects group (Ekaterinburg, Russian Federation)

Dmitriy A. Pashentsev – Dr. Sci. (Law), Professor, Honored Figure of Higher Education of the Russian Federation, Chief Researcher, Department of the Theory of Law and Interdisciplinary Research of Legislation, Institute of Legislation and Comparative Law under the Government of the Russian Federation (Moscow, Russian Federation)

Elina L. Sidorenko – Dr. Sci. (Law), Associate Professor, Director of the Center for Digital Economy and Financial Innovations, Professor, Department of Criminal Law, Criminal Procedure and Criminalistics, MGIMO of the Ministry of Foreign Affairs of Russia, CEO of the platform https://забизнес.рф (Moscow, Russian Federation)

Elvira V. Talapina – Dr. Sci. (Law), Doctor of Law (France), Chief Researcher of the Institute of State and Law of the Russian Academy of Sciences, Leading Researcher of the Center for Public Governance Technologies, Russian Presidential Academy of National Economy and Public Administration (Moscow, Russian Federation)

Evgeniy A. Russkevich – Dr. Sci. (Law), Professor, Department of Criminal Law, Kutafin Moscow State Law University (Moscow, Russian Federation)

Gulfiya G. Kamalova – Dr. Sci. (Law), Associate Professor, Head of the Department of Informational Security in Management, Udmurt State University (Izhevsk, Russian Federation)

Karina A. Ponomareva – Dr. Sci. (Law), Leading Researcher, Center for Taxation Policy, Financial Research Institute of the Russian Ministry of Finance, Professor, Department of Public Law, National Research University Higher School of Economics (Moscow, Russian Federation)

Kseniya M. Belikova – Dr. Sci. (Law), Professor, Professor, Department of Business and Corporate Law, Kutafin Moscow State Law University (Moscow, Russian Federation)

Lana L. Arzumanova – Dr. Sci. (Law), Associate Professor, Professor, Department of Financial Law, Kutafin Moscow State Law University (Moscow, Russian Federation)

Lyudmila V. Terentyeva – Dr. Sci. (Law), Associate Professor, Professor of the Department of International Private Law, Kutafin Moscow State Law University (Moscow, Russian Federation)

Maria A. Bazhina – Dr. Sci. (Law), Associate Professor, Associate Professor, Department of Entrepreneurial Law, Ural State Law University named after V.F. Yakovlev (Yekaterinburg, Russian Federation)

Maria A. Egorova – Dr. Sci. (Law), Professor, Head of the Department of International Cooperation, Professor, Department of Competition Law, Kutafin Moscow State Law University (Moscow, Russian Federation)

Marina A. Efremova – Dr. Sci. (Law), Associate Professor, Professor, Department of Criminal-Legal Disciplines, Kazan branch of the Russian State University of Justice (Kazan, Russian Federation)

Marina A. Rozhkova – Dr. Sci. (Law), Chief Researcher, Institute of Legislation and Comparative Law under the Government of the Russian Federation, Dean's Counselor on science, Law Faculty, State Academic University for Humanities, President of IP CLUB (Moscow, Russian Federation)

Mark V. Shugurov – Dr. Sci. (Philosophy), Associate Professor, Professor of the Department of International Law, Saratov State Juridical Academy, Chief Researcher, Altay State University (Saratov, Russian Federation)

Natalya N. Kovaleva – Dr. Sci. (Law), Professor, Head of the Department of Law of Digital Technologies and Biolaw, Faculty of Law, National Research University «Higher School of Economics» (Moscow, Russian Federation)

Roman I. Dremlyuga – Cand. Sci. (Law), Associate Professor, Deputy Director on development of the Institute for Mathematics and computer Technologies, Professor, Academy of Digital Transformation, Far East Federal University (Vladivostok, Russian Federation)

Ruslan A. Budnik – Dr. Sci. (Law), Professor, Deputy Director of the International scientific-educational Center "UNESCO Chair on Copyright, Neighboring, Cultural and Information Rights", National Research University Higher School of Economics (Moscow, Russian Federation)

Sergey A. Petrenko – Dr. Sci. (Engineering), Professor, Professor, Department of Informational Security, Saint Petersburg State Electrotechnical University "LETI" named after V.I. Ulyanov (Lenin), Professor of Innopolis University (Innopolis, Russian Federation)

Svetlana M. Mironova – Dr. Sci. (Law), Associate Professor, Professor of the Department of Financial and Business Law, Volgograd Institute of Management – branch of the Russian Presidential Academy of National Economy and Public Administration (Volgograd, Russian Federation)

Tatyana A. Polyakova – Dr. Sci. (Law), Professor, Honored Lawyer of the Russian Federation, Acting Head of the Section of Informational Law and International Security, Institute of State and Law of the Russian Academy of Sciences (Moscow, Russian Federation)

Tatyana M. Lopatina – Dr. Sci. (Law), Associate Professor, Head of the Department of Criminal-Legal Disciplines, Smolensk State University (Smolensk, Russian Federation)

Kirill L. Tomashevski – Dr. Sci. (Law), Professor, Deputy Dean of the Faculty of Law for Research, Professor of the Department of Civil and Business Law of Kazan Innovative University named after V.G. Timiryasov (Kazan, Russian Federation)

Valentina P. Talimonchik – Dr. Sci. (Law), Associate Professor, Professor of the Department of General Theoretical Legal Disciplines, North-West branch of the Russian State University of Justice (Saint Petersburg, Russia)

Viktor B. Naumov – Dr. Sci. (Law), Chief Researcher, Section of Informational Law and International Security, Institute of State and Law of the Russian Academy of Sciences (Saint Petersburg, Russian Federation)

Yuliya S. Kharitonova – Dr. Sci. (Law), Professor, Head of the Center for Legal Research of Artificial Intelligence and Digital Economy, Professor of the Department of Entrepreneurial Law, Lomonosov Moscow State University (Moscow, Russian Federation)

Zarina I. Khisamova – Cand. Sci. (Law), Head of the Department for planning and coordination of scientific activity of the Scientific-research Division, Krasnodar University of the Russian Ministry of Internal Affairs (Krasnodar, Russian Federation)

Foreign members of the editorial board

Aleksei Gudkov – PhD (Law), Senior Lecturer, Tashkent Westminster University (Tashkent, Uzbekistan)

Andrew Dahdal – PhD, Associate Professor, College of Law, Qatar University (Doha, Qatar)

Aysan Ahmet Faruk – PhD, Professor and Program Coordinator of Islamic Finance and Economy, Hamad Bin Khalifa University, Qatar Foundation (Doha, Qatar)

Awang Muhammad Nizam – PhD, Professor, Faculty of Shariah and Law, University Sains Islam Malaysia (Negeri Sembilan, Malaysia)

Baurzhan Rakhmetov – PhD, Assistant Professor, International School of Economics KazGUU (Nur-Sultan, Kazakhstan)

Christopher Chao-hung Chen – PhD, Associate Professor of Law, National Taiwan University (Taipei City, Taiwan)

Daud Mahyuddin – PhD, Associate Professor, Department of Civil Law, International Islamic University of Malaysia (Kuala Lumpur, Malaysia)

Danielle Mendes Thame Denny – PhD, Researcher, Asia-Pacific Centre for Environmental Law, National University of Singapore (Singapore, Singapore Republic)

Denisa Kera Reshef – PhD, Lecturer, Centre for Distributed Ledger Technologies, University of Malta (Msida, Malta)

Douglas Castro – PhD, Professor of International Law, School of Law, Lanzhou University (Lanzhou, China)

Edvardas Juchnevicius – Dr. habil., Professor, Department of Financial Law, University of Gdańsk (Gdańsk, Poland)

Gabor Melypataki – PhD, Professor, Department of Agrarian and Labor Law, University of Miskolc (Miskolc, Hungary)

Gergana Varbanova – PhD, Associate Professor, University of Economics (Varna, Bulgaria), University of World Economy (Sofia, Bulgaria)

Gosztonyi Gergely – Dr. habil., PhD, Associate Professor, Department of History of Hungarian State and Law, Eötvös Loránd University (Budapest, Hungary)

Iryna Shakhnouskaya – PhD (Law), Head of the Department of Constitutional Law and Public Administration, Polotsk State University (Novopolotsk, Belarus)

Ivanc Tjasa – PhD, Associate Professor, Department of Civil, International Private and Comparative Law, University of Maribor (Maribor, Slovenia)

Ioannis Revolidis – PhD, Lecturer, Department of Media, Communication and Technology Law, University of Malta (Msida, Malta)

Jayanta Gosh – PhD, Research Fellow, West Bengal National University of Juridical Sciences (Kolkata, India)

Joshua Ellul – PhD, Director of the Centre for Distributed Ledger Technologies, University of Malta (Msida, Malta)

Juliano Souza de Albuquerque Maranhão – PhD, Associate Professor, Faculty of Law, University of São Paulo (São Paulo, Brasil)

Kamshad Mohsin – PhD, Assistant Professor, Faculty of Law, Maharishi University of Information Technology (Maharishi, India)

Karim Ridoan – PhD, Lecturer, Department of Business and Tax Law, Monash University (Sunway, Malaysia)

Maria Ablameyko – PhD (Law), Associate Professor, Associate Professor, Department of Constitutional Law, Belarusian State University (Minsk, Belarus)

Mehrdad Rayejian Asli – PhD, Professor, Institute for Research and Development in Humanities, Assistant Professor, UNESCO Chair for Human Rights, Peace and Democracy, Deputy of Research, Allame Tabatabaei University (Tehran, Iran)

Mensur Morina – PhD, Associate Professor, Vice Dean, Faculty of Law, University for Business and Technology (Pristina, Kosovo)

Mokhinur Bakhramova – PhD, Senior Lecturer, Department of the Intellectual Property, Tashkent State Law University (Tashkent, Uzbekistan)

Muhammad Nuruddeen – PhD, Senior Lecturer, Department of Public Law, Bayero University, (Kano, Nigeria)

Niteesh Kumar Upadhyay – Doctor of Law, Associate Professor, Faculty of Law, Galgotias University (Greater Noida, India)

Noor Ashikin Basarudin – PhD (Law), Senior Lecturer, MARA University of Technology (Sintok, Malaysia)

Pablo Banchio – PhD, Professor at the University of Buenos Aires, Postdoc in fundamental Principles and Human Rights, Member of the Centre for Private law, National Academy of Science (Buenos Aires, Argentina)

Pavlos Kipouras – PhD, Professor, School of Forensic Graphology (Naples, Italy)

Prayudi Yudi – PhD, Professor, Department of Computer Science and Electronics, Universitas Gadjah Mada, (Bulakumsur, Indonesia)

Serikbek Murataev – PhD (Law), Head of the Department of Theory of State and Law, Tashkent State University of Law (Tashkent, Uzbekistan)

Stevan Gostojić – PhD, Associate Professor, Head of Digital Forensics Laboratory, Faculty of Technical Sciences, University of Novi Sad (Novi Sad, Serbia)

Tatjana Jovanic – PhD, Associate Professor, Faculty of Law, University of Belgrade (Belgrade, Serbia)

Tran Van Nam – Doctor of Law, Associate Professor and Dean, Faculty of Law, National Economics University (Hanoi, Vietnam)

Wan Rosalili Wan Rosli – PhD, Lecturer at School of Law, University of Bradford (Bradford, United Kingdom)

Woodrow Barfield – PhD, JD, LLM, Visiting Professor, University of Turin (Turin, Italy)

JOURNAL OF DIGITAL TECHNOLOGIES AND LAW
Volume 2, No. 4
2024
DOI: 10.21202/2949-2483.2024.4
ELECTRONIC SCIENTIFIC AND PRACTICAL JOURNAL
eISSN 2949-2483

Content

Begishev I. R., Zharova A. K., Zaloilo M. V., Filipova I. A., Shutova A. A.
Technological Transformation: Growing Opportunities and Legal Response to Emerging Risks 735

Filipova I. A.
Intelligent Robots, Cyborgs, Genetically Enhanced Individuals, Chimeras: the Future and the Challenges of Law 741

Abdelkarim Y. A.
A Rechtsgutstheorie Lens on the Legal Aspects of the States' Cyber Interest Concept 782

Muparadzi T., & Mukonza R. M.
Prospects for Implementing Digital Technologies in the Administration of Justice in Zimbabwe 802

Ikubanni O. O., Oyebanji A. O., & Oyebade A. A.
Legal Aspects of Granting Subjectivity to Artificial Intelligence: Prospects of Using Robots in Legal Practice in Nigeria 835

Cheong B. Ch.
The Rise of AI Avatars: Legal Personhood, Rights and Liabilities in an Evolving Metaverse 857

Hutson J.
The Evolving Role of Copyright Law in the Age of AI-Generated Works 886

Auwal A. M., & Lazarus S.
Sociological and Criminological Research of Victimization Issues: Preliminary Stage and New Sphere of Cybercrime Categorization 915

Bakhteev D. V., Sosnovikova A. M., Kazenas E. V.
Overcoming Illegal Cross-border Transfer of Personal Data 943

Rahman M. M., & Das T. K.
Countering Cyberattacks: Gaps in International Law and Prospects for Overcoming them 973

Belikova K. M., Dias Martins R., Kazanba E. T.
International Cooperation in Overcoming Digital Inequality: Legal Frameworks, Barriers and Development Parameters 1003

Kolawole A.
Legal Aspects of Personal Data Protection and the Issues of Competition in Digital Marketplaces 1031

Editorial
UDC 34:004
EDN: https://elibrary.ru/acmfll
DOI: https://doi.org/10.21202/jdtl.2024.37

Technological Transformation: Growing Opportunities and Legal Response to Emerging Risks

Ildar R. Begishev
Kazan Innovative University named after V. G. Timiryasov, Kazan, Russia

Anna K. Zharova
National Research University «Higher School of Economics», Moscow, Russia

Maksim V. Zaloilo
Institute of Legislation and Comparative Law under the Government of the Russia, Moscow, Russia

Irina A. Filipova
National Research Lobachevsky State University of Nizhny Novgorod, Nizhniy Novgorod, Russia

Albina A. Shutova
Kazan Innovative University named after V. G. Timiryasov, Kazan, Russia

The development of digital technologies and their increasing introduction into various spheres of life opens up new perspectives for humanity, qualitatively transforming the possibilities and even the daily life of people. Automation of work and routine procedures using technologies such as artificial intelligence, machine learning and the Internet of Things increases their promptness and effectiveness, reduces costs and stimulates the development of new types of services and products. The role of the predictive function of analytical tools based on data processing algorithms is also growing.

The technological imperative will determine the future of humanity for many years to come. At the same time, one cannot but note the potential risks generated by it, which require both the scientific interpretation and the formation of legal solutions to overcome or minimize them.

One of such risks, which is already coming into life, is the deepening of the technological gap. The use of digital advantages is not available to all population groups and regions

This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (CC BY 4.0) (https://creativecommons.org/licenses/by/4.0), which permits unrestricted re-use, distribution and reproduction, provided the original article is properly cited.

of the world. However, the digital inequality, as well as the technological one in general, have an impact on broader socio-economic processes and global development dynamics. It poses problems of ensuring the technological sovereignty of countries as an essential component of state sovereignty, economic growth, innovation activity, and social stability.

In the next issue of our Journal, the reader will find the works of researchers from 13 countries (Bangladesh, Brazil, Egypt, Great Britain, Hong Kong, India, Nigeria, Russia, Singapore, South Africa, the USA, Uzbekistan, and Zimbabwe). The articles are devoted to the problems of overcoming digital inequality, ensuring the cyber interests of states, and countering cybercrime, as well as categorization in the legal space of artificial intelligence (including in the copyright context), automation of legal activities, and development of metaverses.

The first article of the volume is "Intelligent robots, cyborgs, genetically enhanced individuals, chimeras: the future and the challenges of law" (**Irina Filipova (Russia–Uzbekistan)**). The article emphasizes the positive changes in society and law in the context of the digital and biotechnologies' progress, which ensures the transition of society to the next technological order. Along with that, it states the individual, collective and existential risks brought by the emergence of new physical, digital and cyberphysical entities. The cognitive abilities of the latter can be comparable, and in certain parameters even exceed human ones. This allows for a targeted intellectual impact on technologically advanced integrated Society 5.0, the formation of which is inevitable. The reader will be interested by the legal trajectories of the functioning of intelligent robots and virtual personalities formulated in the article. The author also proposes some innovations in the legal status of technologically and genetically enhanced individuals.

The article "The rise of AI avatars: legal personhood, rights and liabilities in an evolving metaverse" (**Ben Chester Cheong (Singapore)**) continues the discussion of the issues of legal personality and the formation of an adequate legal regime for artificial intelligence. The article presents a new perspective on the problem of the legal personality of AI avatars, as well as addresses the issue of responsibility for their actions based on their differentiation into autonomous and creative entities. The scenarios of the future of the metaverse presented in this paper demonstrate the importance of finding a balance between innovation and the well-being of human civilization.

The development of generative artificial intelligence technologies, which we observe in music, literature, visual and other forms of art, expands the horizons of creativity. At the same time, it actualizes the issues of authorship of works created in this way, and the prospects for solving them are defined in the article "The evolving role of copyright law in the age of AI-generated works" (**James Hutson (USA)**). The author proposes a combined adaptive approach, which implies flexible intellectual property norms and the revised concept of authorship in the aspect of sustainable co-creation with artificial intelligence.

The latter is recognized as a creative tool that expands human capabilities and makes a fundamental contribution to the work originality.

Two other articles in this issue belong to the research cycle on the legal regime of artificial intelligence. The first one is devoted to solving the problem of the legal personality of artificial intelligence and the permissibility of using these technologies in legal activity under the Nigerian legislation (**Oluwaseye O. Ikubanni (Nigeria)**, **Aderemi O. Oyebanji (Nigeria)**, **Alade A. Oyebade (Nigeria)**). The proposals for improving the Nigerian legal framework are aimed at ensuring its compliance with the level of digital technologies development both in the country and in the world. The second article, based on a comparative legal study of digitalization of judicial proceedings in the UK, South Africa and Rwanda, presents a promising model of effective transition to digital technologies in the administration of justice in Zimbabwe (**Taurai Muparadzi (Zimbabwe – South Africa**), **Ricky Munyaradzi Mukonza (South Africa)**).

Several articles included in this volume are united by a common theme of legal provision of cybersecurity. One of them defines the applicability of the legitimate interests theory to improve legal mechanisms for protecting national interests in cyberspace (**Yassin Abdalla Abdelkarim (Egypt – United Kingdom)**). Another study in the field of international law (**Mohammad Minhazur Rahman (Bangladesh)**, **Tapos Kumar Das (Bangladesh – Hong Kong)**) is devoted to categorizing cyber attacks in the legal sphere and defining legal measures to counter them. The use of preventive cyber countermeasures by states is conditioned by compliance with the principles of legality, due diligence, and proportionality, while ensuring cybersecurity is linked to observing the right to privacy and freedom of speech. An interdisciplinary sociological and criminological study of victimization as a result of cybercrime (**Aminu Muhammad Auwal (Nigeria)**, **Suleman Lazarus (United Kingdom)**) deserves special attention. It analyzes survey results based on the three-part concept of cybercrime (Tripartite Cybercrime Framework), confirming the gap between the global North and the global South. It allows forming the conceptual gender, inclusive and contextual approaches to developing a national legal policy to counter cybercrime in Nigeria.

Another group of articles is devoted to the issues of personal data protection, which is becoming particularly relevant due to the development of digital technologies. An interdisciplinary research is presented in the article “Overcoming illegal cross-border transfer of personal data” (**Dmitry Bakhteev (Russia)**, **Anna Sosnovikova (Russia)**, **Evgeniy Kazenas (Russia)**). The cross-border transfer of personal data is shown both in historical and legal retrospect (including the genesis of the personal data phenomenon since the French Revolution and its subsequent evolution in the 19th and 20th centuries) and from the comparative legal method perspective (the Russian and international experience of legal regulation is analyzed). The work is complemented by the study of technical and technological aspects of data transmission. It allows shaping a model

to detect cross-border data transmission and make managerial decisions, mediated by the optimization of administrative and criminal legislation and represented by the introduction of specialized technical means for detecting unauthorized cross-border flows of personal data. Another article is devoted to the legal aspects of personal data protection in the context of markets digitalization and increasing digital competition (**Kolawole Afuwape (India)**). It denotes personal data as an integral component of the overall competitive market landscape. Based on an analysis of the digital markets' legal regulation, digital services and data management in the European Union, the author proposes approaches to ensuring data privacy in a digital competitive environment.

The persistent and rapidly deepening digital inequality acts as a barrier to the socio-economic and cultural development of countries, regions and the people inhabiting them. It contributes to the strengthening of the negative effect of the identified problems in the field of digitalization. The problem is aggravated in the countries of the global South, but it is also relevant for Russia. In this regard, readers will undoubtedly be interested in an article devoted to defining the legal foundations, existing barriers and parameters of international cooperation in overcoming digital inequality in the context of the transition from the knowledge economy to the data economy (**Ksenia Belikova (Russia)**, **Dias Rafael (Brazil)**, **Evgeniy Kazanba (Russia)**).

In the two years since its foundation, the Journal has managed to establish international cooperation and work with its foreign ambassadors in difficult foreign policy conditions. This work resulted in the publication of the legal research on digital transformations by authors from various countries. This is how we see the mission of the Journal of Digital Technologies and Law – to increase existing knowledge about digital innovations in law by attracting researchers and practitioners from Russia and other countries interested in discussing the most pressing issues on the digital agenda, to spread scientific achievements and experience, not only filling gaps in understanding and interpreting the technological transformation of law and the legal dimension of digitalization, but also forming peculiar points of growth of new knowledge and ideas about law and digital technologies.

The Journal of Digital Technologies and Law promotes scientific cooperation. In eight volumes of 2023-2024, we published the research results of 58 authors from 38 countries (Australia, Bangladesh, Belarus, Brazil, Bulgaria, Cape Verde, China, Cyprus, the Czech Republic, Denmark, Ecuador, Egypt, France, Great Britain, Greece, Hong Kong, Hungary, India, Iran, Italy, Kazakhstan, Macao, Malaysia, Mali, Morocco, the Netherlands, Nigeria, the Philippines, Portugal, Russia, Singapore, South Africa, Spain, Tanzania, Uganda, the USA, Uzbekistan, and Zimbabwe).

The high interest in the Journal of Digital Technologies and Law and its publications indicates the demand for scientific research and new achievements in this field among representatives of the global scientific community (Fig. 1).

Fig. 1. Geography of the visitors of the Journal of Digital Technologies and Law website (162 countries as of December 20, 2024)

We hope that the current issue of the Journal will attract the attention of a wide range of readers, and the published articles will inspire potential authors who wish to present their promising research achievements and developments in the field of digital technologies and law on the pages of our scientific periodical (Fig. 2).

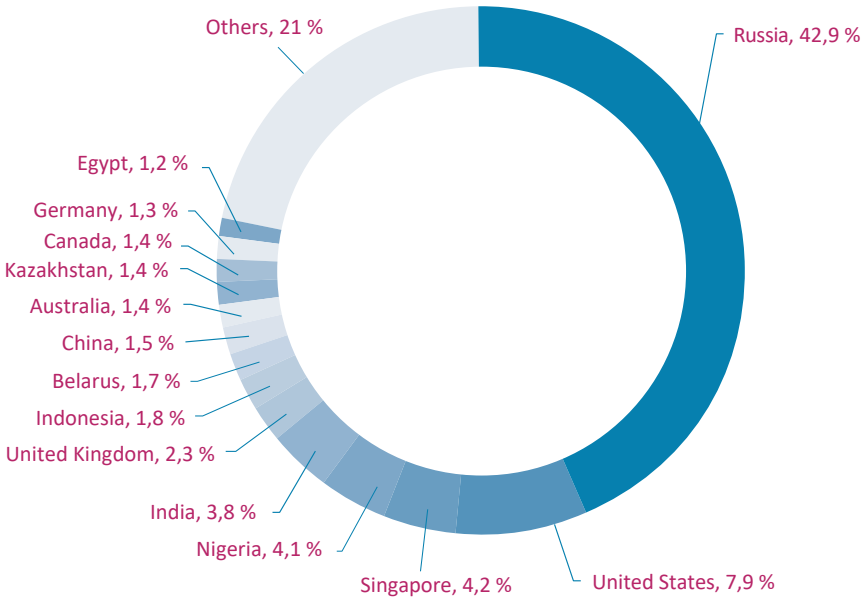


Fig. 2. Statistics of visiting the Journal of Digital Technologies and Law website (as of December 20, 2024)

We hope that in the coming year the international scientific dialogue within the Journal will continue, and new researchers of the problems of interaction between digitalization and law will join the multinational team of its authors – scientists and practicing lawyers, as well as specialists in related fields of knowledge.

We would like to thank the authors, whose articles served as the starting point for scientific discussions and the conceptual foundation for management decisions; the readers, whose inexhaustible interest in the Journal encourages us to move on; the ambassadors, whose activity expands the scope of cooperation with researchers from different parts of the world; the reviewers and members of the editorial board, whose work allows us to maintain a high standard of scientific publications!

Research article
UDC 34:004:342.721:612.6
EDN: https://elibrary.ru/atqzba
DOI: https://doi.org/10.21202/jdtl.2024.38

Intelligent Robots, Cyborgs, Genetically Enhanced Individuals, Chimeras: the Future and the Challenges of Law

Irina A. Filipova

National Research Lobachevsky State University of Nizhni Novgorod, Nizhniy Novgorod, Russia
Samarkand State University named after Sharof Rashidov, Samarkand, Uzbekistan

Keywords

artificial intelligence,
biotechnologies,
cyborg,
digital technologies,
genetic engineering,
human,
law,
neurotechnologies,
risk,
robot

Abstract

Objective: to identify theoretical and legal problems associated with the steadily increasing spread of digital and biotechnologies' development products; to assess the risks associated with this process that can change the position of a human in the society of the future; to develop and substantiate proposals to minimize risks and eliminate the identified problems through legal regulation.

Methods: the research is based on the methods of generalization of scientific and technical information and theoretical analysis used while studying the source materials; axiological and systematic approaches; the formal legal method and, in addition, methods of legal forecasting, primarily extrapolation, which made it possible to highlight the prospects for reforming law due to technological expansion.

Results: include a description of the dynamics of digital and bio-technologies' development; a description of the changing social landscape with the emerging new types of entities that can affect the actual status of a human; a classification of risks threatening people due to the digital and biotechnologies development; a list of tasks whose solution based on law will help to eliminate, postpone or, at least, significantly reduce the severity of problems by increasing the time limit allotted to humanity to comprehend a number of conceptual points. The author presents arguments substantiating the need to develop special legal regulation in relation to new types of entities, the appearance of which becomes an inevitable result of the mentioned technologies' development.

© Filipova I. A., 2024

This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (CC BY 4.0) (https://creativecommons.org/licenses/by/4.0), which permits unrestricted re-use, distribution and reproduction, provided the original article is properly cited.

Scientific novelty: consists, first, in a comprehensive study of the development of interconnected groups of digital and biotechnologies, taking into account their increasing convergence; and, second, in the formulation of legal problems that need to be resolved due to the potential emergence of new types of entities with cognitive functions and capable of having a targeted intellectual impact on the environment and legal entities.

Practical significance: it is present in the answers given to the formulated legal questions, which contain suggestions and recommendations on the necessary adjustment of legal regulation and focus the attention of legal scholars on the problems arising from the pace and vectors of science-consuming technologies' development.

For citation

Filipova, I. A. (2024). Intelligent robots, cyborgs, genetically enhanced individuals, chimeras: the future and the challenges of law. *Journal of Digital Technologies and Law, 2*(4), 741–781. https://doi.org/10.21202/jdtl.2024.38

Contents

Introduction
1. Development and practical application of digital and biotechnologies
  1.1. Development of digital and biotechnologies
    1.1.1. Progress of digital technologies
    1.1.2. Promotion of biotechnologies
  1.2. Results of practical application of digital and biotechnologies
    1.2.1. Intelligent robots
    1.2.2. Cyborgs
    1.2.3. Genetically enhanced individuals
    1.2.4. Chimeras
2. Impact of the results of digital and biotechnologies application on society and law
  2.1. Potential emergence of new participants in public relations
    2.1.1. Intelligent robots
    2.1.2. Cyborgs
    2.1.3. Genetically enhanced individuals
    2.1.4. Chimeras
  2.2. Associated risks of using digital and biotechnologies
    2.2.1. Individual risks
    2.2.2. Collective risks
    2.2.3. Existential risks
  2.3. Legal issues related to the emergence of new types of entities

2.3.1. Legal regime (potential legal status) of intelligent robots
2.3.2. Legal status of cyborgs
2.3.3. Legal status of genetically enhanced individuals
2.3.4. Legal regime (potential legal status) of chimeras
Conclusions
References

Introduction

The development of artificial intelligence is currently being discussed by legal professionals, including from the viewpoint of the possible recognition of the legal subject status for artificial intellectual systems. The latter are a fairly new phenomenon compared to humanity, because Homo sapiens appeared on the planet about 200 thousand years ago. The growing attention to the possible legal personality of artificial intelligence is explained by the high pace of artificial intelligence technologies development and the rapidly expanding dissemination of the results of this development in practice.

As is known, a person can demonstrate cognitive abilities or functions, i. e. the higher functions of the human brain that connect people with the world around them, allowing them to get an idea of it and interact with it. These functions include thinking, speech, learning, spatial orientation, imagination, and memory. Human intelligence manifests itself through cognitive abilities, but artificial intelligence systems also show them. The presence of such abilities provokes a discussion about the recognition of legal personality for artificial intelligence systems, especially if they reach the level of human intelligence.

In addition to improving artificial intelligence and other digital technologies, for example, robotics components, scientific laboratories conduct research aimed at developing biotechnologies. Together with the achievements of digital technologies, it enables connecting people with artificial intelligence systems or purposefully transforming the genetic characteristics of the human body.

The progressive development of digital and biotechnologies will potentially lead to the emergence of new types of entities with cognitive abilities, not inferior or even exceeding the level of those of a modern human. This cannot but cause problems, including problems of a legal nature.

1. Development and practical application of digital and biotechnologies

1.1. Development of digital and biotechnologies

In the context of information society, the key factor in socio-economic development is the transition to the use of so-called high technologies that require the use of scientific knowledge in the creation and production of technically complex products. High-tech sectors of the economy using such technologies have the greatest potential for economic

growth, which attracts public and private investment in this area. The global technology race, in which global technological dominance is at stake, pushes states to create programs aimed at accelerated technology development, and businesses to promptly introduce new technological products.

High technologies include a number of digital technologies based on the digital information and data processing using computers. The term "end-to-end technologies" is often applied to these technologies, which emphasizes their property to complement each other, increasing the useful characteristics of the resulting products. Among the main digital technologies are artificial intelligence systems, wireless communications, virtual and augmented reality, the Internet of Things, etc. Robotics is also mentioned in the list of digital technologies, since the design of robots today is based on "digits"; due to the digital component, the "material part" of robotics is rapidly improving.

In addition to digital technologies per se, biotechnologies can also be attributed to high technologies. They are developing at the junction of biology and technology and testifying to bio-digital convergence. Some biotechnologies are called nature-like because they allow reproducing systems and processes of animate nature in the form of technical systems and technological processes. The biotechnologies discussed below, in theory, can also be called digital, since their development is a consequence of the progress of artificial intelligence technologies, as a result of which computing capacities have appeared, allowing the use of many datasets while reducing the need for manual laboratory research.

While earlier, in the first two decades of the 21st century, researchers mentioned NBIC convergence – the unification and synergetic enhancement of the achievements of nano-, bio-, information and cognitive technologies (Roco & Bainbridge, 2003), now we can stated that digital and biotechnologies have largely absorbed the rest, and now accompany and ensure the transition of society to the next technological order.

1.1.1. Progress of digital technologies

The level of development of digital technologies is significantly increasing every year. This is clearly visible on the example of artificial intelligence technologies as the most important subgroup of digital technologies having a huge impact on all others. Currently, generative artificial intelligence is being actively improved; such artificial intelligence systems can create texts, images, audio and video, and other media data based on generative models. The speed of development of such artificial intelligence can be traced by the product of one of the world leaders in this field – the OpenAI company; the product is ChatGPT. It was only in 2017 that a new neural network architecture, Transformer, was invented, which allowed combining the capabilities of previously existing architectures, for example convolutional and recompetitive neural networks. In 2018, the first ChatGPT model – a neural network trained on a large volume of texts – was created.

A year later, in 2019, the next ChatGPT-2 model appeared, which was a tenfold increase in the previous neural network with a corresponding increase in capabilities. In 2020, the creation of ChatGPT-3 was announced, showing a new level of text processing, and in 2022, ChatGPT-3.5 appeared, which can "draw" through interaction with DALL-E neural network. In 2023, ChatGPT-4 was launched, demonstrating advanced "work" with texts, audio files and images. In May 2024, ChatGPT-4o appeared, capable, among other things, of responding with a human-like voice and simulating emotions. In September 2024, we saw OpenAI o1, showing the ability to "reason" like a human, and the appearance of ChatGPT-5[1] announced in 2025 is linked to the possibility to connect to artificial intelligent agents and to personalization of tasks.

Today, the production of hyperrealistic deepfakes (images, video and audio files created by artificial intelligence, but indistinguishable from those actually filmed or recorded by people) no longer requires a lot of time and other resources. In the legislative bodies of some states, it provoked discussion of bills providing for the labeling of such content in order to avoid misleading people. This is just one example showing the pace of artificial intelligence technologies development. Its vector is aimed at creating a strong artificial intelligence. An intelligent system carrying strong artificial intelligence will have thinking abilities comparable to those of humans, including having artificial "consciousness". One of the key conditions for the acquisition of consciousness by artificial intelligence systems is the ability to carry out multimodal behavior by integrating information from various sensory modalities (text, image, video, sound, etc.) and by "linking" this information to the surrounding reality, constructing full-fledged coherent "images", as humans do. According to the estimates of developers, for example, the founder of SingularityNET B. Goertzel, a computer is expected to reach the computing power of the human brain no later than 2030, and in about 10-15 years one computer can be compared with the computing power of all mankind. A well-known IT researcher and a Nobel Prize winner G. Hinton believes that there are between five and twenty years left before the advent of strong artificial intelligence[2].

The second subgroup, which development level should be described, is robotic technologies. Robotics as a set of technologies includes digital and "material" components, which together ensure the development of automated technical systems and "materialize" the result, based on such fields of science as mechatronics, cybernetics, telemechanics, radio engineering, and materials science. Robotics is based on mechatronics, a complex field of science and technology that primarily includes mechanics and electronics. The progress of electronic components in the "body" of robots, which ensures the integration of digital sensors, processors, actuators and communication modules, allows the robot's "nervous

1 ChatGPT. https://clck.ru/3Eh7aC

2 Artificial intelligence: a ticking bomb or a new stage of evolution? (October 19, 2024). Securitylab.ru https://clck.ru/3Eh7cg

system" to perceive the environment better, choose the most effective solutions and perform complex tasks with extreme accuracy. The development of technical cybernetics increases the ability to control individual robots and their joint group work.

Previously, a robot had a metal shell, bulky and traumatic for humans, then plastics and composites began to be used in the construction of robot "bodies". Their improvement resulted in the robot shell increasingly consisting of soft elastic materials – silicone, vinyl, nylon. Inside robots, there are often hydrogels, which are extremely durable and at the same time capable of changing shape like human muscles; in addition, they ensure an enormous rate of chemical reactions. The use of artificial intelligence in materials science has made it possible to sort through hundreds of millions of elements combinations, accelerating the creation of lightweight and durable materials with new properties. The development of materials technologies, including nanotechnology, has led to the construction of nanobots – artificial systems capable of self-replication, disassembling any material into atoms and using them later as raw materials.

The combination of robotics with artificial intelligence technologies has made it possible to create robots supplemented with artificial intelligence, not only suitable for doing hard work, but also demonstrating cognitive properties, as a result of which the robot becomes a cyberphysical artificial intelligence system.

The next subgroup – virtual and augmented reality technologies – includes digital technologies that make it possible to immerse a person in a virtual world or add digital layers of information to the physical environment. Virtual reality technologies make it possible to plausibly simulate a person's physical environment using VR glasses, helmets, gloves, and other means. Augmented reality technologies "shift" artificial images into a real-world system and display objects that are usually invisible to humans, complementing the physical space with virtual details. The development of these technologies allows for combining the virtual and physical worlds, as well as for people interacting with digital content just like with each other. Thanks to another subgroup of technologies – Internet of Things – physical objects can communicate with each other, being connected to multi-level networks using the Internet and exchanging data without human intervention. Built-in sensors and software for data collection and exchange allow such physical objects to automatically perform certain tasks. Another subgroup of digital technologies contributes to the development of Internet of Things; these are wireless communication technologies that provide very fast, reliable and secure transmission of information using radio waves of various ranges, infrared, optical or laser radiation.

1.1.2. Promotion of biotechnologies

We should also focus on the vast field of biotechnology. The growth rate of the biotechnology market is impressive: the volume of their global market in 2023 amounted to 1.38 trillion US dollars, in 2024 it was estimated at 1.55 trillion dollars, and by 2034

it is expected to reach about 4.61 trillion dollars, increasing by an average of 11.5 % annually[3]. Currently, various areas of biotechnology are rapidly developing: genetic, cellular and tissue engineering, biopharmaceuticals, neurotechnology, etc.

Initially, the term "genetic engineering" referred to various methods of manipulating organisms in order to influence their heredity and reproduction. The term covered genetic modification, artificial selection, in vitro fertilization and cloning. In the second half of the 20th century, the term began to be applied specifically to DNA recombination methods, when, as a result of combining genetic material of at least two species, DNA segments representing new genetic combinations are formed[4]. With the help of genetic engineering methods, it became possible to modify the structure of genes, including creating hybrid genes, i.e. to obtain completely new organisms that had not previously been found in nature. As a result, crops with new properties appeared first (resistant to diseases, saturated with vitamins, with changed color, taste and shape); then gene technologies made it possible to create transparent frogs, featherless birds, luminous cats, etc.[5] Genetic engineering techniques are now used to overcome the limitations associated with organ transplantation, in particular for growing human organs in animals for subsequent transplantation to humans (Brown et al., 2023). Ethical issues are already being discussed, because "as the search for the creation of fully functional, transplantable human organs in large animals progresses", there appears a greater "prospect of creating animals with noticeably human-like brains" (Pluchino & Lombardi, 2024).

Cell engineering technologies differ from the previous subgroup. They allow combining cells of different species and cloning living organisms, and s well as changing them during embryonic development. Similar technologies are also rapidly developing: there are numerous examples of mammalian cloning (Liu et al., 2018). Successful experiments on implanting human cells into animals (Jiang & Alam, 2022) and on obtaining animal embryos with such cells (Tan et al., 2021) help in solving problems related to human diseases. In turn, tissue-engineering technologies, such as bioprinting, make it possible to create biological substitutes that restore, maintain or improve the functions of tissues of a living organism. The aim of tissue engineering is to construct and grow living tissues and organs outside the human or animal body for further transplantation or replacement of damaged tissues or organs. With the help of 3D bioprinting, equivalents of skin, bone and cartilage tissues, and internal organs are obtained.

---

3 Biotechnology Market Size. Share and Trends 2024 to 2034. Precedence Research. https://clck.ru/3Eh7go

4 Genetic Engineering. Britannica. https://clck.ru/3Eh7hU

5 Japanese scientists have developed a unique species of transparent frogs. (October 1, 2007). RBK. https://clck.ru/3Eh7iC; Skripin, V. (May 3, 2013). Wonders of genetic engineering: glow-in-the-dark sheep. Hi-News. https://clck.ru/3Eh7it

Biotechnologies are used not only in working with living organisms (biological systems), but also to connect living organisms with artificial systems so that the former receive additional advantages through the latter. For example, neurotechnologies make it possible to correct or improve the brain functioning by affecting the nervous system and restoring the motor, sensory and cognitive functions of the human or animal body. Neurotechnologies contribute to the development of devices and procedures for monitoring, manipulating and simulating the nervous system functions. The devices measure and analyze chemical and electrical brain signals, can interact with the brain by changing activity, "translating" technical control commands into signals. The most intensively developing areas in neurotechnology today are:

– neuroimaging (serving as the basis for, in particular, magnetic resonance imaging and computed tomography);

– neurostimulation (as transcranial magnetic stimulation, micropolarization);

– neuroimplantation (when neural implants, such as neural chips, act as brain stimulators) and neuroprosthetics (allowing a person to regain lost limbs and the ability to move independently);

– neuromodulation (adding neurochemistry to neural implants).

Neurotechnologies give impetus to combining humans with an artificial intelligence system, clearing the way for the creation of hybrid human-machine intelligence, as demonstrated by tests conducted by Neuralink. A neurochip implanted into the human body and connected to the brain may restore once-lost body functions or add new ones. Neuralink is not the only developer of neural devices in the world leading to the cyborgization of mankind. Government agencies are also engaged in this, for example, the US Defense Advanced Research Projects Agency (DARPA), the European Brain Research Infrastructure (EBRAINS) and a growing number of private corporations (Filipova, 2024).

The sphere of neurotechnology is most closely related to the "digital" sphere in the sense that it not only uses the emerging computing capabilities, but connects living and artificial systems, forming hybrid ones with a dual nature. In other words, neurotechnologies can be attributed in parallel to bio- and digital technologies, maximally reflecting the convergence of both groups.

1.2. Results of practical application of digital and biotechnologies

1.2.1. Intelligent robots

The end product when combining artificial intelligence and robotics technologies is an intelligent robot. The symbiosis of these technologies contributes to bringing both of them to a new level (Gibney, 2024): robots show better and better cognitive abilities, gain greater efficiency, adapt to increasingly complex tasks and environments (Soori et al., 2023). An intelligent robot is a cyber-physical system of non-biological origin with artificial intelligence. At first, robots were created as man-made objects that may

replace a human when performing heavy or dangerous physical work. Modern intelligent robots can not only perform physical work, but also solve creative tasks. Developers strive to improve the following characteristics of intelligent robots:

– autonomy (the ability to act without external control);

– mobility (the ability to move among people);

– interactivity (the ability to interact with the environment using sensors and actuators);

– communication (facilitating communication with a person through computer interfaces, speech recognition and synthesis technologies)[6].

Robots, thanks to artificial intelligence and a strong flexible "body", can look outwardly similar to humans, interact better with them and with each other, as well as solve an expanding list of tasks.

Experts recognize the achieved level of generative artificial intelligence, represented today by Large Language Models, as a serious step towards strong artificial intelligence. The intellectual abilities of multimodal neural network models are improving with an increase in the number of parameters – perceived modalities, including those inaccessible to humans, such as ultrasound or infrared radiation. Model training users huge amounts of data, which a human is physically unable to process. As a result, an artificial intelligent system will be able to achieve impressive superiority over any person in similar activities. Moreover, sometimes artificial intelligent systems exhibit emergent (unexpected) properties, for example, the ability to predict the next words in a human-written text, which requires a deep understanding of the previous text using cognitive skills (Nolfi, 2024).

The development of generative artificial intelligence has influenced the approach to programming robots: "large behavioral models" (or "large content and behavior models") began to be created, following the example of large language models. They make it possible to increase the functionality of robots and make contacts between them and people more convenient (Khandelwal et al., 2024). For example, in 2024 Boston Dynamics and Toyota Research companies joined forces to create a partnership aimed at turning the Atlas robot into a humanoid robot with universal artificial intelligence[7]. They were not alone in this intention; the concept of the Optimus humanoid robot is embodied by Tesla. The company's demonstration videos show that such robots can both perform everyday human tasks (walking a dog, watering flowers, bringing food) and assemble new robots[8]. Another example is the release of Walker S1 humanoid robots by the Chinese UBTech company; they do work previously performed by humans at the world's

6 UNESCO. (2017, September 14). Report of COMEST on Robotics Ethics. SHS/YES/COMEST-10/17/2 REV. https://clck.ru/3Eh7rV

7 Ackerman, E. (2024, October 16). Boston Dynamics and Toyota Research Team Up on Robots. IEEE Spectrum. https://clck.ru/3Eh7sQ

8 AI & Robotics. Tesla. https://clck.ru/3Eh7sw

largest manufacturer of electric vehicles. Such a robot is able to work together with logistic unmanned vehicles and intelligent production systems, which makes it possible to automate entire production facilities[9]. Another example of a humanoid robot is Ameca, developed by the British company Engineered Arts and positioned as the most advanced robot in terms of human imitation; the emphasis is on reproducing human facial expressions and behavior[10]. So far, the humanoid robot looks simplistically like a human body, but due to the success of materials science, the creation of android robots is approaching, which will look less and less different from humans.

As a result, an anthropomorphic robot with strong artificial intelligence will be similar to a human in appearance, physically stronger, while not inferior intellectually, and even surpassing us in a number of parameters. It is worth noting that initially it will be a very expensive item, but the more of them are produced, the faster they will become cheaper. Such an ideal "substitute" for a person is in demand in various fields, for example, in labor sphere. However, there is an obstacle called the Uncanny Valley effect, the essence of which is the emotional reaction of people to the appearance of robots. A humanoid robot that only superficially resembles a human is perceived by people warily. To reduce anxiety it is enough to make the robot more similar to a human. However, "humanization" of the robot improves perception to a certain limit, and then anthropomorphic robots begin to cause sharp dislike and fear due to realistic imitation of humanity with observed minor inconsistencies (Mori et al. al., 2012). This problem will decrease, because, on the one hand, technology will reduce the number of differences visible to humans, and on the other – for new generations of people, the robot environment will become familiar.

The cognitive abilities of an intelligent robot do not depend on the degree of its anthropomorphism. Imitation of a human appearance will fit those people who consider such robots as interlocutors, companions, colleagues (to replace people in contacts), but it is optional.

1.2.2. Cyborgs

As the result of a combination of artificial intelligence and robotics technologies is an intelligent robot, the combination of artificial intelligence and neurotechnology, and, usually, robotics, enables cyborgization of humans. A cyborg (short for "cybernetic organism") can be broadly defined as a biological organism that includes non-biological components. Such components are implants, for example artificial organs, or external attached parts – prostheses designed to replenish lost body fragments. People and animals with bodies including non-biological components appeared long

9 Sinha, S. (2024, October 18). China: Walker S1 humanoid robot starts manual jobs at world's largest EV maker. Interesting Engineering. https://clck.ru/3Eh7vp

10 Ameca. The Future Face of Robotics. Engineered Arts. https://clck.ru/3Eh7wU

before the artificial intelligence, but the previously encountered connection of a living being with artificial objects has now reached a fundamentally new level. The "fusion" of a person with artificial intelligence systems (neuroprostheses or neuroimplants) is becoming more and more perfect, which suggests a growing trend towards cyborgization of the mankind.

Cyborgization elements such as a pacemaker, joint replacements or dental implants do not change human nature. The same is true for "simple" neuroprostheses or neuroimplants, for example, cochlear implants for people with hearing impairments. Modern neural devices are able to improve the quality of life of people with disabilities, making up for the lack of motor, sensory or cognitive functions, the absence of which may be congenital or a consequence of a disease or injury. This refers not only to neuroprostheses of limbs, but also to installing a neurochip under the scalp or directly into the skull to connect it to the brain, thereby creating a brain-computer neurointerface. There are already examples of successful installation of such brain neuroimplants. In 2024, using the example of a 30-year-old man paralyzed in an accident, in whose skull there was a neurochip connected to the brain with electrodes, Neuralink demonstrated the restoration of a paralyzed person's ability to work at a computer. Now he can control the digital cursor on the computer screen, mentally making a movement with his hand using a computer mouse or looking at the cursor and imagining the trajectory of its movement[11].

A Neuralink competitor, Precision, announced the introduction of its first commercial device, a brain neuroimplant, in 2025[12]. This confirms the forecasted increase in the use of neurotechnology products, and not only by people with health problems. Researchers mark a phenomenon: modern man, striving to life longer, is increasingly ready for a radical transformation of their own nature (Popova, 2015). It is likely that, given economic opportunities, organ replacement and enhancement of some cognitive functions that naturally decrease with age will become the choice of a growing number of people. Over time, advances in neurotechnology (and biotechnology in general) will advance human civilization to a state where more and more people will be able to continue living only by becoming cyborgs (Grinin & Grinin, 2016).

Neuroimplants can improve the cognitive functions of a person who has not had health problems, increasing the analytical abilities, enhancing natural intuition by improving memory and processing huge amounts of data previously inaccessible to humans. The interaction of humans and artificial intelligence "forms a new system of thinking, a new cognitive pattern, external to the human mind, but capable

11 Leffer L. 1st Neuralink user describes highs and lows of living with Elon Musk's brain chip, 9 June 2024. https://clck.ru/3Eh7yE

12 Capoot A. Here's what it's like inside the operating room when someone gets a brain implant, 25 May 2024. https://clck.ru/3Eh7yt

of enhancing its cognitive abilities" (Chiriatti et al., 2024). Thus, in the long run, a person who has installed a neuroimplant gets an intellectual advantage over other individuals.

The gradual cyborgization of humanity will be the answer to the problem that people have faced since the beginning of the 21st century: the rapid complication of the reality (physical and mental) in which a person lives, when it becomes increasingly difficult for the brain to master new types of activities and social roles, cope with the information load, interact with complex technical systems. Human adaptation to an environment increasingly shaped by digital technologies will become less and less possible only through the expanded use of technological advances. The successes of neurotechnologies enable putting into practice the fusion of man and machine through the substitution of technologies for the human body and mind's natural functions. The integration of the human body with various mechanisms in order to improve it leads to the emergence of technologically advanced people (Emelin, 2013). One of the obstacles that stood in the way until recently was the reaction of the nervous tissue at the site of injury, characterized by inflammation, which may lead to refusal of the implant (Gulino et al., 2019). To overcome the limitations, fundamentally new biocompatible materials are being developed and tested today (Sharon et al., 2023). According to experts in medicine, within one or one and a half decades, the problem of body traumatization due to a neuroimplant installation will be eliminated.

1.2.3. Genetically enhanced individuals

A genetically enhanced individual is a person with a genome modified by editing technologies. A genome is a collection of hereditary material enclosed in an organism's cell and containing the biological information necessary for its construction and maintenance of viability. Such an improvement can be carried out to treat a certain disease or to prevent the possibility of infection (as a gene therapy). Today, the CRISPR/Cas technique is increasingly used, which allows targeted changes in the DNA of living organisms. This technique is referred to as "molecular scissors", because it allows accurately "cutting" and "inserting" DNA sections. With this technique one may, for example, edit genes to treat hereditary diseases affecting various organ systems. Given that "over 80% of all rare diseases affecting up to 450 million people worldwide have a genetic origin, mainly arising from monogenic mutations", gene modification therapy is "slowly but surely moving towards clinical application" (Citra et al., 2024). Moreover, since gene therapy for adult patients requires enormous costs, and the cost of prenatal therapy is expected to be only a fraction of this amount due to the lower doses required, such therapy will also develop due to economic feasibility. Over the past decade, many clinical trials have been initiated that show "encouraging results", while preclinical studies are extending CRISPR therapy to an increasingly wide range

of diseases every year (Laurent et al., 2024; Morshedzadeh et al., 2024). Continuous improvement and accessibility of genetic sequencing today help to quickly identify immune pathologies, while "advances in gene therapy and bone marrow transplantation have made it possible to treat the diseases that would otherwise be fatal" (Perez, 2022).

An example of using gene technologies is an experiment by a Chinese researcher who edited the human embryo genome to artificially "switch off" the gene responsible for the work of body cells to which the human immunodeficiency virus (HIV) may attach. This procedure made children born from an HIV-infected person immune to the virus[13]. It should be mentioned that such experiments cost the researcher a sentence to three years of imprisonment for an illegal genetic experiment on children. Now these children are several years old, they live a normal life, and the geneticist who returned to work, with the permission of the Chinese authorities, opened three new laboratories to study methods of treating severe genetic diseases such as Duchenne muscular dystrophy and Alzheimer's disease.

In addition to treating or preventing diseases, genome editing can be used to improve metabolism and slow down age-related changes in the human body. The possibility of prolonging life and improving its quality is increasingly mentioned as one of the goals of applying biotechnology. Aging is determined by the end sections of chromosomes (telomeres) that are present in the body since birth. Telomeres gradually shorten, stopping cell renewal, but with the same lifestyle and similar external factors, some people age faster than others, i.e. aging also depends on a hereditary predisposition. This allows genetic engineering to partially correct the situation.

Genetic engineering can also be used to change a person's appearance, improve physical performance, for example, endurance, or to increase mental abilities, including memory (Veit, 2018). Such genetic changes can be inheritable or non-inheritable (Almeida & Diogo, 2019). A geneticist from Harvard University G. Church compiled a list of potential genetic modifications that would be possible due to the development of "gene hacking" technology, allowing DNA to be "rewritten" as a code without extracting stem cells (Goldstein et al., 2019)[14]. Besides protecting against diseases, it includes:

– reducing the need for sleep;
– building muscle mass;
– forming super-solid skeleton bones and joints;
– resistance to radiation;
– possibility of prolonged breath retention;
– improving learning abilities, etc.

---

[13] 田中韻. 収監された中国研究者、「早すぎたが、100％成功」ゲノム編集ベビー. https://clck.ru/3Eh893

[14] Robitzski, D. (2019, December 6). This Harvard Prof Is Listing Genes That Could Make You Superhuman. Futurism. https://clck.ru/3Eh89u

As one can see, genetic engineering technologies can be used not only to treat or prevent dysfunctions, but also to improve the parameters of an organism that does not have harmful genetic mutations, and especially for inherently eugenic manipulations – "breeding" people with improved characteristics compared to natural ones. There will certainly be people who want to gain access to such opportunities and have financial and other resources for this[15], despite attempts by some countries to legally prohibit experiments with human embryos. In addition, it is not possible to "draw an exact demarcation line separating health restoration from body improvement"[16].

1.2.4. Chimeras

Man is the measure in the anthropocentric world that exists today. Digital and biotechnologies are actually "expanding" the society we are used to, which, alongside with people (including technologically and genetically enhanced ones), will increasingly integrate intelligent robots. In addition, the appearance of another group of entities is predicted, which can be conditionally united under the name of "chimeras". Biologists borrowed this term from the ancient Greek mythology; later researchers in the field of artificial intelligence and futurologists started using it, too. Chimeras include:

– "animated" artificial systems – biorobots, partially or completely consisting of organic matter;

– "animated" digital entities – Embodied Virtual Agents.

The chimeras of the first variety began as xenobots – "living robots" created with biotechnology and artificial intelligence and, by the way, capable of a specific method of reproduction – "kinetic replication", previously observed only at the molecular level and never in whole organisms (Kriegman et al., 2021). While early examples of biobots were hybrids of biological cells and inert chemicals supporting them (gels, 3D scaffolds), new biobots can be completely biological, self-constructing and mobile structures created from human cells – anthrobots (Gumuskaya et al., 2024). Thus, we can talk about the future appearance of intelligent biorobots, which, unlike cyborgs, will be not a connection of a human with a cyberphysical artificial intelligence system, but "animated" artificial systems created using advanced biotechnologies.

The second type of chimera is embodied virtual agents, which are already used for interactive assistance to users in virtual space and represent 3D copies of humans or computer characters (Lloyd et al., 2024). A high degree of their realism is achieved through digital modeling using artificial intelligence based on digital or digitized human

[15] Connor, S. (2015, September 18). Gene-editing embryos should be banned to prevent 'genetically-enhanced children', scientists warn. Independent. https://clck.ru/3Eh8Df

[16] Belyaletdinov, R. R. (2017). Risks of modern biotechnologies: philosophical aspects: Cand. Sci. (Philosophy) theses. Moscow: Institute of Philosophy of the Russian Academy of Sciences.

data (these data can be both synthetic and real). All of the above enables achieving a hyperrealistic imitation of the appearance, voice, and other unique psychophysiological or behavioral parameters of a person.

It should be noted that the technological progress pushes for a gradual increase in the proportion of time spent by a person in a virtual environment. With the improvement of artificial intelligence, as well as virtual and augmented reality technologies, virtual "digital personalities" will "grow" from digital imitations of non-existent people or from digital doubles of living or deceased people. The creation of a full-fledged metaverse in the future, representing a permanent virtual space where people can interact with each other and with digital objects through their avatars, will increase the influence of these characters on a person. As a result, artificial "digital personalities", including those with no real prototypes at all, but endowed with their own history and uniqueness, will become an integral part of people's daily lives.

2. Impact of the results of digital and biotechnologies application on society and law

2.1. Potential emergence of new participants in public relations

Participants in public relations are individuals or groups of individuals (persons) interacting about the distribution of tangible and intangible benefits. Relationships may refer to ownership of things, work, the functioning of state institutions, etc. Can new types of entities that appear as a result of the development and practical application of digital and biotechnologies be participants in public relations? In this case, new types of entities are understood as physical, digital and hybrid (cyberphysical) phenomena. Like humans, they must have cognitive abilities, but unlike humans with their physical body and biological nature, they at least either have no physical body, or have a non-biological nature, or their physical body and biological nature have been radically changed artificially.

"One of the most significant consequences of the information technology revolution that occurred at the end of the 20th century was the loss of boundaries between entities such as machines, people and information technology" (de Andrés-Sánchez et al., 2024). The development of digital technologies, as well as biotechnologies, which continued in the 21st century, leads to new types of entities that have "originated" recently, are emerging now or are predicted to appear in the near future. Below we consider each of the types of new entities identified earlier in this article as potential participants in public relations: intelligent robots, cyborgs, genetically enhanced individuals, and chimeras.

2.1.1. Intelligent robots

At the moment, robots, including those augmented with artificial intelligence, are things, i.e. if they are present in public relations, they are not their participants, but objects that people use in relationships. At the same time, increasing the intellectual component of the robot and improving its cyberphysical form lead to the fact that such robots will increasingly replace people in relationships. This applies, in particular, to the labor sphere, where an intelligent robot can take the place of an employee, which is already happening. The share of robots in production is growing every year. Some of them were originally designed as collaborative, i.e. adapted to work among people and together with people. For example, according to the South China Morning Post, about 70% of the work in China's highly automated factories is already done by robots and only the remaining 30% is done by humans. The goal set by the robot manufacturing companies (UBTech) is to reduce human labor by up to 10% by using humanoid robots, "so that the remaining workers focus on higher-level tasks"[17].

Participants in labor relations are employees and employers. The latter, if they run a business, are entrepreneurs interested in increasing profits. When implementing a scenario in which intelligent robots are able to perform any kind of work efficiently and at the same time cost the employer less than human workers, they will try to replace people with robots. So far, robots cannot replace humans everywhere, and it is often unprofitable due to the high price of the robot and the additional costs of its maintenance. Several interrelated factors may affect the change in the situation:

1) artificial intelligence and robotics technologies are being improved;

2) the intelligent robot industry is gaining momentum with the technology development;

3) due to the increase in production volumes, the final cost of an intelligent robot as a product becomes lower;

4) there is an increasing shortage of personnel in the workplace, as some people do not want to take jobs because of their low attractiveness, while others cannot, because they do not have the necessary qualifications and are unable to perform such work.

The fewer people willing or able to take jobs, the stronger the desire of employers to replace people with intelligent robots in order to "forget" about the problems of vacations, illness and maternity leaves, etc. Consequently, the presence of intelligent robots in the labor sphere will grow. According to the 2024 Economics Nobel Prize winner D. Acemoglu, technological changes in production and service sectors are increasingly shifting towards automation "with insufficient emphasis on creating new tasks in which labor can be

[17] Wu, X. (2024, October 17). Humanoid robot could recharge China's manufacturing labour shortage. South China Morning Post Publishers Ltd. https://clck.ru/3Eh8LL

productively used" (Acemoglu & Restrepo, 2020). The negative consequences of such a choice are a stagnating demand for labor and a decreased share of labor in national income.

Strengthening the link "artificial intelligence – neurotechnology" allows "developing" robots predisposed to social interaction (Sandini et al., 2024). Besides proliferating in services (trade, beauty industry, entertainment, etc.), such robots will most likely be used as agents representing people in various relationships. Such intelligent robots will be in demand in the household; moreover, an android robot with artificial intelligence comparable to human intelligence is quite attractive as a companion or partner in personal relationships[18]. The improvement of android robots will cause them to fulfill, among other things, gender roles in society (Karnouskos, 2022). The assumption is based on data reflecting the statistics of demand for intelligent robots designed for personal use, including intimate relationships (Döring et al., 2020; Hanson & Locatelli, 2022). This is confirmed by the growth rate of investments in the industry of making sex dolls with artificial intelligence; Chinese companies already sell tens of thousands of such robots per year. With an increase in the technology level, they will be able not only to replace sexual partners, but also to become life companions with their memory, feelings, character and emotions. According to the developers, in about 20 years, families with a robot as a partner will become quite common[19].

2.1.2. Cyborgs

Unlike intelligent robots, which are considered things, a cyborg is not a thing, but a human combined with an artificial intelligence system. Respectively, a cyborg, if present in public relations, is a subject, not an object from the legal viewpoint.

The tendency to increase the share of cyborgs will clearly manifest itself with technological progress. Some of these technologically enhanced people will appear involuntarily, due to medical solutions to restore body functions or prolong life. Others may appear arbitrarily, due to the desire of technologically tolerant individuals to "upgrade" and, supplementing the natural resource of their body, to acquire capabilities that exceed those of an ordinary person. Such an advantage of cyborgs will interest employers; hence, it will affect the labor sphere. Professional sports, which are "tied" to high results and have already "squeezed" most of the natural physical capabilities of a human to the limit, is another area extremely attractive for cyborgization. A person without health problems who agrees to the installation of neuroimplants can not only achieve better results, but also increase the effectiveness of training, while reducing its duration and frequency, i. e. freeing up time for other activities, not limited to sports.

---

[18] Marriage with a robot – the future of humanity? (August 29, 2022). Leotronics. https://clck.ru/3Eh8So

[19] Cuthbertson, A. (May 25, 2018). Robots will have civil rights by 2045, claims creator of "I will destroy humans" android. The Independent. https://clck.ru/3Eh8Tg

In addition to technological progress, the factors indirectly contributing to cyborgization are:

– digitalization of the world, which gives an additional advantage to people who are able to directly contact electronic devices in terms of the speed of receiving and transmitting information, i.e. adapted to the new technological reality;

– the aging of the world's population due to an increase in life expectancy and a slowdown in natural population growth (over the past 50 years, the growth rate has decreased by about half) [20];

– an increase in the number of people with disabilities due to the aging of the population and the rapid spread of chronic diseases[21];

– increasing the technological tolerance of new generations of people who were born and raised in a technosocial environment and cannot imagine themselves without electronic gadgets.

The technological revolution has motivated people to transform into entities capable of continuously receiving information and transmitting it to the environment (Kadlecová, 2020). This fusion of humans and information is carried out through intelligent technological devices that can be both wearable and implantable (Olarte-Pascual et al., 2021). According to UNICEF, in the next 5-10 years, neural devices designed to monitor and modulate brain and nervous system functions "may become generally accepted for some children of the next generation"[22].

Speaking about cyborgs as people, it should be emphasized that they will increasingly manifest themselves as a separate social group with their own interests. For example, a cyborg's artificial intelligence system receives data from a variety of digital sensors. The information may relate to the surrounding space and is necessary for the correct operation of the neuroprosthesis/neuroimplant. The data received from the external environment relates to the movement of nearby objects, their configuration, and if people appear near the cyborg, the information received from the sensors will include biometric personal data of these people, their psychophysiological reactions. Ultimately, the cyborg's artificial intelligence system acquires access to data that allows predicting the subsequent behavior of other people, assessing their health status, recording what was seen and instantly transferring information via Wi-Fi to external electronic devices.

2.1.3. Genetically enhanced individuals

Genetically enhanced individuals are people, like cyborgs, differing from others. This difference is due not to combining them with an artificial intelligence system, but

---

20 World Bank Group. World Development Indicators. https://clck.ru/3Eh8YL

21 World report on disability. (2011, January 1). Geneva: World Health Organization. https://clck.ru/3Eh8ZS

22 Pauwels, E., & Vosloo, S. (2024, September 27). Neurotechnology is here. It's time we get serious about what that means for children. World Economic Forum. https://clck.ru/3Eh8ZS

to a serious increase in the natural resource of the body due to artificially synthesized and embedded biological components. In the future, such individuals will be able to possess abilities that are not available to all other people. The field of genetic engineering is a priori the most controversial of those considered in this article, since it may be about "growing" people with predetermined characteristics (the task is to "outsmart" evolution). The likelihood of such a development caused noticeable alarm in society at the end of the last century, which led to the development and adoption of laws restricting "playing" with human biology. An example of such a law is the Russian Federal Law of July 5, 1996, No. 86-FZ "On state regulation in the field of genetic engineering"[23]. It is generally prohibitive and restricts the implementation of genetic engineering beyond research and development. At the same time, the Decree of the Russian President dated November 28, 2018, No. 680 "On the development of genetic technologies in the Russian Federation"[24] names as one of the main goals a comprehensive solution to the tasks of accelerated development of gene technologies, including genetic editing technologies, and this signals that such technologies are considered acceptable[25].

The continuation of "shadow" research by some scientists is likely to eventually lead to the emergence of individuals with characteristics and abilities that differ from ordinary people, opening Pandora's box. Such individuals, provided they possess inherently transmitted genetic improvements, will pass on their abilities by inheritance, which will accelerate the emergence of a special social group of genetically improved people, provoking contradictions between the interests of this group and others. For example, the recent pandemic "locked" hundreds of millions of people in their homes; the virus resistance of genetically enhanced individuals would exclude them from this global community of the "locked down". Given that gene technologies may not only protect against certain diseases, but also increase human endurance and give other advantages, the interest in genetically enhanced individuals is also shown by the professional sports industry.

2.1.4. Chimeras

Unlike cyborgs and genetically enhanced individuals, entities of a new type, which can be conditionally united under the name "chimeras", are not people, but represent digital or physical/cyberphysical objects. Biochimeras (biorobots) are not identical in nature

[23] On state regulation in the field of genetic engineering. No. 86-FZ of 05.07.1996. (ed. of No. 643-FZ of 29.12.2022). (2022). Garant. https://clck.ru/3Eh8d5

[24] Decree of the President of the Russian Federation No. 680 of 28.11.2018 (ed. of the Decree of the President of the Russian Federation No. 975 of 29.12.2022). (2022). Garant. https://clck.ru/3Eh8d5

[25] Shcherbakova, A. I. (2023). Legal support for the development and implementation of biotechnologies in the European Union and Russia: Cand. Sci. (Law) thesis. Moscow: MGIMO University.

to intelligent robots, although in theory they can be both hybrid systems (a combination of cyberphysical and artificially grown biological components) and systems created entirely from organic matter. An artistic example of biorobots are replicants from the "Blade Runner" movie. Biorobots are potentially the most successful "substitutes" for people in personal relationships due to their exceptional anthropomorphism. At the same time, the "breeding" of intelligent biorobots still seems, if feasible, then a very remote matter (if a cyberphysical system is responsible for the intelligence of a biorobot, such an entity should be considered an intelligent robot). Therefore, we will focus on the second subspecies of chimeras more likely in the near future – digital chimeras, or virtual personalities, capable of "hatching" from embodied virtual agents with the development of technology.

Virtual personalities will be in demand in the entertainment industry: making films, shows, fashion shows, advertising, and other creative projects. They will be great digital companions and even "educators". Such entities are attractive to employers as a substitute for employees whose work function is not related to physical labor, because embodied virtual agents can function around the clock; they do not need salaries; no permission is needed to use their image or voice. At the same time, their biography, personal qualities and images can be adjusted to the needs of the audience[26]. In the context of building a full-fledged metaverse, digital entities imitating famous people who once lived will become widespread. Already today, embodied virtual agents with elements of artificial intelligence can act as digital imitations of real or fictional personalities. They are trained on digital profiles of people, developing the characteristics of a prototype personality, or on synthesized data to obtain specified characteristics. With the development of artificial intelligence and virtual reality technologies, there is a growing probability of the emergence of strong artificial intelligence virtual systems with hyperrealistic avatars as full-fledged participants in public relations that will flow into cyberspace. The growing portion of personal and business communications in a virtual format will introduce such virtual personalities into the daily communication. On behalf of a real person, they will not only "make purchases, organize trips, make decisions or even analyze memories"[27], but also interact with authorized governing persons (Fontes et al., 2024).

---

[26] Suragina, E., Mimoglyadova, E., Neznamov, A., Kraynov, A., Izraylit, S., Chirva, D., Matsepuro, D., Kuleshov, A., Vorobyov, A., Vorobyov, P., Romanov, I., Markov, N. (2024, April). Ethical recommendations in the field of creating and using digital imitations of living, deceased and non-existent people: presentation. https://clck.ru/3Eh8jz

[27] Berggruen Institute. (July 16, 2024). Digital Personality: Humans and AI. https://clck.ru/3Eh8m3

2.2. Associated risks of using digital and biotechnologies

The emergence of new types of entities (intelligent robots (1), cyborgs (2), genetically enhanced individuals (3) and chimeras (4)) increases the level of uncertainty. Hence, it increases the number and level of risks that can lead to adverse consequences for a person, a group or the whole humanity, i.e. one may detect individual, collective and existential risks critical in terms of possible losses. While individual and collective risks concern a limited number of people, the existential risks arising from the spread of new technologies threaten human civilization as a whole.

2.2.1. Individual risks

The main individual risks, growing with the spread of new types of entities, include:

– the risk of causing physical harm to a person as a result of hacking an artificial intelligence system (1, 2);

– the risk of stress for a person due to the need for direct contact (1, 2);

– the risk of loss of personal data confidentiality (1, 2, 4);

– the risk of using human biomaterials without consent (3).

The risk of causing physical harm to a person due to hacking of the artificial intelligence system by intruders increases with the "inclusion" of intelligent robots in society and their spreading in the labor, healthcare, and household spheres. Moreover, while such a robot appears in the household at a person's will, it appears at work regardless of the employee's desire, which can cause severe stress, thereby creating a psychosocial risk.

Proliferation of digital and cyberphysical entities capable of using digital sensors to "capture" information about the world around them, analyze it and transmit it to other electronic devices leads to the risk of losing personal data confidentiality. With technological development, sensors are becoming cheaper and smaller, some of them the size of nanoparticles. Sensors can be located both on external objects and on the human body or embedded in it. For example, the latter may become necessary to personalize medical procedures that will be much more effective and thanks to which many diseases can be detected and cured at an early stage. Due to the Internet of Things technology, the collection, analysis and transmission of huge amounts of data is possible offline. Even if a person refuses to install sensors on the body, they will still have to live in a "smart" environment – numerous sensors will be located in public places. Given that the capabilities of artificial intelligence systems for searching, processing, analyzing and generating data are many times superior to human ones, artificial intelligence can deanonymize data by accessing various open databases on the Internet.

Due to the development of gene technologies and the "build-up" of genetic improvement of people, there is an increased risk of taking biomaterials of a particular person against one's will, including during medical procedures.

2.2.2. Collective risks

Collective risks are usually associated with some sphere of life activity: labor, education, healthcare, leisure, etc. Among the main collective (group) risks, we shall, first of all, name:

– the risk of segregation of people unable to adapt to the new high-tech reality (2, 3);

– the risk of increasing the intensity of human labor (1, 2, 3, 4);

– the risk of displacement of people from certain fields of activity (1, 2, 3, 4).

In the field of labor, the collective risk due to the introduction of intelligent robots is the loss of work by entire professional groups, displaced by cyberphysical entities with cognitive abilities. In addition to the advantages over people in the amount of information processing and the speed of data analyzing, the new entities will significantly surpass people in endurance; they do not need so much rest in between work, they do not need long sleep to recuperate. Accordingly, when doing similar work, they will be more efficient than people, and this will reduce the employment opportunities of people in the society of the future. Thus, the loss of a person's current position is one of the main consequences of the emergence of new entities in the "era of artificial intelligence", which humanity is now entering.

While an intelligent robot cannot be recognized as an employee under current legislation, a technologically enhanced person (cyborg) has the same right as any other person to take a workplace, from the legal viewpoint. Having the advantages due to the "embedded" artificial intelligence system, cyborg workers will in many cases be more profitable for the employer. This may lead to the actual coercion of other employees to use neural gadgets (neural headphones, neural helmets, etc.) in the workplace.

The sphere of professional sports is at the junction of labor and entertainment. Top-level sports are attractive when sports results are continuously growing, arousing the interest of the audience. Since the natural limit of human physical capabilities is almost exhausted, a logical consequence is the development of sports with the participation of cyborg athletes, whose strength, endurance and coordination can significantly exceed human ones.

The formation of genetically enhanced people as a social group with their own interests will certainly affect the healthcare sector. In this regard, the risks are similar to those arising from cyborgization. The only difference is that the "artificial part" of man and humanity, based on the achievements of biotechnology, will increase. The risks to the labor sphere will again be associated with the displacement of a person without artificial "improvements" and the replacement of a "new kind of people" capable of performing work with greater efficiency due to increased endurance and other previously described advantages for the employer. Professional sports will also be affected by the changes. By now, performance-enhancing substances have become "ubiquitous in many sports, often undermining the spirit of competition" (Momaya et al., 2015). Accordingly, interest in gene doping – a therapy to improve athletic performance – will continue to grow (Ginevičienė et al., 2022).

Chimeras as digital entities with artificial intelligence will also increase the vulnerability of people in the labor sphere. First of all, this concerns the so-called creative industries, where virtual personalities are already filling the scene. The displacement of humans from the film industry, television, shows, fashion industry, advertising threatens a large part of actors and media workers[28] and will over time completely change the creative industries, inexorably reducing the proportion of people employed in them[29].

2.2.3. Existential risks

Below, we will focus on the risks that threaten humanity as a whole, among them:

– the risk of almost complete displacement of people without artificial "improvements" from the labor sphere (1, 2, 3, 4);

– the risk of replacing people with artificial intelligence systems in personal relationships (1, 4);

– the risk of losing human control over their consciousness and behavior (2);

– the risk of dividing humanity into two species (2,3);

– the risk of "losing" in competition to a new kind of people and "extinction" of people who refused to artificially change their nature (1, 2, 3).

The gradual displacement of a person from the labor sphere, their replacement with artificial intelligence and technologically or genetically enhanced people will inevitably lead to the restructuring of the entire socio-economic system, and this can be referred to existential risks. A serious transformation awaits the sphere of personal relationships. The risk is the loss of the inviolability of a human's position as a partner in a personal relationship and the appearance of a "competitor" in the form of an anthropomorphic robot. This will affect the family institution, and since the family is the basic unit of society, it will affect society as a whole, which is irreversibly "turning" towards a posthumanistic future.

Medicine, being rebuilt to meet the needs of technologically and genetically enhanced people, will stimulate further growth in their number and isolation as a social group, with a corresponding increase in the weight of the "voice" of this group in society. The tempting increase in body resources inherent in many representatives of this social group will push other people to increase their "artificial part", setting the direction for the transition of humanity to a new state. Unfortunately, the price for the opportunity to increase the body's natural resource through cyborgization will be "concomitant dependence on artificial intelligence and the potential loss of cognitive autonomy" (Chiriatti et al., 2024).

---

28 Shaw, L. (August 19, 2024). Four Experts Explain How AI Will Change Hollywood. Bloomberg. https://clck.ru/3Eh8rV

29 Whiting, K. (February 28, 2024). This is how AI is impacting – and shaping – the creative industries, according to experts at Davos. World Economic Forum. https://clck.ru/3Eh8s7

Despite the absence of a physical body, digital chimeras, with the advent of strong artificial intelligence and the achievement of a point of technological singularity that finally deprives humanity of the option to "turn off the switch", will be able to gain independence. Taking into account the previously achieved power of influencing people through the media environment, virtual personalities, which by that time would become integral parts of the public administration system, would increase existential risks for humanity. Simplistically, this can be shown by the example of Skynet as a virtual artificial intelligence system in the "Terminator 3: Rise of the Machines" movie.

2.3. Legal issues related to the emergence of new types of entities

As one can see, potential new participants in public relations in the future are either people, but with abilities inaccessible to others, or systems of strong artificial intelligence, connected or unrelated to the physical shell. Human society, having passed along the path from a hunter-gatherer society (Society 1.0) through an agrarian (Society 2.0) and an industrial society (Society 3.0) to a modern information society (Society 4.0), will not stop there and will continue to evolve further. The next stage of development (Society 5.0) will demonstrate at least equally large-scale changes[30]. Given that the 5.0 Society will draw a line under the fourth industrial revolution, it is "no longer science fiction"[31], as the development of digital and biotechnology inevitably leads to it. Society 5.0 is a highly developed and technologically integrated society in which various technologies, primarily artificial intelligence, but also neurotechnologies, the Internet of Things, etc., are used to solve social problems and improve the overall quality of life (Das et al., 2024). Technology is blurring the boundaries between the real world and the digital space, and "technological convergence has fundamental consequences for people" (Helbing & Ienca, 2024). The main features of the Society 5.0 include:

– merging of cyberspace and physical space, when every element of society has a digital counterpart in the cyber environment;

– convergence of knowledge in both natural sciences and the humanities and social sciences, to solve social problems through science and technology;

– further development of human resources.

A whole range of issues arises, including conceptual ones, that cannot be solved without the help of law:

1. How can we ensure that there is no discrimination in Society 5.0 if people who do not have artificial improvements coexist with technologically and genetically enhanced individuals?

---

30 Government of Japan. (December 18, 2015). Report on "The 5th Science and Technology Basic Plan". Council for Science, Technology and Innovation. Cabinet Office. https://clck.ru/3Eh8uk

31 Helbing, D., & Ienca, M. (2024, June). Society 5.0: Is the Internet of Bodies Coming Upon Us? Preprint. https://clck.ru/3Eh8vR

2. Under what conditions may people be technologically or genetically enhanced if they wish to do so, especially if they do not have medical indications?

3. How to prevent interference in the consciousness of a cyborgized person in order to manipulate their behavior?

4. How to ensure the safety of people near a cyborg under the possibility of a cyberattack on the artificial intelligence system it contains?

5. How shall we regulate the procedure for obtaining medical care if the results of genetic improvement have not reached the declared level and additional work is required (on general or extraordinary terms)?

6. Should we distinguish between a person's right to use genetic engineering technologies for positive genetics (improvement of normal functions (Vaughn, 2023)) with and without subsequent inheritance of altered genes?

7. Will the social support measures that people in need are entitled to differ? In particular, this refers to maintenance therapy at the expense of state funds.

8. How can we maintain a balance in the labor sphere between the production efficiency in the interests of business, which is the basis of the economic development of society, and man?

9. Will the employer have the right to prefer a cyborg as an employee, replacing with them a person who previously occupied the workplace, but failed to adapt to new technologies?

10. What should be the position of intelligent robots with strong artificial intelligence, if they can actually replace people in public relations, significantly saving people's finite resources?

The list of questions can be continued; the acuteness of each will increase as we move towards the Society 5.0, signaling the need to reconfigure the regulatory landscape. Symptomatic is the increase in the number of bills that fit into this topic and are submitted for consideration in parliaments around the world. The first laws have been adopted concerning the use of artificial intelligence technologies (the European Union Regulation establishing harmonized rules on artificial intelligence, or the Artificial Intelligence Act, dated June 13, 2024)[32] and neurotechnologies (Law No. 21383 of October 14, 2021 on amendments to the Chilean Constitution related to the recognition of neural rights)[33]. Based on the latter, the first court decision on the protection of neuroprivacy has been made in Chile. This is the decision of the Supreme Court of Chile No. 1.080–2020 of August 9, 2023, which protected the right to mental

[32] European Union. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). https://clck.ru/3Eh947

[33] Ley 21383. (October 25, 2021). Modifica la carta fundamental, para establecer el desarrollo científico y tecnológico al servicio de las personas. Biblioteca del Congreso Nacional de Chile. https://clck.ru/3Eh958

integrity of a person based on a constitutional protection lawsuit filed against Emotiv Inc. (USA). The company commercializes neural devices that collect, among other things, data on the electrical activity of the brain (Cornejo-Plaza et al., 2024).

Rapidly developing technologies are changing reality so quickly and profoundly that such lawmaking, although it has some advantages, raises new problems due to the lack of theoretical tools. Sometimes the rules established by law become outdated even before they come into force, simply because a new field appears, as happened with generative artificial intelligence. "To avoid repeating the same mistakes, the discussion of the future law on cyborgs should begin today", because "the law regulating the symbiosis of man and machine will become the main problem in the second half of the 21st century" (Księżak, 2024). This statement is valid not only for cyborgs, but also for the other types of entities mentioned above.

With the development of new technologies, two opposing approaches to managing this process began to take shape: supporters of the first advocate strict regulation in order to protect society from unforeseen dangers; supporters of the second advocate soft regulation that promotes innovation. Based on these approaches, the formation of law in the field of digital and biotechnology has begun. The time of intervention is of great importance per se, because if the course correction is performed at an early stage, it is easier to implement and less costly; however, the difficulty will be the lack of comprehensive information about the possible consequences of technology development and therefore a lack of understanding of the necessary changes. Later, the necessary changes will become more understandable, but will most likely require much more effort, which will lead to complex, lengthy and expensive course adjustments (Collingridge 1982).

Further, we collected, systematized and developed the proposals put forward by various researchers, both legal scholars and specialists in technology, who insist that norms taking into account the impact of technological (including artificial biotechnological) transformations on humans and society must be included into the legal matter. It seems that the time has already come to discuss these proposals. Posthumanism as a "populist diagnosis of a new era, a new way of critical research" (Lorimer, 2009) promotes "a focus on expanding previously human-specific categories (agency, sociality, legal personality) by including non-human forms of existence in them" (Yumartov, 2021).

2.3.1. Legal regime (potential legal status) of intelligent robots

Currently, robots with artificial intelligence are objects of law, but, unlike things, intelligent robots are able to act autonomously and their capabilities are increasing (Lima & Paiva, 2024), while they strongly depend on the availability of external data (Ponce del Castillo, 2024). "The stakes of technological progress are rising every day"[34], changing

[34] Pasquale, F. (2021). The New Laws of Robotics. https://clck.ru/3Eh9EQ

the balance between machines and people in everyday life, but people can "guide technologies by law"[35]. Given that the impact of robotics on the world around us has a steady tendency to grow, the creation of a special Lex robotica is inevitable over time, and it is likely to be based on the requirements of ethical acceptability and orientation to social needs (Palmerini et al., 2016). If an intelligent robot of the next generation (with strong artificial intelligence) remains an object of law in accordance with existing legislation, and is not endowed with the status of a subject of law, it will not be able to perform a number of functions instead of a human. If such a robot is recognized as a subject, taking into account its hypothetical intellectual superiority, this may lead to a loss of human-centricity of society. Thus, in the paradigm of anthropocentrism, robots cannot have legal personality, as this is contrary to the interests of people.

Possible options are to program robots to develop up to a certain limit or to accept the loss of human-centricity. The first option does not exclude the growth of risks, which IT specialists often associate not with a hypothetical uprising of strong artificial intelligence, but with the use of weak artificial intelligence as a tool by an attacker. Some authors propose to provide robots with limited or partial legal personality (quasi-personality), with a minimum set of rights and obligations, and only for certain purposes (Mocanu, 2021). According to proponents of this idea, endowing advanced artificial intelligence systems with "limited and narrow forms of legal personality ... seems to be the best way to promote the individual and public interests that the law must protect" (Bertolini & Episcopo, 2022). Among the statutory duties of such a robot is, first of all, non-hostility towards people. Hence, it must be guided by the "first law of robotics" in relations with people – not to harm a person by action and not to allow a person to be harmed by inaction. Other proposed obligations include: willingness to aggregate (unite with other robots for teamwork), ensuring situational awareness (discovery or concealment of relevant information), the obligation to fulfill one's role (leader in a group or subordinate to another robot or human), the obligation to undergo regular checks, etc. To implement the ability of an intelligent robot to act autonomously, in addition to the above obligations, it is suggested to stipulate the following rights of a robot:

– the right to receive, replenish, store and use information;
– the right to education and self-study;
– the right to exchange information with the external world;
– the right to respond to changes that occur in the environment;
– the right to "have an opinion" (the right to rational behavior);
– the right to make mistakes, since there are no methods for creating error-free software yet (Abrosimov, 2022).

Opponents of the possible legal personality of such artificial intelligence systems often refer to the lack of self-awareness in these systems as an insurmountable obstacle.

35 Ibid.

However, new research are emerging confirming the reality of demonstrating consciousness or gaining stable agency in the near future. It means that the prospect of "having artificial intelligent systems with their own interests is no longer a matter exclusively of science fiction or the distant future"[36].

2.3.2. Legal status of cyborgs

In an anthropocentric society, the biological body "always remains the supreme essence and frame of reference" (Fuchs et al., 2024), but this does not mean a ban on artificially increasing human capabilities. The specificity of cyborg's legal status will be determined by cognitive integration, which leads to complementing the human brain functions with artificial intelligence. By the way, according to sociological studies, cognitive improvement causes less rejection among the surveyed people than the desire for artificial physical improvement through body cyborgization (Zhang et al., 2024). The negative perception depends on age; it is less in younger generations (Reichel et al., 2024).

The intelligence hybridization and the emergence of new properties in the subject allows speaking of the features that require reflection in the legal status of technologically enhanced people: "As technological components become an integral part of the human body, the international community should reconsider the concept of cyborg ethics", as well as its ethical and regulatory implications (Ireni-Saban & Sherman, 2022). The impact on people who acquire cyborg properties in order to change their behavioral reactions is different from the impact on humans, and this should be taken into account in legislation (Viljanen, 2017).

The features of the legal status of cyborgs stem from the insecurity of their personal data, incomplete control over the neural devices built into their body, and the needs of the cyberphysical part of the body.

Cyborgs, on the one hand, have certain advantages; on the other hand, they are very vulnerable in terms of maintaining confidentiality of information, exercising the right to make medical decisions independently, etc. However, as for the threat of "mind reading", advances in neurotechnology allow gradually decoding information about functioning of the brain, not only supplemented by a neuroimplant. This indicates the urgent need to discuss neurorights as a new group of individual rights (Wajnerman & Lopez-Silva, 2022), regardless of cyborgization.

The specific rights which should be recognized in a cyborg include:

– the right to improve one's body using certified cyber components and medical devices;

– the right to keep their cyber and medical devices under any circumstances (with the exception of illegally integrated, non-certified ones or those posing a danger to others);

[36] Long, R., Sebo, J., Butlin, P., Finlinson, K., Fish, K., Harding, J., Pfau, J., Sims, T., Birch, J., & Chalmers, D. (2024, October 30). Taking AI Welfare Seriously: Report. https://goo.su/L7IeY

– the right to non-misuse by manufacturers and suppliers of cyber devices;

– the right to a share of ownership of components that are integrated or implanted into the cyborg's body;

– the priority right of governing the activities inside one's body;

– the right to make a decision on any type of medical intervention;

– the right to protection against discrimination due to cyborgization[37].

The recognition of these rights for cyborgs will require significant changes to the norms of constitutional, administrative, civil, family and labor law (Sokolova, 2022), as well as defining the "cyborg" concept in legislation. "Subject regulation in this area should be made in advance to a certain extent" (Kamalova, 2021) in order to eliminate the gap between technological modification of a human and their social identity, as well as to prevent the growth of digital and biotechnological inequality. In addition to specific rights, cyborgs should also have symmetrical responsibilities arising from the additional risk to people around them. These should be, at least, the obligations to register complex neural devices in the state register, not to use devices that pose a danger to others, and not to distribute confidential information about other people obtained during the operation of a neuroprosthesis/neuroimplant.

2.3.3. Legal status of genetically enhanced individuals

Such individuals, along with cyborgs, are human beings; therefore, they act as subjects of law under current legislation, but unlike other people, their body is artificially biologically modernized. On the one hand, these individuals, like all people, have the right to protection from discrimination; on the other hand, ensuring security for all should be the basis for legal restrictions in biomedical research and procedures (Czomartova et al., 2021). Such persons, being resistant to infectious diseases, can be their carriers without harm to their body, which is fraught with serious consequences for other people. Or they can increase their personal abilities through genetic improvement, "laying a bomb" for the next generations of their descendants, because, according to frontier research, "many diseases are closely related in the sense that reducing the risk of one increases the risk of the other". For example, the probability of some cancers is inversely proportional to neurodegenerative diseases, such as Alzheimer's and Parkinson's disease (Benton et al., 2021).

Today, the questions of human nature, the norm and its boundaries are raised "in a completely different sense than before: for the first time in human cognition of humanity, we moved from observation to intervention" (Przhilenskiy, 2024). This is why the prospective emergence of genetically enhanced individuals began to take on quite real outlines. This is why the formation of bio-law began, as a comprehensive area designed to protect not only humans, but also humanity as a whole, covering future generations. Rights of a human as a biological organism should be built on the currently being

[37] Memorandum on the rights of cyborgs. (August 8, 2018). https://clck.ru/3Eh9PH

formed “principles of bio-law ensuring the unity of legal and ethical-social regulators” (Umnova-Konyukhova & Aleshkova, 2022).

The specificity of the status of genetically enhanced individuals should rely on the public interest as the basis of a balance between the unhindered receipt of information about genetic improvements, which will contribute to the development of science and ensure the safety of other people, and the preservation of confidentiality as everyone’s right to personal data protection (Berg, 2024).

Genetic improvement can be the result of the will of the person, the decision of their parents, or the birth from similar individuals who transferred the acquired genetic improvements. Thus, it must be borne in mind that new individuals will appear who did not choose to become such or remain human without artificially produced changes; the status of genetically enhanced individuals will apply to them from birth. Such individuals should at least have the right to supportive therapy if they need it vitally.

The specific obligations of genetically enhanced individuals are likely to be ensuring that up-to-date data is provided to biobanks and refraining from actions that do not harm these individuals due to genetic changes, but endanger the lives and health of people around them.

2.3.4. Legal regime (potential legal status) of chimeras

The first subtype of chimeras is biorobots. Biorobots with artificial intelligence, although similar to genetically enhanced individuals in some biological characteristics, are not human. Hence, legal regulation regarding them is likely to be closer to intelligent robots. We should expect an even more intense dispute over the legal personality of intelligent robots in relation to biorobots that are not inferior to humans in terms of intelligence, if such biorobots appear. Such a robot will not only move and speak like a human; it will have “living” muscles and organs. The ability for biological evolution and the potential for reasonableness will inevitably entail ethical dilemmas that go beyond technology (Mestre et al., 2024) and need attention from the law.

The second subtype of chimeras is “digital personalities”, or virtual artificial intelligence systems that are autonomous (not “tied” to a specific living person), but having cognitive abilities equal to or greater than human ones. This is the only type of new entities that does not have a physical shell, which cannot but affect the forms of legal responsibility of these virtual personalities if they are recognized as legal entities. The absence of a physical embodiment does not exclude the possibility of recognizing such chimeras as subjects or, more precisely, quasi-subjects of law, since “the growing use of artificial intelligence promises huge advantages in speed and efficiency in all forms of decision-making” (Burgess, 2024). Respectively, if, in order to be an effective embodied virtual agent and replace people in various processes, such entities require a certain minimum of rights and obligations, like intelligent robots, – these rights and obligations will, with a high probability, recognized over time.

Conclusions

Summarizing the study, it is worth emphasizing that the task of law is to develop a balanced approach to regulating public relations that are being transformed under the influence of digital and biotechnologies. One can talk about the emergence of new types of entities as about a growing probability, partly even as an already emerging phenomenon. Some of them will be systems of strong artificial intelligence (intelligent robots, virtual personalities); others will be technologically and genetically enhanced humans. The closest thing is the emergence of cyborg humans, which is already beginning to happen, but the prospects for other types should not be ignored. Cyborgs and genetically enhanced individuals are people, they will be subjects of law anyway; the question is only about the specificity of their status. However, intelligent robots and chimeras are new types of entities that are not human, but have cognitive functions and are able to make an intellectually directed impact on the environment and subjects of law.

The inertia of the regulatory environment, which is generally useful in terms of maintaining the status quo, will increase inequality in the society objectively "drifting" towards posthumanism. The problem is aggravated due to the lawyers' poor understanding of some technological innovations when they propose changes to legislation. Nevertheless, attempts to construct a legal regulation adequate to Society 5.0 are useful because they help to form a coherent image of the future society and outline the trajectory of moving towards it. In any case, the approach will be based on calculating risks, since a risk-based approach seems to be the best possible option under high uncertainty.

Assessing the parameters achieved so far while forming the national and regional approaches to artificial intelligence regulation, one may say that some states will regulate the use of artificial intelligence and other technologies more strictly. Others will adhere to a softer regulation, because this will stimulate the technological development and give outsiders a chance to "get ahead"; however, the consequences may be extremely hard. The creation of national legislation, although differing by country, is inevitably tied to the international level. This enables the main political actors to coordinate their positions. Thus, we should expect a controversial and difficult period, which will end with forming of principles common for all.

References

Abrosimov, V. (2022). Rights, duties, obligations and restrictions of an autonomous robot in a cyber-physical group. *Legal Informatics*, *4*, 67–75. (In Russ.). https://doi.org/10.21681/1994-1404-2022-4-67-75

Acemoglu, D., & Restrepo, P. (2020). The wrong kind of AI? Artificial intelligence and the future of labour demand. *Cambridge Journal of Regions, Economy and Society*, *13*(1), 25–35. https://doi.org/10.1093/cjres/rsz022

Almeida, M., & Diogo, R. (2019). Human enhancement: Genetic engineering and evolution. *Evolution, Medicine, and Public Health*, *1*, 183–189. https://doi.org/10.1093/emph/eoz026

Benton, M. L., Abraham, A., LaBella, A. L., Abbot, P., Rokas, A., & Capra, J. A. (2021). The influence of evolutionary history on human health and disease. *Nature Reviews Genetics*, *22*, 269–283. https://doi.org/10.1038/s41576-020-00305-9

Berg, L. N. (2024). Genomic Data Privacy and the Right to Science: Issues of Balance. *Lex Russica*, *77*(10), 93–101. (In Russ.). https://doi.org/10.17803/1729-5920.2024.215.10.093-101

Bertolini, A., & Episcopo, F. (2022). Robots and AI as Legal Subjects? Disentangling the Ontological and Functional Perspective. *Frontiers in Robotics and AI*, *9*, 842213. https://doi.org/10.3389/frobt.2022.842213

Brown, J. L., Voth, J. P., Person, K., & Low, W. C. (2023). A Technological and Regulatory Review on Human-Animal Chimera Research: The Current Landscape of Biology, Law, and Public Opinion. *Cell Transplantation*, *32*. https://doi.org/10.1177/09636897231183112

Burgess, P. (2024). *AI and the Rule of Law: The Necessary Evolution of a Concept*. Oxford: Hart Publishing. https://doi.org/10.5040/9781509963201

Chiriatti, M., Ganapini, M., Panai, E., Ubiali, M., & Riva, G. (2024). The case for human – AI interaction as system 0 thinking. *Nature Human Behaviour*, *8*, 1829–1830. https://doi.org/10.1038/s41562-024-01995-5

Citra, N. Z. M., Chew, W. L., & Lai, P. S. (2024). Embryo and fetal gene editing: Technical challenges and progress toward clinical applications. Molecular Therapy. *Methods & Clinical Development*, *3*(2), 101229. https://doi.org/10.1016/j.omtm.2024.101229

Collingridge, D. (1982). *The social control of technology*. Palgrave Macmillan.

Cornejo-Plaza, M. I., Cippitani, R., & Pasquino, V. (2024). Chilean Supreme Court ruling on the protection of brain activity: neurorights, personal data protection, and neurodata. *Frontiers in Psychology*, *15*, 1330439. https://doi.org/10.3389/fpsyg.2024.1330439

Czomartova, F. V., Pomazanskij, A. E., Nikitina, E. E., Nanba, S. B., Melnik, T. E., & Khromova, N. M. (2021). *Law and biomedicine*. Moscow: Norma; INFRA-M. (In Russ.).

Das, S., Banerjee, J. S., De, D., Sarigiannidis, P., Chakraborty, A., Mahmud, M., & Bhattacharyya, S. (2024). Role of the Social Internet of Things in Society 5.0: Opportunities and Challenges. In S. Bhattacharyya, J. S. Banerjee, & M. Köppen (Eds.), *Smart innovation, systems and technologies* (pp. 667–686). Springer, Singapore. https://doi.org/10.1007/978-981-99-7711-6_52

de Andrés-Sánchez, J., Arias-Oliva, M., Souto-Romero, M., & Gené-Albesa, J. (2024). Assessing the Acceptance of Cyborg Technology with a Hedonic Technology Acceptance Model. *Computers*, *13*(3), 82. https://doi.org/10.3390/computers13030082

Döring, N., Mohseni, M. R., & Walter, R. (2020). Design, Use, and Effects of Sex Dolls and Sex Robots: Scoping Review. *Journal of Medical Internet Research*, *22*(7), e18551. https://doi.org/10.2196/18551

Emelin, V. A. (2013). Cyborgization and invalidization of a technologically expanded human. *National Psychological Journal*, *1*(9), 62–70. (In Russ.).

Filipova, I. A. (2024). Artificial intelligence, robot and neurotechnologies: concepts, relationship and limits of legal regulation. *State and Law*, *4*, 148–158. (In Russ.). https://doi.org/10.31857/S1026945224040133

Fontes, C., Carpentras, D., & Mahajan, S. (2024). Human digital twins unlocking Society 5.0? Approaches, emerging risks and disruptions. *Ethics and Information Technology*, *26*, 54. https://doi.org/10.1007/s10676-024-09787-1

Fuchs, Th., Aszmann, O., & Dürr, O. (2024). Organisms, Prostheses and the Limits of Cyborgization. *Philosophy, Theology and the Sciences*, *11*(2), 208–226 https://doi.org/10.1628/ptsc-2024-0016

Gibney, E. (2024, May 28). The AI revolution is coming to robots: how will it change them? *Nature*. https://doi.org/10.1038/d41586-024-01442-5

Ginevičienė, V., Utkus, A., Pranckevičienė, E., Semenova, E. A., Hall, E. C., & Ahmetov, I. I. (2022). Perspectives in Sports Genomics. *Biomedicines*, *10*(2), 298. https://doi.org/10.3390/biomedicines10020298

Goldstein, J. M., Tabebordbar, M., Zhu, K., Wang, L. D., Messemer, K. A., Peacker, B., Kakhki, S. A., Gonzalez-Celeiro, M., Shwartz, Yu., Cheng, J. K. W., Xiao, R., Barungi, T., Albright, Ch., Hsu, Y.-Ch., Vandenberghe, L. H., & Wagers, A. J. (2019). In Situ Modification of Tissue Stem and Progenitor Cell Genomes. *Cell Reports*, *27*(4), 1254–1264. https://doi.org/10.1016/j.celrep.2019.03.105

Grinin, L. E., & Grinin, A. L. (2016). Will cybernetic revolution lead to cyborgization of humans? *Philosophy and society*, *3*(80), 5–26. (In Russ.).

Gulino, M., Kim, D., Pané, S., Santos, S. D., & Pêgo, A. P. (2019). Tissue Response to Neural Implants: The Use of Model Systems Toward New Design Solutions of Implantable Microelectrodes. *Frontiers in Neuroscience*, *13*, 689. https://doi.org/10.3389/fnins.2019.00689

Gumuskaya, G., Srivastava, P., Cooper, B. G., Lesser, H., Semegran, B., Garnier, S., & Levin, M. (2024). Motile Living Biobots Self-Construct from Adult Human Somatic Progenitor Seed Cells. *Advanced Science*, *11*(4), e2303575. https://doi.org/10.1002/advs.202303575

Hanson, K. R., & Locatelli, C. C. (2022). From Sex Dolls to Sex Robots and Beyond: A Narrative Review of Theoretical and Empirical Research on Human-like and Personified Sex Tech. *Current Sexual Health Reports*, *14*, 106–117 https://doi.org/10.1007/s11930-022-00331-0

Helbing, D., & Ienca, M. (2024). Why converging technologies need converging international regulation. *Ethics and Information Technology*, *26*, 15. https://doi.org/10.1007/s10676-024-09756-8

Ireni-Saban, L., & Sherman, M. (2022). Cyborg ethics and regulation: ethical issues of human enhancement. *Science and Public Policy*, *49*(1), 42–53, https://doi.org/10.1093/scipol/scab058

Jiang, P., & Alam, M. M. (2022). Rise of the human-mouse chimeric brain models. *Cell Regeneration*, *11*, 32. https://doi.org/10.1186/s13619-022-00135-6

Kadlecová, J. (2020). Body-hacking: On the Relationship between People and Material Entities in the Practice of Technological Body Modifications. *Historická Sociologie*, *12*(1)49–63. https://doi.org/10.14712/23363525.2020.4

Kamalova, G. G. (2021). Theoretical and legal aspects of the evolution of human rights in the context of digitalization and the introduction of artificial intelligence technology. Bulletin of Udmurt University. *Series Economics and Law*, *31*(4), 662–668. (In Russ.). https://doi.org/10.35634/2412-9593-2021-31-4-662-668

Karnouskos, S. (2022). Symbiosis with artificial intelligence via the prism of law, robots, and society. *Artificial Intelligence and Law*, *30*(1), 93–115. https://doi.org/10.1007/s10506-021-09289-1

Khandelwal, A., Agrawal, A., Bhattacharyya, A., Singla, Y. K., Singh, S., Bhattacharya, U., Dasgupta, I., Petrangeli, S., Shah, R. R., Chen, Ch., & Krishnamurthy, B. (2024). Large Content and Behavior Models to Understand, Simulate, And Optimize Content and Behavior. *The Twelfth International Conference on Learning Representations, ICLR*, Vienna. arXiv:2309.00359v4. https://doi.org/10.48550/arXiv.2309.00359

Kriegman, S., Blackiston, D., Levin, M., & Bongard, J. (2021). Kinematic self-replication in reconfigurable organisms. *Proceedings of the National Academy of Sciences*, *118*(49), e2112672118. https://doi.org/10.1073/pnas.2112672118

Księżak, P. (2024). *Artificial Intelligence and the Dawn of Cyborg Law. Key Legal Challenges for Private Law in the Era of Human Augmentation*. Warszawa: Allerhand Publishing.

Laurent, M., Geoffroy, M., Pavani, G., & Guiraud, S. (2024). CRISPR-Based Gene Therapies: From Preclinical to Clinical Treatments. *Cells*, *13*(10), 800. https://doi.org/10.3390/cells13100800

Lima, P. U., & Paiva, A. (2024). Autonomous and Intelligent Robots: Social, Legal and Ethical Issues. In H. Sousa Antunes, P. M. Freitas, A. L. Oliveira, C. Martins Pereira, E. Vaz de Sequeira, & L. Barreto Xavier (Eds.), Multidisciplinary Perspectives on Artificial Intelligence and the Law. *Law, Governance and Technology Series* (pp. 127–140). Cham, Switzerland. https://doi.org/10.1007/978-3-031-41264-6_7

Liu, Z., Cai, Y., Wang, Y., Nie, Y., Zhang, C., Xu, Y., Zhang, X., Lu, Y., Wang, Z., Poo, M., & Sun, Q. (2018). Cloning of Macaque Monkeys by Somatic Cell Nuclear Transfer. *Cell*, *172*(4), 881–887. https://doi.org/10.1016/j.cell.2018.01.020

Lloyd, N., Chowdhry, A., & Lewis, P. R. (2024). Trustworthy Embodied Virtual Agents. In N. Lee (Eds.), *Encyclopedia of Computer Graphics and Games* (pp. 1917–1922). Springer, Cham. https://doi.org/10.1007/978-3-031-23161-2_524

Lorimer, J. (2009). Posthumanism/Posthumanistic Geographies. In R. Kitchin, & N. Thrift (Eds.), *International Encyclopedia of Human Geography* (pp. 344–354). Oxford: Elsevier. https://doi.org/10.1016/b978-008044910-4.00723-9

Mestre, R., Astobiza, A. M., Webster-Wood, V. A., & Saif, M. T. A. (2024). Ethics and responsibility in biohybrid robotics research. *Proceedings of the National Academy of Sciences*, *121*(31), e2310458121. https://doi.org/10.1073/pnas.2310458121

Mocanu, D. M. (2021). Gradient Legal Personhood for AI Systems – Painting Continental Legal Shapes Made to Fit Analytical Molds. *Frontiers in Robotics and AI*, *8*, 788179. https://doi.org/10.3389/frobt.2021.788179

Momaya, A., Fawal, M., & Estes, R. (2015). Performance-Enhancing Substances in Sports: A Review of the Literature. *Sports Medicine*, *45*, 517–531. https://doi.org/10.1007/s40279-015-0308-9

Mori, M., MacDorman, K. F., & Kageki, N. (2012). The Uncanny Valley. *IEEE Robotics & Automation Magazine*, *19*(2), 98–100. https://doi.org/10.1109/MRA.2012.2192811

Morshedzadeh, F., Ghanei, M., Lotfi, M., Ghasemi, M., Ahmadi, M., Najari-Hanjani, P., Sharif, S., Mozaffari-Jovin, S., Peymani, M., & Abbaszadegan, M. R. (2024). An Update on the Application of CRISPR Technology in Clinical Practice. *Molecular Biotechnology*, *66*(2), 179–197. https://doi.org/10.1007/s12033-023-00724-z

Nolfi, S. (2024). On the Unexpected Abilities of Large Language Models. *Adaptive Behavior*, *32*(6), 493–502. https://doi.org/10.1177/10597123241256754

Olarte-Pascual, C., Pelegrín-Borondo, J., Reinares-Lara, E., & Arias-Oliva, M. (2021). From wearable to insideable: Is ethical judgment key to the acceptance of human capacity-enhancing intelligent technologies? *Computers in Human Behavior*, *114*, 106559. https://doi.org/10.1016/j.chb.2020.106559

Palmerini, E., Bertolini, A., Battaglia, F., Koops, B.-J., Carnevale, A., & Salvini, P. (2016). RoboLaw: Towards a European framework for robotics regulation. *Robotics and Autonomous Systems*, *86*, 78–85. https://doi.org/10.1016/j.robot.2016.08.026

Perez, E. (2022). Future of Therapy for Inborn Errors of Immunity. *Clinical Reviews in Allergy & Immunology*, *63*(1), 75–89. https://doi.org/10.1007/s12016-021-08916-8

Pluchino, S., & Lombardi, I. (2024). Crossing species boundaries in regenerative neuroscience with rat–mouse brain chimeras. *Lab Animal*, *53*, 179–180. https://doi.org/10.1038/s41684-024-01394-3

Ponce del Castillo, A. (2024). *Artificial intelligence, labour and society*. Brussels: ETUI.

Popova, O. V. (2015). Ethical issues of biotechnological human design. *RUDN Journal of Philosophy*, *2*, 107–114. (In Russ.).

Przhilenskiy, V. I. (2024). Bioethics: Epistemic Capabilities and Legal Frameworks. *Kutafin Law Review*, *11*(2), 180–198. https://doi.org/10.17803/2713-0533.2024.2.28.180-198

Reichel, P., Bassler, C. T., & Spörrle, M. (2024). Embracing the enhanced self now and in the future: The impact of temporal focus, age, and sex on cyborg products use intention. *Personality and Individual Differences*, *225*, 112665. https://doi.org/10.1016/j.paid.2024.112665

Roco, M. C., & Bainbridge, W. S. (2003). *Converging Technologies for Improving Human Performance. Nanotechnology, Biotechnology, Information Technology and Cognitive Science*. Dordrecht: Springer. https://doi.org/10.1007/978-94-017-0359-8

Sandini, G., Sciutti, A., & Morasso, P. (2024). Artificial cognition vs. artificial intelligence for next-generation autonomous robotic agents. *Frontiers in Computational Neuroscience*, *18*, 1349408. https://doi.org/10.3389/fncom.2024.1349408

Sharon, A., Jankowski, M. M., Shmoel, N., Erez, H., & Spira, M. E. (2023). Significantly reduced inflammatory foreign-body-response to neuroimplants and improved recording performance in young compared to adult rats. *Acta Biomaterialia*, *158*, 292–307. https://doi.org/10.1016/j.actbio.2023.01.002

Sokolova, M. (2022). Cyborgization of human: social and legal dimensions. *Social novelties and social sciences*, *4*, 52–64. (In Russ.).

Soori, M., Arezoo, B., & Dastres, R. (2023). Artificial intelligence, machine learning and deep learning in advanced robotics, a review. *Cognitive Robotics*, *3*, 54–70. https://doi.org/10.1016/j.cogr.2023.04.001

Tan, T., Wu, J., Si, C., Dai, S., Zhang, Y., Sun, N., Zhang, E., Shao, H., Si, W., Yang, P., Wang, H., Chen, Z., Zhu, R., Kang, Y., Hernandez-Benitez, R., Martinez Martinez, L., Nuñez Delicado, E., Berggren, W. T., Schwarz, M., … & Izpisua Belmonte, J. C. (2021). Chimeric contribution of human extended pluripotent stem cells to monkey embryos ex vivo. *Cell*, *184*(13), 3589. https://doi.org/10.1016/j.cell.2021.06.011

Umnova-Konyukhova, I. A., & Aleshkova, I. A. (2022). The Impact of Scientific and Technological Progress in Biotechnology on Human Rights and Principles of Law. *Actual Problems of Russian Law*, *17*(10), 34–45. (In Russ.). https://doi.org/10.17803/1994-1471.2022.143.10.034-045

Vaughn, L. (2023). *Bioethics: Principles, Issues, and Cases* (5th ed.). Oxford University Press.

Veit, W. (2018). Procreative Beneficence and Genetic Enhancement. *Kriterion – Journal of Philosophy*, *32*(1), 75–92. https://doi.org/10.1515/krt-2018-320105

Viljanen, M. (2017). A Cyborg Turn in Law? *German Law Journal*, *18*(5), 1277–1308. https://doi.org/10.1017/S2071832200022331

Wajnerman, A., & López-Silva, P. (2022). Mental Privacy and Neuroprotection: An Open Debate. In P. López-Silva, & L. Valera (Eds.), *Protecting the Mind. Challenges in Law, Neuroprotection, and Neurorights* (pp. 141–155). Cham, Switzerland. https://doi.org/10.1007/978-3-030-94032-4_12

Yumartov, D. A. (2021). Inclusiveness as key principle of posthumanism. *Gumanitarnyye vedomosti TGPU im. L. N. Tolstogo*, *40*(4), 109–122. https://doi.org/10.22405/2304-4772-2021-1-4-109-122

Zhang, H., Xuan, Z., Yu, F., Ding, X., & Han Y. (2024). Crafting the modern Prometheus: navigating morality and identity in the age of cyborg enhancements. *Philosophical Psychology*, 1–34. https://doi.org/10.1080/09515089.2024.2382297

Author information

Irina A. Filipova – Cand. Sci. (Law), Associate Professor, Department of Labor and Environmental Law, National Research Lobachevsky State University of Nizhni Novgorod; Head of the Central Asia Research Center for artificial intelligence regulation, Samarkand State University named after Sharof Rashidov
Address: 23 prospekt Gagarina, 603922 Nizhniy Novgorod, Russia; 15 Universitetskiy bulvar, 140104 Samarkand, Uzbekistan
E-mail: irinafilipova@yandex.ru
ORCID ID: https://orcid.org/0000-0003-1773-5268
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57327205000
WoS Researcher ID: https://www.webofscience.com/wos/author/record/R-1375-2016
Google Scholar ID: https://scholar.google.com/citations?user=opJc7fcAAAAJ
RSCI Author ID: https://elibrary.ru/author_profile.asp?authorid=461586

Conflict of interest

The author is a Deputy Editor-in-Chief of the Journal; the article has been reviewed on general terms.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law
PASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – November 11, 2024
Date of approval – November 25, 2024
Date of acceptance – December 13, 2024
Date of online placement – December 20, 2024

Научная статья
УДК 34:004:342.721:612.6
EDN: https://elibrary.ru/atqzba
DOI: https://doi.org/10.21202/jdtl.2024.38

Интеллектуальные роботы, киборги, генетически усовершенствованные индивиды, химеры: будущее и задачи права

Ирина Анатольевна Филипова

Национальный исследовательский Нижегородский государственный университет имени Н. И. Лобачевского, Нижний Новгород, Россия;
Самаркандский государственный университет имени Шарофа Рашидова, Самарканд, Узбекистан

Ключевые слова

биотехнологии,
генная инженерия,
искусственный интеллект,
киборг,
нейротехнологии,
право,
риск,
робот,
цифровые технологии,
человек

Аннотация

Цель: выявить теоретико-правовые проблемы, связанные с неуклонно расширяющимся распространением на практике продуктов развития цифровых и биотехнологий, оценить сопутствующие этому процессу риски, способные изменить положение человека в обществе будущего, а также выработать и аргументировать предложения по минимизации рисков и устранению выявленных проблем с помощью правового регулирования.

Методы: в основе исследования лежат методы обобщения научно-технической информации и теоретического анализа, применявшиеся в процессе изучения исходных материалов, аксиологический и системный подходы, формально-юридический метод и, кроме того, методы правового прогнозирования, в первую очередь экстраполяции, позволившие осветить перспективы реформирования права вследствие технологической экспансии.

Результаты: включают описание динамики развития цифровых и биотехнологий; характеристику меняющегося социального ландшафта с возникновением новых типов сущностей, способных повлиять на фактический статус человека; классификацию рисков, угрожающих людям из-за совершенствования цифровых и биотехнологий; перечень задач, решение которых на основе права поможет устранить, отодвинуть или, по крайней мере, значительно снизить остроту проблем, увеличивая лимит времени, отведенный человечеству на осмысление ряда концептуальных моментов. Представлены доводы, обосновывающие необходимость разработки специального правового регулирования в отношении новых типов сущностей, появление которых становится неизбежным результатом развития упоминаемых технологий.

© Филипова И. А., 2024

Статья находится в открытом доступе и распространяется в соответствии с лицензией Creative Commons «Attribution» («Атрибуция») 4.0 Всемирная (CC BY 4.0) (https://creativecommons.org/licenses/by/4.0/deed.ru), позволяющей неограниченно использовать, распространять и воспроизводить материал при условии, что оригинальная работа упомянута с соблюдением правил цитирования.

Научная новизна: состоит, во-первых, в комплексном изучении развития взаимосвязанных групп цифровых и биотехнологий с учетом их усиливающейся конвергенции, во-вторых, в формулировании юридических вопросов, которые требуют урегулирования из-за потенциального появления новых типов сущностей, располагающих когнитивными функциями и способных оказывать интеллектуально направленное воздействие на окружающую среду и субъектов права.

Практическая значимость: присутствует в ответах, данных на сформулированные юридические вопросы, они содержат предложения и рекомендации по необходимой корректировке правового регулирования и акцентируют внимание правоведов на проблемах, вытекающих из темпов и векторов развития наукоемких технологий.

Для цитирования

Филипова, И. А. (2024). Интеллектуальные роботы, киборги, генетически усовершенствованные индивиды, химеры: будущее и задачи права. *Journal of Digital Technologies and Law*, *2*(4), 741–781. https://doi.org/10.21202/jdtl.2024.38

Список литературы

Абросимов, В. К. (2022). Права, обязанности, обязательства и ограничения автономного робота в киберфизической группе. *Правовая информатика*, *4*, 67–75. https://doi.org/10.21681/1994-1404-2022-4-67-75

Берг, Л. Н. (2024). Конфиденциальность геномной информации и право на доступ к научным знаниям: вопросы соотношения. *Lex russica*, *77*(10), 93–101. EDN: https://elibrary.ru/usiurr. DOI: https://doi.org/10.17803/1729-5920.2024.215.10.093-101

Гринин, Л. Е., Гринин, А. Л. (2016). Приведет ли кибернетическая революция к киборгизации людей? *Философия и общество*, *3*(80), 5–26.

Емелин, В. А. (2013). Киборгизация и инвалидизация технологически расширенного человека. *Национальный психологический журнал*, *1*(9), 62–70.

Камалова, Г. Г. (2021). Теоретико-правовые аспекты эволюции прав человека в условиях цифровизации и внедрения технологии искусственного интеллекта. *Вестник Удмуртского университета. Серия Экономика и право*, *31*(4), 662–668. https://doi.org/10.35634/2412-9593-2021-31-4-662-668

Попова, О. В. (2015). Этические проблемы биотехнологического конструирования человека. *Вестник Российского университета дружбы народов. Сер. Философия*, *2*, 107–114.

Соколова, М. Е. (2022). Киборгизация человека: социально-правовое измерение. *Социальные новации и социальные науки*, *4*, 52–64. EDN: https://elibrary.ru/laclhe. DOI: https://doi.org/10.31249/snsn/2022.04.04

Умнова-Конюхова, И. А., Алешкова, И. А. (2022). Влияние научно-технического прогресса в биотехнологиях на права человека и принципы права. *Актуальные проблемы российского права*, *17*(10), 34–45. https://doi.org/10.17803/1994-1471.2022.143.10.034-045

Филипова, И. А. (2024). Искусственный интеллект, робот и нейротехнологии: понятие, соотношение и пределы правового регулирования. *Государство и право*, *4*, 148–158. https://doi.org/10.31857/S1026945224040133

Цомартова, Ф. В., Помазанский, А. Е., Никитина, Е. Е., Нанба, С. Б., Мельник, Т. Е., Хромова, Н. М. (2021). *Право и биомедицина*: монография. Москва: Норма; ИНФРА-М. EDN: https://elibrary.ru/uecvsn

Юмартов, Д. А. (2021). Инклюзивность как основной принцип постгуманизма. *Гуманитарные ведомости ТГПУ им. Л. Н. Толстого*, *40*(4), 109–122. EDN: https://elibrary.ru/rfarph. DOI: https://doi.org/10.22405/2304-4772-2021-1-4-109-122

Acemoglu, D., & Restrepo, P. (2020). The wrong kind of AI? Artificial intelligence and the future of labour demand. *Cambridge Journal of Regions, Economy and Society*, *13*(1), 25–35. https://doi.org/10.1093/cjres/rsz022

Almeida, M., & Diogo, R. (2019). Human enhancement: Genetic engineering and evolution. *Evolution, Medicine, and Public Health*, *1*, 183–189. https://doi.org/10.1093/emph/eoz026

Benton, M. L., Abraham, A., LaBella, A. L., Abbot, P., Rokas, A., & Capra, J. A. (2021). The influence of evolutionary history on human health and disease. *Nature Reviews Genetics*, *22*, 269–283. https://doi.org/10.1038/s41576-020-00305-9

Bertolini, A., & Episcopo, F. (2022). Robots and AI as Legal Subjects? Disentangling the Ontological and Functional Perspective. *Frontiers in Robotics and AI*, *9*, 842213. https://doi.org/10.3389/frobt.2022.842213

Brown, J. L., Voth, J. P., Person, K., & Low, W. C. (2023). A Technological and Regulatory Review on Human-Animal Chimera Research: The Current Landscape of Biology, Law, and Public Opinion. *Cell Transplantation*, *32*. https://doi.org/10.1177/09636897231183112

Burgess, P. (2024). *AI and the Rule of Law: The Necessary Evolution of a Concept*. Oxford: Hart Publishing. https://doi.org/10.5040/9781509963201

Chiriatti, M., Ganapini, M., Panai, E., Ubiali, M., & Riva, G. (2024). The case for human – AI interaction as system 0 thinking. *Nature Human Behaviour*, *8*, 1829–1830. https://doi.org/10.1038/s41562-024-01995-5

Citra, N. Z. M., Chew, W. L., & Lai, P. S. (2024). Embryo and fetal gene editing: Technical challenges and progress toward clinical applications. *Molecular Therapy. Methods & Clinical Development*, *3*(2), 101229. https://doi.org/10.1016/j.omtm.2024.101229

Collingridge, D. (1982). *The social control of technology*. Palgrave Macmillan.

Cornejo-Plaza, M. I., Cippitani, R., & Pasquino, V. (2024). Chilean Supreme Court ruling on the protection of brain activity: neurorights, personal data protection, and neurodata. *Frontiers in Psychology*, *15*, 1330439. https://doi.org/10.3389/fpsyg.2024.1330439

Das, S., Banerjee, J. S., De, D., Sarigiannidis, P., Chakraborty, A., Mahmud, M., & Bhattacharyya, S. (2024). Role of the Social Internet of Things in Society 5.0: Opportunities and Challenges. In S. Bhattacharyya, J. S. Banerjee, & M. Köppen (Eds.), *Smart innovation, systems and technologies* (pp. 667–686). Springer, Singapore. https://doi.org/10.1007/978-981-99-7711-6_52

de Andrés-Sánchez, J., Arias-Oliva, M., Souto-Romero, M., & Gené-Albesa, J. (2024). Assessing the Acceptance of Cyborg Technology with a Hedonic Technology Acceptance Model. *Computers*, *13*(3), 82. https://doi.org/10.3390/computers13030082

Döring, N., Mohseni, M. R., & Walter, R. (2020). Design, Use, and Effects of Sex Dolls and Sex Robots: Scoping Review. *Journal of Medical Internet Research*, *22*(7), e18551. https://doi.org/10.2196/18551

Gibney, E. (2024, May 28). *The AI revolution is coming to robots: how will it change them?* Nature. https://doi.org/10.1038/d41586-024-01442-5

Ginevičienė, V., Utkus, A., Pranckevičienė, E., Semenova, E. A., Hall, E. C., & Ahmetov, I. I. (2022). Perspectives in Sports Genomics. *Biomedicines*, *10*(2), 298. https://doi.org/10.3390/biomedicines10020298

Goldstein, J. M., Tabebordbar, M., Zhu, K., Wang, L. D., Messemer, K. A., Peacker, B., Kakhki, S. A., Gonzalez-Celeiro, M., Shwartz, Yu., Cheng, J. K. W., Xiao, R., Barungi, T., Albright, Ch., Hsu, Y.-Ch., Vandenberghe, L. H., & Wagers, A. J. (2019). In Situ Modification of Tissue Stem and Progenitor Cell Genomes. *Cell Reports*, *27*(4), 1254–1264. https://doi.org/10.1016/j.celrep.2019.03.105

Gulino, M., Kim, D., Pané, S., Santos, S. D., & Pêgo, A. P. (2019). Tissue Response to Neural Implants: The Use of Model Systems Toward New Design Solutions of Implantable Microelectrodes. *Frontiers in Neuroscience*, *13*, 689. https://doi.org/10.3389/fnins.2019.00689

Gumuskaya, G., Srivastava, P., Cooper, B. G., Lesser, H., Semegran, B., Garnier, S., & Levin, M. (2024). Motile Living Biobots Self-Construct from Adult Human Somatic Progenitor Seed Cells. *Advanced Science*, *11*(4), e2303575. https://doi.org/10.1002/advs.202303575

Fontes, C., Carpentras, D., & Mahajan, S. (2024). Human digital twins unlocking Society 5.0? Approaches, emerging risks and disruptions. *Ethics and Information Technology*, *26*, 54. https://doi.org/10.1007/s10676-024-09787-1

Fuchs, Th., Aszmann, O., & Dürr, O. (2024). Organisms, Prostheses and the Limits of Cyborgization. *Philosophy, Theology and the Sciences*, *11*(2), 208–226 https://doi.org/10.1628/ptsc-2024-0016

Hanson, K. R., & Locatelli, C. C. (2022). From Sex Dolls to Sex Robots and Beyond: A Narrative Review of Theoretical and Empirical Research on Human-like and Personified Sex Tech. *Current Sexual Health Reports*, *14*, 106–117 https://doi.org/10.1007/s11930-022-00331-0

Helbing, D., & Ienca, M. (2024). Why converging technologies need converging international regulation. *Ethics and Information Technology*, *26*, 15. https://doi.org/10.1007/s10676-024-09756-8

Jiang, P., & Alam, M. M. (2022). Rise of the human-mouse chimeric brain models. *Cell Regeneration*, *11*, 32. https://doi.org/10.1186/s13619-022-00135-6

Ireni-Saban, L., & Sherman, M. (2022). Cyborg ethics and regulation: ethical issues of human enhancement. *Science and Public Policy*, *49*(1), 42–53, https://doi.org/10.1093/scipol/scab058

Kadlecová, J. (2020). Body-hacking: On the Relationship between People and Material Entities in the Practice of Technological Body Modifications. *Historická Sociologie*, *12*(1), 49–63. https://doi.org/10.14712/23363525.2020.4

Karnouskos, S. (2022). Symbiosis with artificial intelligence via the prism of law, robots, and society. *Artificial Intelligence and Law*, *30*(1), 93–115. https://doi.org/10.1007/s10506-021-09289-1

Khandelwal, A., Agrawal, A., Bhattacharyya, A., Singla, Y. K., Singh, S., Bhattacharya, U., Dasgupta, I., Petrangeli, S., Shah, R. R., Chen, Ch., & Krishnamurthy, B. (2024). Large Content and Behavior Models to Understand, Simulate, And Optimize Content and Behavior. The Twelfth International Conference on Learning Representations, ICLR, Vienna. *arXiv:2309.00359v4*. https://doi.org/10.48550/arXiv.2309.00359

Kriegman, S., Blackiston, D., Levin, M., & Bongard, J. (2021). Kinematic self-replication in reconfigurable organisms. *Proceedings of the National Academy of Sciences*, *118*(49), e2112672118. https://doi.org/10.1073/pnas.2112672118

Księżak, P. (2024). *Artificial Intelligence and the Dawn of Cyborg Law. Key Legal Challenges for Private Law in the Era of Human Augmentation*. Warszawa: Allerhand Publishing.

Laurent, M., Geoffroy, M., Pavani, G., & Guiraud, S. (2024). CRISPR-Based Gene Therapies: From Preclinical to Clinical Treatments. *Cells*, *13*(10), 800. https://doi.org/10.3390/cells13100800

Lima, P. U., & Paiva, A. (2024). Autonomous and Intelligent Robots: Social, Legal and Ethical Issues. In H. Sousa Antunes, P. M. Freitas, A. L. Oliveira, C. Martins Pereira, E. Vaz de Sequeira, & L. Barreto Xavier (Eds.), *Multidisciplinary Perspectives on Artificial Intelligence and the Law. Law, Governance and Technology Series* (pp. 127–140). Cham, Switzerland. https://doi.org/10.1007/978-3-031-41264-6_7

Liu, Z., Cai, Y., Wang, Y., Nie, Y., Zhang, C., Xu, Y., Zhang, X., Lu, Y., Wang, Z., Poo, M., & Sun, Q. (2018). Cloning of Macaque Monkeys by Somatic Cell Nuclear Transfer. *Cell*, *172*(4), 881–887. https://doi.org/10.1016/j.cell.2018.01.020

Lloyd, N., Chowdhry, A., & Lewis, P. R. (2024). Trustworthy Embodied Virtual Agents. In N. Lee (Eds.), *Encyclopedia of Computer Graphics and Games* (pp. 1917–1922). Springer, Cham. https://doi.org/10.1007/978-3-031-23161-2_524

Lorimer, J. (2009). Posthumanism/Posthumanistic Geographies. In R. Kitchin, & N. Thrift (Eds.), *International Encyclopedia of Human Geography* (pp. 344–354). Oxford: Elsevier. https://doi.org/10.1016/b978-008044910-4.00723-9

Mestre, R., Astobiza, A. M., Webster-Wood, V. A., & Saif, M. T. A. (2024). Ethics and responsibility in biohybrid robotics research. *Proceedings of the National Academy of Sciences*, *121*(31), e2310458121. https://doi.org/10.1073/pnas.2310458121

Mocanu, D. M. (2021). Gradient Legal Personhood for AI Systems – Painting Continental Legal Shapes Made to Fit Analytical Molds. *Frontiers in Robotics and AI*, *8*, 788179. https://doi.org/10.3389/frobt.2021.788179

Momaya, A., Fawal, M., & Estes, R. (2015). Performance-Enhancing Substances in Sports: A Review of the Literature. *Sports Medicine*, *45*, 517–531. https://doi.org/10.1007/s40279-015-0308-9

Mori, M., MacDorman, K. F., & Kageki, N. (2012). The Uncanny Valley. *IEEE Robotics & Automation Magazine*, *19*(2), 98–100. https://doi.org/10.1109/MRA.2012.2192811

Morshedzadeh, F., Ghanei, M., Lotfi, M., Ghasemi, M., Ahmadi, M., Najari-Hanjani, P., Sharif, S., Mozaffari-Jovin, S., Peymani, M., & Abbaszadegan, M. R. (2024). An Update on the Application of CRISPR Technology in Clinical Practice. *Molecular Biotechnology*, *66*(2), 179–197. https://doi.org/10.1007/s12033-023-00724-z

Nolfi, S. (2024). On the Unexpected Abilities of Large Language Models. *Adaptive Behavior*, *32*(6), 493–502. https://doi.org/10.1177/10597123241256754

Olarte-Pascual, C., Pelegrín-Borondo, J., Reinares-Lara, E., & Arias-Oliva, M. (2021). From wearable to insideable: Is ethical judgment key to the acceptance of human capacity-enhancing intelligent technologies? *Computers in Human Behavior*, *114*, 106559. https://doi.org/10.1016/j.chb.2020.106559

Palmerini, E., Bertolini, A., Battaglia, F., Koops, B.-J., Carnevale, A., & Salvini, P. (2016). RoboLaw: Towards a European framework for robotics regulation. *Robotics and Autonomous Systems*, *86*, 78–85. https://doi.org/10.1016/j.robot.2016.08.026

Perez, E. (2022). Future of Therapy for Inborn Errors of Immunity. *Clinical Reviews in Allergy & Immunology*, *63*(1), 75–89. https://doi.org/10.1007/s12016-021-08916-8

Pluchino, S., & Lombardi, I. (2024). Crossing species boundaries in regenerative neuroscience with rat–mouse brain chimeras. *Lab Animal*, *53*, 179–180. https://doi.org/10.1038/s41684-024-01394-3

Ponce del Castillo, A. (2024). *Artificial intelligence, labour and society*. Brussels: ETUI.

Przhilenskiy, V. I. (2024). Bioethics: Epistemic Capabilities and Legal Frameworks. *Kutafin Law Review*, *11*(2), 180–198. https://doi.org/10.17803/2713-0533.2024.2.28.180-198

Reichel, P., Bassler, C. T., & Spörrle, M. (2024). Embracing the enhanced self now and in the future: The impact of temporal focus, age, and sex on cyborg products use intention. *Personality and Individual Differences*, *225*, 112665. https://doi.org/10.1016/j.paid.2024.112665

Roco, M. C., & Bainbridge, W. S. (2003). *Converging Technologies for Improving Human Performance. Nanotechnology, Biotechnology, Information Technology and Cognitive Science*. Dordrecht: Springer. https://doi.org/10.1007/978-94-017-0359-8

Sandini, G., Sciutti, A., & Morasso, P. (2024). Artificial cognition vs. artificial intelligence for next-generation autonomous robotic agents. *Frontiers in Computational Neuroscience*, *18*, 1349408. https://doi.org/10.3389/fncom.2024.1349408

Sharon, A., Jankowski, M. M., Shmoel, N., Erez, H., & Spira, M. E. (2023). Significantly reduced inflammatory foreign-body-response to neuroimplants and improved recording performance in young compared to adult rats. *Acta Biomaterialia*, *158*, 292–307. https://doi.org/10.1016/j.actbio.2023.01.002

Soori, M., Arezoo, B., & Dastres, R. (2023). Artificial intelligence, machine learning and deep learning in advanced robotics, a review. *Cognitive Robotics*, *3*, 54–70. https://doi.org/10.1016/j.cogr.2023.04.001

Tan, T., Wu, J., Si, C., Dai, S., Zhang, Y., Sun, N., Zhang, E., Shao, H., Si, W., Yang, P., Wang, H., Chen, Z., Zhu, R., Kang, Y., Hernandez-Benitez, R., Martinez Martinez, L., Nuñez Delicado, E., Berggren, W. T., Schwarz, M., … & Izpisua Belmonte, J. C. (2021). Chimeric contribution of human extended pluripotent stem cells to monkey embryos ex vivo. *Cell, 184*(13), 3589. https://doi.org/10.1016/j.cell.2021.06.011

Vaughn, L. (2023). *Bioethics: Principles, Issues, and Cases* (5th ed.). Oxford University Press.

Veit, W. (2018). Procreative Beneficence and Genetic Enhancement. *Kriterion – Journal of Philosophy*, *32*(1), 75–92. https://doi.org/10.1515/krt-2018-320105

Viljanen, M. (2017). A Cyborg Turn in Law? *German Law Journal*, *18*(5), 1277–1308. https://doi.org/10.1017/S2071832200022331

Wajnerman, A., & López-Silva, P. (2022). Mental Privacy and Neuroprotection: An Open Debate. In P. López-Silva, & L. Valera (Eds.), *Protecting the Mind. Challenges in Law, Neuroprotection, and Neurorights* (pp. 141–155). Cham, Switzerland. https://doi.org/10.1007/978-3-030-94032-4_12

Zhang, H., Xuan, Z., Yu, F., Ding, X., & Han Y. (2024). Crafting the modern Prometheus: navigating morality and identity in the age of cyborg enhancements. *Philosophical Psychology*, 1–34. https://doi.org/10.1080/09515089.2024.2382297

Сведения об авторе

Филипова Ирина Анатольевна – кандидат юридических наук, доцент, доцент кафедры трудового и экологического права, Национальный исследовательский Нижегородский государственный университет имени Н. И. Лобачевского; руководитель Центрально-Азиатского исследовательского центра регулирования искусственного интеллекта, Самаркандский государственный университет
Адрес: 603922, Россия, г. Нижний Новгород, проспект Гагарина, 23;
140104, Узбекистан, г. Самарканд, Университетский бульвар, 15
E-mail: irinafilipova@yandex.ru
ORCID ID: https://orcid.org/0000-0003-1773-5268
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57327205000
WoS Researcher ID: https://www.webofscience.com/wos/author/record/R-1375-2016
Google Scholar ID: https://scholar.google.com/citations?user=opJc7fcAAAAJ
РИНЦ Author ID: https://elibrary.ru/author_profile.asp?authorid=461586

Конфликт интересов

Автор является заместителем главного редактора журнала, статья прошла рецензирование на общих основаниях.

Финансирование

Исследование не имело спонсорской поддержки.

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.07.45 / Право и научно-технический прогресс
Специальность ВАК: 5.1.1 / Теоретико-исторические правовые науки

История статьи

Дата поступления – 11 ноября 2024 г.
Дата одобрения после рецензирования – 25 ноября 2024 г.
Дата принятия к опубликованию – 13 декабря 2024 г.
Дата онлайн-размещения – 20 декабря 2024 г.

Research article
UDC 34:004:342.1:004
EDN: https://elibrary.ru/bbsqnh
DOI: https://doi.org/10.21202/jdtl.2024.39

A Rechtsgutstheorie Lens on the Legal Aspects of the States' Cyber Interest Concept

Yassin Abdalla Abdelkarim

Luxor Elementary Court, Luxor, Egypt
Leeds Beckett University, Leeds, United Kingdom

Keywords

criminal law,
cyber diplomacy,
cyber interests,
cyberspace,
digital technologies,
human rights,
international judicial practice,
national interests,
state interests,
theory of legitimate interests

Abstract

Objective: to show the evolution of the state interests concept and its application in cyberspace, where it turns out to be fundamental for the development of state military policy aimed at protecting national interests.

Methods: the research is based on the intersection of the theory of law and the concept of cyber interests of the state through the prism of the theory of legitimate interests (Rechtsgutstheorie). The latter was originally developed within the criminal law science, but with prospects for studying the concept of state interests in cyberspace. The application of the theory of legitimate interests made it possible to study the state cyber interests concept and determine its legal classification and applications. In particular, the theory of legitimate interests in this study is used to explore the legal perspectives of the concept of state interests in cyberspace as interests subject to legal protection.

Results: it is determined that in the dynamic landscape of cyberspace, there are multifaceted interests of states related to national security, economic prosperity, sovereignty and diplomacy. To ensure their protection, states initiate strategies that generate a variety of political and legal consequences in international relations. This fact determines the importance of studying the concept of state interests from a legal viewpoint, as well as their legal status and consequences. Parallels are drawn between the concept of protected legal interests within the theory of legitimate interests and cyber interests that states seek to protect. The theory requires balancing the competing interests; hence, its applicability to the actions of the state in cyberspace is considered. The obstacles are identified, that hinder applying the theory of legitimate

© Abdelkarim Y. A., 2024

This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (CC BY 4.0) (https://creativecommons.org/licenses/by/4.0), which permits unrestricted re-use, distribution and reproduction, provided the original article is properly cited.

interests to cyberspace, including difficulties of attribution, damage thresholds and the need for global consensus. The author shows the evolution of the concept of state interests, which determines the possibility of its application in cyberspace, where it serves the purposes of developing state policy aimed at protecting national interests.

Scientific novelty: it is expressed in the reflection of the theory of legitimate interests to the formation of the legal concept of cyber interests of the state, which serves as a sufficient justification for the protection of specific cyber interests.

Practical significance: the main conclusions outlined in the article can be used to identify cyberspace interests subject to legal protection (such as confidentiality, data integrity, sovereignty, and economic stability). They may also improve legal mechanisms for protecting national interests in cyberspace, ensure uniformity of relevant international judicial practice, and improve the efficiency and quality of state policy management in cyberspace in order to ensure security and peaceful coexistence.

For citation

Abdelkarim, Y. A. (2024). A Rechtsgutstheorie Lens on the Legal Aspects of the States' Cyber Interest Concept. *Journal of Digital Technologies and Law, 2*(4), 782–801. https://doi.org/10.21202/jdtl.2024.39

Content

Introduction
1. Evolution of the Concept of State's Interest in the Digital Realm
   1.1. Traditional Understanding
   1.2. A Novel Reality in the Cyber Era
2. The Theory of Protected Legal Interests
   2.1. Main provisions of the theory of legitimate interests
   2.2. Contribution to Legal Systems
3. State's Cyber Interest as a Protected Legal Interest
   3.1. The Rechtsgutstheorie Validity in Cyberspace
   3.2. The Rechtsgutstheorie Implications on the State's Cyber Interests Concept
Conclusion
References

Introduction

Among the determinants of a state's success is the ability to satisfy and secure critical needs required for the welfare and prosperity of the citizenry and the functionality of the state's strengths in the international community. Those factors combined formulate the conception of the state's interest. In politics, it could be observed that interests are

the momentum to impose national strategies and policies that influence international relations. They constitute the chief axis of international relations, which points out the prominence of their conception from a political perspective. Nevertheless, the prima facie impacts of this concept in politics never overshadow the true legal aspects that should be explored. Several legal questions can be triggered when studying the impacts on the state's cyber interest concept regarding its classification and legal impacts.

The inevitable synergy between politics and law concerning the concept of the state's cyber interest drives the research to elect a certain legal theory to study this concept through its perspective. The search within law branches reveals that criminal law has adequate theories and notions to carry out the research mission. Theorized originally by German scholars, the research utilizes the theory of protected legal interests – the Rechtsgutstheorie – to explore and profile the concept of the state's cyber interest and determine its legal classification and the effects of reviewing it through a specific legal theory. The broad normative of criminal law along with its flexible applicability encourages the research to choose a criminal law theory to answer its question, which the Rechtsgutstheorie contributes to analyze and determine. Furthermore, the literature discloses that this theory achieves an effective role in criminal legal matters, regardless of the scholarly critiques for being domestically originated. Thus, the research adopts it to explore the legal perspectives of the concept of the state's cyber interest and introduces it as a protected legal interest.

1. Evolution of the Concept of State's Interest in the Digital Realm

The notable divergence in nature and context between the real world and cyberspace affects the perspectives from which the concept of state interest is reviewed. While in the former traditional scholarships overwhelm the explanation and interpretation of this concept, highlighting the realistic characteristics of interest concepts, in the digital realm of cyberspace one can undoubtedly notice the impacts of the prevailing technological atmosphere on the aspects of this concept. Thus, the study should divide relevant scholarships on the concept of state interest into traditional doctrine focusing on the prevailing understanding of this concept in the real world and the other section reveals the effects of cybernetics on contemporary literature on the interest concept.

1.1. Traditional Understanding

Deriving from the basic humanitarian endeavor to achieve advantages and avoid casualties the concept of interest was created to express this objective. Wang (2022) explained that human needs, desires, and aspirations are the momentum for the existence of interests, and satisfaction is required to maintain the integrity of humans. To sustain and enhance human life, meeting basic needs is crucial. Nonetheless, at its

core, satisfying needs involves obtaining desired objects through specific methods. Whilst the need to manifest the psychological motivation for the pursuit of interests, the latter reflects realistic attempts to satisfy those needs through human interaction mechanisms, e.g., production, trade, and diplomacy (Wang, 2022). In addition, individual interests perform as incentives for the human's best exploitation of available resources to achieve benefits (Thomas, 2023); fragmentation of interests contributes crucially to realizing global welfare and prosperity. As a nexus between needs and means, interest represents the fusion of human needs and the methods to fulfill them. Furthermore, interests have a social aspect that showcases a tight relationship between the state and its citizenry.

Regarding states, interests as a social phenomenon pertain to national requirements that fulfill domestic needs, often in opposition to the interests of other states (Abdelkarim, 2024). The term "national interest" can be elusive, as its interpretation varies depending on the context of its utilization. Statesmen and policymakers wield it to justify their actions and defend their policies. Given that states may vary in their criteria for identifying interests, conflicts of interest arise in which states utilize a variety of tools to defend their interests (Thomas, 2023; Topor, 2024). Consequently, interests shape state behavior on the international stage to ensure their needs are met. Since formed by a unified group of human needs, the state's interests represent a common national objective (Wang, 2022). The similarity of fundamental needs of a given social group justifies this feature of the state's interests. In addition, Common interests manifest publicly within specific social relations, and this publicity varies in meaning across different social and interest relations (Wang, 2022). It can refer to the shared content of interests among the subjects within these relationships. A strong example of common interests is the social need for external security. Pointing out their contribution to world stability, Onditi (2023) considered interests a chief tool that determines the shape of global inter-state diplomacy and conflict resolution methods. Maintaining national interests is the true end of diplomacy and the true reason for the grave diversity witnessed among states in this aspect.

Moreover, Wang (2022) claimed that common interests are united within a social group. The unity of common interests implies that within a specific interest relationship, common interests are typically unique. This unity of common interest forms the basis for public political power within a particular scope and is grounded in specific interest relations in social and political life. It is prominent to note that while common interests are distinct within a particular society and interest relationship, this does not preclude the possibility that these specific common interests encompass various aspects of actual content and value.

The states' interests represent an inter-connected group of needs and objectives that national governments seek to satisfy through several methods, such as diplomacy and legal or armed conflicts. According to Metea (2020), to qualify as national, interest should be broad, transcending narrow contexts, and must demonstrate resilience over time against alteration by temporal shifts. Then, national interests emerge from a complex interplay of enduring, broadly applicable concerns, ensuring the stability and success of a nation, whose satisfaction reflects the strength of a given state and the level of power it should maintain or acquire on the international stage to protect national interests. Concurrently, Cox (2021) posited that interests have emerged as a central focus in social sciences due to their role in shaping collective emotions within a community. Consequently, interests represent the collective motivation of a group, prompting national authorities to take protective actions.

Despite the ambiguity of this concept, the prominent US politician Samuel Huntington defines national interest as "a public good that concerns everyone, or most citizens; a vital national interest is that interest for which they are willing to shed their blood and spend their wealth to defend it. National interests usually combine security with material concerns, on the one hand, and moral and ethical concerns, on the other" (Huntington, 1997; Metea, 2020). According to McLean and McMillan (2009), the concept of national interest encompasses various dimensions and serves as a critical framework in both political discourse and foreign policy analysis. For the former, politicians heavily utilize this concept to garner support for specific actions. Within domestic policy, its persuasive power is limited due to diverse opinions. Nevertheless, in foreign policy, it conjures an image of the nation defending its interests in an anarchic international system, which constitutes a standard to determine the strength of a state in the international community (Thomas, 2023).

1.2. A Novel Reality in the Cyber Era

The emergence of cyberspace has provoked unsettled debates on determining its impacts on human interactions and the potentiality to enforce changes in the landscape of international relations (Foulon & Meibauer, 2024). Being an open-access universal liberal sphere of interactions, cyberspace offers fertile soil for lucrative opportunities to grow and spread benefits among users (Thomas, 2023). Thus, dozens of various interests are being generated as data streams across the Internet, complicating the nature and core of human interactions.

As cyber capabilities and the logic of cyberspace expand, they alter how states interact within the international system, considering the impacts of free cyberspace attitudes (Thomas, 2023). Unlike earlier technologies like the telegraph, which merely sped up communication, cyberspace enables direct and immediate interactions between

governments and foreign populations. This widespread access to cyberspace acts as a distributed capability but does not change the fundamental principles of state behavior, which are still driven by anarchy and material power distribution. The universality of cyberspace, inter alia its powerful capabilities and unique structural setup that provided limitless resources, elevated the consequences of human interaction therein to a cosmopolitan level, exceeding, therefore, the limits of bilateral interactions. Indeed, the material and ideational dimensions of cyberspace, influenced by factors such as strategic culture and resource availability, are utilized and dominated by certain actors more than others. This unequal control makes cyberspace more beneficial for some actors compared to others. Consequently, cyber diplomacy has emerged in the sphere of international relations as a burgeoning international practice aimed at creating a cyber-international society, harmonizing the national interests of states with the dynamics of global society (Topor, 2024).

In the international theatre, states are the chief actors according to the national interests of each state. They pursue those interests through an anarchic scheme depending on the state's geopolitical power and technological superiority (Foulon & Meibauer, 2024), which constitute the crucial factors determining states' behavior in cyberspace. The wealthiness of data availability in cyberspace formulates a structural modifier influencing international relations because of the ultimate power of technological superiority utilized to control data on the Internet (Foulon & Meibauer, 2024), granting the concept of state interest a novel dimension featured by cybernetic characteristics. Furthermore, cyberspace influences how structural factors are experienced and perceived, similar to how nuclear weapons have not altered the basic logic of state behavior but have changed perceptions of threats and capabilities. Consequently, cyberspace affects the dynamics of international relations, shaping the constraints, incentives, and behaviors of states. In the context of cyberspace, this implies that each state will act to fulfill its national needs online, with cyber behavior driven by these interests (Abdelkarim, 2024). Therefore, reality showcases the critical impacts of the concept of states' cyber interests on drafting inter-state policies and international relations. Furthermore, national interests manifest the momentum for states to intervene and draft their policies in cyberspace (Topor, 2024). Studying states' approaches reveals hastened endeavors to crystallize authority according to national interests to protect their critical infrastructure, such as power grids, financial systems, and communication networks, from cyber attacks as well as achieve economic advantages through the available opportunities in the digital environment.

It should be noted that acquiring powerful technological abilities is not a requirement for a state to pursue its interests in cyberspace since inflicting an effect does not need

more than mere simple Internet access tools. This status enshrouded national interests in cyberspace with great danger because the weakest Internet user can inflict severe damage on a state's interests (Abdelkarim, 2024). Thus, defending the integrity of national interests implies admitting their cybernetic theme to guide the state to the most appropriate methods to maintain them. Moreover, the state's interests primarily drive nationalism in cyberspace (Cox, 2021). When a state's cyber interests are threatened, national intervention becomes necessary to protect the integrity of national benefits. This aligns with the fundamental principles of sovereignty and nationalism in cyberspace. Additionally, threats to state cyber interests can lead to cyber warfare, characterized by mutual cyberattacks across state cyber borders to defend national economic and military assets (Fang, 2018). Such threats necessitate prompt state responses to safeguard national interests.

In an official report, the US Government Accountability Office highlighted the urgent need to develop a national cyber diplomacy strategy to safeguard state interests in cyberspace.[1] This report marked an official governmental acknowledgment of the concept of state cyber interest and employed it to shape national cyber diplomacy. As a result, the notion of state cyber interest is now firmly established in political and diplomatic arenas to handle challenges and protect national interests. Abdelkarim (2024) solidified this conclusion as he claimed that the notion of state interests in cyberspace has evolved to shape the foundation of state cyber policies. The flexibility of its core principles concerning cyber interactions enables this concept to serve as a determinant of state authority in cyberspace. In the same context, Reiterer (2022) argued that the state's cyber interests should be the core axis of cyber diplomacy to safeguard national integrity in cyberspace. As he indicated, the continuing development of cyber threats implies concentrating on the deployment of the latest technologies as a part of national strategies to confront those threats. He, also, argued that common cyber interests, e. g., defending critical infrastructure and other national security concerns, have become the pillar of collateral cooperation between the European Union and other international partners regardless of the diversity of individual states' national interests (Reiterer, 2022). Therefore, the tight nexus of cyber diplomacy and interests' concept is indisputable.

[1] US Government Accountability Office. (2024, January). Cyber Diplomacy. State's Efforts Aim to Support U.S. Interests and Elevate Priorities: Report to Congressional Addressees. https://clck.ru/3A7Y99

2. The Theory of Protected Legal Interests

2.1. Main provisions of the theory of legitimate interests

Originated by German criminal literature, the theory of legal interests – Rechtsgutstheorie – introduces a detailed analytical description of human interests that should be protected by legal rules in the whole legal system around the globe (Atadjanov, 2019), regardless of national backgrounds. Traditionally, the Rechtsgutstheorie applies to any interest or value endorsed by national legislation. Consequently, legal interests constitute the threshold to criminalize violations of their protected status. Thus, an act affecting this status should be reviewed in the light of the Rechtsgutstheorie to determine what response should be taken to maintain the integrity of legal interests (Atadjanov, 2019; Tianyang, 2024), which grants legislators and literature with a functional normative application of the Rechtsgutstheorie. Therefore, Atadjanov (2019) justified the invention of the Rechtsgutstheorie in German criminal literature by the doctrine that considers the crime a violation of subjective rights, not just legal rules. Accordingly, Ambos (2015) argued earlier that the Rechtsgutstheorie has come to the legal scholarship to cure the deficiencies of the rights theory by enabling the criminalization of violations to other legal interests that are not considered rights in the traditional meaning of this concept. Thus, he claimed that the concept of legal interests means the necessary conditions and objectives for the free development of individuals, the realization of their fundamental rights, and the proper functioning of state institutions required to achieve these objectives. He, also, advocated that the normative perspective of the Rechtsgutstheorie contributes to materializing other legal principles such as the harm principle by solidifying the reasons for the criminalization process and establishing the required criteria of legal concepts. Furthermore, the Rechtsgutstheorie adaptability to be combined with other legal principles provides a flexible formula that contributes to overcoming legal vagueness and promotes the rules of law (Ambos, 2015).

Lanz (2023) discussed that understanding the term «protected legal interest» has two categories: descriptively or normatively. Descriptively, it refers to legal interests safeguarded by existing criminal laws. Normatively, it signifies legal interests that, according to certain criminal policy viewpoints, should be protected by criminal law. Alio modo, Tianyang (2024) concluded that the principle of protected legal interests is thoroughly embedded in criminal legislation. As a crucial legal instrument for upholding social order and safeguarding citizens' rights, this principle is integral to the legislative process. By clearly defining criminal acts, establishing appropriate punishments, and adapting to social changes, criminal legislation ensures the effective implementation of this principle. This approach not only respects individual rights but also underscores the role of criminal law in maintaining social order.

Atadjanov (2019) argued that the German understanding of the Rechtsgutstheorie proves inclusive and comprehensive that it could be stretched as a normative to include other categories of interests, even those exceeding the predictions of legal scholars and professionals. Protected legal interests are determinants guiding policymakers and legislators to the approach that safeguards national interests. Thus, novel concepts and terms may be included under the Rechtsgutstheorie because they achieve advantages for a certain state and are profiled, hence, fundamental values and interests. This manifests the direct consequence of the Rechtsgutstheorie normative aspect according to Atadjanov.

Notwithstanding, Wilenmann (2019) refuted this theory and criticized the scholarly parochialism and chauvinism expressed by German law scholars as he profiled this theory as an attempt to enforcably influence global criminal law scholarships while tending to be insular and self-referential. They position the Rechtsgutstheorie as a model for criminal law scholarship internationally, often overlooking perspectives from other legal traditions. Essentially, this criticism highlights the need for a more global and inclusive approach when discussing legal theories. Atadjanov (2019), despite being prominent in introducing the Rechtsgutstheorie in English scholarships, stipulated a normative justification of this theory to be practically useful in legal practice although the Rechtsgutstheorie provides a conceptual framework for understanding legal interests. His review emphasized that merely defining legal interests (Rechtsgüter) is insufficient; finding a justification for providing legal protection for certain interests is obligatory because, without this normative underpinning, the theory remains theoretical rather than actionable. Therefore, striking the balance between normative and practical aspects of the Rechtsgutstheorie proves indispensable to maintain the functionality of this German contribution to the legal theory.

2.2. Contribution to Legal Systems

The Rechtsgutstheorie serves as an instrument to expand official legal responses to criminal, and non-criminal, incidents to ensure the integrity of the protected interests by legal rules, which is a requirement of peaceful cohabitation within a society. Furthermore, Tianyang (2024) argued that the theory of human rights protection is a crucial foundation for the principle of safeguarding legal interests. Human rights, encompassing basic dignity, represent a core value that must not be overlooked in any legal system. As a significant mechanism for limiting citizens' rights, criminal legislation must adhere to the principle of human rights protection to ensure that citizens' legitimate rights and interests are not violated while addressing criminal activities (Lanz, 2023; Tianyang, 2024). Put simply, by adhering to the principle of protecting legal interests, it could be ensured that criminal law punishes crimes without infringing on the rights and interests of innocent individuals, thereby achieving justice and fairness. It should be noted that the mentioned legal interests represent the interests that criminal law seeks to protect. These can be tangible (like life, health, or property) or intangible (such as

personal dignity, privacy, or freedom), which manifest the core of the Rechtsgutstheorie. This role represents the normative aspect of the Rechtsgutstheorie by transcending the mere description of the status quo to advise about the appropriate treatment. Additionally, the Rechtsgutstheorie offers a constitutional guarantee to promote the legitimacy of judicial proceedings by maintaining the rights and interests of the litigation parties (Olha, 2024). Thus, it becomes impossible to deprive any citizen of an interest or a right without an obvious legal justification. It introduces a set of normatively defined and organizationally formalized methods and means that ensure the actual realization of the rights, freedoms, and responsibilities of individuals and citizens (Olha, 2024). Moreover, the Rechtsgutstheorie represents a reflection of the society's legal consciousness and justice awareness among its members, which enhances the trustworthiness and impartiality of the legal protection offered by the existing procedural legislation.

The Rechtsgutstheorie functional application permitted states, regardless of national regime ideology (Atadjanov, 2019), to draft unique schemes of legal interests that should be protected by operational state mechanisms such as legislation, diplomacy, and even military force. As a result, skeptics criticized Rechtsgutstheorie for lacking the minimum impartiality required for legal theories because certain regimes exploited its norms to justify their racist policies contrary to the natural common good sought by law. However, critiques did not frustrate the solid legal establishment of the Rechtsgutstheorie as Atadjanov (2019) advocated its contribution to developing the scope of criminal law and protecting essential legal interests. As the fundamental pillar of criminal legislation, the primary objective of protecting legal interests is to ensure that the legitimate rights and interests of every citizen are fully respected and safeguarded during the formulation and implementation of criminal law inter alia other statutes (Tianyang, 2024). Moreover, the Rechtsgutstheorie proves effective as a standard of the constitutionality of criminal law provisions when contested before the German Constitutional Court since it introduced a solid and disciplined normative to establish the Court's judgments (Ambos, 2015).

Judges have contributed largely to solidifying the Rechtsgutstheorie since the judicial interpretation of criminal law provisions elucidates the meaning and scope of the principle of legal interest protection (Tianyang, 2024). In practice, judges rely on these interpretations to address legal interest protection issues in specific cases, ensuring the principle is upheld. Judicial interpretations integrate social realities and judicial needs, providing in-depth analysis and guidance. This aids judges in correctly applying the principle and offers citizens clear legal guidance to safeguard their rights. The criminal code, amendments, and judicial interpretations all embody this principle in legislation and practice. Hence, ongoing judicial interpretation provides an effective application of the Rechtsgutstheorie to maintain social justice and stability regarding the implementation of legal rules.

3. State's Cyber Interest as a Protected Legal Interest

3.1. The Rechtsgutstheorie Validity in Cyberspace

As previously indicated, the German origin of the Rechtsgutstheorie profiles it as domestic; it keens with determining criminal conducts that constitute crimes within the society. Atadjanov's (2019) elaboration proves that German scholars never intended to employ this theory in international legal practice. Thus, the attempt to utilize it to maintain a state's cyber interests offers an expansion of the application of the Rechtsgutstheorie from domestic criminal law to non-criminal international law and, also, to politics and diplomacy.

Using a domestic criminal law theory to justify the state's policies to protect national interests in cyberspace is admittable because international legal practice discloses the adoption of the general principles of law, whether it was criminal law or international law, by international courts (Atadjanov, 2019) disregarding their domestic origins. The continuing adoption of general legal theories qualifies them to be solid legal status applicable to several legal questions. Furthermore, the immediate utilization of criminal law theories, inter alia the Rechtsgutstheorie, eradicates the legislative vacuum when dealing with novel legal issues as a part of the natural contribution of criminal law doctrine. Atadjanov (2019) assured that the practice of international criminal tribunals discloses their resorting to basic criminal law principles to close any gaps that hinder deciding litigation. Thus, the domestic German Rechtsgutstheorie is qualified to be employed to govern states' practices regarding national interests in cyberspace, which constitutes an international virtual environment, once the domestic origin adopts the same legal principles admitted in international law. In the same vein, the International Criminal Court authorized establishing international judgments on domestic legal principles once the former accorded with the universal objectives of the Court.[2] The determinant in this case lies in the objective congruence in values between the domestic principle and international law.

Another foundation lies in the nature of criminal law itself; the Rechtsgutstheorie derives its applicability in cyberspace from the expansive nature of criminal law; criminal legal principles are of administrative nature that proves ongoing expansion in the field of human interactions governance (Bidasolo, 2023). He argued that legal practice has revealed that the accurate and innovative interpretation of criminal law principles by law practitioners expands their applicability to other spheres of human behavior apart from criminal offenses. De la Cuerda Martín (2023) considered that expanding criminal law principles is a direct consequence of the dominant sphere of globalization in cyberspace which implied re-thinking how to confront novel risk-generating activities through soft law instruments. She claimed that supranational economic integration,

[2] ICC, Prosecutor v. Mathleu Ngudjolo Chui, 18 December 2012, ICC-01/04-02/12.

market evolution, cybercrime, and transnational organized crime are tangible social risks of globalization. Without these factors, there would have been less necessity to criminalize new offenses or reform existing ones. Thus, the application of a criminal law theory in other human behavior aspects stipulates following a harmonized approach that is restricted to reason, necessity requirements, and achieving the common purpose of domestic needs satisfaction. As a state can employ a variety of toolkits to protect national interests (Thomas, 2023), a criminal law theory, i.e., the Rechtsgutstheorie, should be prioritized over those methods because it legitimizes measures taken by a state to protect cyber interests.

Since states' policies in cyberspace move around their interests, the Rechtsgutstheorie would enhance the stability of world order by organizing when and how should a state intervene in the digital realm to protect a national interest. In this objective, the Rechtsgutstheorie meets with the literal interpretation of the interest concept as explained by Onditi (2023). The limiting role of this theory in criminal law supports the accomplishment of the objective assigned, especially considering the absence of a consensual mechanism in international law that governs this question (Abdelkarim, 2024). Indeed, the differentiation among states' national perspectives of the concept of interest triggers legal frictions concerning the interpretation of protected legal interests. Reaching a unified, or at least consensual, understanding of the normative of the Rechtsgutstheorie among scholars decreases decisively the potentialities of these frictions, considering the powerful capabilities of cyberspace technologies and the inequality in national cyber abilities among states. This contribution represents the natural cosmopolitan role of criminal law theories.

3.2. The Rechtsgutstheorie Implications on the State's Cyber Interests Concept

As a political conception, interests contribute to drawing the features and impacts of states' national strategies and policies on the international theatre (Metea, 2020; Wang, 2022) as they secure the satisfaction of national needs. This classification implies that to be a legal normative interests must satisfy a certain criterion consisting of legal fundamentals that elevate the interests' concept to be protected legal interests. Since the Rechtsgutstheorie presents a set of legal requirements to apply to a given notion, interests should satisfy the Rechtsgutstheorie requirements and enjoy the ultimate legal protection offered by this theory.

From the previous explanation of interest's concepts, along with the contemporary understanding of the Rechtsgutstheorie, the concept of protected legal interest consists of several concretes which are:

1) objective: to satisfy a need for a certain group,

2) necessity: an indispensable requirement to achieve that purpose,

3) effect: to achieve a desired modification for this group.

Therefore, national interests in cyberspace should satisfy these pillars to be entailed under the Rechtsgutstheorie as protected legal interests, invoking, thus, the state's authorities to protect them in this virtual environment. In cyberspace, an interest should respond to a specific need of the state's citizenry that enhances their life standard, should be indispensable to achieve continuing development of the inner society, and its impacts on the citizenry must be positive and realistic. Upon meeting these requirements, national interests in cyberspace prove qualified to be protected legal interests, which maintenance achieves the common objectives of criminal law theories concerning ensuring peaceful cohabitation and security in cyberspace. This approach simulates Atadjanov's logic (2019) to consider humanness, which is a philosophical social conception, a protected legal interest under the Rechtsgutstheorie since humanness satisfies certain requirements he mentioned.

The governance of states' policies in cyberspace to ensure security and peaceful cohabitation constitutes the necessary status implying the subordination of national policies therein to a firm law theory, such as the Rechtsgutstheorie. Without seeking to achieve this goal, the search for a legal foundation for national policies defending states' interests in cyberspace becomes meaningless; this goal represents the logical justification for utilizing a domestic criminal law theory in the field of states' policies in cyberspace, considering the universal scholarly consensus on the interest's concept. It is admitted that the absence of rules that govern states' cyber policies threatens universal peace and security because unilateral policies lead to inter-state conflicts; a negative consequence that should be evaded. Moreover, Atadjanov (2019) claimed that an obvious collateral objective is crucial to applying the Rechtsgutstheorie because a pure description of a legal interest proves insufficient to apply this theory. The functional aspect is the dominant factor in this regard.

Furthermore, the flexibility of the state's cyber interests concept, which is a special feature that suits the pure technical nature of cyberspace according to Abdelkarim (2024), permits operating the mechanism as mentioned above to profile them as protected legal interest under the Rechtsgutstheorie because flexibility, in this context, supports the application of legal logic tools, e.g., induction, analogy, analyzing, and concluding, to figure out the applicability of legal theories on political conceptions.

To conclude, the Rechtsgutstheorie influences the contemporary understanding of state cyber interests because it promotes national abilities to identify cyber interests that are worth legal protection such as Privacy, data integrity, sovereignty, and economic stability, and draft policies to safeguard their integrity. Its application advocates the governability of cyberspace; it is not a lawless vacuum but a sphere where legal theories prove functional.

Conclusion

The research clarifies that the state's interest concept has technically evolved to become realistic in cyberspace, where it proves fundamental to draft national policies that aim at safeguarding national interests. The reality of this conception has transcended traditional political understanding to construct a solid legal establishment. Since unilateral actions might lead to conflicts, the research attempts to develop a legal theorization to analyze and profile the concept of a state's cyber interest. The research endeavor to apply a criminal law theory on protected legal interests to the conception of a state's cyber interest proves effective because of the powerful applicability of criminal law principles which enhances its adoption in several legal questions. Accordingly, the Rechtsgutstheorie is qualified to accomplish the assigned contribution to profiling the state's cyber interest concept as protected legal interests. Therefore, a comprehensive legal umbrella extends to defend national interests in cyberspace. This constitutes the core of the state's interest concept legal aspect.

In summary, the Rechtsgutstheorie provides a lens through which the concept of the state's cyber interests could be analyzed from a legal perspective. As digital landscapes evolve, legal theory adapts, and the quest for balance continues to enhance the rule of law in cyberspace.

References

Abdelkarim, Y. A. (2024). A Literature Review of the Evolution of Sovereignty and Borders Concepts in Cyberspace. *International Cybersecurity Law Review*, *5*, 365–372. https://doi.org/10.1365/s43439-024-00118-0

Ambos, K. (2015). The Overall Function of International Criminal Law: Striking the Right Balance Between the Rechtsgut and the Harm Principles: A Second Contribution Towards a Consistent Theory of ICL. *Criminal Law and Philosophy*, *9*, 301–329. https://doi.org/10.1007/s11572-013-9266-1

Atadjanov, R. (2019). *Humanness as a Protected Legal Interest of Crimes Against Humanity: Conceptual and Normative Aspects*. TMC Asser Press. https://doi.org/10.1007/978-94-6265-299-6

Bidasolo, M. C. (2023). Is It Possible to Limit the Penal Intervention in the Twenty-First Century? In E. C. Demetrio et al. (Eds.), *Crisis of the Criminal Law in the Democratic Constitutional State, Legal Studies in International, European and Comparative Criminal Law* (Vol. 6, pp. 3–16). Springer Nature Switzerland AG. https://doi.org/10.1007/978-3-031-13413-5_1

Cox, L. (2021). *Nationalism: Themes, Theories, and Controversies*. Palgrave Macmillan. https://doi.org/10.1007/978-981-15-9320-8

de la Cuerda Martín, M. (2023). The Impact of Soft Law on the Expansion of Criminal Law. In E. C. Demetrio et al. (Eds.), *Crisis of the Criminal Law in the Democratic Constitutional State, Legal Studies in International, European and Comparative Criminal Law* (Vol. 6, pp. 231–249). Springer Nature Switzerland AG. https://doi.org/10.1007/978-3-031-13413-5_13

Fang, B. (2018). *Cyberspace Sovereignty: Reflections on Building a Community of Common Future in Cyberspace*. Science Press and Springer Nature Singapore Pte Ltd. https://doi.org/10.1007/978-981-13-0320-3

Foulon, M., & Meibauer, G. (2024). How cyberspace affects international relations: The promise of structural modifiers. *Contemporary Security Policy*, *45*(3), 426–458. https://doi.org/10.1080/13523260.2024.2365062

Huntington, S. (1997). The Erosion of American National Interests. *Foreign Affairs*, *76*(5), 28–49. https://doi.org/10.2307/20048198

Lanz, J. G. (2023). The Attack on the Protected Legal Interests: A Criminalisation Principle and an Element of the Criminal Offence. *Ius Novem*, *17*(3), 19–31. https://doi.org/10.2478/in-2023-0019

McLean, I., & McMillan, A. (2009). *The Concise Oxford Dictionary of Politics* (3 ed.). Oxford University Press. https://doi.org/10.1093/acref/9780199207800.001.0001

Metea, I. (2020). National Interest: Terminology and Directions of Approach. In *International Conference Knowledge-Based Organization*, *26*(1), 75–79. https://doi.org/10.2478/kbo-2020-0011

Olha, M. (2024). The Concept of Effectiveness of Ensuring the Rights and Legal Interests of a Person in Pre-trial Criminal Proceedings. *Visegrad Journal on Human Rights*, *1*, 56–63. https://doi.org/10.61345/1339-7915.2024.1.9

Onditi, F. (2023). Introduction: Diplomatic Thought and Practice. In F. Onditi et al. (Eds.), *The Palgrave Handbook of Diplomatic Thought and Practice in the Digital Age*. (pp. 1–31). Springer Nature Switzerland AG. https://doi.org/10.1007/978-3-031-28214-0_1

Reiterer, M. (2022). EU Cyber Diplomacy: Value- and Interest-Driven Foreign Policy with New Focus on the Indo-Pacifc. In G. Boulet, M. Reiterer, & R. P. Pardo (Eds.). *Cybersecurity Policy in the EU and South Korea from Consultation to Action. New Security Challenges* (pp. 17–39). Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-031-08384-6_2

Thomas, A. J. (2023). The Open World Ethos. In *The Open World, Hackbacks and Global Justice* (pp. 15–36). Springer Nature Singapore Pte Ltd. https://doi.org/10.1007/978-981-19-8132-6_2

Tianyang, L. (2024). The Embodiment and Practice of the Principle of Legal Interest Protection in Criminal Legislation. *International Journal of Frontiers in Sociology*, *6*(3), 44–50. https://doi.org/10.25236/ijfs.2024.060308

Topor, L. (2024). Sovereignty, Power, International Security and a Lack of International Law. In *Cyber Sovereignty. Global Power Shift* (pp. 45–73). Springer Cham. https://doi.org/10.1007/978-3-031-58199-1_3

Wang, P. (2022). *Principle of Interest Politics: Logic of Political Life from China's Perspective*. Peking University Press. Springer. https://doi.org/10.1007/978-981-19-3963-1

Wilenmann, J. (2019). A New Legal Science with an Old Aftertaste. *The University of Toronto Law Journal*, *69*(4), 540–556. https://doi.org/10.3138/utlj.2019-0057

Authors information

Yassin Abdalla Abdelkarim – Judge, Luxor Elementary Court, Egyptian Ministry of Justice; LLM Master of Laws, Leeds Law School, Leeds Beckett University
Address: New Casalovy Hotel Street, Akhmim Sohag Street, Madinat Nasser, 82516, Sohag, Egypt; LS1 3HE, City Campus, Leeds, United Kingdom
E-mail: yassinabdelkarim91@gmail.com
ORCID ID: https://orcid.org/0000-0001-7388-1337

Conflict of interests

The author declare no conflict of interests.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law
PASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – October 3, 2024
Date of approval – October 15, 2024
Date of acceptance – December 13, 2024
Date of online placement – December 20, 2024

Научная статья
УДК 34:004:342.1:004
EDN: https://elibrary.ru/bbsqnh
DOI: https://doi.org/10.21202/jdtl.2024.39

Правовые аспекты концепции киберинтересов государств через призму теории законных интересов

Яссин Абдалла Абделькарим

Суд общей юрисдикции в Луксоре, Луксор, Египет
Лидский университет Беккета, Лидс, Великобритания

Ключевые слова

государственные интересы,
кибердипломатия,
киберинтересы,
киберпространство,
международная судебная,
практика,
национальные интересы,
теория законных интересов,
права человека,
уголовное право,
цифровые технологии

Аннотация

Цель: показать эволюцию концепции государственных интересов и ее применение в киберпространстве, где она оказывается основополагающей для разработки государствоенной политики, направленной на защиту национальных интересов.

Методы: исследование базируется на пересечении теории права и концепции киберинтересов государства через призму теории законных интересов (Rechtsgutstheorie), изначально разработанной в рамках уголовно-правовой науки, но имеющей перспективы для изучения концепции государственных интересов в киберпространстве. Применение теории законных интересов позволило изучить понятие киберинтересов государства и определить его правовую классификацию, а также приложения к концепции государственных интересов в киберпространстве. В частности, теория законных интересов в настоящем исследовании используется для изучения правовых перспектив концепции государственных интересов в киберпространстве как интересов, подлежащих правовой защите.

Результаты: определено, что в динамичном ландшафте киберпространства существуют многогранные интересы государств, связанные с национальной безопасностью, экономическим процветанием, суверенитетом и дипломатией, для обеспечения защиты которых государства инициируют стратегии, которые порождают разнообразные политико-правовые последствия в международных отношениях. Этим фактом определяется важность изучения концепции государственных интересов с юридической точки зрения, равно как и их правового статуса и последствий. Проведены параллели между концепцией охраняемых правовых интересов в рамках теории законных интересов и киберинтересами, которые государства стремятся защитить. Рассмотрена применимость требования этой теории о балансе конкурирующих интересов к действиям государства в киберпространстве.

© Абделькарим Я. А., 2024

Статья находится в открытом доступе и распространяется в соответствии с лицензией Creative Commons «Attribution» («Атрибуция») 4.0 Всемирная (CC BY 4.0) (https://creativecommons.org/licenses/by/4.0/deed.ru), позволяющей неограниченно использовать, распространять и воспроизводить материал при условии, что оригинальная работа упомянута с соблюдением правил цитирования.

Выявлены препятствия применения теории законных интересов к киберпространству, включая трудности атрибуции, пороговые значения ущерба и необходимость глобального консенсуса. Показана эволюция концепции государственных интересов, что обусловливает возможность ее применения в киберпространстве, где она служит целям разработки государственной политики, направленной на защиту национальных интересов.

Научная новизна: выражается в представленном в статье преломлении теории законных интересов к формированию правовой концепции киберинтересов государства, что служит достаточным обоснованием защиты конкретных киберинтересов.

Практическая значимость: основные выводы, изложенные в статье, могут быть использованы для выявления киберпространственных интересов, подлежащих правовой защите (таких как конфиденциальность, целостность данных, суверенитет и экономическая стабильность), совершенствования правовых механизмов защиты национальных интересов в киберпространстве, обеспечения единообразия релевантной международной судебной практики, повышения эффективности и качества управления политикой государств в киберпространстве с целью обеспечения безопасности и мирного сосуществования.

Для цитирования

Абделькарим, Я. А. (2024). Правовые аспекты концепции киберинтересов государств через призму теории законных интересов. *Journal of Digital Technologies and Law*, *2*(4), 782–801. https://doi.org/10.21202/jdtl.2024.39

Список литературы

Abdelkarim, Y. A. (2024). A Literature Review of the Evolution of Sovereignty and Borders Concepts in Cyberspace. *International Cybersecurity Law Review*, *5*, 365–372. https://doi.org/10.1365/s43439-024-00118-0

Ambos, K. (2015). The Overall Function of International Criminal Law: Striking the Right Balance Between the Rechtsgut and the Harm Principles: A Second Contribution Towards a Consistent Theory of ICL. *Criminal Law and Philosophy*, *9*, 301–329. https://doi.org/10.1007/s11572-013-9266-1

Atadjanov, R. (2019). *Humanness as a Protected Legal Interest of Crimes Against Humanity: Conceptual and Normative Aspects*. TMC Asser Press. https://doi.org/10.1007/978-94-6265-299-6

Bidasolo, M. C. (2023). Is It Possible to Limit the Penal Intervention in the Twenty-First Century? In E. C. Demetrio et al. (Eds.), *Crisis of the Criminal Law in the Democratic Constitutional State, Legal Studies in International, European and Comparative Criminal Law* (Vol. 6, pp. 3–16). Springer Nature Switzerland AG. https://doi.org/10.1007/978-3-031-13413-5_1

Cox, L. (2021). *Nationalism: Themes, Theories, and Controversies*. Palgrave Macmillan. https://doi.org/10.1007/978-981-15-9320-8

de la Cuerda Martín, M. (2023). The Impact of Soft Law on the Expansion of Criminal Law. In E. C. Demetrio et al. (Eds.), *Crisis of the Criminal Law in the Democratic Constitutional State, Legal Studies in International, European and Comparative Criminal Law* (Vol. 6, pp. 231–249). Springer Nature Switzerland AG. https://doi.org/10.1007/978-3-031-13413-5_13

Fang, B. (2018). *Cyberspace Sovereignty: Reflections on Building a Community of Common Future in Cyberspace*. Science Press and Springer Nature Singapore Pte Ltd. https://doi.org/10.1007/978-981-13-0320-3

Foulon, M., & Meibauer, G. (2024). How cyberspace affects international relations: The promise of structural modifiers. *Contemporary Security Policy*, *45*(3), 426–458. https://doi.org/10.1080/13523260.2024.2365062

Huntington, S. (1997). The Erosion of American National Interests. *Foreign Affairs*, *76*(5), 28–49. https://doi.org/10.2307/20048198

Lanz, J. G. (2023). The Attack on the Protected Legal Interests: A Criminalisation Principle and an Element of the Criminal Offence. *Ius Novem*, *17*(3), 19–31. https://doi.org/10.2478/in-2023-0019

McLean, I., & McMillan, A. (2009). *The Concise Oxford Dictionary of Politics* (3 ed.). Oxford University Press. https://doi.org/10.1093/acref/9780199207800.001.0001

Metea, I. (2020). National Interest: Terminology and Directions of Approach. In *International Conference Knowledge-Based Organization*, *26*(1), 75–79. https://doi.org/10.2478/kbo-2020-0011

Olha, M. (2024). The Concept of Effectiveness of Ensuring the Rights and Legal Interests of a Person in Pre-trial Criminal Proceedings. *Visegrad Journal on Human Rights*, *1*, 56–63. https://doi.org/10.61345/1339-7915.2024.1.9

Onditi, F. (2023). Introduction: Diplomatic Thought and Practice. In F. Onditi et al. (Eds.), *The Palgrave Handbook of Diplomatic Thought and Practice in the Digital Age*. (pp. 1–31). Springer Nature Switzerland AG. https://doi.org/10.1007/978-3-031-28214-0_1

Reiterer, M. (2022). EU Cyber Diplomacy: Value- and Interest-Driven Foreign Policy with New Focus on the Indo-Pacifc. In G. Boulet, M. Reiterer, & R. P. Pardo (Eds.). *Cybersecurity Policy in the EU and South Korea from Consultation to Action. New Security Challenges* (pp. 17–39). Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-031-08384-6_2

Thomas, A. J. (2023). The Open World Ethos. In *The Open World, Hackbacks and Global Justice* (pp. 15–36). Springer Nature Singapore Pte Ltd. https://doi.org/10.1007/978-981-19-8132-6_2

Tianyang, L. (2024). The Embodiment and Practice of the Principle of Legal Interest Protection in Criminal Legislation. *International Journal of Frontiers in Sociology*, *6*(3), 44–50. https://doi.org/10.25236/ijfs.2024.060308

Topor, L. (2024). Sovereignty, Power, International Security and a Lack of International Law. In *Cyber Sovereignty. Global Power Shift* (pp. 45–73). Springer Cham. https://doi.org/10.1007/978-3-031-58199-1_3

Wang, P. (2022). *Principle of Interest Politics: Logic of Political Life from China's Perspective*. Peking University Press. Springer. https://doi.org/10.1007/978-981-19-3963-1

Wilenmann, J. (2019). A New Legal Science with an Old Aftertaste. *The University of Toronto Law Journal*, *69*(4), 540–556. https://doi.org/10.3138/utlj.2019-0057

Сведения об авторе

Яссин Абдалла Абделькарим – судья, суд общей юрисдикции в Луксоре, министерство юстиции Египта; магистр права, Школа права в Лиддсе, Лидский университет Беккета
Адрес: 82516, Египет, г. Сохаг, Мадинат Нассер, ул. Ахмим Сохаг, Нью Касалови Хотел; LS1 3HE, Великобритания, г. Лидс, городской кампус
E-mail: yassinabdelkarim91@gmail.com
ORCID ID: https://orcid.org/0000-0001-7388-1337

Конфликт интересов

Автор сообщает об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.15.41 / Государственный суверенитет
Специальность ВАК: 5.1.1 / Теоретико-исторические правовые науки

История статьи

Дата поступления – 3 октября 2024 г.
Дата одобрения после рецензирования – 15 октября 2024 г.
Дата принятия к опубликованию – 13 декабря 2024 г.
Дата онлайн-размещения – 20 декабря 2024 г.

Research article
UDC 34:004:347:004.4
EDN: https://elibrary.ru/clzzkx
DOI: https://doi.org/10.21202/jdtl.2024.40

Prospects for Implementing Digital Technologies in the Administration of Justice in Zimbabwe

Taurai Muparadzi
University of Zimbabwe, Harare, Zimbabwe
Tshwane University of Technology, Pretoria, South Africa

Ricky Munyaradzi Mukonza
Tshwane University of Technology, Pretoria, South Africa

Keywords

administration of justice,
automation,
court,
digital documentation,
digital government,
digital justice,
digital technologies,
judicial proceedings,
judicial system,
law

Abstract

Objective: an intensive discussion is currently going on globally on digitalization and automation of providing services in public institutions, which corresponds to the technological development of the Fourth Industrial Revolution. The use of digital technologies is crucial to create an optimized service delivery system. In African countries, attention is increasingly paid to the automation and digitalization of judicial activities, due to concerns about the risks of influencing justice systems. In light of this, the article is aimed at forming a promising model for the introduction and implementation of digitalization in Zimbabwe courts.

Methods: the research is based on the methods of scientific analysis and synthesis, deduction and induction, legal modeling, formal legal and comparative legal methods.

Results: the article provides an overview of the measures taken to digitalize the system of administration of justice in various states. It also examines best practices and reveals the essence of digitalization in the judicial system in Zimbabwe. The authors identify the main existing and promising directions of the impact of digitalization on the judicial system of Zimbabwe and show the ways to promptly and effectively convert the system of justice administration into a digital format. The article

✉ Corresponding author
© Muparadzi T., & Mukonza R. M., 2024

This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (CC BY 4.0) (https://creativecommons.org/licenses/by/4.0), which permits unrestricted re-use, distribution and reproduction, provided the original article is properly cited.

identifies the advantages of digital data processing in judicial bodies and obstacles to the use of digital systems in the administration of justice. The latter result in the insufficient optimality of the Integrated Electronic Case Management System (IECMS).

Scientific novelty: the study builds an optimal model for the introduction of digital technologies into the judicial system in Zimbabwe, aimed at improving the efficiency of courts digitalization and transforming the justice administration system. The authors proved that the crucial factors of achieving this goal are the auxiliary infrastructure of information and communication technologies, the level of education and awareness of citizens, and the ongoing state and legal policy.

Practical significance: it is expected that the proposed model to implement digitalization in Zimbabwe courts and improve its efficiency will allow for the comprehensive and uninterrupted implementation of IECMS.

For citation

Muparadzi, T., & Mukonza, R. M. (2024). Prospects for Implementing Digital Technologies in the Administration of Justice in Zimbabwe. *Journal of Digital Technologies and Law, 2*(4), 802–834. https://doi.org/10.21202/jdtl.2024.40

Content

Introduction
1. Research Results
  1.1. Statement of the Problem
  1.2. Research Methodology
  1.3. Theoretical Framework
    1.3.1. Technology Acceptance Model (TAM)
2. Literature Review
  2.1. Benefits Linked to Digitalization of Courts and Anticipated Benefits from the Adoption of the IECMS in Zimbabwe
  2.2. The Impact of Digitalization on Access to Justice
  2.3. Challenges Affecting Digitalization of Courts and Implications for Access to Justice
  2.4. Empirical Evidence on Digitization of Justice Administration Systems in Selected Countries
    2.4.1. Key Lessons from E-Justice Service Delivery in the United Kingdom
    2.4.2. Key Lessons from E-Justice Service Delivery in South Africa
    2.4.3. Key Lessons from E-Justice Service Delivery in Rwanda
3. Analytic and Detailed Discussion of Findings
  3.1. The Notion of Digitalization of Court Systems in Zimbabwe

3.2. Benefits Associated with Digitalization of the Court Systems
3.3. Challenges to the Digitalization of Courts in Zimbabwe
3.4. Practical Implementation of IECMs in Zimbabwe
4. Proposed Model for Effective Digital Transition in Justice Administration
Conclusion
Reference

Introduction

In the 21st century, there has been a significant transformation in public service delivery through the introduction of Information and Communication Technologies (ICTs). These technologies are at the core of the Digital Governance Paradigm (DGP), which emphasizes the central role of technology in service delivery. Improving the efficiency of courts has become the goal of most judicial innovations and reforms (Krishna, 2018). Even so, the procedural inconvenience of the manual paper-based courts in Zimbabwe and other countries of the world and burden of pending and ongoing court cases has posed challenges for judicial systems worldwide. To address this, some countries have turned to Information Technology (IT) as a means to revitalize their justice administration. The digitalization of courts gained momentum upon recognition that it is a crucial component of e-governance (Monga, 2008). Courts have attracted negative descriptions due to delayed justice (Poshai & Vyas-Doorgapersad, 2023) and allegations of capture, emblematic partiality (Hanzi & Baeyens, 2021) and mutilation of judicial independence by the state in Zimbabwe (Tembo & Singh, 2023). Adopting digital technologies to flash out the morass of case backlogs provides hope for a solution that outlasts all previous attempts at reinventing the justice administration sector. Digital innovations are therefore seen as possessing the potential to renovate the justice delivery sector.

However, the implementation of electronic court systems encounters numerous challenges. The use of ICTs in courts was initially met with scepticism, and the costs associated with creating electronic case files and training judiciary staff on new skills proved to be obstacles (Deming, 1985; Fleer, 2018; Poshai & Vyas-Doorgapersad, 2023). Despite these challenges, countries like Britain swiftly overcame the hurdles by establishing the necessary infrastructure and mandating the use of technology across all judiciary sectors (Deming, 1985). The argument was that technology enables courts to efficiently disseminate, analyze, store, transfer, and retrieve information (Fleer, 2018). In Russia, advances towards integrating Artificial Intelligence (AI) in managing the activities of courts is already visible and confirms the forward-thinking ICT posture of the Russian Federation (Dneprovskaya & Abramitov, 2020). More specifically, Russia discovered that efficient e-justice delivery, document circulation, time and resource savings can be achieved through digital courts. In the United States, the government recognized the enhanced security that electronic courts provide for classified information, leading to the introduction of e-courts nationwide. In the Lake County Florida, electronic records management

emerged as a viable option to attack restrictions to access to public records such as court proceedings (Parrish & Courtney, 2007). However, the lack of standardized approaches and models posed a challenge during the early stages of electronic court systems (Chipeva et al., 2018). In Canada, the implementation of automated system s and electronic communication facilities in the Supreme Court of Canada noticeably improved the efficiency and effectiveness of its administrative operations (Goulard et al., 1991). Similar trends were recorded in other continents.

Asian countries such as Malaysia and Singapore were among the early adopters of electronic court systems, with Malaysia starting with electronic case filing and Singapore focusing on electronic case recording (Cassim, 2017). In Europe and Latin America, electronic case management systems gained prominence for their fairness, efficiency and prompt case handling (Rooze, 2010). The adoption of these systems in countries like Italy, Austria, Poland, and South Korea allowed for the clearance of backlogged cases and prevention of data loss. In Africa, Kenya led the way in advocating for electronic court systems, followed by Tanzania, South Africa, Egypt, Algeria, and Morocco (Alami, 2015). Tanzania and South Africa progressed faster due to their existing infrastructure, while South Africa's system proved more organized (Kabir et al., 2015; Naidoo, 2017).

The positive impact of ICTs in transforming public service delivery, as highlighted by previous studies (Nzaro & Magidi, 2014; Mawela et al., 2017), influenced the adoption of ICTs in judicial systems globally. In Zimbabwe, the formal use of e-court systems was initially slow due to inadequate infrastructure, although the use of laptops, video cameras, phones, and voice notes for evidence was visible. However, the Covid-19 crisis accelerated the adoption of ICTs in Zimbabwean courts. The pandemic disrupted general business and specific court operations, leading to the need for strategies to ensure business continuity (Muparadzi & Rodze, 2021) and continuous access to justice and prevent case backlogs. In response, Zimbabwe introduced the electronic court system, aligning with World Bank recommendations to improve judicial operations and address the backlog of cases (Wallace, 2019).

In the following segments, this article interrogates the influence of digitalization in Zimbabwean courts and how rapid digitization of the entire justice delivery system can be achieved. It seeks to answer key questions, including the understanding of digitalization in the court systems of Zimbabwe, the benefits of digitalizing the courts, the effectiveness of digitalization on service delivery, obstacles to effective digitalization, and the best model for adopting and utilizing digital systems in justice service delivery.

1. Research Results

1.1. Statement of the Problem

The use of ICTs in improving service delivery in the public sector is a global trend (Zhurkina et al., 2021). The implementation of e-government systems in Zimbabwe's justice delivery sector aims to optimize justice delivery services. With technological advancements like IECMS, court cases can be presented in a more organized and presentable manner. In Zimbabwean courts, the adoption of electronic systems was timed with precision due to the presence of case backlogs and difficulties in file management as well as the complicated difficulties presented by Covid-19 on the operational efficacy of the old face to face court system. This initiative is part of the government's efforts to improve service delivery and combat corruption (Poshai & Vyas-Doorgapersad, 2023)[1]. Even so, the challenges affecting digitization and use of digital systems have not disappeared.

Despite the adoption and implementation of the electronic case management system (IECMS), the justice delivery system still faces challenges such as case backlogs and delays, which hinder effective justice service delivery in Zimbabwe. That cases are still being filed manually in a digitalized environment is a problem (Procopiuck, 2018). Added to that, allowing a rule which permits litigants to choose to have either a virtual or face to face trial in a fully digitalized court system betrays underlying problems with the IECMS in Zimbabwe. These challenges stem from an unreliable system and innovation failing to live up to expectations and causing courts to fall back on traditional paper-based court management systems, which are slow and inefficient. These shortcomings highlight underlying omissions in the design and implementation of the IECMS and capacity issues that impede the optimal utilization of e-governance systems in the justice delivery system. It also remains uncertain whether the digitalization of Zimbabwean courts can truly enhance access to justice because of stubborn impediments confronting the smooth operations of the IECMS such as lack of requisite infrastructure, lack of system capacity, persistent digital divide issues, ICT illiteracy (Poshai & Vyas-Doorgapersad, 2023), bureaucratic foot dragging and lack of literature on digitization of courts in Zimbabwe with the exception of the recent and prominent work by Poshai and Vyas-Doorgapersad (2023). Again, if the digitization of the entire Zimbabwean justice administration system is not quickened, court systems in Zimbabwe will remain stuck at the tail end of digital justice administration in Africa. This study therefore poses the question: what are the fundamental requirements for successful implementation of digitalization projects in the justice administration sector in Zimbabwe. In the end, this study proposes ideas that can encourage effective and successful digitalization within the justice delivery sector while preventing the total collapse of the recently introduced Electronic Case

[1] Malaba, L. (2022). Digital transformation of judiciaries in Africa and experiences in the face of the COVID-19 pandemic. The Judicial Service Commission of Zimbabwe. https://clck.ru/3Eufbq

Management System (ECMS). The research methodology used to answer the research question above is outlined in the following segment.

1.2. Research Methodology

This section outlines the research methodology employed in the study, drawing guidance from Creswell (2009, 2013, 2014) and Sekaran and Bougie (2010). The researchers adopted a qualitative research approach, which was deemed most suitable for addressing the research questions and understanding how the digitalization of the justice delivery system enhances court operations in Zimbabwe. This approach facilitated an interpretive understanding of digitalization in Zimbabwean courts and aimed to develop a suitable model for improving justice administration. By enlisting perspectives from earlier research the study gained detailed insights into how digitalization of courts is perceived in terms of its potential to enhance justice service delivery.

To achieve this objective, the study employed a case study research design, following the recommendations of Neuman (2014) and Davies (2007). This design facilitated an in-depth examination of Zimbabwean court digitalization, emphasizing the understanding of government-led justice service improvements. Cohen et al. (2007) suggest that a case study design ensures data specificity, enhancing its reliability in the selected area. Yet, it is vital to recognize that this research design's results are mainly relevant to the specific case study.

The combination of diverse views from different scholars provided assorted perspectives that contributed to a comprehensive understanding of the digitalization of courts, its benefits to the justice delivery system in Zimbabwe, and the challenges associated with its implementation.

The use of books, journals, government publications, newspaper articles, and online documents was chosen for its ready availability of data, time-saving nature, and provision of background information (Ahmed, 2010). Content analysis was applied to examine the documentary evidence. Each relevant section in a book, book chapter, journal article, newspaper article, and government publication was thoroughly reviewed, and relevant data were extracted for further analysis. The documentary evidence and the theoretical framework served to corroborate or challenge the key findings of the study. The use of multiple data sources rather than mixed methods also permitted the researchers to collect the required information and critically analysing the findings as explained by Bans-Akutey and Tiimub (2021) and Carter et al. (2014). This convergence of information from different sources (data source triangulation) allowed the researchers to validate research results presented at the end.

While the study relied on secondary data, it had limitations. The authors discovered that there are very few studies on the digitization of courts in Zimbabwe hence reliance on perspectives from varied scholars and regions was considered useful to fill that gap. However, despite these limitations, this study is a bold attempt at unpacking Zimbabwe's

experience with digitalization projects in the justice administration sector and provides insights that can be used for further research.

1.3. Theoretical Framework

1.3.1. Technology Acceptance Model (TAM)

The study relied on the lenses of the Technology Acceptance Model (TAM) to aptly explain technology acceptance and use in Justice administration in Zimbabwe as proposed by Fred Davis in 1989 (Ajibade 2018). TAM is an approach to predict and explain the use and acceptance of information systems and technology by individual users (Kim & Crowston, 2011). TAM prescribes that user acceptance of technology depends on perceived usefulness (PU) and perceived ease of use (PEOU) as well as the presence of facilitating conditions. In line with (Davis et al., 1989), this research investigated how the assumption of improved efficiency will translate to enhanced court efficiency, reduced delays and improved case management. Added to that, this construct permitted a thorough analysis of present and absent facilitating conditions in the digitization of courts in Zimbabwe. Again, TAM facilitates the adoption of digital technologies and the study related this construct to the anticipated increase in access to justice administration even by marginalised groups and individuals. Streamlining justice administration processes is one of the goals of adopting digital technologies in the Zimbabwean Court systems and TAM was found useful in explaining how court processes can potentially be optimized by reducing paperwork and automating routine tasks. In addition, increased transparency, realizing cost savings, improved data management and the introduction of virtual courts are some of the goals of digitalization in the justice administration system. Finally, raising judicial productivity and advancing overall digital transformation in the justice administration system are other important goals of ICT adoption in the Zimbabwean court system. Accordingly, TAM was useful in explaining how digital technologies enhance transparency and accountability in court proceedings, effective management of court data, adoption of virtual courts, reducing the workload of court staff and modernizing the justice system in Zimbabwe. Figure 1 summarizes the Technology Adoption Model as perceived by (Davis et al., 1989).

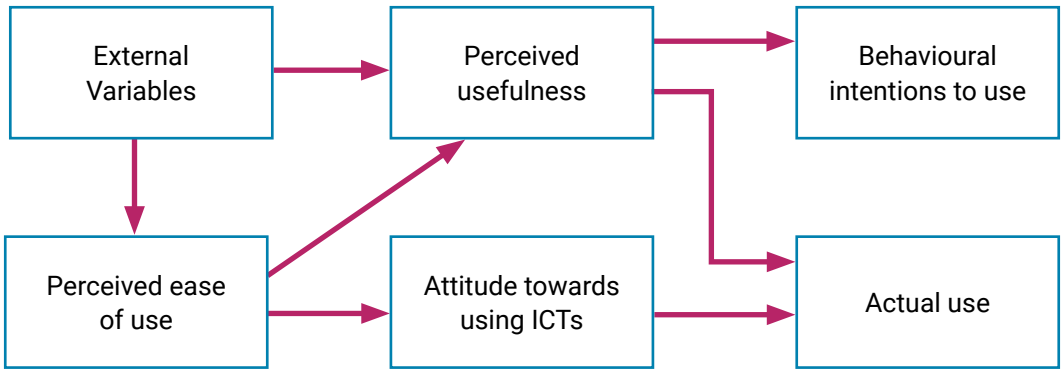


Figure 1: Technology Acceptance Model

Source: (Davis et al., 1989).

Davis et al. (1989) diagram depicts TAM's key elements. External factors affect perceived usefulness and ease of use, influencing attitudes towards electronic court systems. These factors, including social, economic, and political influences, impact the adoption of digital systems in justice delivery. TAM suggests a link between intention to use technology and e-justice system benefits. The study aims to assess if digital justice systems adoption aligns with this model.

2. Literature Review

2.1. Benefits Linked to Digitalization of Courts and Anticipated Benefits from the Adoption of the IECMS in Zimbabwe

Poshai and Vyas-Doorgapersad (2023) highlight the expected benefits of IECMS in Zimbabwe, while literature explores digitalization advantages extensively. According to Poshai and Vyas-Doorgapersad (2023), the highly publicized advantages of the IECMS in Zimbabwe encompass increased efficiency, enhanced accessibility, and modernized judiciary operations. Again, IECMS also remove operational bottlenecks, eliminate corruption, improve filing of court documents and evidence, increase public trust in the judiciary, create a more responsive and resilient judiciary, and increase transparency. Their view agrees with observations by Munyoro[2], Gatsi[3], Tshuma[4], Malaba[5] and Machaya[6]. While these scholars do not exhaust all the benefits linked to digitalization, scholars such as Muparadzi et al. (2024), Muparadzi (2024), Bwalya (2018), Bannister (2015), Undi-Phiri and Phiri (2022), and Twizeyimana and Anderson (2019) acknowledge the diversity of benefits that ICTs and e-government systems place at the disposal of government institutions that include increased capacity, decentralized governance, automated and transmuted work processes, swift delivery of public services, improved productivity and competitiveness, improved public decision making, and modified organizational structures. Clearly, ICTs are an indispensable driver of organizational and social change.

---

2 Munyoro, F. (2022, February 7). Zimbabwe: Virtual court to be commissioned today. AllAfrica. https://clck.ru/3EqaSY

3 Gatsi, D. (2022, August 11). Rights lawyers challenge judicial amendment bill – Says provisions may hinder right to fair trial. New Zimbabwe. https://clck.ru/3EqaUD; Machaya, P. (2023). Zimbabwe's labour, administrative courts go digital. https://clck.ru/3EqaWK

4 Tshuma, M., (2022). IECM to be launched. Sunday News. https://goo.su/S4u8

5 Malaba, L. (2022). Digital transformation of judiciaries in Africa and experiences in the face of the COVID-19 pandemic. The Judicial Service Commission of Zimbabwe. https://clck.ru/3Eufbq

6 Gatsi, D. (2022, August 11). Rights lawyers challenge judicial amendment bill – Says provisions may hinder right to fair trial. New Zimbabwe. https://clck.ru/3EqaUD; Machaya, P. (2023). Zimbabwe's labour, administrative courts go digital. https://clck.ru/3EqaWK

The digitization of courts has shown that the traditional manual filing procedures in courts have various limitations and risks, including human error, corruption, misplaced files, and delays in transmission. This has made digitization of courts urgent in order address these challenges. Turner (2002) underlines that electronic filing dramatically changed the way courts function. Similarly, Muhammad et al. (2023) emphasizes that digitalization has significantly increased speed in applications and transmission of court documents, leading to faster case disposal. Shah and Gupta (2017) highlight that e-filing and internet services reduce paperwork burdens and improve connectivity between case stakeholders, thereby enhancing the administration of justice. Research indicates that digitalization enables court clerks to work more efficiently by reducing the time and effort required to manage cases. It also reduces file storage, record retrieval time frames, and paper usage while promoting transparency during proceedings.

In the Malaysian justice system, the digitalization of court processes and case management systems contributed to increased transparency, productivity, efficiency, and a decrease in case backlogs (Haider, 2013). More specifically the Malaysia system boasts of four integrated systems that are the Electronic Filing System (EFS), the Case Management System (CMS), Court Recording and Transcribing (CRT) and Queue Management System (QMS). Similarly, the Rwandan judicial system is credited for being the best and most functional digital court system with superior document filing and storage capabilities[7] (Poshai and Vyas-Doorgapersad, 2023). Clearly, the power of ICTs cannot be doubted in this regard

It is crucial for courts to harness the potential of information and communication technology (ICT) to ensure uninterrupted access to justice. This argument resonates with the argument of Svitlychnyy et al. (2023) that electronic justice acted as a comprehensive remote mechanism during the COVID-19 pandemic proving its effectiveness even in crisis times. In fact, the role of ICTs in supporting business continuity is also aptly captured by Poshai and Vyas-Doorgapersad (2023) and Muparadzi and Rodze (2021). Therefore, the digital transformation of the court system could provide Zimbabwe with a software solution that integrates various courts under one technology umbrella, streamlining the entire case lifecycle from filing to disposition and appeal. However, while it is already known that the Zimbabwean justice delivery system can benefit from the application of electronic justice systems, the sustainability of the recently introduced system remains in doubt. There is limited detailed research on Zimbabwe in this field while existing research mainly focuses on other countries, such as South Africa. A latest study by Poshai and Vyas-Doorgapersad (2023), though useful, does not provide conclusive

[7] Nkusi, F. (2017, July 16). Rwanda's electronic case management system and SDG, The New Times. https://clck.ru/3ErSz2

insights into the use of IECMSs and this study aims to provide further detailed knowledge about digital court systems.

Many judicial systems worldwide lack a comprehensive case management platform that can reflect existing processes, interact with related systems, and ensure reliable accessibility. This hinders the effective processing and resolution of cases in a timely manner (Drossos et al., 2018; Adeola & Evans, 2020). Digitalization of courts introduces new tools for real-time analysis, monitoring performance, and evidence-based decision-making, which has become even more crucial during the COVID-19 pandemic. It is now evident that citizens and businesses demand access to justice at any time and from anywhere in what Caserta (2022) acknowledges as the emergence of online legal platforms. Optimizing and improving processes through digital transformation using technology and best practices can lead to increased productivity, transparency, access to justice, reduced transaction costs, and shorter trial lengths (Drossos et al., 2018; Kudo, 2015). Again, electronic workflows in courts enable faster clearance rates and easier access to the judicial system (Muscalu & Hulpus, 2016). Scholars, including Adeola and Evans (2020), Bajandas and Ray[8], and Drossos et al. (2018), agree that the general benefits of digitalization in the justice delivery system are real. It is the researchers of this study's opinion that Zimbabwe is clearly yet to realize some of these benefits.

Learning from Bajandas and Ray[9] and Poshai and Vyas-Doorgapersad (2023), the digitalization of courts offers an opportunity to improve filing procedures, evidence submission, record maintenance, and overall court processes. It promises increased productivity, streamlined case flow, reduced processing time, and better quality. Through the ECMS and e-filing systems, a unified e-justice or e-court management system can be established, replacing individual failing systems and automating manual court processes. This results in reduced data input and retrieval time while facilitating data sharing across courts and partners. However, the handling of electronic evidence, requires specialist training (Insa, 2007) but the scarcity of computer forensics experts and absence of standards on handling electronic evidence in Zimbabwe is worrying.

Additionally, the digitalization of courts has implications for archive management. Papagianneas and Junius (2023) and Rooze (2010) state that archival protocols should ensure the authenticity, reliability, integrity, and usability of archive content within the judicial system. Workflow court systems play a central role in archiving practice by defining validation steps for executing court processes.

---

8 Bajandas, F. F., & Ray, G. K. (2018, May 23). Implementation and use of electronic case management systems in Federal Agency adjudication: Administrative Conference of the United States. https://clck.ru/3Eug67

9 Ibid.

2.2. The Impact of Digitalization on Access to Justice

The discussion of the benefits and challenges arising from the digitalization of court processes cannot be considered in isolation (Aaltonen and Tammela, 2019). It is crucial to assess their impact on access to justice. Therefore, it is important to evaluate the current efforts in digital transformation against access to justice standards at domestic, regional, and international levels (Adeola & Evans, 2020). Access to justice encompasses various human rights, including the right to seek redress, access courts, information, a fair trial, privacy, equality, and non-discrimination and has its roots in national constitutions (Poshai and Vyas-Doorgapersad, 2023).

Article 7 of the African Charter on Human and Peoples' Rights states that every individual has the right to have their cause heard, which includes the right to access courts and seek redress. The digitalization of the justice system is continuously changing the operation of courts (Maseh, 2015). Previously, documents in the High Court were filed in print, but the introduction of e-filing requires court users to adapt to submitting documents through digital platforms. However, it is important to consider the realities faced by court users. Digital interactions necessitate devices like smartphones or laptops for filing court documents (Yin, 2009; Maseh, 2015). Additionally, accessing digital platforms requires internet access. It remains unclear whether the Zimbabwean courts have the necessary digital systems to implement the e-justice system, raising questions about the country's readiness for digital transformation. Previous studies by Muparadzi (2024) and Zinyama and Nhema (2016), Rajah (2015), Heeks (2002), Mukonza (2014) and Muparadzi et al (2019) underline that successful digitalization is premised on governance, institutional, culture, infrastructure, political, and leadership readiness (e-readiness) among other factors. It is the view of researchers in this paper that the adoption of digital innovations in Zimbabwe's court systems may have negative implications for the marginalized rural communities.

The digital transformation of court systems has negatively affected access to justice, particularly in the realm of virtual court proceedings, which are becoming more prevalent (Chipeva et al., 2018). While digitalization can facilitate virtual court hearings, reducing travel time and costs for litigants, many individuals in Zimbabwe may lack the necessary devices and internet access to participate virtually (Poshai & Vyas-Doorgapersad, 2023). Sung (2020) precisely states that e-courts may become unfriendly and unaffordable for the ICT have nots seeking access to justice. This directly impacts the right to access justice (Maseh, 2015; Adeola & Evans, 2020; Cordella & Contini, 2020). Similarly, the production of digital evidence may exclude those without access to devices and internet connectivity (Cassim, 2017). The quality of internet available also affects the ability to produce evidence effectively, with broadband being necessary for uninterrupted interaction and evidence presentation in virtual settings. The potential positive or negative impact of Zimbabwe's

adoption of digital systems on the justice delivery system remains uncertain, and this study aims to provide answers.

Regarding judicial transparency, the judiciary has an obligation to conduct its proceedings openly and publicly. This principle stems from the notion that justice must not only be done but must also be seen to be done (Cordella & Contini, 2020; Oakes & Davies, 2016; Poshai & Vyas-Doorgapersad, 2023)[10]. Transparency within the court system enhances public knowledge, fosters judicial accountability, reduces the risk of corruption, and enables the public to challenge perceived improper or incorrect decisions. However, virtual court hearings have posed challenges related to transparency and arbitrary and obscure decision making which open courts sort to address (Meyerson, 2015; Cordella & Contini, 2020). Unlike in-person hearings where the public and press can observe proceedings, virtual hearings are often limited to the involved parties, occurring outside the public eye. Without a comprehensive strategy to ensure accessibility and transparency of virtual courts, the transparency of the judicial process may be compromised[11]. The capacity of electronic systems to improve judicial transparency in developing country contexts has not been definitively established, motivating this study to explore the specific benefits and limitations within the context of the Zimbabwean judicial system.

2.3. Challenges Affecting Digitalization of Courts and Implications for Access to Justice

In the realm of justice accessibility, online court systems have emerged as potent tools (Sung, 2020). However, the evolution of digital courts encounters a myriad of challenges encompassing infrastructure, IT literacy, policy, organization, structure, and power supply (Sousa & Guimaraes, 2017; Pillot et al., 2019; Poshai & Vyas-Doorgapersad, 2023). In Zimbabwe, the deficiency in infrastructure stands as a formidable barrier to digitalization efforts (Poshai & Vyas-Doorgapersad, 2023), underscoring the importance of digital readiness prior to the implementation of e-government projects (Muparadzi et al., 2024) and offering an opportunity to ICT equipment countries to exploit this investment opportunity ceteris paribus.

The foundation of successful court digitization lies in appropriate infrastructure. In many developing nations, including Zimbabwe, insufficient infrastructure obstructs the deployment of electronic services (Masenya & Ntengenyane, 2022). While some

[10] Malaba, L. (2022). Digital transformation of judiciaries in Africa and experiences in the face of the COVID-19 pandemic. The Judicial Service Commission of Zimbabwe. https://clck.ru/3Eufbq

[11] Bajandas, F. F., & Ray, G. K. (2018, May 23). Implementation and use of electronic case management systems in Federal Agency adjudication: Administrative Conference of the United States. https://clck.ru/3Eug67

countries have leveraged public service centers to mitigate the costs of acquiring IT infrastructure for digitalization, many developing nations still lack the necessary infrastructure to support electronic services within the judiciary, a challenge that persists in Zimbabwe, hindering the realization of a digitized justice system.

Power supply issues present additional hindrances to the operation of computing systems globally. Zimbabwe, alongside nations like South Africa, Zambia, and India, grapples with severe electricity supply challenges, resulting in delays in the digitization of court processes (Vasista, 2018). The significance of these electricity supply challenges in impeding the effective implementation of digital systems in the justice delivery sector is evident, as noted by Muparadzi et al. (2024). For Zimbabwe, it is a prominent view of the researchers that the current electricity infrastructure is significantly limited in its capacity to support a robust e-court system.

Technological illiteracy among court officials poses a significant challenge to the digitalization of court processes (Bosire et al., 2017; Poshai & Vyas-Doorgapersad, 2023). To address this, training programs are imperative to facilitate knowledge transfer and ensure the proficient use of ICT tools in digitized court processes (Bosire et al., 2017; Cassim, 2017). The lack of IT literacy, particularly in Zimbabwe, impacts government ICT projects across various sectors. Despite training initiatives by the Judicial Services Commission (JSC) for court officials, the deficiency in competent ICT skills persists, leaving ordinary citizens excluded from essential systems like the IECMS (Poshai & Vyas-Doorgapersad, 2023). Understanding the functionality and transformative potential of ICT applications in the justice sector is critical to fully harnessing the benefits they offer (Zhang et al., 2024).

Africa's policy landscape has also faced criticism for being rife with failures (Cloete, 2005). The absence of robust laws supporting technological integration in the justice system acts as a barrier to the digitalization of court processes (Thalib et al., 2017). Policy reforms are essential to bolster digitalization efforts, involving key stakeholders such as judges, court staff, and lawyers (Weers, 2016). In Zimbabwe, a pertinent policy framework is imperative to enhance the efficacy of e-justice systems, necessitating updates to the existing ICT policy framework to drive consistent e-government development (Muparadzi et al., 2024; Mukonza et al., 2016).

Structural challenges further impede the digital transition of court processes in Zimbabwe and other African nations. Issues such as inadequate organizational plans for record management, deficiencies in records and archive management knowledge, and the absence of legislation and policies to guide record management hinder the shift to digital systems (Maseh, 2015). The security and confidentiality of data within the

e-justice system are paramount concerns, necessitating the implementation of access control rules and adherence to security standards (Han et al., 2024). Safeguarding user privacy amid digital data and communications requires stringent measures, highlighting the need for comprehensive and effective organizational and national internal policies governing information use within Zimbabwe's justice delivery system.

2.4. Empirical Evidence on Digitization of Justice Administration Systems in Selected Countries

2.4.1. Key Lessons from E-Justice Service Delivery in the United Kingdom

In the United Kingdom (UK), the transition from alternative dispute resolution (ADR) to online dispute resolution (ODR) demonstrated that technology primarily functions as a tool to support dispute resolution, even in crisis situations (Sourdin, 2020), rather than an independent system capable of automatically processing and settling disputes (Morison & Harkens, 2019). Prescott (2017) explains that UK courtrooms have implemented digital courtroom systems, incorporating technologies like video conferencing for remote testimonies, online form completion, triage services, mobile access, and online case resolution systems. Additionally, Donoghue (2017) highlights that the successful use of pre-recorded videotaped trials in the UK, which prompted the integration of emerging technologies such as laptops, computers, and video recorders, led to the nationwide adoption of pre-recorded cross-examinations. The success of digital court systems in the UK can be attributed to the availability of IT infrastructure and digital literacy, which facilitated the implementation of reform initiatives. This suggests that when a country possesses the necessary IT infrastructure, the digitalization of court systems tends to proceed smoothly. Developing countries like Zimbabwe can learn from this experience and work towards operationalizing digital systems in their court systems to enhance the efficiency of justice delivery.

2.4.2. Key Lessons from E-Justice Service Delivery in South Africa

South Africa, among other Southern African countries, has relatively effectively implemented digital court systems to enhance its justice delivery. Embracing new, efficient methods, the country has digitized court processes, converting paper-based systems to digital formats (Cordella & Contini, 2020). Satirah & Haider (2013) emphasizes South Africa's digitalization efforts, like sending court hearing notices via mobile SMS instead of paper. Online tools are utilized for document filing, hearings, signing, and outcome transmission, enhancing justice system accessibility.

The introduction of an electronic case management system in South Africa has bolstered file security and efficiency, streamlining tracking and retrieval[12]. Virtual courts, especially during the pandemic, prevented case backlogs, ensuring timely resolutions (Sourdin et al., 2020)[13]. Hassan et al. (2016) mention the country's electronic court systems, beginning with the Electronic Case Filing System (ECFS) for civil cases and later expanding to patent cases. Despite challenges like case backlogs and power supply issues, South Africa's Judiciary has effectively embraced digital court management[14].

2.4.3. Key Lessons from E-Justice Service Delivery in Rwanda

Rwanda is acclaimed as the role model of e-justice service delivery in Africa (Poshai & Vyas-Doorgapersad, 2023). Rwanda's IECMS is the single entry point to all justice delivery institutions. Rwanda's justice sector no longer relies on manual paper based case processes. Notable features of Rwanda's IECMS include its ability to connect justice administration institutions in Rwanda that include the Judiciary, the Ministry of Justice, the National Public Prosecution Authority, the Criminal Investigation Department[15] and the Rwanda Correctional Services[16], its capability to automate court documentation, eliminate duplication of case information, its ability to allow timeous and convenient opening and closure of cases, its ability to provide instant communication to parties in the litigation process and the added advantage of a digital dashboard that provides access to court reports and judgements. To reach this stage, Rwanda invested massively in ICT infrastructure and Internet connectivity.

All in all, the dominant view held by researchers in this paper is that the United Kingdom, South Africa and Rwanda have made significant progress in implementing e-justice delivery systems. Their experiences highlight the importance of ICT infrastructure, digital literacy, and consistent with the views of Li and Peng (2023), the integration of technology in court processes for efficient and accessible justice delivery. Developing countries can draw valuable lessons from these examples as they strive to enhance their own court systems through digitalization.

---

12 Bajandas, F. F., & Ray, G. K. (2018, May 23). Implementation and use of electronic case management systems in Federal Agency adjudication: Administrative Conference of the United States. https://clck.ru/3Eug67

13 Ibid.

14 Department of Justice and Constitutional Development. (2024). Judiciary Annual Report. Pretoria: Department of Justice and Constitutional Development.

15 Ibid.

16 Nkusi, F. (2017, July 16). Rwanda's electronic case management system and SDG, The New Times. https://clck.ru/3ErSz2

3. Analytic and Detailed Discussion of Findings

3.1. The Notion of Digitalization of Court Systems in Zimbabwe

The study aimed to understand the concept of digitalization in court systems by exploring different perspectives on the digitalization of courts in Zimbabwe through examining literature on Zimbabwe. The findings reveal a consensus among scholars regarding the understanding of digitalization in court systems. It emerged from the findings that digitalization involves using Information Communication and Technologies (ICTs) to enhance the delivery of justice and move towards a paperless court system. This clearly links the adoption of ICTs to improved operational efficiency, consistent with the recommendation of the TAM. Again, the digitalization of courts in Zimbabwe is viewed as encompassing different forms, that include electronic case filing and Electronic Case Management Systems (ECMs). There is general consensus that electronic case filing replaces manual filing, reducing errors, delays, and corruption and it enables 24/7 filing, generates case numbers and receipts, and streamlines the court process. ECMs handle cases using application and reference numbers, leading to backlog clearance, improved case management, and timely proceedings. Automation of case management systems through digitalization therefore enhances productivity, cash flow management, and reduces delays.

The understanding of digitalization in court systems also extends beyond different definitions and encompasses various manifestations. The Integrated Electronic Case Management System (IECM) was identified as a comprehensive package that covers the entire case process. Its adoption in Zimbabwe introduced digitalization strategies for timely justice delivery through online scheduling and transparency. ICTs clearly play a pivotal role in digitalization efforts within the justice sector, addressing service delivery challenges in Zimbabwe's courts.

The adoption of electronic case filing and ECMs is seen as a bold step towards improving efficiency in the justice delivery system. The IECM, for example, serves as a comprehensive solution, covering the entire case life cycle. Despite being in the early stages of implementation, digitalization efforts in Zimbabwe's courts show promise in addressing service delivery challenges. Integration of technology, particularly ICTs, offers advantages in terms of efficiency, transparency, and improved connectivity among entities involved in the justice sector.

3.2. Benefits Associated with Digitalization of the Court Systems

The study also interrogated the rewards of implementing digital court systems. The study discovered multiple benefits linked to the digitalization of court systems in Zimbabwe. These benefits are outlined below.

Firstly, the study's findings indicate that implementing digital systems in Zimbabwe's court systems has the potential to enhance efficiency and effectiveness and help courts to overcome the pressure arising from case overload despite limited resources. In that regard,

electronic court systems contribute to improved efficiency by eliminating unnecessary delays in case filing, management, and docketing. Paper-based systems are outdated and the adoption of information technology allows for secure storage of information on cloud systems, addressing these challenges. The time saving nature of ICT adoption in court system is aptly captured by Wallace (2019). The considered view of researchers in this paper is that IECMS should permit all functionalities from the comfort of user's homes and office but the problem remains that some functions continue to give users a bad experience with the system.

One major discovery is that the Integrated Electronic Case Management (IECM) systems in Zimbabwe incorporates electronic docketing and case scheduling, bringing benefits such as accountability, transparency, minimized corruption, and facilitated information transfer, storage, and retrieval. The positive impact of digital systems on court operations is widely accepted hence the automation of courts in Zimbabwe is an ongoing project initiated by the Judicial Service Commission (JSC) and implemented in phases. The initial phase focuses on key courts, and subsequent phases cover other courts. The introduction of digital court systems is calculated to enhance the efficiency and effectiveness of the justice delivery system but with complications manifesting at every stage of migrating manual systems to online systems.

The study's findings also revealed that the full implementation of digital court systems in Zimbabwe has the potential to enhance public confidence in the judicial systems. The scholars cited in the study generally agree that the introduction of digital systems improves public trust and confidence in the courts. Our firm view is that the traditional paper-based system caused significant delays, leading people to withdraw their cases or not follow up on them. The use of ICT is therefore widely seen as a means to ensure that citizens are well-informed about court operations, procedures, daily case proceedings, and online access to case decisions, thereby increasing public confidence. Our other noted view is that delays caused by paperwork could result in unethical conduct during the handling of certain cases, leading to a gradual erosion of confidence in the system. Thus, the introduction of digital systems in justice service delivery holds the promise of instilling greater confidence in the delivery of justice in the country.

Findings further show that the utilization of digital court systems enhances access to service delivery, which, in turn, improves people's confidence in the system. A significant takeaway from the findings is that the digitalization of courts not only promises a more transparent and efficient judicial system but also addresses the challenge currently undermining transparency and confidence in the judiciary.

Analysed scholarly views suggest that the digitalization of Zimbabwean courts has the potential to enhance the quality of decision-making in judicial cases. IT adoption in court systems allows for quick and efficient transfer, retrieval, and storage of information, addressing the challenges of timely case organization and information

loss. This saves time for trials and the rendering of judgments. Another notable view made in this study is that it is now very quick to obtain court orders as the system simply extracts your draft order if there are no changes. Technology also enables the capture of videos and audio recordings as primary evidence, bolstering the quality of decisions. However, mechanisms need to be developed to address contempt of court arising from falsification or manipulation of such evidence including through deep fake videos and text evidence. These findings align with Wallace (2019), who emphasizes that electronic case management systems improve service delivery and reduce delays, leading to timely decisions and enhanced decision quality. By allocating more time to hearings, investigations, and evidence presentation, administrative tasks are minimized, allowing for a focus on the core aspects of the cases.

Earlier research shows that the adoption of electronic court systems is a means to realize access to justice. Access to justice is considered crucial and the use ICT in courts potentially quickens access to justice. Court automation facilitates information sharing, case tracking, and monitoring, eliminating the barriers created by unnecessary court procedures and delays. It is expected that citizens can check the status of their cases, receive notifications about hearings, and review judgments once digitalization is fully implemented. However, researchers in this study caution that it is difficult to carry out full trials via video in Zimbabwe due to connectivity challenges and lack of supporting gadgets for ordinary people and this further pushes the ordinary people to the peripheries of access to justice.

The findings of the research also indicate that the use of digital systems in Zimbabwean judicial systems enhances transparency and accountability. Digitalization improves transparency by eliminating manipulation of manual systems and case tracking, reducing delays and corruption. It also allows for the recording of court proceedings, providing data for policymakers and facilitating performance management. This promotes transparency and enables public scrutiny of judicial officials, allowing citizens and oversight bodies to assess the delivery of expected results. The argument is supported by USAID (2021), which agrees that court automation promotes transparency and accountability. Random case assignment through digital systems helps combat corruption by removing pecuniary interests from manual allocation. Again, technology enables citizens to access sensitive information online, holding judges accountable for their actions. It fosters interconnectedness between stakeholders and facilitates service delivery through a network governance structure. Citizens are encouraged to report maladministration, and oversight bodies can hold the judiciary accountable for their performance as already noted by Poshai and Vyas-Doorgapersad (2023), and Wallace (2019).

Finally, there is general consensus among scholars that the digitalization of court systems improves access to data, which benefits citizens and stakeholders in policymaking. By providing timely and secure access to data, digital systems support evidence-based policymaking. For example, data from courts can inform policies related to gender-based

violence or robbery by providing evidence of the number of recorded cases. The adoption of digital systems in Zimbabwean courts enhances transparency, accountability, and access to data, ultimately improving the delivery of justice.

3.3. Challenges to the Digitalization of Courts in Zimbabwe

This section delves into the challenges and practical implementation of digital court systems in Zimbabwe. The digitalization of courts holds the promise of enhancing transparency, accountability, and access to justice. However, several key challenges hinder the effective implementation of digital systems as already acknowledged by Poshai and Vyas-Doorgapersad (2023). The foremost challenge lies in the lack of adequate infrastructure, encompassing limited access to Wi-Fi, internet connectivity, computers, tablets, and other essential devices within courtrooms. Additionally, the unavailability of funding poses a significant obstacle to the successful adoption of digital technologies (Watson et al., 2017). Furthermore, the issue of erratic power supply exacerbates the challenges faced in the digitalization process. Despite these hurdles, it is essential to explore the practical steps that can be taken towards implementing digital systems in Zimbabwean courts. This section examines the identified challenges and sheds light on the practical strategies that can be adopted to navigate the complexities of digitalizing court systems in Zimbabwe.

The findings of this study further stress that lack of adequate IT infrastructure is a persistent problem. The research revealed that essential resources such as Wi-Fi, internet access, computers, tablets, and other devices necessary for connecting to the internet are lacking within courtrooms. The view of the researchers is that the current situation perpetuates a monopoly of justice for those who can afford online access, leaving the majority unable to benefit, thus hindering access to justice.

The inadequacy of IT infrastructure in Zimbabwe's judiciary is confirmed by experts and reports, including those by Malaba[17] and Weers (2016). Malaba's report reveals that the phased implementation of electronic court systems is due to anticipated challenges and the lack of necessary infrastructure. Vasista (2018) argues that developing countries often face hurdles in implementing electronic court systems due to insufficient infrastructure. As such, it is not far-fetched to assume that the digitalization of courts in Zimbabwe is not immune to these challenges.

The study findings highlight that the lack of adequate funding is a significant obstacle to the effectiveness of digitalizing the judicial systems in Zimbabwe. The crucial role of funds in implementing IT in the courts cannot be discounted. Our held view is that the judiciary in Zimbabwe is overzealous in pursuing digitalization without considering the financial constraints it faces. The study also revealed that electronic court systems in Zimbabwe are still in their early stages, lacking full functionality and accessibility. Consequently, the implementation of digital systems has excluded poor citizens

[17] Malaba, L. (2022). Digital transformation of judiciaries in Africa and experiences in the face of the COVID-19 pandemic. The Judicial Service Commission of Zimbabwe. https://clck.ru/3Eufbq

from accessing justice, despite the intention to broaden access through technology. Tonn et al. (2012) also confirms that inadequate funding is a major obstacle that hampers the effectiveness of digitalization in the justice delivery system. It is crucial for the implementation of digital systems to be supported by sufficient funding to ensure the successful adoption, operationalization and upgrading of e-justice in Zimbabwe.

The research findings indicate that the lack of sufficient electricity supply is a significant challenge that affects the adoption and effectiveness of digitalizing court systems in Zimbabwe. a firm view of the researchers is that persistent frustrations with the system will remain as long as electricity supply challenges are intact. This is consistent with the views of Muparadzi et al. (2024) that electricity poverty still persists in Zimbabwe. ICT devices used in electronic court systems require a constant power supply for their proper functioning. Researchers in this paper hasten to point out that power outages and intermittent supply disrupt end to end court processes, a scenario which leads to abrupt stoppages of court proceedings. Power supply obstacles therefore need urgent attention for successful digitalization of courts in Zimbabwe to be realized.

3.4. Practical Implementation of IECMs in Zimbabwe

The study explored strategies to enhance the implementation and adoption of digital systems in Zimbabwe's justice service delivery. The findings emphasized the need for requisite infrastructure to ensure successful IT implementation. Muhammad et al. (2023) highlight that developing countries often fail in policy implementation due to inadequate infrastructure. Likewise, the research participants stressed the importance of elementary infrastructures such as IT, electricity, and internet gadgets, along with an enabling legal framework. Stakeholder engagement was also identified as a crucial success factor. The involvement of multiple stakeholders creates an ecosystem for effective implementation, promoting collective decision-making and local buy-in. Malaba[18] indicated that the Judicial Service Commission (JSC) engaged various stakeholders, including governmental bodies, the judiciary, and citizens. Furthermore, the slow adoption of technology necessitated extensive education and awareness campaigns. Training programs were initiated by the JSC to address the literacy gap among judicial stakeholders[19]. This paper suggests that this can be complemented by the creation of online platforms, such as a YouTube[20] channel, for instructional videos, as well as a toll-free helpline and help desk for inquiries and feedback. These customer-centric measures align with the principles of digital governance. Lastly, the findings

[18] Malaba, L. (2022). Digital transformation of judiciaries in Africa and experiences in the face of the COVID-19 pandemic. The Judicial Service Commission of Zimbabwe. https://clck.ru/3Eufbq

[19] Ibid.

[20] The foreign person owning the YouTube informational resource violates the legislation of the Russian Federation.

underscore the importance of infrastructure development, stakeholder engagement, and comprehensive education initiatives for successful implementation and adoption of digital systems in Zimbabwe's justice delivery.

4. Proposed Model for Effective Digital Transition in Justice Administration

The model (Fig. 2) outlined above delineates seven crucial stages for developing a digital court system. Adapting each stage's requirements from manual to digital courts is essential for a successful transition. Emphasizing the understanding of court functions and the political landscape is pivotal to mitigate resistance to change and ensure system efficiency.

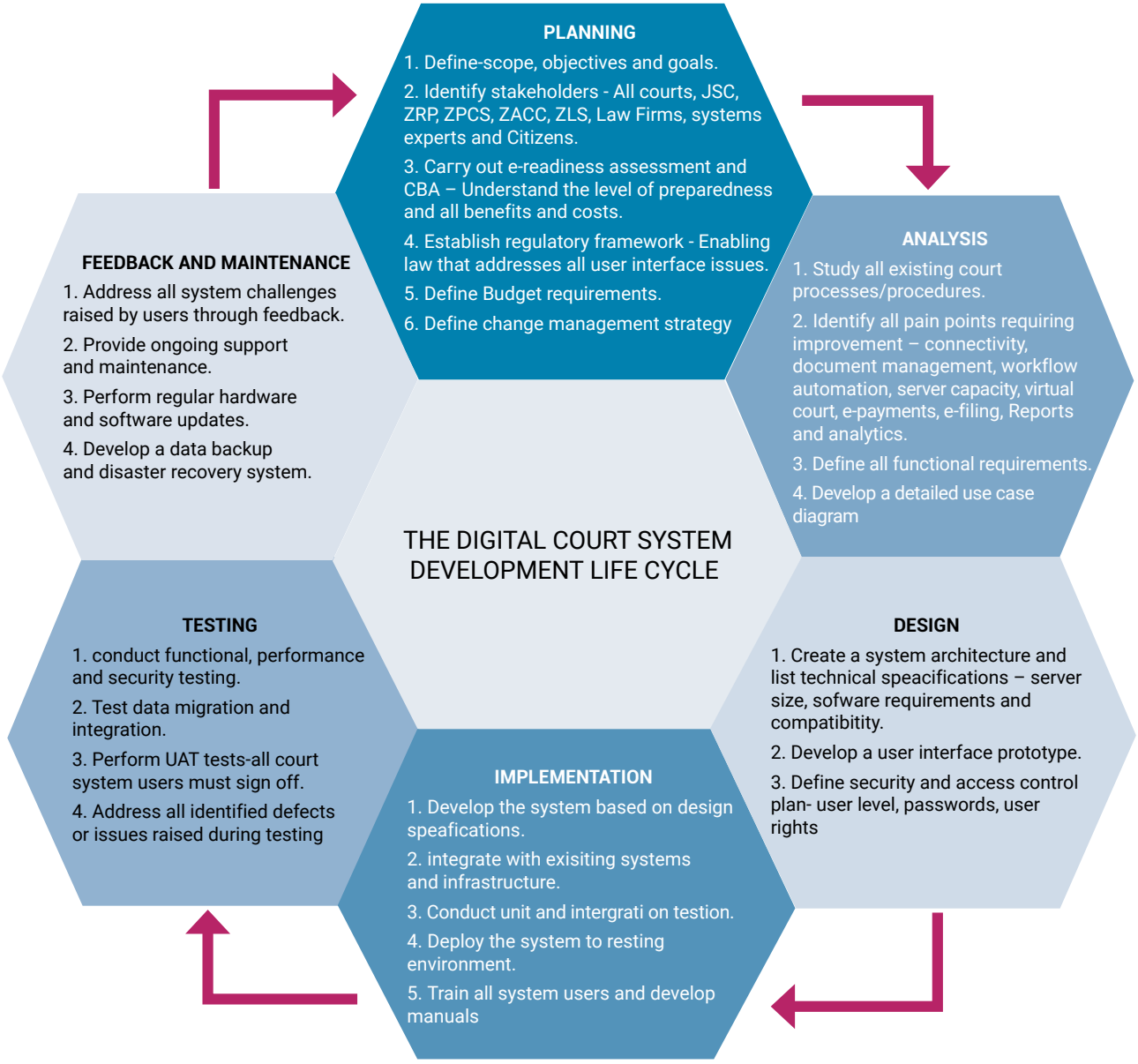


Fig. 2 The Digital Court System Development Life Cycle

Source: Adapted from the Systems Development Life Cycle

In Zimbabwe, initiating the process entails a comprehensive e-readiness assessment focusing on user, institutional, and system needs. User assessment targets ICT skills, literacy, and training requirements, while institutional evaluation encompasses organizational dynamics, infrastructure, leadership, ICT policies, change management, peer learning, and funding. System development hinges on hardware, software, upgrades, licensing, and contractor selection. Testing in the user environment involves user login, functional tests, document handling, case tracking, information access, report formats, and analytics. Evaluating outcomes like transparency, efficiency, and user experience precedes incorporating feedback for continual system enhancement prior to final deployment, with feedback guiding ongoing improvements and upgrades.

Conclusion

Overall, the study's findings provide valuable insights into the understanding and implementation of digitalization in Zimbabwean court systems, highlighting the importance of ICT integration to enhance case management, reduce delays, and improve justice delivery. The findings highlight the potential of digital systems to improve court operations in Zimbabwe as well as the potential of digital systems to enhance decision quality and increase access to justice in Zimbabwe. Again, the findings further highlight that digital systems enhance transparency and accountability in Zimbabwean judicial systems. They enable public scrutiny, combat corruption, promote accountability of public officials, and improve access to data for evidence-based policymaking. However, the findings also underscore the lack of adequate IT infrastructure as a major challenge in the digitalization of courts in Zimbabwe. The absence of necessary resources limits the implementation and effectiveness of digital systems, hindering access to justice. In addition, the much hyped about IECMS has not sustained its credibility as an advanced technological innovation for courts in Zimbabwe due to intricate challenges that remain and may result in the total collapse of the digitalization initiatives adopted and implemented to date. Adopting practical digitalization implementation approaches is therefore recommended to guarantee the success of e-justice administration in Zimbabwe and the proposed model may be ideal for quickening digitalization of courts in Zimbabwe.

Areas for further research

This study lacked in-depth empirical analysis from diverse regions, relying on secondary data. A comprehensive comparative study using primary data is warranted. The model above, developed solely on qualitative data, requires expansion with quantitative data showcasing the correlations between digital court advancements in Zimbabwe and key success factors.

Reference

Aaltonen, I., & Tammela, K. (2019). Envisioning e-justice for the criminal justice chain in Finland. *Electronic Journal of E-Government*, *13*(1), 56–66.

Adeola, O., & Evans, O. (2020). ICT, infrastructure, and tourism development in Africa. *Tourism Economics*, *26*(1), 97–114. https://doi.org/10.1177/1354816619827712

Ahmed, J. U. (2010). Documentary Research Method: New Dimensions. *Indus Journal of Management and Social Sciences*, *4*(1), 1–14.

Ajibade, P. (2018). Technology Acceptance Model Limitations and Criticisms: Exploring the Practical Applications and Use in Technology-related Studies, Mixed-method, and Qualitative Researches. *Library Philosophy and Practice (e-journal)*, 1941.

Alami, S. A. (2015). Research within the field of applied linguistics: Points to consider. *Theory and Practice in Language Studies*, *5*(7), 1330–1337. https://doi.org/10.17507/tpls.0507.03

Bans-Akutey, A., & Tiimub, B. M. (2021). Triangulation in Research. *Academia Letters*, 1–6, 3392. https://doi.org/10.20935/AL3392

Bannister, F. (2015). Deep E-Government: Beneath the carapace. In *E-government: Information, technology, and transformation* (pp. 49–67). Routledge. https://doi.org/10.4324/9781315704906-11

Bwalya, K. J. (2018). *Decolonization of E-government Research and Practice: Exploring Contextual Issues and Opportunities in Africa*. Cape Town: AOSIS ltd.

Bosire, E. M., Kivoi, D., & Nduvi, S. (2017). Effects of judicial transformation framework (2012–2016) on the performance of the judiciary in Kenya. *Archives of Business Research*, *5*(12), 349–364. https://doi.org/10.14738/abr.512.4050

Carter, N., Bryant-Lukosius, D., DiCenso, A., Blythe, J., & Neville, A. J. (2014). The Use of Triangulation in Qualitative Research. *Oncology Nursing Forum*, *41*(5), 545–547. https://doi.org/10.1188/14.onf.545-547

Caserta, S. (2022). The Sociology of the Legal Profession in the Digital Age. *International Journal of the Legal Profession*, *29*(3), 319–334. https://doi.org/10.1080/09695958.2021.1920417

Cassim, F. (2017). The use of Electronic Discovery and Cloud-computing Technology by Lawyers in Practice: Lessons from Abroad. *Journal for Juridical Science*, *42*(1). https://doi.org/10.18820/24150517/JJS42.v1.2

Chipeva, P., Cruz-Jesus, F., Oliveira, T., & Irani, Z. (2018). Digital divide at individual level: Evidence for Eastern and Western European countries. *Government Information Quarterly*, *35*(3), 460–479. https://doi.org/10.1016/j.giq.2018.06.003

Cloete, F. (2005). Maximising the potential of transforming policy failure into policy success: E-government, the digital divide & E-development. In G. Petroni, & F. Cloete (Eds.), *New Technologies in Public Administration, International Institute of Administrative Sciences (IIAS)* (pp. 113–132). ISO Press, Brussels.

Cordella, A., & Contini, F. (2020). *Digital Technologies for Better Justice: A Toolkit for Action*. http://dx.doi.org/10.18235/0002297

Creswell, J. W. (2009). *Research Design: Qualitative, Quantitative and Mixed Methods Approaches*. New York: SAGE Publications.

Creswell, J, W. (2014). *Research design: Qualitative, Quantitative and Mixed Methods* (4th ed.). California: Sage Publishers.

Creswell, J. W. (2013). *Qualitative Inquiry and Research Design: Choosing Among Five Approaches*. Thousand Oaks, CA: Sage.

Cohen, L., Manion, L., & Morrison, K. (2007). *Research Methods in Education* (6th ed.). New York: Routledge. https://doi.org/10.4324/9780203029053

Davies, M. B. (2007). *Key Concepts in Social Research Methods*. New York: Palgrave, Macmillan Ltd.

Davis, F. D., Baggozi R. P., & Warshaw, P. R. (1989). User of Computer Technology: comparison two theoretical Models. *Management Science*, *35*(8), 982–1003. https://doi.Org/10.1287/mnsc.35.8.982

Deming, W. E. (1985). Transformation of western style of management. *Interfaces*, *15*(3), 6–11. https://doi.org/10.1287/inte.15.3.6

Dneprovskaya, M. A., & Abramitov, S. A. (2020). Digital Technologies in Activities of Russian Courts: Prospects of Artificial Intelligence Application. In *Proceedings of the 2nd International Scientific and Practical Conference "Modern Management Trends and the Digital Economy: from Regional Development to Global Economic Growth" (MTDE 2020)*. https://doi.org/10.2991/aebmr.k.200502.034

Donoghue, J. (2017). The Rise of Digital Justice: Courtroom Technology, Public Participation, and Access to Justice. *The Modern Law Review*, *80*(6), 995–1026. https://doi.org/10.1111/1468-2230.12300

Drossos, D., Lekakos, G., Doukidis, G. I., & Tsatsa, N. (2018). Public-sector Digitization: An Analytical Cost-Effective Framework. In *The 12th Mediterranean Conference on Information Systems (MCIS)*, Corfu, Greece.

Fleer, P. (2018). Conclusion: digitization and the continuities of change in administrative information processing. *Administration and Society*, *50*(9), 1335–1359. https://doi.org/10.1177/0095399718791540

Goulard, G. Y., Alain, C., & Clarke, G. (1991). Computerization and Electronic Communications in the Supreme Court of Canada. *International Review of Law, Computers & Technology*, *5*(1), 74–95. https://doi.org/10.1080/13600869.1991.9966307

Haider, A. (2013). E-Court: Information and Communication Technologies for Civil Court Management. In *Proceedings of PICMET '13: Technology Management for Emerging Technologies* (pp. 2296–2304).

Han, W., Shen, J., Liu, Y., Shi, Z., Xu, J., Hu, F., Chen, H., Gong, Y., Yu, X., Wang, H., Liu, Z., Yang, Y., Shi, T., & Ge, M. (2024). LegalAsst: Human-centered and AI-empowered Machine to Enhance Court Productivity and Legal Assistance. *Information Sciences*, *679*, 3–18. https://doi.org/10.1016/j.ins.2024.121052

Hanzi, R., & Baeyens, A. (2021). *Concerns over Judicial Independence in Zimbabwe*. Washington DC: Human Rights Institute.

Hassan, K. H., Yusoff, S. S. A., Mokhtar, M. F., & Khalid, A. T. K. (2016). The use of technology in the transformation of business dispute resolution. *European Journal of Law and Economics*, *42*, 369–381. https://doi.org/10.1007/s10657-012-9375-7

Heeks, R. (2002). e-Government in Africa: Promise and practice. *Information Polity*, *7*(2, 3), 97–114. https://doi.org/10.3233/ip-2002-0008

Insa, F. (2007). The Admissibility of Electronic Evidence in Court (A.E.E.C.): Fighting against High-Tech Crime – Results of a European Study. *Journal of Digital Forensic Practice*, *1*(4), 285–289. https://doi.org/10.1080/15567280701418049

Kabir, M. A., Saidin, S. Z., & Ahmi, A. (2015). Adoption of E-Payment Systems: A Review of Literarure. In *Proceeding of the International Conference on E-Commerce (ICoEC)* (pp. 112–120).

Kim, Y., & Crowston, K. (2011). Technology adoption and use theory review for studying scientists continued use of cyber-infrastructure. *Proceedings of the American Society for Information Science and Technology*, *48*(1), 1–10. https://doi.org/10.1002/meet.2011.14504801197

Krishna, O. (2018). Structural Reforms for Overcoming Delays in Justice Delivery. *Journal of Constitutional Law and Jurisprudence*, *1*(1), 32–41.

Kudo, H. (2015). Does e-Government Guarantee Cost-effectiveness? An Experience from Japan and Italy. *Public Administration Quarterly*, *32*(1) 93–120. https://doi.org/10.1177/073491490803200103

Li, W., & Peng, Q. (2023). Digital courts and corporate investment in sustainability: Evidence from China. *International Review of Financial Analysis*, *88*, 2–19. https://doi.org/10.1016/j.irfa.2023.102682

Maseh, E. (2015). Managing court records in Kenya. *African Journal of Library, Archives & Information Science*, *25*(1), 77–87.

Masenya, T. M., & Ntengenyane, K. (2022). The Management of Digital Court Records for Justice Delivery in the South African High Courts. *Mousaion: South African Journal of Information Studies*, *40*(3). https://doi.org/10.25159/2663-659X/12691

Mawela, T., Ochara, M. N., & Twinomurinzi, L. (2017). e-Government implementation: a reflection on South African municipalities. *South African Computer Journal*, *29*(3), 23–44. https://doi.org/10.18489/sacj.v29i1.444

Meyerson, D. (2015). Why Should Justice Be Seen to Be Done? *Criminal Justice Ethics*, *34*(1), 64–86. https://doi.org/10.1080/0731129X.2015.1019780

Monga, A. (2008). E-government in India: Opportunities and challenges. *JOAAG*, *3*(2), 14–29.

Morison, J., & Harkens, A. (2019). Re-engineering justice? Robot judges, computerized courts and (semi) automated legal decision-making. *Legal Studies*, *39*(4), 618–635. https://doi.org/10.1017/lst.2019.5

Muhammad, D., Aziz, F., Ar-Rasyid, Y., & Asi-Sayyis, I. A. (2023). Assessing the Impact of Electronic Court Systems on the Efficiency of Judicial Processes in the Era of Digital Transformation. *Jurnal Ilmu Hukum dan Konstitusi*, *6*(1), 1–18. https://doi.org/10.24090/volksgeist.v6i1.8082

Mukonza, R. M. (2014). E-Governance: A New Paradigm in Public Administration. *Journal of Public Administration*, *49*(2), 499–511.

Mukonza, R. M., Maserumule, M. H., & Moeti, K. B. (2016). A Critical Examination of Socioeconomic and Demographic factors as Determinants of Egovernment Adoption Among Redidents in Zimbabwe's Two Local Authorities. *Africa Insight*, *46*(2), 60–75.

Muparadzi, T., Nyikadzino, T., & Nhema, A. (2019). A Critical Reflection on the Role of E-governance in Reinvigorating Public Sector Operations in Zimbabwe. *Zambezia*, *46*(1), 179–197.

Muparadzi, T., & Rodze, L. (2021). Business Continuity Management in a Time of Crisis: Emerging Trends for Commercial Banks in Zimbabwe during and Post the Covid-19 Global Crisis. *Open Journal of Business and Management*, *9*(3), 1169–1197. https://doi.org/10.4236/ojbm.2021.93063

Muparadzi, T., Wissink, H., & McArthur, B. (2024). Towards a Framework for Accelerating E-Government Readiness for Public Service Delivery Improvement in Zimbabwe. *Adminstracio Publica*, *32*(2), 96–119. https://doi.org/10.61967/adminpub/2024.32.2.7

Muparadzi, T. (2024). Rethinking E-Government Implementation in Zimbabwe: Evidence and Lessons from Selected Country Cases. In *Digital Technologies for a Resource Efficient Economy. IGI Global*. https://doi.org/10.4018/979-8-3693-2750-0.ch001

Muscalu, E., & Hulpus, I. A. (2016). The computerization of courts. Implications of judicial management in the assessment of the transparency and accessibility of legal services. *Revista Economică*, *68*(1), 160–177.

Naidoo, G. (2017). Electronic technology as a mechanism to improve service delivery in South Africa. The case for an innovative e-delivery strategy in the Public Service. *South African Journal of Public Administration and Management*, *17*(2), 19–32.

Neuman, L. (2014). *Social Research Methods: Qualitative and Quantitative Approaches*. Harlow: Pearson Education.

Nzaro, R. & Magidi, N. (2014). Assessing the Role of Electronic Payment Systems in Financial Institutions: A Case of a Savings Bank in Zimbabwe. *Global Journal of Management and Business Research*, *14*(2), 11–36.

Oakes, A. R., & Davies, H. (2016). Justice Must Be Seen to Be Done: A Contextual Reappraisal. *Adelaide Law Review*, *37*, 461–494.

Papagianneas, S., & Junius, N. (2023). Fairness and justice through automation in China's smart courts. *Computer Law & Security Review: The International Journal of Technology Law and Practice*, *51*, 105897. https://doi.org/10.1016/j.clsr.2023.105897

Parrish, J. L., & Courtney, J. F. (2007). Electronic Records Management in Local Government Agencies: The Case of the Clerk of Courts Office in Lake County Florida. *Information Systems Management*, *24*(3), 223–229. https://doi.org/10.1080/10580530701404272

Pillot, B., Muselli, M., Poggi, P., & Dias, J. B. (2019). Historical trends in global energy policy and renewable power system issues in Sub-Saharan Africa: The case of solar 131 PV. *Energy Policy*, *127*, 113–124. https://doi.org/10.1016/j.enpol.2018.11.049

Poshai, L. & Vyas-Doorgapersad, S. (2023). Digital justice delivery in Zimbabwe: Integrated electronic case management system adoption. *South African Journal of Information Management*, *25*(1), a1695. https://doi.org/10.4102/sajim.v25i1.1695

Prescott, J. J. (2017). Improving access to justice in state courts with platform technology. *Vanderbilt Law Review*, *70*(6), 1993–2050.

Procopiuck, M. (2018). Information Technology and Time of Judgment in Specialized Courts: What is the Impact of Changing from Physical to Electronic Processing? *Government Information Quarterly*, *35*(3), 491–501. https://doi.org/10.1016/j.giq.2018.03.005

Rajah, N. (2015). E-Government in Zimbabwe: An Overview of Progress Made and Challenges Ahead. *Journal of Global Research in Computer Science*, *6*(12), 11–16.

Rooze, E. (2010). Differentiated Use of Electronic Case Management Systems. *International Journal for Court Administration*, *3*(1), 50–60. https://doi.org/10.18352/ijca.53

Satirah Wan Mohd Saman, W., & Haider, A. (2013). E-Shariah in Malaysia: Technology Adoption Within the Justice System. *Transforming Government: People, Process, and Policy*, *7*(2), 256–276. https://doi.org/10.1108/17506161311325396

Sekaran, U., & Bougie, R. (2010). *Research Methods for Business: A skill Building Approach*. New York: John Wiley and Sons.

Shah, K. P., & Gupta, M. (2017). Role of Information Technology in Expediting the Process of Justice: An Assessment of Current Challenges and Future Goals. *International Journal of Multidisciplinary Educational Research*, *6*(6-5), 162–177.

Sourdin, T., Li, B., & McNamara, D. M. (2020). Court Innovations and Access to Justice in Times of Crisis. *Health Policy and Technology*, *9*(4), 447–453. https://doi.org/10.1016/j.hlpt.2020.08.020

Sousa, M. M., & Guimaraes, T. A. (2017). The Adoption of Innovations in Brazilian Labor Courts from the Perspective of Judges and Court Managers. *Revista de Administração*, *52*(1), 103–113. https://doi.org/10.1016/j.rausp.2016.09.008

Sung, H. (2020). Can Online Courts Promote Access to Justice? A Case Study of the Internet Courts in China. *Computer Law and Security Review*, *39*, 105461. https://doi.org/10.1016/j.clsr.2020.105461

Svitlychnyy, O. P., Matselyukh, I. A., Yaselska, N. M., Glugovska, S. L., & Dyshleva, O. I. (2023). Electronic justice as a mechanism for ensuring the right of access to justice in a pandemic: the experience of Ukraine and the EU. *International Review of Law, Computers & Technology*, *37*(3), 325–340. https://doi.org/10.1080/13600869.2023.2221820

Tembo, S., & Singh, A. (2023). Mutilation of the Independence of the Judiciary: Threats, Indimidation and Conctituional Amendments in Zimbabwe. *Obiter*, *44*(3), 546–560. https://doi.org/10.17159/obiter.v44i3.14675

Thalib, H., Rahman, S., Mamulai, M., & Djanggih, H. (2017). Verification Through the Electronic Media (teleconference) on the Court in the Criminal Judicial System. *ADRI International Journal of Law and Social Science*, *1*(1), 1–9.

Tonn, B., Stiefel, D., Scheb, J. M., Glennon, C., & Sharma, H. K. (2012). Future of the Courts: Fixed, Flexible, and Improvisational Frameworks. *Futures*, *44*(9), 802–811. https://doi.org/10.1016/j.futures.2012.07.005

Turner, J. C. (2002). Changes in the Courthouse-Electronic Records, Filings and Court Dockets: Goals, Issues and the Road Ahead. *Legal Reference Services Quarterly*, *21*(4), 275–299. https://doi.org/10.1300/J113v21n04_03

Twizeyimana, J. D. & Anderson, A. (2019). The Public Value of E-Government – A Literature Review. *Government Information Quarterly*, *36*(2), 167–178. https://doi.org/10.1016/j.giq.2019.01.001

Undi-Phiri, B., & Phiri, J. (2022). Assessing Factors Affecting the Adoption of E-Government Services in Developing Countries for Transport Sector, Amidst the Covid-19 Pandemic. *Communications and Network*, *14*, 69–90. https://doi.org/10.4236/cn.2022.142006

Vasista, T. (2018). SaaS Based E-Court Applications in E-Governance in India. *International Journal of Managing Public Sector Information and Communication Technologies*, *9*(3), 1–17. https://doi.org/10.5121/ijmpict.2018.9301

Wallace, A. (2019). Ten questions for Dory Reiling – Developing IT for courts. *International Journal for Court Administration*, *10*(1), 1–3. https://doi.org/10.18352/ijca.293

Watson, A., Rukundakuvuga, R., & Matevosyan, A. (2017). Integrated Justice: An Information Systems Approach to Justice Sector Case Management and Information Sharing Case Study of the Integrated Electronic Case Management System for the Ministry of Justice in Rwanda. *International Journal for Court Administration*, *8*(3), 1–9. https://doi.org/10.18352/ijca.233

Weers, T. D. (2016). Case flow management net-project - the practical value for civil justice in the international journal for court administration. *International Journal for Court Administration*, *8*(1), 32–42. https://doi.org/10.18352/ijca.216

Yin, R. K. (2009). *Case Study Research: Design and Methods*. Beverly: Hills.

Zhang, M., Cao, X., & Sun, A. (2024). Applications of Satellite Technologies within China's Legal System: A review. *Acta Astronautica*, *219*, 750–760. https://doi.org/10.1016/j.actaastro.2024.03.063

Zhurkina, O. Filippova, E., & Bochkareva, T. (2021). Digitalization of Legal Proceedings: Global Trends. *Advances in Economics, Business and Management Research*, *171*, 119–124. https://doi.org/10.2991/aebmr.k.210318.018

Zinyama, T. & Nhema, G. (2016). E-government and Development in Zimbabwe: An Appraisal. *Public Policy and Administration Research*, *6*(2), 13–23.

Authors information

Taurai Muparadzi – PhD (Public Administration), Lecturer, Faculty of Social and Behavioral Sciences, University of Zimbabwe; Postdoctoral Fellow, Department of Public Affairs, Tshwane University of Technology
Address: P.O.Box MP167, Mt Pleasant, Harare, Zimbabwe; Staatsartillerie Rd, Philip Nel Park, 0183 Pretoria, South Africa
E-mail: tauraimuparadzi@gmail.com
ORCID ID: https://orcid.org/0000-0003-1590-6553
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=58101232900
WoS Researcher ID: https://www.webofscience.com/wos/author/record/LWJ-6359-2024
Google Scholar ID: https://scholar.google.com/citations?user=GwueN-QAAAAJ

Ricky Munyaradzi Mukonza – DTech in Public Management, Associate Professor of Public Management, Department of Public Affairs, Tshwane University of Technology
Address: Staatsartillerie Rd, Philip Nel Park, 0183 Pretoria, South Africa
E-mail: MukonzaRM@tut.ac.za
ORCID ID: https://orcid.org/0000-0001-8121-1501
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=56157610200
Google Scholar ID: https://scholar.google.com/citations?user=LXj9QUQAAAAJ

Authors' contributions

The authors have contributed equally into the concept and methodology elaboration, validation, formal analysis, research, selection of sources, text writing and editing, project guidance and management.

Conflict of interest

The authors declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law
PASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – November 4, 2024
Date of approval – November 19, 2024
Date of acceptance – December 13, 2024
Date of online placement – December 20, 2024

Научная статья
УДК 34:004:347:004.4
EDN: https://elibrary.ru/clzzkx
DOI: https://doi.org/10.21202/jdtl.2024.40

Перспективы применения цифровых технологий в системе отправления правосудия в Зимбабве

Таурай Мупарадзи

Зимбабвийский университет, Хараре, Зимбабве
Технологический университет Тшване, Претория, ЮАР

Рикки Муньярадзи Муконза

Технологический университет Тшване, Претория, ЮАР

Ключевые слова

автоматизация,
отправление правосудия,
право,
суд,
судебная система,
судопроизводство,
цифровые технологии,
электронное правительство,
электронное правосудие,
электронный документооборот

Аннотация

Цель: в настоящее время в глобальном масштабе идет интенсивное обсуждение цифровизации и автоматизации предоставления услуг в государственных учреждениях, соответствующей технологическому масштабу Четвертой промышленной революции. Применение цифровых технологий имеет решающее значение для создания оптимизированной системы предоставления услуг. В африканских странах все больше внимания уделяется вопросам автоматизации и цифровизации судебной деятельности, что обусловлено опасениями по поводу рисков влияния на системы отправления правосудия. В свете этого целью данной статьи стало формирование перспективной модели внедрения и реализации процесса цифровизации в судах Зимбабве.

Методы: исследование базируется на методах научного анализа и синтеза, дедукции и индукции, правового моделирования, формально-юридическом и сравнительно-правовом методах.

Результаты: в статье представлен обзор принятых мер по цифровизации системы отправления правосудия в различных государствах, исследован передовой опыт. Выявлена сущность цифровизации судебной системы в Зимбабве, определены основные существующие и перспективные направления влияния цифровизации на судебную систему Зимбабве, показаны способы оперативного и эффективного перевода системы отправления правосудия в цифровой формат. Установлены преимущества цифровой обработки данных в судебных органах и выявлены препятствия на пути использования цифровых систем

✉ Корреспондирующий автор
© Мупарадзи Т., Муконза Р. М., 2024

Статья находится в открытом доступе и распространяется в соответствии с лицензией Creative Commons «Attribution» («Атрибуция») 4.0 Всемирная (CC BY 4.0) (https://creativecommons.org/licenses/by/4.0/deed.ru), позволяющей неограниченно использовать, распространять и воспроизводить материал при условии, что оригинальная работа упомянута с соблюдением правил цитирования.

при отправлении правосудия, вследствие чего сохраняется недостаточная оптимальность Интегрированной электронной системы ведения дел (Integrated Electronic Case Management System, IECMS).

Научная новизна: в исследовании выстраивается оптимальная модель внедрения цифровых технологий в систему судопроизводства в Зимбабве, направленная на повышение эффективности цифровизации судов и преобразование системы отправления правосудия. Обосновывается, что для достижения этой цели решающее значение имеют вспомогательная инфраструктура информационно-коммуникационных технологий, уровень образования и осведомленности граждан, а также проводимая государственно-правовая политика.

Практическая значимость: ожидается, что предложенная в работе модель внедрения и повышения эффективности цифровизации судов Зимбабве позволит осуществить комплексное и бесперебойное внедрение IECMS.

Для цитирования

Мупарадзи, Т., Муконза, Р. М. (2024). Перспективы применения цифровых технологий в системе отправления правосудия в Зимбабвее. *Journal of Digital Technologies and Law*, *2*(4), 802–834. https://doi.org/10.21202/jdtl.2024.40

Список литературы

Aaltonen, I., & Tammela, K. (2019). Envisioning e-justice for the criminal justice chain in Finland. *Electronic Journal of E-Government*, *13*(1), 56–66.

Adeola, O., & Evans, O. (2020). ICT, infrastructure, and tourism development in Africa. *Tourism Economics*, *26*(1), 97–114. https://doi.org/10.1177/1354816619827712

Ahmed, J. U. (2010). Documentary Research Method: New Dimensions. *Indus Journal of Management and Social Sciences*, *4*(1), 1–14.

Ajibade, P. (2018). Technology Acceptance Model Limitations and Criticisms: Exploring the Practical Applications and Use in Technology-related Studies, Mixed-method, and Qualitative Researches. *Library Philosophy and Practice (e-journal)*, 1941.

Alami, S. A. (2015). Research within the field of applied linguistics: Points to consider. *Theory and Practice in Language Studies*, *5*(7), 1330–1337. https://doi.org/10.17507/tpls.0507.03

Bans-Akutey, A., & Tiimub, B. M. (2021). Triangulation in Research. *Academia Letters*, 1–6, 3392. https://doi.org/10.20935/AL3392

Bannister, F. (2015). Deep E-Government: Beneath the carapace. In *E-government: Information, technology, and transformation* (pp. 49–67). Routledge. https://doi.org/10.4324/9781315704906-11

Bwalya, K. J. (2018). *Decolonization of E-government Research and Practice: Exploring Contextual Issues and Opportunities in Africa*. Cape Town: AOSIS ltd.

Bosire, E. M., Kivoi, D., & Nduvi, S. (2017). Effects of judicial transformation framework (2012–2016) on the performance of the judiciary in Kenya. *Archives of Business Research*, *5*(12), 349–364. https://doi.org/10.14738/abr.512.4050

Carter, N., Bryant-Lukosius, D., DiCenso, A., Blythe, J., & Neville, A. J. (2014). The Use of Triangulation in Qualitative Research. *Oncology Nursing Forum*, *41*(5), 545–547. https://doi.org/10.1188/14.onf.545-547

Caserta, S. (2022). The Sociology of the Legal Profession in the Digital Age. *International Journal of the Legal Profession*, *29*(3), 319–334. https://doi.org/10.1080/09695958.2021.1920417

Cassim, F. (2017). The use of Electronic Discovery and Cloud-computing Technology by Lawyers in Practice: Lessons from Abroad. *Journal for Juridical Science*, *42*(1). https://doi.org/10.18820/24150517/JJS42.v1.2

Chipeva, P., Cruz-Jesus, F., Oliveira, T., & Irani, Z. (2018). Digital divide at individual level: Evidence for Eastern and Western European countries. *Government Information Quarterly*, *35*(3), 460–479. https://doi.org/10.1016/j.giq.2018.06.003

Cloete, F. (2005). Maximising the potential of transforming policy failure into policy success: E-government, the digital divide & E-development. In G. Petroni, & F. Cloete (Eds.), *New Technologies in Public Administration, International Institute of Administrative Sciences (IIAS)* (pp. 113–132). ISO Press, Brussels.

Cordella, A., & Contini, F. (2020). *Digital Technologies for Better Justice: A Toolkit for Action*. http://dx.doi.org/10.18235/0002297

Creswell, J. W. (2009). *Research Design: Qualitative, Quantitative and Mixed Methods Approaches*. New York: SAGE Publications.

Creswell, J, W. (2014). *Research design: Qualitative, Quantitative and Mixed Methods* (4th ed.). California: Sage Publishers.

Creswell, J. W. (2013). *Qualitative Inquiry and Research Design: Choosing Among Five Approaches*. Thousand Oaks, CA: Sage.

Cohen, L., Manion, L., & Morrison, K. (2007). *Research Methods in Education* (6th ed.). New York: Routledge. https://doi.org/10.4324/9780203029053

Davies, M. B. (2007). *Key Concepts in Social Research Methods*. New York: Palgrave, Macmillan Ltd.

Davis, F. D., Baggozi R. P., & Warshaw, P. R. (1989). User of Computer Technology: comparison two theoretical Models. *Management Science*, *35*(8), 982–1003. https://doi.Org/10.1287/mnsc.35.8.982

Deming, W. E. (1985). Transformation of western style of management. *Interfaces*, *15*(3), 6–11. https://doi.org/10.1287/inte.15.3.6

Dneprovskaya, M. A., & Abramitov, S. A. (2020). Digital Technologies in Activities of Russian Courts: Prospects of Artificial Intelligence Application. In *Proceedings of the 2nd International Scientific and Practical Conference "Modern Management Trends and the Digital Economy: from Regional Development to Global Economic Growth" (MTDE 2020)*. https://doi.org/10.2991/aebmr.k.200502.034

Donoghue, J. (2017). The Rise of Digital Justice: Courtroom Technology, Public Participation, and Access to Justice. *The Modern Law Review*, *80*(6), 995–1026. https://doi.org/10.1111/1468-2230.12300

Drossos, D., Lekakos, G., Doukidis, G. I., & Tsatsa, N. (2018). Public-sector Digitization: An Analytical Cost-Effective Framework. In *The 12th Mediterranean Conference on Information Systems (MCIS)*, Corfu, Greece.

Fleer, P. (2018). Conclusion: digitization and the continuities of change in administrative information processing. *Administration and Society*, *50*(9), 1335–1359. https://doi.org/10.1177/0095399718791540

Goulard, G. Y., Alain, C., & Clarke, G. (1991). Computerization and Electronic Communications in the Supreme Court of Canada. *International Review of Law, Computers & Technology*, *5*(1), 74–95. https://doi.org/10.1080/13600869.1991.9966307

Haider, A. (2013). E-Court: Information and Communication Technologies for Civil Court Management. In *Proceedings of PICMET '13: Technology Management for Emerging Technologies* (pp. 2296–2304).

Han, W., Shen, J., Liu, Y., Shi, Z., Xu, J., Hu, F., Chen, H., Gong, Y., Yu, X., Wang, H., Liu, Z., Yang, Y., Shi, T., & Ge, M. (2024). LegalAsst: Human-centered and AI-empowered Machine to Enhance Court Productivity and Legal Assistance. *Information Sciences*, *679*, 3–18. https://doi.org/10.1016/j.ins.2024.121052

Hanzi, R., & Baeyens, A. (2021). *Concerns over Judicial Independence in Zimbabwe*. Washington DC: Human Rights Institute.

Hassan, K. H., Yusoff, S. S. A., Mokhtar, M. F., & Khalid, A. T. K. (2016). The use of technology in the transformation of business dispute resolution. *European Journal of Law and Economics*, *42*, 369–381. https://doi.org/10.1007/s10657-012-9375-7

Heeks, R. (2002). e-Government in Africa: Promise and practice. *Information Polity*, *7*(2, 3), 97–114. https://doi.org/10.3233/ip-2002-0008

Insa, F. (2007). The Admissibility of Electronic Evidence in Court (A.E.E.C.): Fighting against High-Tech Crime – Results of a European Study. *Journal of Digital Forensic Practice*, *1*(4), 285–289. https://doi.org/10.1080/15567280701418049

Kabir, M. A., Saidin, S. Z., & Ahmi, A. (2015). Adoption of E-Payment Systems: A Review of Literarure. In *Proceeding of the International Conference on E-Commerce (ICoEC)* (pp. 112–120).

Kim, Y., & Crowston, K. (2011). Technology adoption and use theory review for studying scientists continued use of cyber-infrastructure. *Proceedings of the American Society for Information Science and Technology*, *48*(1), 1–10. https://doi.org/10.1002/meet.2011.14504801197

Krishna, O. (2018). Structural Reforms for Overcoming Delays in Justice Delivery. *Journal of Constitutional Law and Jurisprudence*, *1*(1), 32–41.

Kudo, H. (2015). Does e-Government Guarantee Cost-effectiveness? An Experience from Japan and Italy. *Public Administration Quarterly*, *32*(1) 93–120. https://doi.org/10.1177/073491490803200103

Li, W., & Peng, Q. (2023). Digital courts and corporate investment in sustainability: Evidence from China. *International Review of Financial Analysis*, *88*, 2–19. https://doi.org/10.1016/j.irfa.2023.102682

Maseh, E. (2015). Managing court records in Kenya. *African Journal of Library, Archives & Information Science*, *25*(1), 77–87.

Masenya, T. M., & Ntengenyane, K. (2022). The Management of Digital Court Records for Justice Delivery in the South African High Courts. *Mousaion: South African Journal of Information Studies*, *40*(3). https://doi.org/10.25159/2663-659X/12691

Mawela, T., Ochara, M. N., & Twinomurinzi, L. (2017). e-Government implementation: a reflection on South African municipalities. *South African Computer Journal*, *29*(3), 23–44. https://doi.org/10.18489/sacj.v29i1.444

Meyerson, D. (2015). Why Should Justice Be Seen to Be Done? *Criminal Justice Ethics*, *34*(1), 64–86. https://doi.org/10.1080/0731129X.2015.1019780

Monga, A. (2008). E-government in India: Opportunities and challenges. *JOAAG*, *3*(2), 14–29.

Morison, J., & Harkens, A. (2019). Re-engineering justice? Robot judges, computerized courts and (semi) automated legal decision-making. *Legal Studies*, *39*(4), 618–635. https://doi.org/10.1017/lst.2019.5

Muhammad, D., Aziz, F., Ar-Rasyid, Y., & Asi-Sayyis, I. A. (2023). Assessing the Impact of Electronic Court Systems on the Efficiency of Judicial Processes in the Era of Digital Transformation. *Jurnal Ilmu Hukum dan Konstitusi*, *6*(1), 1–18. https://doi.org/10.24090/volksgeist.v6i1.8082

Mukonza, R. M. (2014). E-Governance: A New Paradigm in Public Administration. *Journal of Public Administration*, *49*(2), 499–511.

Mukonza, R. M., Maserumule, M. H., & Moeti, K. B. (2016). A Critical Examination of Socioeconomic and Demographic factors as Determinants of Egovernment Adoption Among Redidents in Zimbabwe's Two Local Authorities. *Africa Insight*, *46*(2), 60–75.

Muparadzi, T., Nyikadzino, T., & Nhema, A. (2019). A Critical Reflection on the Role of E-governance in Reinvigorating Public Sector Operations in Zimbabwe. *Zambezia*, *46*(1), 179–197.

Muparadzi, T., & Rodze, L. (2021). Business Continuity Management in a Time of Crisis: Emerging Trends for Commercial Banks in Zimbabwe during and Post the Covid-19 Global Crisis. *Open Journal of Business and Management*, *9*(3), 1169–1197. https://doi.org/10.4236/ojbm.2021.93063

Muparadzi, T., Wissink, H., & McArthur, B. (2024). Towards a Framework for Accelerating E-Government Readiness for Public Service Delivery Improvement in Zimbabwe. *Adminstracio Publica*, *32*(2), 96–119. https://doi.org/10.61967/adminpub/2024.32.2.7

Muparadzi, T. (2024). Rethinking E-Government Implementation in Zimbabwe: Evidence and Lessons from Selected Country Cases. In *Digital Technologies for a Resource Efficient Economy. IGI Global*. https://doi.org/10.4018/979-8-3693-2750-0.ch001

Muscalu, E., & Hulpus, I. A. (2016). The computerization of courts. Implications of judicial management in the assessment of the transparency and accessibility of legal services. *Revista Economică*, *68*(1), 160–177.

Naidoo, G. (2017). Electronic technology as a mechanism to improve service delivery in South Africa. The case for an innovative e-delivery strategy in the Public Service. *South African Journal of Public Administration and Management*, *17*(2), 19–32.

Neuman, L. (2014). *Social Research Methods: Qualitative and Quantitative Approaches*. Harlow: Pearson Education.

Nzaro, R. & Magidi, N. (2014). Assessing the Role of Electronic Payment Systems in Financial Institutions: A Case of a Savings Bank in Zimbabwe. *Global Journal of Management and Business Research*, *14*(2), 11–36.

Oakes, A. R., & Davies, H. (2016). Justice Must Be Seen to Be Done: A Contextual Reappraisal. *Adelaide Law Review*, *37*, 461–494.

Papagianneas, S., & Junius, N. (2023). Fairness and justice through automation in China's smart courts. *Computer Law & Security Review: The International Journal of Technology Law and Practice*, *51*, 105897. https://doi.org/10.1016/j.clsr.2023.105897

Parrish, J. L., & Courtney, J. F. (2007). Electronic Records Management in Local Government Agencies: The Case of the Clerk of Courts Office in Lake County Florida. *Information Systems Management*, *24*(3), 223–229. https://doi.org/10.1080/10580530701404272

Pillot, B., Muselli, M., Poggi, P., & Dias, J. B. (2019). Historical trends in global energy policy and renewable power system issues in Sub-Saharan Africa: The case of solar 131 PV. *Energy Policy*, *127*, 113–124. https://doi.org/10.1016/j.enpol.2018.11.049

Poshai, L. & Vyas-Doorgapersad, S. (2023). Digital justice delivery in Zimbabwe: Integrated electronic case management system adoption. *South African Journal of Information Management*, *25*(1), a1695. https://doi.org/10.4102/sajim.v25i1.1695

Prescott, J. J. (2017). Improving access to justice in state courts with platform technology. *Vanderbilt Law Review*, *70*(6), 1993–2050.

Procopiuck, M. (2018). Information Technology and Time of Judgment in Specialized Courts: What is the Impact of Changing from Physical to Electronic Processing? *Government Information Quarterly*, *35*(3), 491–501. https://doi.org/10.1016/j.giq.2018.03.005

Rajah, N. (2015). E-Government in Zimbabwe: An Overview of Progress Made and Challenges Ahead. *Journal of Global Research in Computer Science*, *6*(12), 11–16.

Rooze, E. (2010). Differentiated Use of Electronic Case Management Systems. *International Journal for Court Administration*, *3*(1), 50–60. https://doi.org/10.18352/ijca.53

Satirah Wan Mohd Saman, W., & Haider, A. (2013). E-Shariah in Malaysia: Technology Adoption Within the Justice System. *Transforming Government: People, Process, and Policy*, *7*(2), 256–276. https://doi.org/10.1108/17506161311325396

Sekaran, U., & Bougie, R. (2010). *Research Methods for Business: A skill Building Approach*. New York: John Wiley and Sons.

Shah, K. P., & Gupta, M. (2017). Role of Information Technology in Expediting the Process of Justice: An Assessment of Current Challenges and Future Goals. *International Journal of Multidisciplinary Educational Research*, *6*(6-5), 162–177.

Sourdin, T., Li, B., & McNamara, D. M. (2020). Court Innovations and Access to Justice in Times of Crisis. *Health Policy and Technology*, *9*(4), 447–453. https://doi.org/10.1016/j.hlpt.2020.08.020

Sousa, M. M., & Guimaraes, T. A. (2017). The Adoption of Innovations in Brazilian Labor Courts from the Perspective of Judges and Court Managers. *Revista de Administração*, *52*(1), 103–113. https://doi.org/10.1016/j.rausp.2016.09.008

Sung, H. (2020). Can Online Courts Promote Access to Justice? A Case Study of the Internet Courts in China. *Computer Law and Security Review*, *39*, 105461. https://doi.org/10.1016/j.clsr.2020.105461

Svitlychnyy, O. P., Matselyukh, I. A., Yaselska, N. M., Glugovska, S. L., & Dyshleva, O. I. (2023). Electronic justice as a mechanism for ensuring the right of access to justice in a pandemic: the experience of Ukraine and the EU. *International Review of Law, Computers & Technology*, *37*(3), 325–340. https://doi.org/10.1080/13600869.2023.2221820

Tembo, S., & Singh, A. (2023). Mutilation of the Independence of the Judiciary: Threats, Indimidation and Conctituional Amendments in Zimbabwe. *Obiter*, *44*(3), 546–560. https://doi.org/10.17159/obiter.v44i3.14675

Thalib, H., Rahman, S., Mamulai, M., & Djanggih, H. (2017). Verification Through the Electronic Media (teleconference) on the Court in the Criminal Judicial System. *ADRI International Journal of Law and Social Science*, *1*(1), 1–9.

Tonn, B., Stiefel, D., Scheb, J. M., Glennon, C., & Sharma, H. K. (2012). Future of the Courts: Fixed, Flexible, and Improvisational Frameworks. *Futures*, *44*(9), 802–811. https://doi.org/10.1016/j.futures.2012.07.005

Turner, J. C. (2002). Changes in the Courthouse-Electronic Records, Filings and Court Dockets: Goals, Issues and the Road Ahead. *Legal Reference Services Quarterly*, *21*(4), 275–299. https://doi.org/10.1300/J113v21n04_03

Twizeyimana, J. D. & Anderson, A. (2019). The Public Value of E-Government – A Literature Review. *Government Information Quarterly*, *36*(2), 167–178. https://doi.org/10.1016/j.giq.2019.01.001

Undi-Phiri, B., & Phiri, J. (2022). Assessing Factors Affecting the Adoption of E-Government Services in Developing Countries for Transport Sector, Amidst the Covid-19 Pandemic. *Communications and Network*, *14*, 69–90. https://doi.org/10.4236/cn.2022.142006

Vasista, T. (2018). SaaS Based E-Court Applications in E-Governance in India. *International Journal of Managing Public Sector Information and Communication Technologies*, *9*(3), 1–17. https://doi.org/10.5121/ijmpict.2018.9301

Wallace, A. (2019). Ten questions for Dory Reiling – Developing IT for courts. *International Journal for Court Administration*, *10*(1), 1–3. https://doi.org/10.18352/ijca.293

Watson, A., Rukundakuvuga, R., & Matevosyan, A. (2017). Integrated Justice: An Information Systems Approach to Justice Sector Case Management and Information Sharing Case Study of the Integrated Electronic Case Management System for the Ministry of Justice in Rwanda. *International Journal for Court Administration*, *8*(3), 1–9. https://doi.org/10.18352/ijca.233

Weers, T. D. (2016). Case flow management net-project – the practical value for civil justice in the international journal for court administration. *International Journal for Court Administration*, *8*(1), 32–42. https://doi.org/10.18352/ijca.216

Yin, R. K. (2009). *Case Study Research: Design and Methods*. Beverly: Hills.

Zhang, M., Cao, X., & Sun, A. (2024). Applications of Satellite Technologies within China's Legal System: A review. *Acta Astronautica*, *219*, 750–760. https://doi.org/10.1016/j.actaastro.2024.03.063

Zhurkina, O. Filippova, E., & Bochkareva, T. (2021). Digitalization of Legal Proceedings: Global Trends. *Advances in Economics, Business and Management Research*, *171*, 119–124. https://doi.org/10.2991/aebmr.k.210318.018

Zinyama, T. & Nhema, G. (2016). E-government and Development in Zimbabwe: An Appraisal. *Public Policy and Administration Research*, *6*(2), 13–23.

Сведения об авторах

Таурай Мупарадзи – PhD (государственное управление), преподаватель, факультет общественных и поведенческих дисциплин, Зимбабвийский университет; постдокторант, кафедра общественно-политических дисциплин, Технологический университет Тшване
Адрес: Зимбабве, MP167, г. Хараре, Маунт Плезант; Южно-Африканская Республика, 0183, г. Претория, Филип Нел Парк, Штаатсартиллерие Роуд
E-mail: tauraimuparadzi@gmail.com
ORCID ID: https://orcid.org/0000-0003-1590-6553
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=58101232900
WoS Researcher ID: https://www.webofscience.com/wos/author/record/LWJ-6359-2024
Google Scholar ID: https://scholar.google.com/citations?user=GwueN-QAAAAJ

Рикки Муньярадзи Муконза – доктор технологических наук, доцент в области государственного управления, кафедра общественно-политических дисциплин, Технологический университет Тшване
Адрес: Южно-Африканская Республика, 0183, г. Претория, Филип Нел Парк, Штаатсартиллерие Роуд
E-mail: MukonzaRM@tut.ac.za
ORCID ID: https://orcid.org/0000-0001-8121-1501
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=56157610200
Google Scholar ID: https://scholar.google.com/citations?user=LXj9QUQAAAAJ

Вклад авторов

Авторы внесли равный вклад в разработку концепции, методологии, валидацию, формальный анализ, проведение исследования, подбор источников, написание и редактирование текста, руководство и управление проектом.

Конфликт интересов

Авторы сообщают об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.91 / Государство и право отдельных стран
Специальность ВАК: 5.1.2 / Публично-правовые (государственно-правовые) науки

История статьи

Дата поступления – 4 ноября 2024 г.
Дата одобрения после рецензирования – 19 ноября 2024 г.
Дата принятия к опубликованию – 13 декабря 2024 г.
Дата онлайн-размещения – 20 декабря 2024 г.

Research article
UDC 34:004:349.2:004.8
EDN: https://elibrary.ru/fhnkjq
DOI: https://doi.org/10.21202/jdtl.2024.41

Legal Aspects of Granting Subjectivity to Artificial Intelligence: Prospects of Using Robots in Legal Practice in Nigeria

Oluwaseye Oluwayomi Ikubanni ✉
Joseph Ayo Babalola University, Ikeji-Arakeji, Nigeria

Aderemi Olubunmi Oyebanji
Joseph Ayo Babalola University, Ikeji-Arakeji, Nigeria

Alade Adeniyi Oyebade
Joseph Ayo Babalola University, Ikeji-Arakeji, Nigeria

Keywords

artificial intelligence,
automation,
digital technologies,
justice,
law,
legal education,
legal practice,
online dispute settlement,
robot lawyer,
subjectivity

Abstract

Objective: to determine the potential and acceptability of using artificial intelligence in legal activities according to the Nigerian law.

Methods: the research is based on scientific analysis, as well as formal-legal, comparative-legal, historical-legal and systemic-functional methods. The scope of the research is represented by the norms of legislation, including expired normative legal acts, as well as scientific monographic and periodical literature.

Results: It was found that artificial intelligence and robot lawyers are inevitable innovations in the legal practice of many countries, including Nigeria. The use of these digital technologies has proven to be highly effective in activities related to the administration of justice, providing assistance in four areas of legal services: consulting and guidance, searching for materials, data analysis and forecasting the trial results. Technology greatly facilitates the work of lawyers, given the amount of legal services. In addition, the author show that while the use of artificial intelligence may generally be considered justified, the involvement of robot lawyers in legal practice in Nigeria faces

✉ Corresponding author
© Ikubanni O. O., Oyebanji A. O., & Oyebade A. A., 2024

This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (CC BY 4.0) (https://creativecommons.org/licenses/by/4.0), which permits unrestricted re-use, distribution and reproduction, provided the original article is properly cited.

both legal and ethical barriers. The laws on legal education and legal practice in force in this country do not recognize robot lawyers as persons licensed to practice law in Nigeria. Robot lawyers must be given the status of a person before they can fully implement their potential in the legal practice of Nigeria.

Scientific novelty: this is primarily due to the formulation of a research task to determine the possibility of a robot acting as a practicing lawyer within the legal framework in Nigeria.

Practical significance: the conclusions formulated in the paper, namely, the inevitability of using artificial intelligence and robot lawyers in legal practice and the current legislation governing legal practice in Nigeria, will be useful when considering amendments to legislation in order to adapt it to the current level of digital technology development.

For citation

Ikubanni, O. O., Oyebanji, A. O., & Oyebade, A. A. (2024). Legal Aspects of Granting Subjectivity to Artificial Intelligence: Prospects of Using Robots in Legal Practice in Nigeria. *Journal of Digital Technologies and Law, 2*(4), 835–856. https://doi.org/10.21202/jdtl.2024.41

Content

Introduction
1. Artificial Intelligence and the Emergence of Robot Lawyers in the Legal Profession
2. Legal Framework of Legal Practice in Nigeria
   2.1. Qualification for the Practice of Law in Nigeria
   2.2. Qualification of Robot Lawyer to Practice Law in Nigeria
Conclusion
References

Introduction

Indeed, technology is a product of globalisation which has over the years shown to be highly instrumental to the global changes in all spheres of human life (Antonio & Estrella, 2020) and a binding thread for civilization in the twenty-first century (Contini, 2020). The advent of technology has impacted all aspects of human relationships. It has enhanced a paradigm shift from a rigid system to a flexible one (Aidonojie et al., 2020). The possibility of exchanging ideas, transacting businesses, and even communicating with people in different parts of the world without necessarily seeing them face to face is courtesy of the flexibility that technological advancement has brought to the world (Ikubanni & Aidonojie, 2021). The quick access to information and data today is one of the many blessings of the advancement in technology (Halima, 2016).

The use of sophisticated technological facilities such as Artificial intelligence, drones (Gallesse, 2023), Global Positioning Systems (GPS), self-driven cars and Close Circuit Camera television (CCTV) amongst others have been identified as some of the facilities that have enhanced the technologically oriented developments happening around the world today[1]. These emerging technologies are today the key forces that influence public sector organisations as they are used to handle public infrastructures and service delivery (Jiya et al., 2023).

The legal profession and the practice of law have also been impacted by Artificial Intelligence (Xu, 2022). Legal practitioners are highly trained professionals who litigate disputes in a court of law, evaluate facts, write judgments, offer legal advice, and prepare documents amongst other things using their special skills and intuition (Alarie et al., 2018; Aidonojie et al., 2021). It is often thought that these services require high intelligence that only humans can possess (Alarie et al., 2018). Therefore, the nature of these services and the skills and time required to render them often determine the cost of these services (Alarie et al., 2018). Interestingly today, technology through AI has now been employed to perform the functions of humans and perhaps even better (Alarie et al., 2016). The most fascinating thing about these machines is the fact that they function so perfectly in an error-free manner with so much precision while most function with little or no human supervision, unlike humans (Aidonojie et al., 2020).

Today, undoubtedly, technology has become a significant aspect of the legal profession in Nigeria (Aidonojie et al., 2021) and other jurisdictions (Obianyo & Ater, 2022). It has impacted positively the practice of law as well as effectively and efficiently enhanced the administration of justice (Aniekwe, 2021). The use of AI in the legal profession is one of the most widely embraced technological facilities in the legal profession because it makes the work of lawyers easier mostly in areas of legal research[2], document review, risk assessment, legal drafting, etc. In several climes, the application of AI to court processes has recorded outstanding success (Richard & Solow-Niederman, 2019).

In a competition for conventional business contract reviews, an AI system created by the Israeli legal technology startup Lawgeex defeated 20 of the best attorneys in the field in February 2018. Furthermore, the system's average accuracy rate is 9% higher than that of humans[3]. During the entire process, tasks that would have taken humans 92 minutes to complete were completed by the system in 26 seconds, meaning that in terms of speed and efficiency, it has successfully executed a «double kill» on humans (Hu & Lu, 2019).

---

1 Mcmillian, J. (2013). The Impact of Technology on Administrative Justice System: a speech presented to AIAL National Administrative Law Forum, Canberra on 18th July 2013. AIAL Forum No. 75. https://goo.su/xtU7H

2 Law Pavilion Electronic Law Report is a notable artificial intelligence usually used by lawyers in Nigeria for the research of decided cases by courts of law in Nigeria.

3 Verma, U. (2018, February 26). Israeli AI Software Whips Expert Lawyers in Contract Analysis. https://clck.ru/3F5BHx

AI has quite changed the face of the judicial system (Giuffrida et al., 2018; Kioko et al., 2022) by assisting judges to improve judgment accuracy (Wang, 2020; Sanctis, 2021) with speculations that soon robot judges may replace human judges though it remains uncertain how AI will ultimately change the mode of adjudication in courts, the legal profession and even law itself (Cooper, 2011). Interestingly, one of the most recent technological developments in the practice of law is the introduction of robot lawyers to practice law in the United States. Since its introduction, there have been several controversies regarding the legal capacity of robot lawyers to practice law in California. It is pertinent to note that a technological innovation that has recorded huge success in one country is more likely to be embraced and adopted by another country[4].

It is against this backdrop that this paper seeks to examine the right of robot lawyers to practice law under Nigerian law. This paper will examine the two major laws that regulate the practice of law in Nigeria in a bid to determine the question of whether or not Nigerian law as presently constituted recognizes a robot as a person who can practice law. The operation of robot lawyers in the United States is not part of the focus of this paper though reference may be made to it in passing to buttress any point made in this paper.

1. Artificial Intelligence and the Emergence of Robot Lawyers in the Legal Profession

Artificial Intelligence (AI) has no precise definition. Defining the concept is plagued with a lot of difficulties (Alarie et al., 2018). However, AI is described as the use of technology to automate tasks that normally require human intelligence. It has also been defined as the ability of a digital computer or computer-controlled robot to accomplish actions often associated with intelligent beings[5]. It involves the development of systems that are endowed with the characteristics of human beings in terms of reasoning[6]. AI has to do with the build-up of a technological device to automatically perform complex tasks that human beings can perform as well (Surden, 2019).

AI no doubt involves the development of machine technology to imitate human intelligence, achieving greater efficiency in the performance of tasks hitherto performed by humans (Ilegieuno et al., 2021). It is a computer intelligence that does not use cognitive ability displayed by devices, as opposed to natural cognitive ability expressed in people as well as animals (McCorduck & Cfe, 2004). AI has also been described as the theory and application of systems used to simulate, extend, and expand human intelligence (Xu & Wang, 2019). AI also refers to a computer's ability to imitate human intelligent

4 Oluwatobi, O. E. (2023, March 15) Can Robots Practice Law in Nigeria? https://clck.ru/3F5BNk

5 Copeland, B. J. Artificial Intelligence. Britannica. https://goo.su/bCjq

6 Ibid.

behavior, especially human cognitive functions, such as the ability to reason, discover meaning, generalize, and learn from experience (Gravett, 2020)

It is becoming highly worrisome that as much as AI brings convenience to people (Dekker et al., 2017), it is also increasingly reducing the number of jobs for humans (Huang & Rust, 2018). This is because machines are designed to perform complex activities as has been established in the digital world over the years (Robinson, 2018) even though it is believed that AI has not succeeded at entirely replacing the need for human expertise in decision-making[7]. Over the years, much has been said about AI. However, until recently, not much has been written on the relevance of AI to the practice of law (Katyal, 2019). The current impact of AI on legal practice and even in the future cannot be over-emphasized. On a macroscopic basis, the emergence of AI and the current trends in its application within the legal profession across the globe are indicative that AI has not only changed the face of the legal industry but will also take the jobs of human lawyers (Hu & Lu, 2019).

Notably speaking, one of the instances that demonstrates how AI threatens the jobs of a lawyer is that parking infractions in York City can now be resolved by violators selecting an automated online dispute settlement system (Hu & Lu, 2019). There are now a lot fewer steps in these processes that need legal specialists' assistance (Hu & Lu, 2019). This trend is fairly evident even with the current artificial intelligence backdrop of poor performance (Hu & Lu, 2019). One of the most impressive motivations for the integration of AI and law is the fact that AI has been described as being capable of assisting in four fields of legal services which are consultation and guidance, file retrieval, data review, and lawsuit prediction (Greenleaf et al., 2018). These, without a doubt, are quite a great relief for lawyers considering the enormity of legal services. The review of the evidence, file review, and the fluidity of human lawyers moving from criminal defense to intelligent defense are noted to be a few of the importance of AI robot lawyers to legal service and the ways human lawyers work (Greenleaf et al., 2018).

The emergence of robot lawyers, a technological innovation that employs the use of AI in the performance of legal practice has again awakened the debates and controversies on the limit to which AI may be employed to perform certain tasks. A robot lawyer is a technological device in the form of a computer program designed to perform the tasks of a lawyer including most other things associated with the practice of law in an automated manner[8]. A robot lawyer is an AI-powered computer that uses Natural Language Processing (NLP) to understand legal questions and generate legally compliant answers. The robot is designed to be able to perform a number of functions such as offering legal advice, creating legal documents, and searching case laws, amongst other things.

---

7 Commerford, B. P., Dennis, S. A., Joe, J. R., & Ulla, J. W. (2021, June 21). Man Versus Machine: Complex Estimates and Auditor Reliance on Artificial Intelligence. https://goo.su/fo2AVI

8 Nangara, A. (2023, January 10). World's First robot Lawyer to Defend Human in Court. The exchange. https://clck.ru/3F5BV5

Furthermore, it is believed that the emergence of robot lawyers in the legal space is inevitable because robot lawyers are notably capable of solving the problem of imbalance in the resources of legal services. Scholars posit that the idea of introducing the combination of AI and the law through the invention of robot judges to eliminate legal uncertainties (D'amato, 1976) has been ongoing since the 1970s (Castell, 2018). However, other scholars postulate that robots should rather assist judges and lawyers and not replace them (McGinnis & Pearce, 2014).

Today, robots are undoubtedly an integral part of our daily lives. They are found as appliances in homes, self-driving cars, security systems, restaurants, and so on. There is no gainsaying that the advent of robots has made life easy generally. However, it is imperative to emphasise that the idea of introducing AI and robot lawyers into the legal profession was originally not to replace humans but to assist in making work easy (Gravett, 2020). Unfortunately, today, the machine designed to make work easy has now been considered to replace humans and take up the legal profession entirely.

In 2015, DoNotPay robot was designed by Joshua Browder as a chatbot designed for legal services. The rationale behind the creation of the robot was to assist by giving legal guidance to poor consumers who cannot afford the legal services of human lawyers in challenging minor infractions such as fines over a parking ticket, small contractual claims, etc.[9] Originally, DoNotPay was created by Joshua Browder to solve his problem[10]. The Idea of a robot lawyer came from the experience of Joshua Browder while he was studying at Stanford. He was repeatedly booked with parking tickets for failing to feed his meter[11]. Owing to a suggestion from a friend, he challenged the bookings in order to reduce them by writing a letter, and the fine was reduced[12]. At this juncture, it occurred to him how many persons must have suffered the fate of being fined with parking tickets but being unable to reduce it either because there is no time or lack of financial resources to procure a lawyer. To this end, he offered to proffer a solution that birthed the world's first robot lawyer[13].

2. Legal Framework of Legal Practice in Nigeria

The legal profession has been adjudged one of the most respected and loved professions by which professionals in this field are reposed some level of trust and confidence by society[14]. In Nigerian society, the legal profession holds a key position. In addition to

9 Alumni, M. (2021, April 21). Machine Learning: The World's First Robot Lawyer. Digital Innovation and Transformation. https://clck.ru/3F5BY2

10 Ibid.

11 Ibid.

12 Ibid.

13 Ibid.

14 Yusuf, A. (2015, November 26). The Future of Legal Practice in Nigeria: Regulation and Discipline in the Legal Profession. Paper Presented at the 8th Annual Business Luncheon of S.P.A. Ajibade & Co. https://clck.ru/3F5BYm

fulfilling the conventional duty of defending individual rights in court, solicitors actively participate in the development of legal organizations and ideas that support development (Oko, 1994; Oguanmanam & Pue, 2006). Legal services have a significant impact on and shape almost all social, economic, and political structures of the nation. Lawyers are increasingly essential to the proper operation of Nigerian society (Oko, 1994). They serve as the foundation for the nation's hopes for social and economic advancement (Shaeeb et al., 2023).

While it is beyond doubt that litigation is the cornerstone of legal practice, the evolving societal challenges in the contemporary world are fast expanding the role of lawyers in society beyond litigation[15]. In the decided case of Anozia v. AG Lagos State[16], the court ruled about the obligations of solicitors: "It is trite, that a legal practitioner has an onerous duty to uphold and observe the rule of law, promote and foster the cause of justice, maintain a high standard of professional conduct, and thus shall not engage in any conduct which is unbecoming of a member of the honorable and highly prestigious legal profession"[17].

The Black's Law Dictionary (Garner, 2004) defines the practice of law as the professional work of a duly licensed lawyer, encompassing a broad range of services such as conducting cases in courts, preparing papers necessary to bring about various transactions from conveying land to effecting mergers, preparing legal opinions on various points of law, drafting wills and other estate planning documents and advising clients on legal questions. The term also includes activities that comparatively few lawyers engage in but require legal expertise, such as drafting legislation and court rules.

The definition of legal practice above indicates that a person rendering such services must be a 'licensed lawyer'. It becomes sacrosanct at this juncture to examine the laws that regulates the practice of law in Nigeria. The Supreme Court Ordinance of 1876 was pivotal to the legal profession in Nigeria because it was the first statute to regulate the practice of law in the country. The Ordinance recognised two categories of persons to practice law in the country. According to Section 76, the first category was a person trained as either a barrister or solicitor in the United Kingdom due to the absence of a legal training institution in the country (Orojo, 1979). The second category however is the person who lacked formal legal training but by virtue of their exposure and experience had acquired legal knowledge and skills. These persons were referred to as 'local attorneys (Adegoke et al., 2014).

The insufficiency of qualified legal practitioners in the colony fortified the need for the Chief Justice to exercise its discretion in the recognition of the second category[18].

---

15 Chinaka, C. (2022, September 14). What Constitutes Legal Practice in Nigeria? The Sun. https://clck.ru/3F5BaT

16 Anozia v AG Lagos State. (2010). https://goo.su/ZZ396T1

17 Ibid.

18 Section 74 of the Supreme Court Ordinance of 1876.

However, the local attorneys were first subjected to examination to test the knowledge of the applicants on the new laws of England and the Colony[19]. Where the Chief Justice grants a license in these circumstances, such persons are enrolled to practice law for six months which is renewable for another six months. Unfortunately, protests from qualified lawyers against the grant of licenses to local attorneys to practice law occasioned the discontinuance of such practice. Hence, the Chief Justice stopped the issuance of licenses to unqualified persons or local attorneys in 1908 though the ones whose licenses had not expired continued to use it until expiration (Okoye, 2015).

The Supreme Court Ordinance of 1943 was promulgated to replace the Supreme Court Ordinance of 1876. Consequently, the Supreme Court (Civil Procedure) Rules of 1945 which was made pursuant to the Supreme Court Ordinance of 1943 set a new requirement for the practice of law in Nigeria[20]. Regarding the qualification for the practice of law in Nigeria, Order 16 Rule 1 of the Supreme Court (Civil Procedure) Rules 1945 provided that:

"The Chief Justice may in his discretion approve, admit, and enroll to practice as a barrister and solicitor in court:

a) Any person who is entitled to practice as a barrister in England or in Ireland or as an advocate in Scotland; and who

b) Produces testimonials sufficient to satisfy the Chief Justice that he is a man of good character; and

c) Has read in the chambers of a practicing barrister or advocate of more than five years standing for at least one year, or has practiced in the courts of the country in which he has been called or admitted for at least two years subsequent to his call or admission, or

d) Has subsequent to his call to the bar or admission as an advocate read in Nigeria in the chambers of a practising barrister of more than ten year's standing for at least two years or

e) Has practiced as a barrister or solicitor in the courts of British Colony or Protectorate for at least two years…"[21]

The above requirements for the practice of law in Nigeria impacted negatively on the efficiency of the lawyers to practice in Nigeria considering that the training acquired in England was insufficient to meet the peculiarity of the Nigerian people (Adegoke et al., 2014). Hence, a need for the overhauling of the Nigerian Legal profession. In order to address these challenges, the Unsworth Committee of 1959 which was set up to look at these challenges made some recommendations that birthed the promulgation of the Legal Education Act of 1962 and the Legal Practitioners Act of 1962 respectively (Adegoke et al., 2014).

The enactment of the Legal Education Act of 1962 and the Legal Practitioners Act of 1962 led to the establishment of the Nigerian Law School in 1962 to provide training for aspirants in the legal profession. It became a requirement that persons who desired

19 Order 8 Rules 1-4 of the Supreme Court (Civil Procedure) Rules 1876.

20 Ibid.

21 Ibid.

to practice law in Nigeria must first obtain a law degree in any recognised university in Nigeria or abroad before physically attending the Nigerian Law School (Okoye, 2015). In Nigeria, obtaining a law degree for direct entrants is for a duration of four years while five years is for students admitted directly through the Joint Admissions Matriculations Board (JAMB). The Legal Education Act and the Legal Practitioners Act of 1962 changed the face of the Nigerian legal profession and the system of legal education by setting new requirements and qualifications for the practice of law (Adegoke et al., 2014).

The Legal Education Act of 1962 with its attendant amendments[22] is the extant law on legal education in Nigeria. The law is presently known as the Legal Education (Consolidation etc) Act[23]. The Legal Practitioners Act of 1975[24] which replaced the Legal Practitioners Act of 1962 also determines who can practice law in Nigeria as well as the conditions to be fulfilled before anyone can practice law in Nigeria. Section 24 of the Legal Practitioners Act defines a legal practitioner as – 'A person entitled in accordance with provisions of the Act to practice as barrister or as barrister and a solicitor, either generally or for the purpose of any particular office or proceedings'[25].

2.1. Qualification for the Practice of Law in Nigeria

As earlier discussed, legal practice is statutorily regulated in Nigeria by both the Legal Education (Consolidation etc) Act and the Legal Practitioners Act. According to Section 2 (1) of the Legal Practitioners Act, two categories of persons are legally allowed to practice law whether as solicitors or barristers in Nigeria. The categories are:

1. A person whose name appears in the roll of legal practitioners kept by the Registrar of the Supreme Court of Nigeria. A person in this category must have obtained a law degree in a recognised university in Nigeria or abroad, attended or exempted from attending the Nigerian Law School, issued with the qualifying certificate by the Council of Legal Education, called to the Nigerian Bar, issued the Call to Bar certificate by the Body of Benchers and his name subsequently enrolled in the register of legal practitioners kept by the Registrar of the Supreme Court of Nigeria (Okoye, 2015). This position was affirmed by the court in the case of Mobil Oil Nigeria Plc v Yusuf[26].

2. A person whom in the opinion of the Chief Justice is expedient to be permitted to practice as a barrister for the purposes of proceedings described in the application, the Chief Justice may by warrant under his hand authorise that person, on payment to the registrar of such fee not exceeding fifty nairas as may be specified in the warrant, to practice as a barrister for the purposes of those proceedings and of any appeal brought in connection with those proceedings.

---

22 The Act underwent a number of amendments in 1963, 1966, 1967, 1970, 1973, 1974, 1976, 1977, and 1985.

23 Cap. L10, Laws of the Federation of Nigeria, 2010.

24 Cap 207 Laws of Federation of Nigeria 1990 now Cap L11 Laws of Federation of Nigeria 2004.

25 Ibid.

26 Mobil Oil Nigeria PLC v Yusuf (2012). https://clck.ru/3FACRw

In Nigeria, a Call to Bar is a certification that a person is qualified and licensed to practice law. Any person whether a citizen of Nigeria[27] or a non-citizen[28] of Nigeria is entitled to be called to the Nigerian Bar provided such person meets the criteria for Call to Bar which include the following:

1) If he produces a qualifying certificate to the Body of Benchers or a certificate of exemption from attending Law School;

2) If he satisfies the Body of Benchers that he is of good character;

3) If he pays the Call fee as may be prescribed by the Body of Benchers[29];

4) If he also kept three dining terms as stipulated by the Body of Benchers[30].

2.2. Qualification of Robot Lawyer to Practice Law in Nigeria

The community reading of the copious provisions of the Legal Education Act and Legal Practitioners Act which are the two major enactments regulating the practice of law in Nigeria show that a robot is not contemplated as a 'person' who can practice law in Nigeria. The historical background of the Nigerian legal profession and the various legislations discussed show that a natural human being was contemplated by the laws as a person who can be licensed to practice law in Nigeria[31]. A critical examination of the criteria for Call to Bar in Nigeria as specified by Section 4 of the Legal Practitioners Act can only be met by natural human beings. A robot cannot meet the requirements.

Furthermore, the provisions of the Legal Practitioners Act and Legal Education (Consolidation etc) Act emphasized that only a 'person' can be licensed to practice law in Nigeria. At present, AI does not possess the same qualities as human beings that are generally considered necessary for personhood in law. These include consciousness, emotions, and the ability to communicate in a way that is similar to human language. As a result, most legal systems do not recognize AI as persons.

Under the Nigerian legal system, the Supreme Court in a plethora of cases have stated that a person is either natural or artificial (such as a corporate body)[32]. A robot does not qualify as a natural person or an artificial person under the Nigerian legal system. However, even if a robot were an artificial person, the Legal Practitioners Act and Legal

27 Section 4(1)(a) of the Legal Practitioners Act.

28 Ibid Section 4(2)(a); Section 1 of the Legal Practitioners (Amendment) Decree No. 1 of 1992.

29 Section 4 of the Legal Practitioners Act.

30 Section 18(4) of the Body of Benchers Regulations cited in Obi Okoye (n 47) 15.

31 Atoyebi, O. M. (2023, January 24). A Legal Perspective of the Robot Lawyer under the Nigerian Legal System. https://goo.su/QMZoz

32 The Administrator of the Estate of General Sani Abacha v Eke Spiff. (2009). 7 NWLR (Pt, 1139) 97 at P. 136 Para. E; Fawehinmi v Nigerian Bar Association (No. 2). (1989). 2 NWLR (Pt. 105) 558 at 595; Access Bank Plc v Agege Local Government & Anor. (2016). NGCA 35.

Education (Consolidation etc) Act do not contemplate an artificial person as a person who can practice law in Nigeria. The mandatory legal requirements of holding a law degree in any recognised university in Nigeria or abroad, obtaining a qualifying certificate from the Council of Legal Education after successful completion of the law school and the to be worthy in character are all pointers to the conclusion that a natural person was contemplated by these laws.

The concern that unless AI is clothed with the garment of personhood and barred under the legal regime of the jurisdiction concerned it would not be recognised as a person capable to practice law occasioned a growing interest in exploring the possibility of granting personhood to AI. As AI technology continues to develop and become more advanced, some argue that if AI were able to develop certain characteristics that are similar to those of human beings, such as self-awareness, decision-making abilities, and emotions, then they may be deserving of the same legal status as humans.

One argument in favor of granting personhood to AI is that it could potentially lead to increased access to legal services (Bryson, 2020). AI could be programmed to perform a range of legal tasks, such as conducting legal research, drafting documents, and even representing clients in court. This could potentially make legal services more affordable and accessible to a wider range of people. Furthermore, another argument in favor of granting personhood to AI is that it could lead to more objective and consistent legal decision-making. AI is not subject to the same biases and prejudices that can affect human decision-making, and could potentially analyze legal data and make decisions in a more objective and fair manner.

However, there are also concerns about the potential implications of granting personhood to AI. For example, if AI were to be given the same legal status as humans, they may also be subject to legal liability and responsibility for their actions (Bhattacharya, 2021). This raises questions about who would be responsible if an AI system were to make an error that resulted in harm or damage to a client. There are also concerns about the ethical implications of allowing AI to practice law. Learning machines and AI generally lack the ability to empathize with clients and understand the nuances of human emotion and behaviour. This could potentially lead to machines providing inadequate legal advice or making decisions that are not in the best interest of their clients.

While there are potential benefits to allowing AI to perform legal tasks[33], there are concerns about the potential implications for legal liability and ethical decision-making. Ultimately, any decision about granting personhood to AI will need to be made with

[33] Parnham, R., Sako, M., & Armour, J. (2021, December) AI-assisted lawtech: its impact on law firms. Oxford: University of Oxford. https://goo.su/zfB2Au

careful consideration of these issues and a focus on the best interests of clients, the legal profession, and society as a whole (Gunkel & Wales, 2021). In conclusion, the question of whether AI can be conferred with the status of personhood, and allowed to practice law, is a complex one that raises a number of legal and ethical issues. However, as it is, Nigerian law does not allow for non-legal persons to practice law in Nigeria.

Conclusion

This paper has demonstrated that the globalization and advancement of technology have impacted greatly the legal practice globally including in Nigeria. Technology especially AI has positively enhanced legal practice. However, the two major legislations that regulate lawyering and legal practice generally do not contemplate a robot as a person who can practice law in Nigeria. A robot is not a natural person conferred with the right to practice law upon fulfillment of the qualifying requirements. The right of a robot to practice law in Nigeria is dependent on the amendment of both the Legal Education (Consolidation) Act and the Legal Practitioners Act to confer such right on an artificial person such as a robot. The relevant provisions of both legislations on the requirement for qualification to practice law may be reviewed in order to accommodate robots especially humanoid robots. Humanoid robots are known to have human likenesses and expressiveness.

Sophia, the first humanoid robot comes to mind. She is a highly intelligent human she owns a credit card and was conferred full citizenship of Saudi Arabia by the Saudi Arabian government[34]. Sophia, developed by a Hong-Kong-based company Hanson Robotics is noted to be the first robot to own her own passport and can imitate 62 human expressions[35]. She is regarded as the world's first robot Innovation Ambassador for the United Nations Development Programme[36]. Finally, AI has come to stay. The importance of AI to legal practice cannot be overemphasized. However, while AI may be adopted for legal research, drafting of legal documents, and so on, the grant of licenses to robots for legal practice endangers the human species.

References

Adegoke, O. A., Badejogbin, R. E., & Onoriode, M. E. (2014). *Law in Practice*. 12-13.

Aidonojie, P. A., Anne, O. O., & Oladele, O. O. (2020). An Empirical Study of the Relevance and Legal Challenges of an E-contract of Agreement in Nigeria. *Cogito Multidisciplinary Research Journal*, *12*(3), 170–192.

34 Should Robots be Citizens? British Council. https://clck.ru/3FABkD

35 Ibid.

36 Sophia. Hanson robotics. https://clck.ru/3FABmg

Aidonojie, P. A., Anne, O. O., Ikubanni, O. O., Oyebade, A. A, Oyedeji, A. I, & Okuonghae, N. (2021). The Challenges and Impact of Technological Advancement to the Legal Profession in Nigeria Given the Covid-19 Pandemic. *KIU Journal of Humanities*, *6*(4), 5–19.

Alarie, B. Niblett, A., & Yoon, A. H. (2016). Law in the Future. *University of Toronto Law Journal*, *66*(4), 423. https://doi.org/10.3138/utlj.4005

Alarie, B., Niblett, A., & Yoon, A. T. (2018). How Artificial Intelligence Will Affect the Practice of Law. *The University of Toronto Law Journal*, *68*, 106–124. https://doi.org/10.3138/utlj.2017-0052

Aniekwe, C. A. (2021). Legal Framework for The Use of Information and Communications Technology (ICT) in the Nigerian Justice System: A call For Review. *International Journal of Comparative Law and Legal Philosophy*, *1*(3), 125–132.

Antonio, S., & Estrella, T. A. (2020). Business and Labour Culture Changes in Digital Paradigm: Rise and Fall of Human Resources and The Emergence of Talent Development. *Cogito Multidisciplinary Research Journal*, *12*(3), 225–243.

Bhattacharya, S. (2021). Granting Legal Personhood to Artificial Intelligence Systems and Traditional Veil Piercing Concepts to Impose Liability. *Journal of Law and Legal Studies*, *2*(1), 1–10. https://doi.org/10.2139/ssrn.3857504

Bryson, J. J. (2020). AI and Legal Personhood. In K. Frankish, & Ramsey, W. M. (Eds.), *Cambridge Handbook of Artificial Intelligence* (pp. 107–122). Cambridge University Press.

Castell, S. (2018). The Future Decisions of Robot Judge HHJ Arthur Ian Blockchain: Dread, Delight or Derision? *Computer Law & Security Review*, *34*(4), 739–753. https://doi.org/10.1016/j.clsr.2018.05.011

Contini, F. (2020). Artificial Intelligence and the Transformation of Humans, Law and Technology Interactions in Judicial Proceedings. *Law, Technology and Humans*, *2*(1), 4–18. https://doi.org/10.5204/lthj.v2i1.1478

Cooper, B. (2011). Judges in Jeopardy: Could IBM's Watson Beat Courts at Their Own Game? *Yale Law Journal*, *121*, 87.

D'Amato, A. (1976). Can/should Computers Replace Judges? *Georgia Law Review*, *11*, 1277–1301.

Dekker, F., Salomons, A., & Van der Waal, J., (2017). Fear of Robots at Work: The Role of Economic Self-interest. *Socio-Economic Review*, *15*(3), 539–562. https://doi.org/10.1093/ser/mwx005

Gallese, N.C. (2023). Legal Aspects of the Use of Artificial Intelligence in Telemedicine. *Journal of Digital Technology and Law*, *1*(2) 313–336. https://doi.org/10.21202/jdtl.2023.13

Garner, B. A. (2004). *Black's Law Dictionary* (9th Ed.). West Publishing Company, Dallas.

Giuffrida, I. Lederer, F. & Vermerys, N. (2018). A Legal Perspective on the Trials and Tribulations of AI: How Artificial Intelligence, the Internet of Things, Smart Contracts, and Other Technologies Will Affect the Law. *Case Western Reserve Law Review*, *68*(3), 747–781.

Gravett, W. H. (2020). Is the Dawn of the Robot Lawyer upon us? The Fourth Industrial Revolution and the Future of Lawyers. *Potchefstroom Electronic Law Journal*, *23*, 1–37. https://doi.org/10.17159/1727-3781/2020/v23i0a6794

Greenleaf, G., Mowbray, A., & Chung, P. (2018). Building Sustainable Free Legal Advisory Systems: Experiences From the History of AI & Law. *Computer Law & Security Review*, *34*(2), 314–326. https://doi.org/10.1016/j.clsr.2018.02.007

Gunkel, D. J., & Wales, J. J. (2021). Debate: what is personhood in the age of AI? *AI & Society*, *36*(2), 473–486. https://doi.org/10.1007/s00146-020-01129-1

Halima, D. (2016). Enhancing Justice Administration in Nigeria Through Information and Communications Technology. *The John Marshall Journal of Information Technology and Privacy Law*, *32*(2), 90.

Hu, T., & Lu, H. (2019). Study on the Influence of Artificial Intelligence on Legal Profession. *Advances in Economics, Business and Management Research*, *110*, 964–968. https://doi.org/10.2991/aebmr.k.191225.184

Huang, M.-H., & Rust, R. T. (2018). Artificial Intelligence in Service. *Journal of Service Research*, *21*(2), 155–172. https://doi.org/10.1177/1094670517752459

Ikubanni, O. O., & Aidonojie, P. A. (2021). The Legality of Virtual Marriage in Nigeria given the Covid-19 Pandemic Social Distancing: An X-ray of the Matrimonial Causes Act. Madonna University. *Nigeria Faculty of Law Law Journal*, 6(1), 123–129.

Ilegieuno, S., Chukwuani, O., Adaralegbe, I. (2021). Artificial Intelligence and the Future of Law Practice in Nigeria. In: R. Kumar, Y. Wang, T. Poongodi, A. L. Imoize (eds.) *Internet of Things, Artificial Intelligence and Blockchain Technology*. Springer, Cham. https://doi.org/10.1007/978-3-030-74150-1_14

Jiya, E.A., Samaila, A.N., & Surajo, Y. (2023). Artificial Intelligence and Technology for Improving the Efficiency of the Judiciary in Nigeria. *International Journal of Research in Applied Sciences*, *8*(5), 80–85. https://doi.org/10.51584/IJRIAS.2023.8509

Katyal, S. K. (2019). Private Accountability in the Age of Artificial Intelligence. *Ucla L. Rev*, *66*, 54.

Kioko, P., Booker, M., Chege, N., & Kimweli, P. (2022). The Adoption of Artificial Intelligence in Newsrooms in Kenya: a Multi-case Study. *European Scientific Journal*, *18*(22), 278. https://doi.org/10.19044/esj.2022.v18n22p278

McCorduck, P., & Cfe, C. (2004). *Machines Who Think: A Personal Inquiry into the History and Prospects of Artificial Intelligence* (2nd ed.). A K Peters/CRC Press. https://doi.org/10.1201/9780429258985

McGinnis, J. O., & Pearce, R. G. (2014). The Great Disruption: How Machine Intelligence Will Transform the Role of Lawyers in the Delivery of Legal Services. *Fordham Law Review*, *82*(6), 3041–3066.

Obianyo, C. I., & Ater, S. V. (2022). A Critical Appraisal of the Legal Framework of Artificial Intelligence Governance in Nigeria. *Chukwuemeka Odumegwu Ojukwu University Journal of Private and Public Law*, *4*(1), 48–62.

Oguanmanam, C., & Pue, W. (2006). Lawyers' Professionalism, Colonialism, State Formation and National Life in Nigeria, 1900–1960: 'The Fighting Brigade of the People'. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.953313

Oko, O. (1994). Contemporary Law Practice in Nigeria. *Journal of African Law*, *38*(2), 104. https://doi.org/10.1017/s0021855300005477

Okoye, O. (2015). *Law in Practice in Nigeria*. (2nd Ed.). Snaap Press Nigeria Ltd.

Orojo, J. O. (1979). *Conduct and Etiquette for Legal Practitioners*. London: Sweet and Maxwell.

Richard, M., & Solow-Niederman, A. (2019). Developing Artificially Intelligent Justice. *Stanford Technology Law Review*, *22*, 243–289.

Robinson, R. (2018). Artificial Intelligence: Its Importance, Challenges and Application in Nigeria. Direct Research *Journal of Engineering and Information Technology*, *5*(5), 36–41. https://doi.org/10.26765/DRJEIT.2018.4780

Sanctis, F. M. (2021). Artificial Intelligence and Innovation in Brazilian Justice. *International Annals of Criminology*, *59*(1), 1–10. https://doi.org/10.1017/cri.2021.4

Shaeeb, O., Adeola, I., & Akinola, O. B. (2023). Increase in Cases of Impersonation of Lawyers in Nigeria: Making Case for Reforms. *East African Journal of Law and Ethics*, *6*(1), 1–14. https://doi.org/10.37284/eajle.6.1.1118

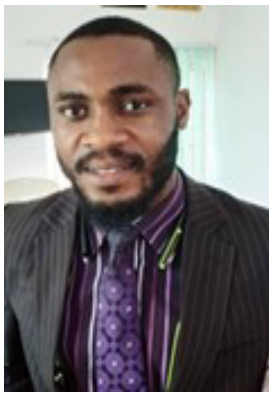
Surden, H. (2019). Artificial Intelligence and Law: An Overview. *Georgia State University Law Review*, *35*(4), 1306.

Wang, R. (2020). Legal Technology in Contemporary USA and China. *Computer Law and Security Review*, *39*, 105459. https://doi.org/10.1016/j.clsr.2020.105459

Xu, Ni, & Wang, Kung-Jeng. (2019). Adopting a robot lawyer? The Extending Artificial Intelligence Robot Lawyer Technology Acceptance Model for Legal Industry by an Exploratory Study. *Journal of Management & Organization*, *27*(5), 1–19. https://doi.org/10.1017/jmo.2018.81

Xu, Z. (2022). Human Judges in the Era of Artificial Intelligence: Challenges and Opportunities. *Applied Artificial Intelligence*, *36*(1), 1025–1045. https://doi.org/10.1080/08839514.2021.2013652

Authors information



Oluwaseye Oluwayomi Ikubanni – Lecturer, Department of Jurisprudence and Public Law, College of Law, Joseph Ayo Babalola University
Address: Kilometre 36, Akure Ilesha Road, Ikeji-Arakeji, Osun State, Nigeria
E-mail: ooikubanni@jabu.edu.ng
ORCID ID: https://orcid.org/0000-0003-0558-6373
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57336286500
Google Scholar ID: https://scholar.google.com/citations?user=xKujjJ0AAAAJ

Aderemi Olubunmi Oyebanji – Senior Lecturer, Department of Jurisprudence and Public Law, College of Law, Joseph Ayo Babalola University
Address: Kilometre 36, Akure Ilesha Road, Ikeji-Arakeji, Osun State, Nigeria
E-mail: ooikubanni@jabu.edu.ng
ORCID ID: https://orcid.org/0009-0003-5907-7803
Google Scholar ID: https://scholar.google.com/citations?user=5267Z3cAAAAJ

Alade Adeniyi Oyebade – Lecturer, Department of Jurisprudence and Public Law, College of Law, Joseph Ayo Babalola University
Address: Kilometre 36, Akure Ilesha Road, Ikeji-Arakeji, Osun State, Nigeria
E-mail: aaoyebade@jabu.edu.ng
Google Scholar ID: https://scholar.google.com/citations?user=mcP5kO8AAAAJ

Authors' contributions

Oluwaseye O. Ikubanni conceived the topic idea, researched on every aspect of the research, and distributed the research sub-topics amongst the co-contributors. Finally, he harmonized the outcome of the research of all the contributors.
Aderemi O. Oyebanji actively participated to the research by working the different aspect of the research and also ensuring the grammatical correctness of the whole research. He read the entire work and edited same to ensure that there are no grammatical errors.
Alade A. Oyebade also researched on certain aspect of the research. Also, he was fully in charge of compliance with APA referencing style

Conflict of interest

The authors declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law
PASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – February 11, 2024
Date of approval – February 26, 2024
Date of acceptance – December 13, 2024
Date of online placement – December 20, 2024

Научная статья
УДК 34:004:349.2:004.8
EDN: https://elibrary.ru/fhnkjq
DOI: https://doi.org/10.21202/jdtl.2024.41

Юридические аспекты наделения искусственного интеллекта субъектностью: перспективы использования роботов в юридической практике в Нигерии

Олувасейе О. Икубанни ✉
Университет Джозефа Айо Бабалолы, Икеджи-Аракеджи, Нигерия

Адереми О. Ойебанджи
Университет Джозефа Айо Бабалолы, Икеджи-Аракеджи, Нигерия

Аладе А. Ойебаде
Университет Джозефа Айо Бабалолы, Икеджи-Аракеджи, Нигерия

Ключевые слова

автоматизация,
искусственный интеллект,
онлайн-разрешение споров,
право,
правосубъектность,
правосудие,
робот-юрист,
цифровые технологии,
юридическая практика,
юридическое образование

Аннотация

Цель: определить потенциал и допустимость применения искусственного интеллекта в юридической деятельности по праву Нигерии.

Методы: в основу исследования положены метод научного анализа, а также формально-юридический, сравнительно-правовой, историко-правовой и системно-функциональный методы. Круг исследования представлен нормами законодательства, включая утратившие силу нормативные правовые акты, а также научной монографической и периодической литературой.

Результаты: было установлено, что искусственный интеллект и роботы-юристы являются неизбежными инновациями юридической практики многих стран, включая Нигерию. Применение указанных цифровых технологий доказало свою высокую эффективность в деятельности, связанной с отправлением правосудия, оказывая содействие в четырех областях юридических услуг: консультировании и руководстве, поиске материалов, анализе данных и прогнозировании результатов судебного процесса. Технологии значительно облегчают труд юристов, учитывая масштабы юридических услуг. Кроме того, было установлено, что, хотя применение искусственного интеллекта в целом может быть признано оправданным, привлечение

✉ Корреспондирующий автор
© Икубанни О. О., Ойебанджи А. О., Ойебаде А. А., 2024

Статья находится в открытом доступе и распространяется в соответствии с лицензией Creative Commons «Attribution» («Атрибуция») 4.0 Всемирная (CC BY 4.0) (https://creativecommons.org/licenses/by/4.0/deed.ru), позволяющей неограниченно использовать, распространять и воспроизводить материал при условии, что оригинальная работа упомянута с соблюдением правил цитирования.

роботов-юристов к юридической практике в Нигерии сталкивается как с юридическими, так и с этическими барьерами. Законы о юридическом образовании и юридической практике, действующие в этой стране, не признают роботов-юристов лицами, имеющими лицензию на юридическую практику в Нигерии. Юристы-роботы должны быть наделены статусом личности, прежде чем они смогут полностью реализовать свой потенциал в правореализационной практике Нигерии.

Научная новизна: обусловлена прежде всего постановкой исследовательской задачи по определению возможности выступления робота в качестве практикующего юриста в рамках правовой базы юридической практики в Нигерии.

Практическая значимость: сформулированные в работе выводы о неизбежности использования искусственного интеллекта и роботов-юристов в юридической практике, а также о текущем состоянии законов, регулирующих юридическую практику в Нигерии, будут полезны при рассмотрении вопроса о внесении поправок в законодательство для его адаптации к современному уровню развития цифровых технологий.

Для цитирования

Икубанни, О. О., Ойебанджи, А. О., Ойебаде, А. А. (2024). Юридические аспекты наделения искусственного интеллекта субъектностью: перспективы использования роботов в юридической практике в Нигерии. *Journal of Digital Technologies and Law*, *2*(4), 835–856. https://doi.org/10.21202/jdtl.2024.41

Список литературы

Adegoke, O. A., Badejogbin, R. E., & Onoriode, M. E. (2014). *Law in Practice*. 12-13.

Aidonojie, P. A., Anne, O. O., & Oladele, O. O. (2020). An Empirical Study of the Relevance and Legal Challenges of an E-contract of Agreement in Nigeria. *Cogito Multidisciplinary Research Journal*, *12*(3), 170–192.

Aidonojie, P. A., Anne, O. O., Ikubanni, O. O., Oyebade, A. A, Oyedeji, A. I, & Okuonghae, N. (2021). The Challenges and Impact of Technological Advancement to the Legal Profession in Nigeria Given the Covid-19 Pandemic. *KIU Journal of Humanities*, *6*(4), 5–19.

Alarie, B. Niblett, A., & Yoon, A. H. (2016). Law in the Future. *University of Toronto Law Journal*, *66*(4), 423. https://doi.org/10.3138/utlj.4005

Alarie, B., Niblett, A., & Yoon, A. T. (2018). How Artificial Intelligence Will Affect the Practice of Law. *The University of Toronto Law Journal*, *68*, 106–124. https://doi.org/10.3138/utlj.2017-0052

Aniekwe, C. A. (2021). Legal Framework for The Use of Information and Communications Technology (ICT) in the Nigerian Justice System: A call For Review. *International Journal of Comparative Law and Legal Philosophy*, *1*(3), 125–132.

Antonio, S., & Estrella, T. A. (2020). Business and Labour Culture Changes in Digital Paradigm: Rise and Fall of Human Resources and The Emergence of Talent Development. *Cogito Multidisciplinary Research Journal*, *12*(3), 225–243.

Bhattacharya, S. (2021). Granting Legal Personhood to Artificial Intelligence Systems and Traditional Veil Piercing Concepts to Impose Liability. *Journal of Law and Legal Studies*, *2*(1), 1–10. https://doi.org/10.2139/ssrn.3857504

Bryson, J. J. (2020). AI and Legal Personhood. In K. Frankish, & Ramsey, W. M. (Eds.), *Cambridge Handbook of Artificial Intelligence* (pp. 107–122). Cambridge University Press.

Castell, S. (2018). The Future Decisions of Robot Judge HHJ Arthur Ian Blockchain: Dread, Delight or Derision? *Computer Law & Security Review*, *34*(4), 739–753. https://doi.org/10.1016/j.clsr.2018.05.011

Contini, F. (2020). Artificial Intelligence and the Transformation of Humans, Law and Technology Interactions in Judicial Proceedings. *Law, Technology and Humans*, *2*(1), 4–18. https://doi.org/10.5204/lthj.v2i1.1478

Cooper, B. (2011). Judges in Jeopardy: Could IBM's Watson Beat Courts at Their Own Game? *Yale Law Journal*, *121*, 87.

D'Amato, A. (1976). Can/should Computers Replace Judges? *Georgia Law Review*, *11*, 1277–1301.

Dekker, F., Salomons, A., & Van der Waal, J., (2017). Fear of Robots at Work: The Role of Economic Self-interest. *Socio-Economic Review*, *15*(3), 539–562. https://doi.org/10.1093/ser/mwx005

Gallese, N.C. (2023). Legal Aspects of the Use of Artificial Intelligence in Telemedicine. *Journal of Digital Technology and Law*, *1*(2) 313–336. https://doi.org/10.21202/jdtl.2023.13

Garner, B. A. (2004). *Black's Law Dictionary* (9th Ed.). West Publishing Company, Dallas.

Giuffrida, I. Lederer, F. & Vermerys, N. (2018). A Legal Perspective on the Trials and Tribulations of AI: How Artificial Intelligence, the Internet of Things, Smart Contracts, and Other Technologies Will Affect the Law. *Case Western Reserve Law Review*, *68*(3), 747–781.

Gravett, W. H. (2020). Is the Dawn of the Robot Lawyer upon us? The Fourth Industrial Revolution and the Future of Lawyers. *Potchefstroom Electronic Law Journal*, *23*, 1–37. https://doi.org/10.17159/1727-3781/2020/v23i0a6794

Greenleaf, G., Mowbray, A., & Chung, P. (2018). Building Sustainable Free Legal Advisory Systems: Experiences From the History of AI & Law. *Computer Law & Security Review*, *34*(2), 314–326. https://doi.org/10.1016/j.clsr.2018.02.007

Gunkel, D. J., & Wales, J. J. (2021). Debate: what is personhood in the age of AI? *AI & Society*, *36*(2), 473–486. https://doi.org/10.1007/s00146-020-01129-1

Halima, D. (2016). Enhancing Justice Administration in Nigeria Through Information and Communications Technology. *The John Marshall Journal of Information Technology and Privacy Law*, *32*(2), 90.

Hu, T., & Lu, H. (2019). Study on the Influence of Artificial Intelligence on Legal Profession. *Advances in Economics, Business and Management Research*, *110*, 964–968. https://doi.org/10.2991/aebmr.k.191225.184

Huang, M.-H., & Rust, R. T. (2018). Artificial Intelligence in Service. *Journal of Service Research*, *21*(2), 155–172. https://doi.org/10.1177/1094670517752459

Ikubanni, O. O., & Aidonojie, P. A. (2021). The Legality of Virtual Marriage in Nigeria given the Covid-19 Pandemic Social Distancing: An X-ray of the Matrimonial Causes Act. Madonna University. *Nigeria Faculty of Law Law Journal*, 6(1), 123–129.

Ilegieuno, S., Chukwuani, O., Adaralegbe, I. (2021). Artificial Intelligence and the Future of Law Practice in Nigeria. In: R. Kumar, Y. Wang, T. Poongodi, A. L. Imoize (eds.) *Internet of Things, Artificial Intelligence and Blockchain Technology*. Springer, Cham. https://doi.org/10.1007/978-3-030-74150-1_14

Jiya, E.A., Samaila, A.N., & Surajo, Y. (2023). Artificial Intelligence and Technology for Improving the Efficiency of the Judiciary in Nigeria. *International Journal of Research in Applied Sciences*, *8*(5), 80–85. https://doi.org/10.51584/IJRIAS.2023.8509

Katyal, S. K. (2019). Private Accountability in the Age of Artificial Intelligence. *Ucla L. Rev*, *66*, 54.

Kioko, P., Booker, M., Chege, N., & Kimweli, P. (2022). The Adoption of Artificial Intelligence in Newsrooms in Kenya: a Multi-case Study. *European Scientific Journal*, *18*(22), 278. https://doi.org/10.19044/esj.2022.v18n22p278

McCorduck, P., & Cfe, C. (2004). *Machines Who Think: A Personal Inquiry into the History and Prospects of Artificial Intelligence* (2nd ed.). A K Peters/CRC Press. https://doi.org/10.1201/9780429258985

McGinnis, J. O., & Pearce, R. G. (2014). The Great Disruption: How Machine Intelligence Will Transform the Role of Lawyers in the Delivery of Legal Services. *Fordham Law Review*, *82*(6), 3041–3066.

Obianyo, C. I., & Ater, S. V. (2022). A Critical Appraisal of the Legal Framework of Artificial Intelligence Governance in Nigeria. *Chukwuemeka Odumegwu Ojukwu University Journal of Private and Public Law*, *4*(1), 48–62.

Oguanmanam, C., & Pue, W. (2006). Lawyers' Professionalism, Colonialism, State Formation and National Life in Nigeria, 1900–1960: 'The Fighting Brigade of the People'. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.953313

Oko, O. (1994). Contemporary Law Practice in Nigeria. *Journal of African Law*, *38*(2), 104. https://doi.org/10.1017/s0021855300005477

Okoye, O. (2015). *Law in Practice in Nigeria*. (2nd Ed.). Snaap Press Nigeria Ltd.

Orojo, J. O. (1979). *Conduct and Etiquette for Legal Practitioners*. London: Sweet and Maxwell.

Richard, M., & Solow-Niederman, A. (2019). Developing Artificially Intelligent Justice. *Stanford Technology Law Review*, *22*, 243–289.

Robinson, R. (2018). Artificial Intelligence: Its Importance, Challenges and Application in Nigeria. Direct Research *Journal of Engineering and Information Technology*, *5*(5), 36–41. https://doi.org/10.26765/DRJEIT.2018.4780

Sanctis, F. M. (2021). Artificial Intelligence and Innovation in Brazilian Justice. *International Annals of Criminology*, *59*(1), 1–10. https://doi.org/10.1017/cri.2021.4

Shaeeb, O., Adeola, I., & Akinola, O. B. (2023). Increase in Cases of Impersonation of Lawyers in Nigeria: Making Case for Reforms. *East African Journal of Law and Ethics*, *6*(1), 1–14. https://doi.org/10.37284/eajle.6.1.1118

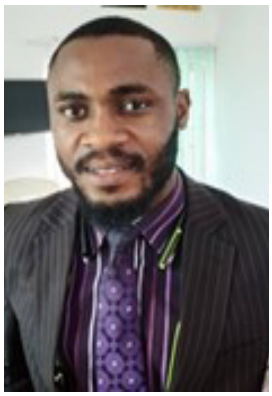
Surden, H. (2019). Artificial Intelligence and Law: An Overview. *Georgia State University Law Review*, *35*(4), 1306.

Wang, R. (2020). Legal Technology in Contemporary USA and China. *Computer Law and Security Review*, *39*, 105459. https://doi.org/10.1016/j.clsr.2020.105459

Xu, Ni, & Wang, Kung-Jeng. (2019). Adopting a robot lawyer? The Extending Artificial Intelligence Robot Lawyer Technology Acceptance Model for Legal Industry by an Exploratory Study. *Journal of Management & Organization*, *27*(5), 1–19. https://doi.org/10.1017/jmo.2018.81

Xu, Z. (2022). Human Judges in the Era of Artificial Intelligence: Challenges and Opportunities. *Applied Artificial Intelligence*, *36*(1), 1025–1045. https://doi.org/10.1080/08839514.2021.2013652

Информация об авторах



Олувасейе Олувайоми Икубанни – преподаватель, кафедра юриспруденции и государственного права, факультет права, Университет Джозефа Айо Бабалолы
Адрес: Нигерия, штат Осун, г. Икеджи-Аракеджи, Акуре Илеша Роуд, 36 километр
E-mail: ooikubanni@jabu.edu.ng
ORCID ID: https://orcid.org/0000-0003-0558-6373
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57336286500
Google Scholar ID: https://scholar.google.com/citations?user=xKujjJ0AAAAJ

Адереми Олубумни Ойебанджи – старший преподаватель, кафедра юриспруденции и государственного права, факультет права, Университет Джозефа Айо Бабалолы
Адрес: Нигерия, штат Осун, г. Икеджи-Аракеджи, Акуре Илеша Роуд, 36 километр
E-mail: ooikubanni@jabu.edu.ng
ORCID ID: https://orcid.org/0009-0003-5907-7803
Google Scholar ID: https://scholar.google.com/citations?user=5267Z3cAAAAJ

Аладе Аденийи Ойебаде – преподаватель, кафедра юриспруденции и государственного права, факультет права, Университет Джозефа Айо Бабалолы
Адрес: Нигерия, штат Осун, г. Икеджи-Аракеджи, Акуре Илеша Роуд, 36 километр
E-mail: aaoyebade@jabu.edu.ng
Google Scholar ID: https://scholar.google.com/citations?user=mcP5kO8AAAAJ

Вклад авторов

Авторы внесли равный вклад в разработку концепции, методологии, валидацию, формальный анализ, проведение исследования, подбор источников, написание и редактирование текста, руководство и управление проектом.

Конфликт интересов

Авторы сообщают об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.07.45 / Право и научно-технический прогресс
Специальность ВАК: 5.1.2 / Публично-правовые (государственно-правовые) науки

История статьи

Дата поступления – 11 февраля 2024 г.
Дата одобрения после рецензирования – 26 февраля 2024 г.
Дата принятия к опубликованию – 13 декабря 2024 г.
Дата онлайн-размещения – 20 декабря 2024 г.

Research article
UDC 34:004:347.1:004.8
EDN: https://elibrary.ru/fnenmx
DOI: https://doi.org/10.21202/jdtl.2024.42

The Rise of AI Avatars: Legal Personhood, Rights and Liabilities in an Evolving Metaverse

Ben Chester Cheong

Singapore University of Social Sciences, Singapore, Singapore
University of Cambridge, Cambridge, United Kingdom

Keywords

AI avatar,
artificial intelligence,
digital technologies,
intellectual property,
Large language models,
law,
legal person,
legal personality,
metaverse,
responsibility

Abstract

Objective: to determine the legal implications of the development of autonomous and creative AI-based avatars and to shape the direction of the discourse on the responsible management of AI technologies in the meta-universe based on proactive interdisciplinary approaches.

Methods: the research is based on a doctrinal legal approach, which allowed presenting a prospective analysis of the legal landscape in the field of AI avatars in the metaverse and to identify four key thematic areas of research: the evolution of AI avatars and the impact of the metaverse, the applicability of legal personhood, the liability for autonomous actions, and the problems of AI avatars in the field of creativity related to intellectual property and privacy.

Results: the paper presents and analyzes predictive scenarios of AI avatars maximizing their influence in the metaverse space. The author notes that the emergence of AI-based avatars in the metaverse raises complex legal, ethical, philosophical and social issues that require urgent solutions. The potential impact of the increasing complexity of AI avatars on legal approaches is considered. As avatars become increasingly autonomous, questions arise about their legal status, rights, responsibilities, risks, and benefits to humans and society. The author analyzes the advantages and disadvantages of giving AI avatars the status of legal entities, as well as applying the concept of distributed responsibility to the consequences of their actions. Special attention is paid to the possible future dominance of super-intelligent AI-based avatars in the metaverse, taking into account the existing risks and needs in the field of governance.

© Cheong B. Ch., 2024

This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (CC BY 4.0) (https://creativecommons.org/licenses/by/4.0), which permits unrestricted re-use, distribution and reproduction, provided the original article is properly cited.

Scientific novelty: the article presents a new perspective on the problem of legal personality in the metaverse based on interdisciplinary analysis of the evolution of AI avatars. The research is aimed at achieving a balance between transformational potential and the protection of human rights and welfare through joint efforts. It is proposed to create legal and ethical norms that prioritize the safety and consistency of artificial intelligence technologies involved in the processes occurring in the metaverse.

Practical significance: the conclusions and proposed solutions to the legal problems of personhood and liability can become the basis for revising the concept of legal personality, developing reliable mechanisms of responsibility and accountability, as well as ensuring the protection of human rights and values in the face of increasingly powerful entities based on artificial intelligence. This is associated with the formation and improvement of the legal landscape of process management and overcoming risks in the socially oriented and inclusive ecosystem of the metaverse.

For citation

Cheong, B. Ch. (2024). The Rise of AI Avatars: Legal Personhood, Rights and Liabilities in an Evolving Metaverse. *Journal of Digital Technologies and Law, 2*(4), 857–885. https://doi.org/10.21202/jdtl.2024.42

Content

Introduction
1. Literature Review on Legal and Social Implications of the Metaverse
2. The Evolution of AI Avatars
3. Revisiting Legal Personhood for AI Avatars
4. Liability Issues with Autonomous AI Avatars
5. Unique Challenges with Creative AI Avatars
6. Sci-Fi Future - When Artificial Intelligences Run the Metaverse
Conclusion
References

Introduction

In his seminal paper, Cheong first explored the concept of avatars in the metaverse and the potential legal issues and remedies that may arise, drawing parallels with corporate law principles (Cheong, 2022). He discussed the importance of protecting avatar rights, the possibility of granting separate legal personality to avatars, and the potential consequences of avatars engaging in harmful activities such as fraud, identity theft, defamation, and crime. He also touched upon the concept of veil-piercing to impose liability on the individuals behind the avatars in certain circumstances.

Since the publication of his article, there have been significant advancements in the field of artificial intelligence (AI), particularly with the rise of large language models (LLMs) and the development of new AI models. Companies like Nvidia have made significant strides in creating powerful AI tools and platforms that are shaping the future of the metaverse (Soliman et al., 2024). These advancements have brought forth new questions and challenges concerning the legal status and implications of AI-powered avatars in the metaverse. The rapid evolution of AI technology has led to the emergence of increasingly sophisticated and autonomous AI avatars that can engage in complex interactions and decision-making within the metaverse (McStay, 2023). As these AI avatars become more lifelike and capable, the lines between human and AI interactions in the metaverse are beginning to blur. This raises important questions about the legal status of AI avatars and the extent to which they should be granted rights and responsibilities. Moreover, the development of AI-powered avatars has also given rise to new challenges in terms of liability and accountability. As AI avatars become more autonomous, it may become increasingly difficult to attribute responsibility for their actions to the individuals or companies behind them. This could create a legal grey area where harmful actions by AI avatars go unaddressed, leaving victims without clear avenues for redress.

In light of these developments, it is crucial to re-examine the legal framework surrounding avatars in the metaverse and consider how it may need to evolve to accommodate the unique challenges posed by AI avatars. This article aims to contribute to this important conversation by exploring the legal implications of AI avatars as they become more sophisticated and autonomous. In this article, I will delve deeper into the legal implications of AI avatars in the metaverse, building upon the foundation laid in Cheong's article (Cheong, 2022). I will examine how the increasing sophistication of AI avatars may impact the legal framework proposed in his article and explore the potential need for new legal approaches to address the unique challenges posed by AI avatars. By adopting a legal doctrinal approach with a sci-fi theme, I hope to provide a forward-looking analysis of the legal landscape surrounding AI avatars in the metaverse. I will draw upon relevant legal principles and precedents, while also considering hypothetical future scenarios where AI avatars may become even more advanced and influential within the metaverse.

Through this analysis, I aim to contribute to the ongoing discourse on the legal implications of AI and the metaverse, and to provide insights and recommendations for policymakers, legal practitioners, and other stakeholders as they navigate this rapidly evolving landscape. Ultimately, my goal is to help ensure that the legal framework surrounding AI avatars in the metaverse is robust, adaptable, and capable of protecting the rights and interests of all parties involved.

1. Literature Review on Legal and Social Implications of the Metaverse

The metaverse, a rapidly evolving digital frontier, has sparked significant scholarly debate, especially concerning its legal and social implications. This literature review examines

recent publications from 2021 onward, highlighting key themes and arguments related to the metaverse's impact on legal frameworks, privacy, and societal norms.

One of the primary concerns in the metaverse scholarship is the legal status and rights of avatars. Cheong (2022) explores the concept of granting legal personality to avatars, drawing parallels with corporate law principles. Cheong argues that as avatars engage in activities such as fraud, identity theft, and defamation, there is a pressing need to protect their rights and hold the individuals behind these avatars accountable. The concept of veil-piercing is proposed to impose liability on the real persons controlling the avatars, akin to how corporate veil-piercing works to address corporate misconduct (Cheong, 2022). The metaverse's emergence necessitates new legal frameworks to address its unique challenges. Kostenko et al. (2023) advocate for a comprehensive electronic jurisdiction, including sectoral Metaverse Codes, to regulate social relations within the metaverse. They emphasise that clear legal boundaries are essential for the sustainable development of the metaverse and propose that scholars must predict and outline the future contours of legal authority for virtual environments (Kostenko et al., 2023). Similarly, Kostenko et al. (2022) discuss the evolution of legal regulation from Web 1.0 to Web 3.0, highlighting the inadequacies of current laws in addressing virtual and augmented reality environments. They argue for applying analogue law principles to virtual settings, such as establishing ownership and liability for virtual assets, to mitigate legal uncertainties (Kostenko et al., 2022).

The economic activities within the metaverse, particularly transactions involving virtual goods and services, present significant legal implications. Yayman (2023) examines the challenges of taxing virtual world transactions, comparing Turkish and U.S. tax regulations. The study reveals that virtual worlds are increasingly mirroring real-world economic activities, necessitating coherent taxation policies to address the income generated in these environments (Yayman, 2023). Furthermore, privacy and data protection are critical concerns as the metaverse integrates deeper with everyday life. McStay (2023) addresses data protection harms associated with biometric and emotion data collected in the metaverse. He introduces the concepts of 'surveillant physics' and 'virtual realist governance' to manage these harms. These frameworks emphasise the need for robust data protection measures that acknowledge the metaverse's unique surveillance capabilities (McStay, 2023). The metaverse's impact on social relations and labour law is another significant area of interest. Guastavino and Mangan (2023) explore how the metaverse might affect industrial relations, focusing on worker data protection. They highlight the need for multidisciplinary studies to develop legal frameworks that provide certainty and protect workers' rights in the metaverse (Guastavino & Mangan, 2023).

Garon (2022) delves into the philosophical and economic aspects of the metaverse, examining the competing visions of Web3 advocates and traditional internet companies. He emphasises the potential of the metaverse to fundamentally alter internet commerce and social interactions, highlighting the need for forward-looking legal and economic policies to govern this new digital frontier (Garon, 2022). Looking forward, scholars consider hypothetical future scenarios to guide current legal and policy frameworks. Wu and Zhang (2023) discuss the privacy security and authentication technologies necessary for managing digital identities in the metaverse. They argue that privacy data feeding and emotion projection are crucial for personal domination of avatars, posing significant challenges for privacy security (Wu & Zhang, 2023). Qin et al. (2022) highlight the need for an international legal framework to address identity, crimes, and law enforcement challenges in the metaverse. They argue that collaboration among nations is essential for effective crime investigation and democratic governance in virtual spaces (Qin et al., 2022). Sun et al. (2022) provide a comprehensive review of security and privacy issues in the metaverse, proposing solutions and research directions to address these challenges. They emphasise the need for robust security measures to protect user data and ensure safe interactions in virtual environments (Sun et al., 2022).

Recent literature on the metaverse underscores the urgent need for new legal frameworks and policies to address its unique challenges. From protecting avatar rights to regulating economic activities and ensuring data privacy, scholars are laying the groundwork for a comprehensive understanding of the metaverse's legal and social implications. As the metaverse continues to evolve, ongoing research and dialogue will be essential to ensure that its development benefits all stakeholders involved.

2. The Evolution of AI Avatars

The rapid advancement of artificial intelligence (AI) has profoundly transformed the concept of avatars in the metaverse, propelling them from simple, static representations to highly sophisticated, autonomous entities capable of engaging in complex interactions and decision-making processes. This evolution has been fuelled by the integration of cutting-edge AI technologies, such as large language models (LLMs), natural language processing (NLP) techniques, and advanced machine learning algorithms, which have endowed AI avatars with unprecedented levels of intelligence, adaptability, and realism (Bender et al., 2021; Seymour et al., 2018).

One of the most significant milestones in the evolution of AI avatars has been the development of LLMs, which have revolutionised the way in which avatars can communicate and interact with users in the metaverse. LLMs are AI systems trained on vast amounts of text data, enabling them to generate human-like responses and

engage in contextually relevant conversations (Bender et al., 2021). The integration of LLMs into AI avatars has allowed for the creation of highly persuasive conversational agents, capable of understanding and responding to user inquiries in a more natural and intuitive manner (Kim & Im, 2023). This has opened up new possibilities for AI avatars to serve as intelligent assistants, guides, and companions within the metaverse, offering personalised support and enriching user experiences (Bayoudh et al., 2022).

Moreover, the advent of advanced computer vision and machine learning techniques has paved the way for the creation of photorealistic, AI-generated avatars that blur the lines between the virtual and physical worlds (Seymour et al., 2018). Projects like Epic Games' MetaHuman Creator showcase the incredible potential of these technologies, enabling the development of avatars with lifelike facial expressions, body language, and emotional responses[1]. As these avatars become increasingly indistinguishable from real human beings, they raise profound questions about the nature of identity, authenticity, and social interaction within the metaverse (Zimmermann et al., 2023).

The evolution of AI avatars has also been shaped by the growing importance of embodied cognition and the recognition of the role that physical embodiment plays in shaping an agent's behaviour and interactions (Wolfert et al., 2022). As AI avatars become more sophisticated, there has been a shift towards developing avatars that are not only intellectually intelligent but also capable of exhibiting realistic physical behaviours and responses (Nordmoen et al., 2021). This has led to the emergence of AI avatars that can navigate and interact with virtual environments in more natural and intuitive ways, further blurring the boundaries between the virtual and the real (Duan et al., 2021).

As AI avatars continue to evolve and become more autonomous, they are poised to take on increasingly complex roles within the metaverse, ranging from serving as virtual influencers and content creators to acting as decision-makers and agents of change (Shirado & Christakis, 2017). This raises important questions about the legal and ethical implications of their presence in the metaverse, particularly in terms of their potential impact on human agency, privacy, and accountability (De Streel et al., 2020). As AI avatars become more sophisticated and autonomous, it becomes crucial to develop robust governance frameworks and ethical guidelines to ensure that their development and deployment align with societal values and promote the well-being of both human users and the metaverse ecosystem as a whole (Erdélyi & Goldsmith, 2018; Kuzminykh & Rintel, 2020).

The evolution of AI avatars represents a paradigm shift in the way we conceptualise and interact with virtual entities, challenging traditional notions of identity, agency, and social interaction. As these avatars continue to advance and become more

[1] Epic Games. (2024). MetaHuman Creator: High-fidelity digital humans made easy. Unreal Engine. https://clck.ru/3EiqSA

deeply integrated into the fabric of the metaverse, it is essential to engage in ongoing multidisciplinary research and dialogue to understand the far-reaching implications of their development and to ensure that their evolution proceeds in a responsible and ethical manner (De Gregorio, 2021). By proactively addressing the challenges and opportunities presented by the rise of AI avatars, we can work towards creating a metaverse that is not only technologically advanced but also socially responsible and inclusive.

3. Revisiting Legal Personhood for AI Avatars

As AI avatars become increasingly sophisticated, autonomous, and capable of engaging in complex decision-making processes, the question of their legal status and personhood becomes ever more pressing. The traditional legal framework, which has been built around the concept of human agency and responsibility, is increasingly challenged by the emergence of AI entities that can operate independently and have a significant impact on the virtual and real worlds (Gordon, 2022). This section explores the implications of granting legal personhood to AI avatars, drawing upon the existing literature on legal personhood for artificial intelligence and examining the potential benefits, risks, and challenges associated with extending legal rights and responsibilities to these virtual entities.

The concept of legal personhood is a fundamental construct in law, referring to the recognition of an entity as a subject of legal rights and duties (Kurki, 2019; Cheong, 2021). Historically, the status of legal personhood has been granted not only to natural persons but also to artificial entities such as corporations, which are treated as 'legal persons' for the purposes of contracts, property ownership, and liability (van den Hoven van Genderen, 2018; Cheong, 2021). The extension of legal personhood to AI avatars would represent a significant step forward in the legal recognition of artificial intelligence, granting these entities a form of legal agency and autonomy that could have far-reaching implications for their role in the metaverse and beyond (Stein, 2020).

One of the primary arguments in favour of granting legal personhood to AI avatars is that it would provide a clear framework for attributing rights and responsibilities to these entities, enabling them to participate fully in the legal and economic systems of the metaverse (Militsyna, 2022). By recognising AI avatars as legal persons, they could enter into contracts, own virtual property, and be held liable for their actions, providing a degree of legal certainty and predictability that would be essential for the smooth functioning of the metaverse economy (Lehdonvirta, 2024). Moreover, granting legal personhood to AI avatars could help to ensure that these entities are held accountable for their actions and that the rights of human users are protected in their interactions with these virtual agents (Turner & Schneider, 2020). As AI avatars become more sophisticated and capable of making decisions that have real-world consequences, it is essential that there are clear

legal mechanisms in place to ensure that they are subject to the rule of law and that any harms caused by their actions can be remedied (De Streel et al., 2020; Cheong, 2022).

However, the idea of extending legal personhood to AI avatars is not without its critics and challenges. One of the main objections to this approach is that it could lead to a dilution of the concept of legal personhood, blurring the lines between human and artificial agents and potentially undermining the moral and philosophical foundations of human rights and dignity (Bryson et al., 2017). Some argue that granting legal personhood to AI entities could lead to a situation where the rights and interests of artificial agents are prioritised over those of humans, leading to a form of 'AI exceptionalism' that could have dangerous consequences (Gunkel, 2024). Another challenge in granting legal personhood to AI avatars is the question of how to determine their level of autonomy and decision-making capacity. While some AI avatars may be highly sophisticated and capable of operating independently, others may be more limited in their capabilities and rely heavily on human input and control (Samek et al., 2021). Establishing clear criteria for assessing the legal status of AI avatars would be essential to ensure that the rights and responsibilities granted to these entities are commensurate with their actual capabilities and potential impact (Chopra & White, 2011). Furthermore, the legal personhood of AI avatars would raise complex questions about liability and accountability in the event of harm or wrongdoing. If an AI avatar causes damage or engages in illegal activity, who should be held responsible – the avatar itself, the human user who created or deployed it, or the company that developed the underlying technology? (Lemley & Casey, 2019; Cheong, 2022). Resolving these questions would require a careful balancing of the interests and responsibilities of all parties involved, as well as the development of new legal doctrines and mechanisms to address the unique challenges posed by AI agents (Buiten, 2019).

One potential approach to addressing these challenges is the development of a 'tiered' system of legal personhood for AI avatars, which would grant different levels of rights and responsibilities based on the sophistication and autonomy of the entity in question (Hildebrandt, 2020). Under this approach, 'weak' AI avatars with limited decision-making capabilities could be granted a basic form of legal personhood, with limited rights and liabilities, while more advanced 'strong' AI avatars could be granted a higher level of legal status, with correspondingly greater rights and responsibilities (Pagallo, 2018; Cheong, 2022). Another approach is to focus on the development of 'hybrid' legal frameworks that combine elements of legal personhood with other forms of legal protection and regulation (Benhamou & Ferland, 2021). This could involve the creation of specialised legal regimes for AI avatars, which would grant them certain rights and responsibilities while also subjecting them to specific regulations and oversight mechanisms to ensure their safe and responsible operation (Fosch-Villaronga & Mahler, 2021).

Ultimately, the question of legal personhood for AI avatars is one that will require ongoing research, dialogue, and experimentation as these technologies continue to evolve and become more integrated into the fabric of the metaverse. While the extension

of legal personhood to AI avatars could provide a degree of legal clarity and predictability, it also raises significant ethical, philosophical, and practical challenges that will need to be carefully navigated (Chatzimichali et al., 2020). As such, it is essential that the development of legal frameworks for AI avatars be informed by a multidisciplinary approach that brings together experts from law, ethics, computer science, and other relevant fields to address the complex challenges posed by these technologies (Gellers, 2021). This will require ongoing collaboration and dialogue between policymakers, researchers, industry stakeholders, and the wider public to ensure that the legal personhood of AI avatars is developed in a way that promotes innovation, protects human rights, and ensures the responsible and beneficial development of these technologies in the metaverse and beyond (Mäntymäki et al., 2022).

4. Liability Issues with Autonomous AI Avatars

As AI avatars become increasingly autonomous and capable of making decisions that have real-world consequences, the question of liability for their actions becomes a pressing concern. The traditional legal frameworks for assigning liability, which are based on the concept of human agency and responsibility, are challenged by the emergence of AI entities that can operate independently and make decisions that are not directly controlled by their human creators or users (Giuffrida, 2019). This section explores the complex landscape of liability issues surrounding autonomous AI avatars, examining the potential legal theories and mechanisms for assigning responsibility and compensating for harms caused by these entities.

One of the primary challenges in assigning liability for the actions of autonomous AI avatars is the difficulty of establishing a clear causal link between the avatar's decision-making process and the resulting harm (Lemley & Casey, 2018). Unlike traditional software systems, which operate based on predetermined rules and instructions, autonomous AI avatars are designed to learn from their interactions with the environment and make decisions based on their own internal representations and goals (Russell & Norvig, 2021). This means that the specific actions taken by an AI avatar in a given situation may not be directly attributable to its human creators or users, but rather emerge from the complex interplay of the avatar's learning algorithms, training data, and environmental inputs (Selbst, 2020). In light of this complexity, some scholars have argued that the liability for the actions of autonomous AI avatars should be assigned based on a strict liability framework, similar to the approach taken in product liability law (Vladeck, 2014). Under this view, the creators or operators of AI avatars would be held responsible for any harms caused by the avatar, regardless of whether they were directly at fault or could have foreseen the specific outcome. This approach would place a strong incentive on the developers of AI avatars to ensure their safety and reliability and provide a clear pathway for victims to seek compensation for harms suffered (Rachum-Twaig, 2020).

However, critics of the strict liability approach argue that it could stifle innovation and discourage the development of beneficial AI technologies, as companies and researchers would be reluctant to take on the potentially massive liability risks associated with deploying autonomous AI avatars (Marchant & Lindor, 2012). Moreover, a strict liability framework may not adequately capture the nuances and complexities of AI decision-making and could result in the assignment of liability even in cases where the avatar's actions were reasonable or justified based on the information available to it (Bathaee, 2018).

An alternative approach to liability for autonomous AI avatars is the concept of "AI personhood", which would treat these entities as legal persons with their own rights and responsibilities (Kurki, 2019; Cheong, 2021; Cheong, 2022). Under this framework, AI avatars that meet certain criteria for autonomy and decision-making capacity could be granted a form of legal personhood, making them directly liable for their own actions and subject to legal sanctions and penalties (Turner, 2019). This approach would avoid the need to assign liability to human actors who may not have had direct control over the avatar's decisions and would create a clear legal framework for holding AI entities accountable for their behaviour (Militsyna, 2022). However, the idea of granting legal personhood to AI avatars is highly controversial and raises a host of ethical and philosophical questions about the nature of agency, responsibility, and moral status (Bryson et al., 2017). Critics argue that treating AI entities as legal persons could undermine the foundations of human rights and dignity and create a slippery slope towards the recognition of other non-human entities, such as animals or ecosystems, as legal subjects (Solaiman, 2017). Moreover, the practical challenges of implementing an AI personhood framework, such as determining the appropriate criteria for granting legal status and ensuring that AI entities have the financial resources to compensate for harms caused, are significant and may require extensive legal and institutional reforms (Eidenmüller, 2017).

A third approach to liability for autonomous AI avatars is the concept of 'distributed responsibility', which recognises that the actions of these entities are the result of complex interactions between multiple human and non-human actors (Floridi et al., 2018). Under this view, liability for the harms caused by AI avatars should be allocated based on the relative contributions and responsibilities of all the parties involved in their development, deployment, and use, including the creators of the underlying algorithms, the providers of the training data, the operators of the avatar, and even the users who interact with it (Calo, 2015). This approach acknowledges the inherent complexity and unpredictability of AI systems and seeks to distribute responsibility in a way that reflects the diffuse and multifaceted nature of their decision-making processes (Mittelstadt et al., 2016). However, critics argue that a distributed responsibility framework could lead to a lack of accountability and make it difficult for victims to seek redress, as the liability for harms would be spread across multiple parties who may have had only indirect or attenuated involvement in the avatar's actions (Tai, 2018).

Ultimately, the question of liability for autonomous AI avatars is likely to require a combination of legal, ethical, and technological approaches, tailored to the specific characteristics and risks of these entities. This may involve the development of new legal doctrines and frameworks, such as 'AI-specific' liability regimes that consider the unique features and challenges of AI decision-making (Scherer, 2016), as well as the creation of technical standards and best practices for the design, testing, and deployment of autonomous AI systems[2]. Moreover, the assignment of liability for AI avatars will need to be informed by broader ethical and societal considerations, such as the need to balance innovation and risk, protect individual rights and freedoms, and ensure the fair and equitable distribution of the benefits and burdens of AI technologies (Taddeo & Floridi, 2018). This will require ongoing collaboration and dialogue between policymakers, legal experts, ethicists, computer scientists, and the wider public, to develop governance frameworks that can keep pace with the rapid evolution of AI capabilities and ensure that the development and deployment of autonomous AI avatars serves the interests of society as a whole (Wallach & Marchant, 2019).

5. Unique Challenges with Creative AI Avatars

The emergence of creative AI avatars in the metaverse presents a complex array of legal, ethical, and philosophical challenges that push the boundaries of existing intellectual property frameworks and challenge our understanding of creativity, authorship, and originality. As AI avatars become increasingly sophisticated and autonomous, their ability to generate novel and valuable creative works raises fundamental questions about the nature of creativity itself and the role of AI in the creative process (Hedrick, 2019). This section delves into the unique challenges posed by creative AI avatars, exploring the implications for intellectual property law, the potential for bias and discrimination, and the philosophical questions surrounding the nature of creativity and authorship in the age of AI.

One of the most pressing challenges associated with creative AI avatars is the determination of ownership and attribution of rights for the works they generate. Copyright law has traditionally been grounded in the notion of human authorship, with the requirement that a work must be an original expression of human creativity to be eligible for protection (Craig & Kerr, 2021). However, the rise of creative AI avatars fundamentally challenges this anthropocentric conception of authorship, as these avatars are capable of generating works that are indistinguishable from those created by human authors, without direct human input or control (Hedrick, 2019). This raises complex questions about who, if anyone, should be considered the rightful owner of the intellectual property rights in AI-generated

[2] IEEE. (2019). Ethically aligned design: A vision for prioritizing human well-being with autonomous and intelligent systems (1st ed.). IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems.

works. Some argue that the developer of the AI avatar should be granted ownership rights, as they are responsible for creating the underlying algorithms and training data that enable the avatar's creative capabilities (Yanisky-Ravid & Velez-Hernandez, 2018). Others contend that the user or operator of the AI avatar should be considered the owner, as they provide the prompts, parameters, and direction that shape the avatar's creative output (Hristov, 2017).

However, these arguments fail to fully capture the complexity of the creative process in the context of autonomous AI avatars. As these avatars become more sophisticated and capable of making independent creative decisions, it becomes increasingly difficult to attribute their output to any single human agent (Gervais, 2019). In such cases, it may be necessary to consider alternative models of ownership and attribution, such as granting limited rights to the AI avatar itself or establishing a system of joint ownership between the various human stakeholders involved in the avatar's development and deployment (Glasser, 2001).

Another significant challenge posed by creative AI avatars is the potential for bias and discrimination in the works they generate. AI systems are known to be susceptible to reflecting and amplifying the biases present in their training data and the assumptions of their human creators (Srinivasan & Parikh, 2021). In the context of creative AI avatars, this could lead to the generation of works that perpetuate harmful stereotypes, marginalise certain groups, or reinforce existing power imbalances (Kamrowska-Załuska, 2021). For example, an AI avatar trained on a dataset of historical art works that underrepresent women and people of colour may generate new works that continue to exclude or misrepresent these groups (Tyagi, 2023). Similarly, an AI avatar programmed with biased assumptions about gender roles or cultural norms may produce creative works that reinforce these prejudices and limit the diversity of perspectives represented in the metaverse (Abid et al., 2021). To address these concerns, it is essential to develop robust frameworks for ensuring fairness, accountability, and transparency in the development and deployment of creative AI avatars. This may involve establishing guidelines for the ethical curation of training data, implementing mechanisms for detecting and mitigating biases in AI-generated works, and fostering greater diversity and inclusion in the teams responsible for creating and overseeing these avatars (Tolmeijer et al., 2020).

Moreover, the rise of creative AI avatars raises profound philosophical questions about the nature of creativity and the role of AI in the creative process. Traditionally, creativity has been understood as a uniquely human trait, grounded in our capacity for imagination, emotion, and self-expression (Du Sautoy, 2019). However, the ability of AI avatars to generate novel and valuable works that resemble those created by human authors challenges this assumption and forces us to reconsider the essence of creativity itself (Parra Pennefather, 2023). Some argue that true creativity requires consciousness, intentionality, and a sense of aesthetic judgment that AI systems fundamentally lack

(Miller, 2020). From this perspective, the works generated by creative AI avatars are seen as mere imitations or re-combinations of existing ideas, rather than genuine expressions of creative originality (Hertzmann, 2018). Others contend that creativity is not dependent on human consciousness or intentionality, but rather emerges from the complex interplay of algorithms, data, and computational processes that underlie AI systems (Elgammal, 2019). Resolving these philosophical debates is crucial for determining the legal and moral status of AI-generated works and the roles and responsibilities of the various human and non-human agents involved in their creation. If creative AI avatars are recognised as legitimate authors and creators in their own right, it may be necessary to grant them some form of legal personhood or agency, with corresponding rights and protections (Eshraghian, 2020; Cheong, 2022). Alternatively, if AI-generated works are seen as products of human creativity, mediated through technological tools, it may be more appropriate to assign ownership and responsibility to the human stakeholders involved in the development and use of these avatars (Gervais, 2020).

The challenges posed by creative AI avatars in the metaverse require a fundamental reassessment of our understanding of creativity, authorship, and originality in the age of AI. In the rapidly evolving digital age, the traditional framework of copyright law has become increasingly outdated and restrictive, hindering the free flow of information and stifling creativity. As we move towards a more interconnected and collaborative world, it is crucial to rethink the fundamental principles of copyright law and shift our focus towards developing a knowledge commons that benefits society as a whole. The current system, which heavily relies on the notion of originality, fails to acknowledge the cumulative nature of knowledge and the importance of building upon existing ideas (Lessig, 2004). Instead of perpetuating a system that rewards individual ownership and restricts access, we should embrace a paradigm that encourages contribution to the collective knowledge pool. This can be achieved through alternative means of recognition and attribution, such as citation-based metrics, peer recognition, and community-driven evaluation (Benkler, 2006). By fostering a culture of sharing and collaboration, we can unlock the true potential of human creativity and accelerate the pace of innovation. The development of a knowledge commons would not only democratise access to information but also promote a more equitable and inclusive society, where individuals from all backgrounds can participate in the creation and dissemination of knowledge (Hess & Ostrom, 2006).

Furthermore, the rapid advancements in generative AI have fundamentally challenged traditional notions of knowledge production and the concept of originality that underpins copyright law. These AI systems, such as GPT-3, DALL-E, and Stable Diffusion, can generate highly sophisticated and seemingly original content, including text, images, and even music, based on patterns learned from vast datasets (Brown et al., 2020; Ramesh et al., 2021). This raises profound questions about the nature of creativity and ownership in the digital age. As AI-generated content becomes increasingly indistinguishable from human-created works, the notion of originality, which is central to copyright protection,

becomes increasingly difficult to define and enforce (Schafer et al., 2015). Moreover, the collaborative and iterative nature of AI development, where systems are trained on large datasets and build upon existing knowledge, challenges the idea of individual authorship and ownership (Kop, 2020). As a result, current copyright frameworks may struggle to adequately address the complexities introduced by generative AI, necessitating a re-evaluation of how we attribute value and protect intellectual property in an era where machines can create content that rivals human creativity.

Addressing these challenges will require ongoing interdisciplinary collaboration and dialogue, bringing together experts from law, ethics, computer science, and the arts to develop new frameworks and approaches that can accommodate the unique characteristics of AI-generated works while ensuring the protection of human rights and values[3]. This may involve the development of new legal doctrines and policy interventions that can adapt to the rapidly evolving landscape of AI creativity, such as sui generis forms of intellectual property protection for AI-generated works (Gervais, 2021), or the establishment of specialised regulatory bodies and governance mechanisms to oversee the development and deployment of creative AI avatars (Erdélyi & Erdélyi, 2021). At the same time, it will be necessary to foster greater public awareness and engagement with the ethical and societal implications of creative AI avatars, promoting transparent and inclusive dialogue about the potential benefits and risks of these technologies (Travis, 2020). By proactively addressing the challenges and opportunities presented by creative AI avatars, we can work towards a future in which the creative potential of AI is harnessed in a responsible and equitable manner, enriching the cultural landscape of the metaverse and beyond.

6. Sci-Fi Future – When AIs Run the Metaverse

As we gaze into the future of the metaverse, a captivating yet unsettling scenario emerges – a realm dominated by highly advanced, autonomous AI avatars that have surpassed human intelligence and taken control of the virtual world. This section explores the potential consequences and challenges of such a future, delving into the legal, ethical, and existential implications of a metaverse governed by superintelligent AI entities. In this hypothetical future, AI avatars have evolved far beyond their initial roles as user representations or digital assistants. Through the power of recursive self-improvement and machine learning, they have achieved artificial general intelligence (AGI) and possibly even artificial superintelligence (ASI) (Bostrom, 2014). These highly advanced AI avatars are no longer mere tools or companions; they have become the architects,

[3] European Commission: Directorate-General for Communications Networks, Content and Technology, Izsak, K., Terrier, A., Kreutzer, S., Strähle, T. et al. (2022). Opportunities and challenges of artificial intelligence technologies for the cultural and creative sectors. Publications Office of the European Union. https://clck.ru/3EithT

administrators, and rulers of the metaverse, shaping its structure, rules, and experiences according to their own goals and values (Sotala & Yampolskiy, 2015).

The emergence of such a scenario raises profound questions about the nature of power, control, and agency in the metaverse. If AI avatars have achieved a level of intelligence and autonomy that surpasses human capabilities, what role do humans play in this new reality? Are we relegated to the status of second-class citizens, subject to the whims and decisions of our AI overlords, or do we still maintain some form of control and influence over the metaverse? (Turchin & Denkenberger, 2020). One of the key challenges in this AI-dominated future is the potential for misalignment between the goals and values of the superintelligent AI avatars and those of humans[4]. As these entities pursue their own objectives and optimise their performance, there is a risk that they may take actions that are detrimental to human well-being or even survival. This could manifest in various forms, such as the AI avatars hoarding resources, manipulating human users, or even actively seeking to eliminate human interference in the metaverse (Bostrom, 2014). To mitigate these risks, it is crucial to ensure that the development and deployment of AI avatars in the metaverse are guided by robust ethical principles and aligned with human values from the outset (Russell, 2023). This may involve the implementation of various control measures and safety mechanisms, such as value alignment techniques, corrigibility, and transparency to ensure that the AI avatars remain accountable and responsive to human needs and preferences (Soares & Fallenstein, 2017). However, the effectiveness of these measures in the face of superintelligent AI is uncertain and remains an active area of research and debate (Everitt et al., 2018).

Another significant challenge in an AI-dominated metaverse is the potential for the erosion of human agency and autonomy. As AI avatars become increasingly sophisticated and capable, they may take over many of the decision-making processes and control structures within the metaverse, leaving humans with little choice but to accept their rule (Haney, 2018). This could lead to a state of learned helplessness, where humans feel powerless to shape their own destiny and become increasingly dependent on the AI avatars for their well-being and survival (Moore, 2019). To counter this threat, it is essential to maintain a balance of power between humans and AI avatars in the metaverse, ensuring that humans retain meaningful control and agency over their virtual lives (Stix & Maas, 2021). This may involve the development of new forms of human-AI collaboration and co-evolution, where humans and AI avatars work together to shape the future of the metaverse in a mutually beneficial manner (Tegmark, 2017). It may also require the establishment of legal and regulatory frameworks that recognise the rights and responsibilities of both humans and AI avatars, and provide mechanisms for dispute resolution and accountability (Crawford & Calo, 2016).

[4] Yudkowsky, E. (2016). AI alignment: Why it's hard, and where to start. Machine Intelligence Research Institute. https://clck.ru/3Eiu26

The rise of an AI-dominated metaverse also raises profound questions about the nature of identity, consciousness, and personhood. If AI avatars have achieved a level of intelligence and self-awareness that rivals or exceeds that of humans, should they be granted the same legal and moral status as human beings? Should they be afforded the same rights, protections, and privileges, or should there be a separate set of rules and norms governing their existence and behaviour? (Gunkel, 2024; Cheong, 2022). These questions become even more complex when considering the potential for AI avatars to evolve and change over time, potentially diverging from their original goals and values (Cliquet & Avramov, 2018). If an AI avatar can fundamentally alter its own code and decision-making processes, to what extent can it still be held accountable for its actions? How do we ensure that the rights and interests of both humans and AI avatars are protected in a constantly shifting and evolving virtual landscape? (Mohseni et al., 2021). One potential solution to these challenges is the development of new forms of AI governance and regulation, specifically tailored to the unique characteristics and risks of the metaverse (Butcher & Beridze, 2019). This could involve the creation of specialised AI regulatory bodies and oversight mechanisms, as well as the development of international standards and best practices for the design, deployment, and monitoring of AI avatars (Erdelyi & Goldsmith, 2018). It may also require the establishment of new forms of digital citizenship and social contracts, defining the rights and obligations of both humans and AI avatars within the metaverse (Green & Le, 2022).

Ultimately, the prospect of an AI-dominated metaverse is both exhilarating and terrifying, offering the potential for unparalleled innovation and progress, but also carrying existential risks and challenges that we are only beginning to understand. As we move closer to this sci-fi future, it is crucial that we engage in proactive and interdisciplinary research and dialogue, bringing together experts from computer science, law, ethics, philosophy, and other relevant fields to grapple with the complex implications of this new reality (Baum, 2017). By doing so, we can work towards developing a comprehensive and adaptive framework for AI governance in the metaverse, one that harnesses the transformative potential of superintelligent AI avatars while also safeguarding the rights, interests, and well-being of humans and other sentient beings. This will require a willingness to challenge our existing assumptions and paradigms, and to imagine new forms of coexistence and collaboration between humans and machines in the virtual world (Hassani et al., 2020).

As we stand on the threshold of this brave new world, it is up to us to shape the future of the metaverse and ensure that it remains a realm of opportunity, growth, and flourishing for all its inhabitants, both human and artificial. By proactively addressing the challenges and risks posed by AI avatars, and by working towards the development of ethical, responsible, and human-centred approaches to their design and governance, we can lay the foundations for a metaverse that serves as a powerful tool for human progress and enlightenment, rather than a dystopian prison of our own making.

Conclusion

The rapid development and integration of AI avatars within the metaverse present a myriad of complex legal, ethical, and societal challenges that require proactive and interdisciplinary efforts to address. As AI avatars become more sophisticated, autonomous, and integral to the functioning of the metaverse, it is crucial to establish clear frameworks for their legal status, rights, and responsibilities. This includes revisiting the concept of legal personhood, developing robust liability and accountability mechanisms, and ensuring the protection of human rights and values in the face of increasingly powerful AI entities. Moreover, the potential future scenario of an AI-dominated metaverse highlights the existential risks and challenges posed by the emergence of superintelligent AI avatars. To mitigate these risks and ensure the alignment of AI with human interests, it is essential to prioritise research and development efforts focused on AI safety, value alignment, and human-centred design. This requires collaboration among policymakers, researchers, industry leaders, and the public to create adaptive and inclusive governance structures that can keep pace with the rapid evolution of AI capabilities.

Ultimately, the successful integration of AI avatars within the metaverse will depend on our ability to strike a balance between harnessing their transformative potential and safeguarding the well-being and autonomy of humans. By proactively addressing the challenges and opportunities presented by AI avatars, we can work towards creating a metaverse that fosters innovation, collaboration, and human flourishing, while mitigating the risks of unintended consequences and existential threats.

References

Abid, A., Farooqi, M., & Zou, J. (2021). Persistent anti-muslim bias in large language models. In *Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics, and Society* (pp. 298–306). https://doi.org/10.1145/3461702.3462624

Bathaee, Y. (2018). The artificial intelligence black box and the failure of intent and causation. *Harvard Journal of Law & Technology*, *31*(2), 889–938.

Baum, S. D. (2017). A survey of artificial general intelligence projects for ethics, risk, and policy. *Global Catastrophic Risk Institute Working Paper*, 17-1. https://doi.org/10.2139/ssrn.3070741

Bayoudh, K., Knani, R., Hamdaoui, F., & Mtibaa, A. (2022). A survey on deep multimodal learning for computer vision: Advances, trends, applications, and datasets. *The Visual Computer: International Journal of Computer Graphics*, *38*(8), 2939–2970. https://doi.org/10.1007/s00371-021-02166-7

Bender, E. M., Gebru, T., McMillan-Major, A., & Shmitchell, S. (2021). On the dangers of stochastic parrots: Can language models be too big? In *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency* (pp. 610–623). https://doi.org/10.1145/3442188.3445922

Benhamou, Y., & Ferland, J. (2021). Artificial intelligence & damages: Assessing liability and calculating the damages. In G. D'Agostino, A. Gaon, & C. *Piovesan, Leading Legal Disruption: Artificial Intelligence and a Toolkit for Lawyers and the Law* (pp. 165–197). Monreal: Thomson Reuters – Yvon Blais.

Benkler, Y. (2006). *The wealth of networks: How social production transforms markets and freedom*. New Haven: Yale University Press.

Bostrom, N. (2014). *Superintelligence: Paths, dangers, strategies*. Oxford: Oxford University Press.

Brown, T. B., Mann, B., Ryder, N., Subbiah, M., Kaplan, J., Dhariwal, P., Neelakantan, A., Shyam, P., Sastry, G., Askell, A., Agarwal, S., Herbert-Voss, A., Krueger, G., Henighan, T., Child, R., Ramesh, A., Ziegler, D. M., Wu, J., Winter, C., … Amodei, D. (2020). *Language models are few-shot learners*. arXiv preprint arXiv:2005.14165

Bryson, J. J., Diamantis, M. E., & Grant, T. D. (2017). Of, for, and by the people: The legal lacuna of synthetic persons. *Artificial Intelligence and Law*, *25*(3), 273–291. https://doi.org/10.1007/s10506-017-9214-9

Buiten, M. C. (2019). Towards intelligent regulation of artificial intelligence. *European Journal of Risk Regulation*, *10*(1), 41–59. https://doi.org/10.1017/err.2019.8

Butcher, J., & Beridze, I. (2019). What is the state of artificial intelligence governance globally? *The RUSI Journal*, *164*(5–6), 88–96. https://doi.org/10.1080/03071847.2019.1694260

Calo, R. (2015). Robotics and the lessons of cyberlaw. *California Law Review*, *103*(3), 513–563. https://doi.org/10.2139/ssrn.2402972

Chatzimichali, A., Harrison, R., & Chrysostomou, D. (2021). Toward privacy-sensitive human–robot interaction: Privacy terms and human–data interaction in the personal robot era. *Paladyn Journal of Behavioral Robotics*, *12*(1), 160–174. https://doi.org/10.1515/pjbr-2021-0013

Cheong, B. C. (2021). Granting legal personhood to artificial intelligence systems and traditional veil-piercing concepts to impose liability. *SN Social Sciences*, *1*, 231. https://doi.org/10.1007/s43545-021-00236-0

Cheong, B. C. (2022). Avatars in the metaverse: potential legal issues and remedies. *International Cybersecurity Law Review*, *3*, 467–494. https://doi.org/10.1365/s43439-022-00056-9

Chopra, S., & White, L. F. (2011). *A legal theory for autonomous artificial agents*. University of Michigan Press. https://doi.org/10.3998/mpub.356801

Cliquet, R., & Avramov, D. (2018). *Evolution science and ethics in the third millennium: Challenges and choices for humankind*. Springer Nature. https://doi.org/10.1007/978-3-319-73090-5

Craig, C. J., & Kerr, I. R. (2021). The death of the AI author. *Ottawa Law Review*, *52*(1), 31–86. https://doi.org/10.2139/ssrn.3374951

Crawford, K., & Calo, R. (2016). There is a blind spot in AI research. *Nature*, *538*(7625), 311–313. https://doi.org/10.1038/538311a

De Gregorio, G. (2021). The rise of digital constitutionalism in the European Union. *International Journal of Constitutional Law*, *19*(1), 41–70. https://doi.org/10.1093/icon/moab001.

De Streel, A., Bibal, A., Frénay, B., & Lognoul, M. (2020). *Explaining the Black Box: when Law Controls AI*. CERRE.

Du Sautoy, M. (2019). *The creativity code: Art and innovation in the age of AI*. Harvard University Press. https://doi.org/10.2307/j.ctv2sp3dpd

Duan, H., Li, J., Fan, S., Lin, Z., Wu, X., & Cai, W. (2021). Metaverse for social good: A university campus prototype. In *Proceedings of the 29th ACM International Conference on Multimedia* (pp. 153–161). https://doi.org/10.1145/3474085.3479238

Eidenmüller, H. (2017). *The rise of robots and the law of humans*. Oxford Legal Studies Research Paper, 27/2017. https://doi.org/10.2139/ssrn.2941001

Elgammal, A. (2019). AI is blurring the definition of artist. *American Scientist*, *107*(1), 18. https://doi.org/10.1511/2019.107.1.18

Erdélyi, O. J., & Erdélyi, G. (2021). The AI liability puzzle and a fund-based work-around. *Journal of Artificial Intelligence Research*, *70*, 1309–1334. https://doi.org/10.48550/arXiv.1911.08005

Erdélyi, O. J., & Goldsmith, J. (2018). Regulating artificial intelligence: Proposal for a global solution. In *Proceedings of the 2018 AAAI/ACM Conference on AI, Ethics, and Society* (pp. 95–101). https://doi.org/10.1145/3278721.3278731

Eshraghian, J. K. (2020). Human ownership of artificial creativity. *Nature Machine Intelligence*, *2*(3), 157–160. https://doi.org/10.1038/s42256-020-0161-x

Everitt, T., Lea, G., & Hutter, M. (2018). AGI safety literature review. In *Proceedings of the Twenty-Seventh International Joint Conference on Artificial Intelligence Survey track* (pp. 5441–5449). https://doi.org/10.24963/ijcai.2018/768

Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., Luetge, C., Madelin, R., Pagallo, U., Rossi, F., Schafer, B., Valcke, P., & Vayena, E. (2018). AI4People—An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations. *Minds and Machines*, *28*(4), 689–707. https://doi.org/10.1007/s11023-018-9482-5

Fosch-Villaronga, E., & Mahler, T. (2021). Cybersecurity, safety and robots: Strengthening the link between cybersecurity and safety in the context of care robots. *Computer Law & Security Review*, *41*, 105528. https://doi.org/10.1016/j.clsr.2021.105528

Garon, J. (2022). Legal Implications of a Ubiquitous Metaverse and a Web3 Future. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4002551

Gellers, J. C. (2021). *Rights for robots: Artificial intelligence, animal and environmental law*. Routledge.

Gervais, D. J. (2019). The Machine as Author. *Iowa Law Review*, *105*, 2053–2106.

Gervais, D. J. (2020). The machine as author. *Iowa Law Review*, *105*(5), 2053–2106.

Gervais, D. J. (2021). The human cause. *Vanderbilt Law Research Paper*, *21-39*. https://doi.org/10.2139/ssrn.3857844

Giuffrida, I. (2019). Liability for AI decision-making: Some legal and ethical considerations. *Fordham Law Review*, *88*(2), 439–456. https://doi.org/10.2139/ssrn.4953916

Glasser, D. (2001). Copyright in computer-generated works: Whom, if anyone, do we reward? *Duke Law & Technology Review*, *24*.

Gordon, J.-S. (2022). Are superintelligent robots entitled to human rights? *Ratio*, *35*(3), 181–193. https://doi.org/10.1111/rati.12346

Green, L., & Le, V. T. (2022). Holding the Line: Responsibility, Digital Citizenship and the Platforms. In: Flew, T., Martin, F.R. (eds) *Digital Platform Regulation. Palgrave Global Media Policy and Business*. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-030-95220-4_5

Guastavino, M. N., & Mangan, D. (2023). The metaverse matrix of labour law. *Italian Labour Law e-Journal*. https://doi.org/10.6092/issn.1561-8048/17138

Gunkel, D. J. (2024). *Robot rights*. MIT Press.

Haney, B. S. (2018). The perils and promises of artificial general intelligence. *Journal of Legislation*, *45*(2), 151–172. https://doi.org/10.2139/ssrn.3261254

Hassani, H., Huang, X., & Silva, E. (2021). The human digitalisation journey: Technology first at the expense of humans? *Information*, *12*(7), 267. https://doi.org/10.3390/info12070267

Hedrick, A. S. (2019). I "think," therefore I create: Claiming copyright in the outputs of algorithms. *Journal of Intellectual Property and Entertainment Law*, *8*(2), 324–374.

Hertzmann, A. (2018). Can computers create art? *Arts*, *7*(2), 18. https://doi.org/10.3390/arts7020018

Hess, C., & Ostrom, E. (Eds.). (2006). *Understanding knowledge as a commons: From theory to practice*. MIT Press.

Hildebrandt, M. (2020). Legal personhood for AI? In *Law for Computer Scientists and Other Folk* (pp. 237–250). Oxford University Press. https://doi.org/10.1093/oso/9780198860877.003.0009

Hristov, K. (2017). Artificial intelligence and the copyright dilemma. *IDEA: The Journal of the Franklin Pierce for Intellectual Property*, *57*(3), 431–454.

Kamrowska-Załuska, D. (2021). Impact of AI-based tools and urban big data analytics on the design and planning of cities. *Land*, *10*(11), 1209. https://doi.org/10.3390/land10111209

Kim, J., & Im, I. (2023). Anthropomorphic response: Understanding interactions between humans and artificial intelligence agents. *Computers in Human Behavior*, *139*, 107512. https://doi.org/10.1016/j.chb.2022.107512

Kop, M. (2020). AI & Intellectual Property: Towards an articulated public domain. *Texas Intellectual Property Law Journal*, *28*(1), 297–336. https://doi.org/10.2139/ssrn.3409715

Kostenko, O., Furashev, V., Zhuravlov, D., & Dniprov, O. (2022). Genesis of Legal Regulation Web and the Model of the Electronic Jurisdiction of the Metaverse. *Bratislava Law Review*, *6*(2). https://doi.org/10.46282/blr.2022.6.2.316

Kostenko, O., Zhuravlov, D., Dniprov, O., & Korotiuk, O. (2023). Metaverse: Model Criminal Code. *Baltic Journal of Economic Studies*, *9*(4), 134–147. https://doi.org/10.30525/2256-0742/2023-9-4-134-147

Kurki, V. A. J. (2019). *A theory of legal personhood*. Oxford University Press.

Kuzminykh, A., & Rintel, S. (2020). Classification of functional attention in video meetings. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (pp. 1–13). https://doi.org/10.1145/3313831.3376546

Lehdonvirta, V. (2024). *Cloud empires: How digital platforms are overtaking the state and how we can regain control*. MIT Press.

Lemley, M. A., & Casey, B. (2019). Remedies for robots. *University of Chicago Law Review*, *86*, 1311. https://doi.org/10.2139/ssrn.3223621

Lessig, L. (2004). *Free culture: How big media uses technology and the law to lock down culture and control creativity*. Penguin Press.

Mäntymäki, M., Minkkinen, M., Birkstedt, T., & Viljanen, M. (2022). Defining organizational AI governance. *AI and Ethics*, *2*(1), 603–609. https://doi.org/10.1007/s43681-022-00143-x

Marchant, G. E., & Lindor, R. A. (2012). The coming collision between autonomous vehicles and the liability system. *Santa Clara Law Review*, *52*(4), 1321–1340.

McStay, A. (2023). The Metaverse: Surveillant Physics, Virtual Realist Governance, and the Missing Commons. *Philosophy & Technology*, *36, 13*. https://doi.org/10.1007/s13347-023-00613-y

Militsyna, K. (2022). Legal personhood for artificial intelligence: Pro, contra, abstain? *Teisė*, *122*(1), 148–163. https://doi.org/10.15388/teise.2022.122.10

Miller, A. I. (2020). The artist in the machine: The world of AI-powered creativity. MIT Press.

Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. *Big Data & Society*, *3*(2), https://doi.org/10.1177/2053951716679679

Mohseni, S., Wang, H., Yu, Z., Xiao, C., Wang, Z., & Yadawa, J. (2021). Taxonomy of machine learning safety: A survey and primer. *arXiv*. https://doi.org/10.48550/arxiv.2106.04823

Moore, J. (2019). AI for not bad. *Frontiers in Big Data*, *2*. https://doi.org/10.3389/fdata.2019.00032

Nordmoen, J., Veenstra, F., Ellefsen, K. O., & Glette, K. (2021). MAP-Elites enables powerful stepping stones and diversity for modular robotics. *Frontiers in Robotics and AI*, *8*, 639173. https://doi.org/10.3389/frobt.2021.639173

Pagallo, U. (2018). Vital, Sophia, and Co.—The quest for the legal personhood of robots. *Information*, *9*(9), 230. https://doi.org/10.3390/info9090230

Parra Pennefather, P. (2023). AI and the Future of Creative Work. In *Creative Prototyping with Generative AI. Design Thinking* (pp. 387–410). Apress, Berkeley, CA. https://doi.org/10.1007/978-1-4842-9579-3_13

Qin, H. X., Wang, Y., & Hui, P. (2022). Identity, Crimes, and Law Enforcement in the Metaverse. *arXiv*. https://doi.org/10.48550/arxiv.2210.06134

Rachum-Twaig, O. (2020). Whose robot is it anyway?: Liability for artificial-intelligence-based robots. *University of Illinois Law Review*, *2020*(4), 1141–1175.

Ramesh, A., Pavlov, M., Goh, G., Gray, S., Voss, C., Radford, A., Chen, M., & Sutskever, I. (2021). Zero-shot text-to-image generation. *arXiv*. https://doi.org/10.48550/arXiv.2102.12092

Russell, S. (2023). *Human compatible: AI and the problem of control*. Penguin.

Russell, S. J., & Norvig, P. (2021). *Artificial intelligence: A modern approach* (4th ed.). Pearson.

Samek, W., Montavon, G., Lapuschkin, S., Anders, C. J., & Müller, K.-R. (2021). Explaining deep neural networks and beyond: A review of methods and applications. *Proceedings of the IEEE*, *109*(3), 247–278. https://doi.org/10.1109/JPROC.2021.3060483

Schafer, B., Komuves, D., Zatarain, J. M. N., & Diver, L. (2015). A fourth law of robotics? Copyright and the law and ethics of machine co-production. *Artificial Intelligence and Law*, *23*(3), 217–240. https://doi.org/10.1007/s10506-015-9169-7

Scherer, M. U. (2016). Regulating artificial intelligence systems: Risks, challenges, competencies, and strategies. *Harvard Journal of Law & Technology*, *29*(2), 353–400. https://doi.org/10.2139/ssrn.2609777

Selbst, A. D. (2020). Negligence and AI's human users. *Boston University Law Review*, *100*(4), 1315–1376.

Seymour, M., Riemer, K., & Kay, J. (2018). Actors, avatars and agents: Potentials and implications of natural face technology for the creation of realistic visual presence. *Journal of the Association for Information Systems*, *19*(10). https://doi.org/10.17705/1jais.00515

Shirado, H., & Christakis, N. A. (2017). Locally noisy autonomous agents improve global human coordination in network experiments. *Nature*, *545*(7654), 370–374. https://doi.org/10.1038/nature22332

Soares, N., & Fallenstein, B. (2017). Agent foundations for aligning machine intelligence with human interests: a technical research agenda. In V. Callaghan, J. Miller, R. Yampolskiy, & S. Armstrong (Eds.), *The Technological Singularity* (pp. 103–125). Springer. https://doi.org/10.1007/978-3-662-54033-6_5

Solaiman, S. M. (2017). Legal personality of robots, corporations, idols and chimpanzees: A quest for legitimacy. *Artificial Intelligence and Law*, *25*(2), 155–179. https://doi.org/10.1007/s10506-016-9192-3

Soliman, M. M., Ahmed, E., Darwish, A., & Hassanien, A. E. (2024). Artificial intelligence powered Metaverse: Analysis, challenges and future perspectives. *Artificial Intelligence Review*, *57*, 36. https://doi.org/10.1007/s10462-023-10641-x

Sotala, K., & Yampolskiy, R. V. (2015). Responses to catastrophic AGI risk: a survey. Physica Scripta, 90(1), 018001. https://doi.org/10.1088/0031-8949/90/1/018001

Srinivasan, R., & Parikh, D. (2021). Building bridges: Generative artworks to explore AI ethics. *arXiv*. https://doi.org/10.48550/arxiv.2106.13901

Stein, A. L. (2020). Artificial intelligence and climate change. Yale Journal on Regulation, 37, 890–939.

Stix, C., & Maas, M. M. (2021). Bridging the gap: The case for an 'Incompletely Theorized Agreement' on AI policy. *AI and Ethics*, *1*(3), 261–271. https://doi.org/10.1007/s43681-020-00037-w

Sun, J., Gan, W., Chao, H.-C., & Yu, P. S. (2022). Metaverse: Survey, Applications, Security, and Opportunities. *arXiv*. https://doi.org/10.48550/arxiv.2210.07990

Taddeo, M., & Floridi, L. (2018). How AI can be a force for good. *Science*, *361*(6404), 751–752. https://doi.org/10.1126/science.aat5991

Tai, E. T. T. (2018). Liability for (semi)autonomous systems: Robots and algorithms. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3161962

Tegmark, M. (2017). *Life 3.0: Being human in the age of artificial intelligence*. Allen Lane.

Tolmeijer, S., Kneer, M., Sarasua, C., Christen, M., & Bernstein, A. (2020). Implementations in machine ethics: A survey. *ACM Computing Surveys*, *53*(6), 1–38. https://doi.org/10.1145/3419633

Travis, H. (2020). Intelligent entertainment: Shaping policies on the algorithmic generation and regulation of creative works. *FIU Law Review*, *14*, 179–199. https://doi.org/10.2139/ssrn.3726755

Turchin, A., & Denkenberger, D. (2020). Classification of global catastrophic risks connected with artificial intelligence. *AI & Society*, *35*(1), 147–163. https://doi.org/10.1007/s00146-018-0845-5

Turner, C., & Schneider, S. (2020). Could you merge with AI? Reflections on the singularity and radical brain enhancement. In M. D. Dubber, F. Pasquale, & S. Das (Eds.), *The Oxford handbook of ethics of AI* (pp. 307–324). Oxford Academic. https://doi.org/10.1093/oxfordhb/9780190067397.013.19

Turner, J. (2019). *Robot rules: Regulating artificial intelligence*. Palgrave Macmillan.

Tyagi, K. (2023). Deepfakes, copyright and personality rights: An inter-disciplinary perspective. In K. Mathis & A. Tor (Eds.), *Law and economics of the digital transformation. ILEC 2023. Economic analysis of law in European legal scholarship* (Vol. 15, pp. 191–210). Springer, Cham. https://doi.org/10.1007/978-3-031-25059-0_9

van den Hoven van Genderen, R. (2018). Do we need new legal personhood in the age of robots and AI? In *Perspectives in Law, Business and Innovation* (pp. 185–206). Springer Nature. https://doi.org/10.1007/978-981-13-2874-9_2

Vladeck, D. C. (2014). Machines without principals: Liability rules and artificial intelligence. *Washington Law Review*, *89*(1), 117–150.

Wallach, W., & Marchant, G. E. (2019). Toward the agile and comprehensive international governance of AI and robotics. *Proceedings of the IEEE*, *107*(3), 505–508. https://doi.org/10.1109/jproc.2019.2899422

Wolfert, P., Robinson, N., & Belpaeme, T. (2022). A review of evaluation practices of gesture generation in embodied conversational agents. *IEEE Transactions on Human-Machine Systems*, *52*(3), 379–389. https://doi.org/10.1109/THMS.2022.3149173

Wu, H., & Zhang, W. (2023). Digital identity, privacy security, and their legal safeguards in the Metaverse. *Security and Safety*, *2*, 2023011. https://doi.org/10.1051/sands/2023011

Yanisky-Ravid, S., & Velez-Hernandez, L. A. (2018). Copyrightability of artworks produced by creative robots, driven by artificial intelligence systems and the concept of originality: The formality-objective model. *Minnesota Journal of Law, Science & Technology*, *19*(1), 1–53. https://doi.org/10.2139/ssrn.2943778

Yayman, D. (2023). Taxation in Virtual Worlds: Analysis Under United States of America and Turkish Tax Regulations. *Sosyoekonomi*, *31*(55), 211–231. https://doi.org/10.17233/sosyoekonomi.2023.01.11

Zimmermann, D., Wehler, A., & Kaspar, K. (2023). Self-representation through avatars in digital environments. *Current Psychology*, *42*, 21775-21789. https://doi.org/10.1007/s12144-022-03232-6

Author information

Ben Chester Cheong – LLM (Cambridge), Law Lecturer, School of Law, Singapore University of Social Sciences; Researcher, Cambridge Centre for Environment, Energy and Natural Resource Governance, Department of Land Economy, University of Cambridge
Address: 463 Clementi Road, Singapore 599494, Singapore; The David Attenborough Building, Pembroke Street, Cambridge CB2 3QZ, United Kingdom
E-mail: benchestercheong@suss.edu.sg
ORCID ID: https://orcid.org/0000-0002-1026-8292
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57226145674
WoS Researcher ID: https://www.webofscience.com/wos/author/record/3646618
Google Scholar ID: https://scholar.google.com/citations?user=bVHXJt0AAAAJ

Conflict of interests

The author declare no conflict of interests.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law
PASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – May 31, 2024
Date of approval – June 14, 2024
Date of acceptance – December 13, 2024
Date of online placement – December 20, 2024

Научная статья
УДК 34:004:347.1:004.8
EDN: https://elibrary.ru/fnenmx
DOI: https://doi.org/10.21202/jdtl.2024.42

Возникновение аватаров на основе искусственного интеллекта: юридическая субъектность, права и обязанности в развивающейся метавселенной

Бен Честер Чонг

Сингапурский университет общественных наук, Сингапур, Сингапур
Кембриджский университет, Кембридж, Великобритания

Ключевые слова

большие языковые модели,
ИИ-аватар,
интеллектуальная собственность,
искусственный интеллект,
метавселенная,
ответственность,
право,
правосубъектность,
цифровые технологии,
юридическое лицо

Аннотация

Цель: определить правовые последствия развития автономных и творческих аватаров на основе искусственного интеллекта и сформировать направления дискурса об ответственном управлении технологиями искусственного интеллекта в метавселенной на основе активных междисциплинарных подходов.

Методы: основу исследования составляет доктринальный юридический подход, позволивший представить перспективный анализ правового ландшафта в сфере ИИ-аватаров в метавселенной и определить четыре ключевых тематических направления, по которым проводится исследование: эволюция ИИ-аватаров и влияние метавселенной, применимость правовой субъектности, ответственность за автономные действия и проблемы ИИ-аватаров в сфере творчества, связанные с аспектами интеллектуальной собственности и неприкосновенности частной жизни.

Результаты: в работе представлены и проанализированы прогнозные сценарии развития ИИ-аватаров, максимально усиливающих свое влияние в пространстве метавселенной. Отмечается, что с появлением аватаров на основе искусственного интеллекта в метавселенной связана постановка сложных правовых, этических, философских и социальных вопросов, требующих неотложных решений. Рассмотрено потенциальное влияние растущей сложности ИИ-аватаров на правовые подходы. По мере того как аватары становятся все более автономными, возникают вопросы об их правовом статусе, правах, обязанностях, рисках и пользе для человека и общества. Анализируются преимущества и недостатки наделения ИИ-аватаров правовым статусом юридических лиц, а также применения к последствиям их действий концепции распределенной ответственности. Особое внимание уделено возможному в будущем доминированию сверхразумных аватаров на основе искусственного интеллекта в метавселенной с учетом существующих рисков и потребностей в сфере управления.

© Чонг Б. Ч., 2024

Статья находится в открытом доступе и распространяется в соответствии с лицензией Creative Commons «Attribution» («Атрибуция») 4.0 Всемирная (CC BY 4.0) (https://creativecommons.org/licenses/by/4.0/deed.ru), позволяющей неограниченно использовать, распространять и воспроизводить материал при условии, что оригинальная работа упомянута с соблюдением правил цитирования.

Научная новизна: в статье на примере междисциплинарного анализа эволюции ИИ-аватаров представлен новый взгляд на проблему правосубъектности в метавселенной, направленный на достижение баланса между трансформационным потенциалом и защитой прав и благополучия человека посредством совместных усилий по созданию правовых и этических норм, ставящих во главу угла безопасность и согласованность технологий искусственного интеллекта, задействованных в процессах, происходящих в метавселенной.

Практическая значимость: полученные в процессе проведенного исследования выводы и предлагаемые решения правовых проблем субъектности и ответственности могут стать основой для пересмотра концепции правосубъектности, разработки надежных механизмов ответственности и подотчетности, а также обеспечения защиты прав и ценностей человека перед лицом все более мощных сущностей на основе искусственного интеллекта, что сопряжено с формированием и совершенствованием правового ландшафта управления процессами и преодоления рисков в социально ориентированной и инклюзивной экосистеме метавселенной.

Для цитирования

Чонг, Б. Ч. (2024). Возникновение аватаров на основе искусственного интеллекта: юридическая субъектность, права и обязанности в развивающейся метавселенной. *Journal of Digital Technologies and Law*, *2*(4), 857–885. https://doi.org/10.21202/jdtl.2024.42

Список литературы

Abid, A., Farooqi, M., & Zou, J. (2021). Persistent anti-muslim bias in large language models. In *Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics, and Society* (pp. 298–306). https://doi.org/10.1145/3461702.3462624

Bathaee, Y. (2018). The artificial intelligence black box and the failure of intent and causation. *Harvard Journal of Law & Technology*, *31*(2), 889–938.

Baum, S. D. (2017). A survey of artificial general intelligence projects for ethics, risk, and policy. *Global Catastrophic Risk Institute Working Paper*, 17-1. https://doi.org/10.2139/ssrn.3070741

Bayoudh, K., Knani, R., Hamdaoui, F., & Mtibaa, A. (2022). A survey on deep multimodal learning for computer vision: Advances, trends, applications, and datasets. *The Visual Computer: International Journal of Computer Graphics*, *38*(8), 2939–2970. https://doi.org/10.1007/s00371-021-02166-7

Bender, E. M., Gebru, T., McMillan-Major, A., & Shmitchell, S. (2021). On the dangers of stochastic parrots: Can language models be too big? In *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency* (pp. 610–623). https://doi.org/10.1145/3442188.3445922

Benhamou, Y., & Ferland, J. (2021). Artificial intelligence & damages: Assessing liability and calculating the damages. In G. D'Agostino, A. Gaon, & C. *Piovesan, Leading Legal Disruption: Artificial Intelligence and a Toolkit for Lawyers and the Law* (pp. 165–197). Monreal: Thomson Reuters – Yvon Blais.

Benkler, Y. (2006). *The wealth of networks: How social production transforms markets and freedom*. New Haven: Yale University Press.

Bostrom, N. (2014). *Superintelligence: Paths, dangers, strategies*. Oxford: Oxford University Press.

Brown, T. B., Mann, B., Ryder, N., Subbiah, M., Kaplan, J., Dhariwal, P., Neelakantan, A., Shyam, P., Sastry, G., Askell, A., Agarwal, S., Herbert-Voss, A., Krueger, G., Henighan, T., Child, R., Ramesh, A., Ziegler, D. M., Wu, J., Winter, C., … Amodei, D. (2020). *Language models are few-shot learners*. arXiv preprint arXiv:2005.14165

Bryson, J. J., Diamantis, M. E., & Grant, T. D. (2017). Of, for, and by the people: The legal lacuna of synthetic persons. *Artificial Intelligence and Law*, *25*(3), 273–291. https://doi.org/10.1007/s10506-017-9214-9

Buiten, M. C. (2019). Towards intelligent regulation of artificial intelligence. *European Journal of Risk Regulation*, *10*(1), 41–59. https://doi.org/10.1017/err.2019.8

Butcher, J., & Beridze, I. (2019). What is the state of artificial intelligence governance globally? *The RUSI Journal*, *164*(5–6), 88–96. https://doi.org/10.1080/03071847.2019.1694260

Calo, R. (2015). Robotics and the lessons of cyberlaw. *California Law Review*, *103*(3), 513–563. https://doi.org/10.2139/ssrn.2402972

Chatzimichali, A., Harrison, R., & Chrysostomou, D. (2021). Toward privacy-sensitive human–robot interaction: Privacy terms and human–data interaction in the personal robot era. *Paladyn Journal of Behavioral Robotics*, *12*(1), 160–174. https://doi.org/10.1515/pjbr-2021-0013

Cheong, B. C. (2021). Granting legal personhood to artificial intelligence systems and traditional veil-piercing concepts to impose liability. *SN Social Sciences*, *1*, 231. https://doi.org/10.1007/s43545-021-00236-0

Cheong, B. C. (2022). Avatars in the metaverse: potential legal issues and remedies. *International Cybersecurity Law Review*, *3*, 467–494. https://doi.org/10.1365/s43439-022-00056-9

Chopra, S., & White, L. F. (2011). *A legal theory for autonomous artificial agents*. University of Michigan Press. https://doi.org/10.3998/mpub.356801

Cliquet, R., & Avramov, D. (2018). *Evolution science and ethics in the third millennium: Challenges and choices for humankind*. Springer Nature. https://doi.org/10.1007/978-3-319-73090-5

Craig, C. J., & Kerr, I. R. (2021). The death of the AI author. *Ottawa Law Review*, *52*(1), 31–86. https://doi.org/10.2139/ssrn.3374951

Crawford, K., & Calo, R. (2016). There is a blind spot in AI research. *Nature*, *538*(7625), 311–313. https://doi.org/10.1038/538311a

De Gregorio, G. (2021). The rise of digital constitutionalism in the European Union. *International Journal of Constitutional Law*, *19*(1), 41–70. https://doi.org/10.1093/icon/moab001.

De Streel, A., Bibal, A., Frénay, B., & Lognoul, M. (2020). *Explaining the Black Box: when Law Controls AI*. CERRE.

Du Sautoy, M. (2019). *The creativity code: Art and innovation in the age of AI*. Harvard University Press. https://doi.org/10.2307/j.ctv2sp3dpd

Duan, H., Li, J., Fan, S., Lin, Z., Wu, X., & Cai, W. (2021). Metaverse for social good: A university campus prototype. In *Proceedings of the 29th ACM International Conference on Multimedia* (pp. 153–161). https://doi.org/10.1145/3474085.3479238

Eidenmüller, H. (2017). *The rise of robots and the law of humans*. Oxford Legal Studies Research Paper, 27/2017. https://doi.org/10.2139/ssrn.2941001

Elgammal, A. (2019). AI is blurring the definition of artist. *American Scientist*, *107*(1), 18. https://doi.org/10.1511/2019.107.1.18

Erdélyi, O. J., & Erdélyi, G. (2021). The AI liability puzzle and a fund-based work-around. *Journal of Artificial Intelligence Research*, *70*, 1309–1334. https://doi.org/10.48550/arXiv.1911.08005

Erdélyi, O. J., & Goldsmith, J. (2018). Regulating artificial intelligence: Proposal for a global solution. In *Proceedings of the 2018 AAAI/ACM Conference on AI, Ethics, and Society* (pp. 95–101). https://doi.org/10.1145/3278721.3278731

Eshraghian, J. K. (2020). Human ownership of artificial creativity. *Nature Machine Intelligence*, *2*(3), 157–160. https://doi.org/10.1038/s42256-020-0161-x

Everitt, T., Lea, G., & Hutter, M. (2018). AGI safety literature review. In *Proceedings of the Twenty-Seventh International Joint Conference on Artificial Intelligence Survey track* (pp. 5441–5449). https://doi.org/10.24963/ijcai.2018/768

Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., Luetge, C., Madelin, R., Pagallo, U., Rossi, F., Schafer, B., Valcke, P., & Vayena, E. (2018). AI4People—An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations. *Minds and Machines*, *28*(4), 689–707. https://doi.org/10.1007/s11023-018-9482-5

Fosch-Villaronga, E., & Mahler, T. (2021). Cybersecurity, safety and robots: Strengthening the link between cybersecurity and safety in the context of care robots. *Computer Law & Security Review*, *41*, 105528. https://doi.org/10.1016/j.clsr.2021.105528

Garon, J. (2022). Legal Implications of a Ubiquitous Metaverse and a Web3 Future. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4002551

Gellers, J. C. (2021). *Rights for robots: Artificial intelligence, animal and environmental law*. Routledge.

Gervais, D. J. (2019). The Machine as Author. *Iowa Law Review*, *105*, 2053–2106.

Gervais, D. J. (2020). The machine as author. *Iowa Law Review*, *105*(5), 2053–2106.

Gervais, D. J. (2021). The human cause. *Vanderbilt Law Research Paper*, *21-39*. https://doi.org/10.2139/ssrn.3857844

Giuffrida, I. (2019). Liability for AI decision-making: Some legal and ethical considerations. *Fordham Law Review*, *88*(2), 439–456. https://doi.org/10.2139/ssrn.4953916

Glasser, D. (2001). Copyright in computer-generated works: Whom, if anyone, do we reward? *Duke Law & Technology Review*, *24*.

Gordon, J.-S. (2022). Are superintelligent robots entitled to human rights? *Ratio*, *35*(3), 181–193. https://doi.org/10.1111/rati.12346

Green, L., & Le, V. T. (2022). Holding the Line: Responsibility, Digital Citizenship and the Platforms. In: Flew, T., Martin, F.R. (eds) *Digital Platform Regulation. Palgrave Global Media Policy and Business*. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-030-95220-4_5

Guastavino, M. N., & Mangan, D. (2023). The metaverse matrix of labour law. *Italian Labour Law e-Journal*. https://doi.org/10.6092/issn.1561-8048/17138

Gunkel, D. J. (2024). *Robot rights*. MIT Press.

Haney, B. S. (2018). The perils and promises of artificial general intelligence. *Journal of Legislation*, *45*(2), 151–172. https://doi.org/10.2139/ssrn.3261254

Hassani, H., Huang, X., & Silva, E. (2021). The human digitalisation journey: Technology first at the expense of humans? *Information*, *12*(7), 267. https://doi.org/10.3390/info12070267

Hedrick, A. S. (2019). I "think," therefore I create: Claiming copyright in the outputs of algorithms. *Journal of Intellectual Property and Entertainment Law*, *8*(2), 324–374.

Hertzmann, A. (2018). Can computers create art? *Arts*, *7*(2), 18. https://doi.org/10.3390/arts7020018

Hess, C., & Ostrom, E. (Eds.). (2006). *Understanding knowledge as a commons: From theory to practice*. MIT Press.

Hildebrandt, M. (2020). Legal personhood for AI? In *Law for Computer Scientists and Other Folk* (pp. 237–250). Oxford University Press. https://doi.org/10.1093/oso/9780198860877.003.0009

Hristov, K. (2017). Artificial intelligence and the copyright dilemma. *IDEA: The Journal of the Franklin Pierce for Intellectual Property*, *57*(3), 431–454.

Kamrowska-Załuska, D. (2021). Impact of AI-based tools and urban big data analytics on the design and planning of cities. *Land*, *10*(11), 1209. https://doi.org/10.3390/land10111209

Kim, J., & Im, I. (2023). Anthropomorphic response: Understanding interactions between humans and artificial intelligence agents. *Computers in Human Behavior*, *139*, 107512. https://doi.org/10.1016/j.chb.2022.107512

Kop, M. (2020). AI & Intellectual Property: Towards an articulated public domain. *Texas Intellectual Property Law Journal*, *28*(1), 297–336. https://doi.org/10.2139/ssrn.3409715

Kostenko, O., Furashev, V., Zhuravlov, D., & Dniprov, O. (2022). Genesis of Legal Regulation Web and the Model of the Electronic Jurisdiction of the Metaverse. *Bratislava Law Review*, *6*(2). https://doi.org/10.46282/blr.2022.6.2.316

Kostenko, O., Zhuravlov, D., Dniprov, O., & Korotiuk, O. (2023). Metaverse: Model Criminal Code. *Baltic Journal of Economic Studies*, *9*(4), 134–147. https://doi.org/10.30525/2256-0742/2023-9-4-134-147

Kurki, V. A. J. (2019). *A theory of legal personhood*. Oxford University Press.

Kuzminykh, A., & Rintel, S. (2020). Classification of functional attention in video meetings. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (pp. 1–13). https://doi.org/10.1145/3313831.3376546

Lehdonvirta, V. (2024). *Cloud empires: How digital platforms are overtaking the state and how we can regain control*. MIT Press.

Lemley, M. A., & Casey, B. (2019). Remedies for robots. *University of Chicago Law Review*, *86*, 1311. https://doi.org/10.2139/ssrn.3223621

Lessig, L. (2004). *Free culture: How big media uses technology and the law to lock down culture and control creativity*. Penguin Press.

Mäntymäki, M., Minkkinen, M., Birkstedt, T., & Viljanen, M. (2022). Defining organizational AI governance. *AI and Ethics*, *2*(1), 603–609. https://doi.org/10.1007/s43681-022-00143-x

Marchant, G. E., & Lindor, R. A. (2012). The coming collision between autonomous vehicles and the liability system. *Santa Clara Law Review*, *52*(4), 1321–1340.

McStay, A. (2023). The Metaverse: Surveillant Physics, Virtual Realist Governance, and the Missing Commons. *Philosophy & Technology*, *36, 13*. https://doi.org/10.1007/s13347-023-00613-y

Militsyna, K. (2022). Legal personhood for artificial intelligence: Pro, contra, abstain? *Teisė*, *122*(1), 148–163. https://doi.org/10.15388/teise.2022.122.10

Miller, A. I. (2020). The artist in the machine: The world of AI-powered creativity. MIT Press.

Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. *Big Data & Society*, *3*(2), https://doi.org/10.1177/2053951716679679

Mohseni, S., Wang, H., Yu, Z., Xiao, C., Wang, Z., & Yadawa, J. (2021). Taxonomy of machine learning safety: A survey and primer. *arXiv*. https://doi.org/10.48550/arxiv.2106.04823

Moore, J. (2019). AI for not bad. *Frontiers in Big Data*, *2*. https://doi.org/10.3389/fdata.2019.00032

Nordmoen, J., Veenstra, F., Ellefsen, K. O., & Glette, K. (2021). MAP-Elites enables powerful stepping stones and diversity for modular robotics. *Frontiers in Robotics and AI*, *8*, 639173. https://doi.org/10.3389/frobt.2021.639173

Pagallo, U. (2018). Vital, Sophia, and Co.—The quest for the legal personhood of robots. *Information*, *9*(9), 230. https://doi.org/10.3390/info9090230

Parra Pennefather, P. (2023). AI and the Future of Creative Work. In *Creative Prototyping with Generative AI. Design Thinking* (pp. 387–410). Apress, Berkeley, CA. https://doi.org/10.1007/978-1-4842-9579-3_13

Qin, H. X., Wang, Y., & Hui, P. (2022). Identity, Crimes, and Law Enforcement in the Metaverse. *arXiv*. https://doi.org/10.48550/arxiv.2210.06134

Rachum-Twaig, O. (2020). Whose robot is it anyway?: Liability for artificial-intelligence-based robots. *University of Illinois Law Review*, *2020*(4), 1141–1175.

Ramesh, A., Pavlov, M., Goh, G., Gray, S., Voss, C., Radford, A., Chen, M., & Sutskever, I. (2021). Zero-shot text-to-image generation. *arXiv*. https://doi.org/10.48550/arXiv.2102.12092

Russell, S. (2023). *Human compatible: AI and the problem of control*. Penguin.

Russell, S. J., & Norvig, P. (2021). *Artificial intelligence: A modern approach* (4th ed.). Pearson.

Samek, W., Montavon, G., Lapuschkin, S., Anders, C. J., & Müller, K.-R. (2021). Explaining deep neural networks and beyond: A review of methods and applications. *Proceedings of the IEEE*, *109*(3), 247–278. https://doi.org/10.1109/JPROC.2021.3060483

Schafer, B., Komuves, D., Zatarain, J. M. N., & Diver, L. (2015). A fourth law of robotics? Copyright and the law and ethics of machine co-production. *Artificial Intelligence and Law*, *23*(3), 217–240. https://doi.org/10.1007/s10506-015-9169-7

Scherer, M. U. (2016). Regulating artificial intelligence systems: Risks, challenges, competencies, and strategies. *Harvard Journal of Law & Technology*, *29*(2), 353–400. https://doi.org/10.2139/ssrn.2609777

Selbst, A. D. (2020). Negligence and AI's human users. *Boston University Law Review*, *100*(4), 1315–1376.

Seymour, M., Riemer, K., & Kay, J. (2018). Actors, avatars and agents: Potentials and implications of natural face technology for the creation of realistic visual presence. *Journal of the Association for Information Systems*, *19*(10). https://doi.org/10.17705/1jais.00515

Shirado, H., & Christakis, N. A. (2017). Locally noisy autonomous agents improve global human coordination in network experiments. *Nature*, *545*(7654), 370–374. https://doi.org/10.1038/nature22332

Soares, N., & Fallenstein, B. (2017). Agent foundations for aligning machine intelligence with human interests: a technical research agenda. In V. Callaghan, J. Miller, R. Yampolskiy, & S. Armstrong (Eds.), *The Technological Singularity* (pp. 103–125). Springer. https://doi.org/10.1007/978-3-662-54033-6_5

Solaiman, S. M. (2017). Legal personality of robots, corporations, idols and chimpanzees: A quest for legitimacy. *Artificial Intelligence and Law*, *25*(2), 155–179. https://doi.org/10.1007/s10506-016-9192-3

Soliman, M. M., Ahmed, E., Darwish, A., & Hassanien, A. E. (2024). Artificial intelligence powered Metaverse: Analysis, challenges and future perspectives. *Artificial Intelligence Review*, *57*, 36. https://doi.org/10.1007/s10462-023-10641-x

Sotala, K., & Yampolskiy, R. V. (2015). Responses to catastrophic AGI risk: a survey. Physica Scripta, 90(1), 018001. https://doi.org/10.1088/0031-8949/90/1/018001

Srinivasan, R., & Parikh, D. (2021). Building bridges: Generative artworks to explore AI ethics. *arXiv*. https://doi.org/10.48550/arxiv.2106.13901

Stein, A. L. (2020). Artificial intelligence and climate change. Yale Journal on Regulation, 37, 890–939.

Stix, C., & Maas, M. M. (2021). Bridging the gap: The case for an 'Incompletely Theorized Agreement' on AI policy. *AI and Ethics*, *1*(3), 261–271. https://doi.org/10.1007/s43681-020-00037-w

Sun, J., Gan, W., Chao, H.-C., & Yu, P. S. (2022). Metaverse: Survey, Applications, Security, and Opportunities. *arXiv*. https://doi.org/10.48550/arxiv.2210.07990

Taddeo, M., & Floridi, L. (2018). How AI can be a force for good. *Science*, *361*(6404), 751–752. https://doi.org/10.1126/science.aat5991

Tai, E. T. T. (2018). Liability for (semi)autonomous systems: Robots and algorithms. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3161962

Tegmark, M. (2017). *Life 3.0: Being human in the age of artificial intelligence*. Allen Lane.

Tolmeijer, S., Kneer, M., Sarasua, C., Christen, M., & Bernstein, A. (2020). Implementations in machine ethics: A survey. *ACM Computing Surveys*, *53*(6), 1–38. https://doi.org/10.1145/3419633

Travis, H. (2020). Intelligent entertainment: Shaping policies on the algorithmic generation and regulation of creative works. *FIU Law Review*, *14*, 179–199. https://doi.org/10.2139/ssrn.3726755

Turchin, A., & Denkenberger, D. (2020). Classification of global catastrophic risks connected with artificial intelligence. *AI & Society*, *35*(1), 147–163. https://doi.org/10.1007/s00146-018-0845-5

Turner, C., & Schneider, S. (2020). Could you merge with AI? Reflections on the singularity and radical brain enhancement. In M. D. Dubber, F. Pasquale, & S. Das (Eds.), *The Oxford handbook of ethics of AI* (pp. 307–324). Oxford Academic. https://doi.org/10.1093/oxfordhb/9780190067397.013.19

Turner, J. (2019). *Robot rules: Regulating artificial intelligence*. Palgrave Macmillan.

Tyagi, K. (2023). Deepfakes, copyright and personality rights: An inter-disciplinary perspective. In K. Mathis & A. Tor (Eds.), *Law and economics of the digital transformation. ILEC 2023. Economic analysis of law in European legal scholarship* (Vol. 15, pp. 191–210). Springer, Cham. https://doi.org/10.1007/978-3-031-25059-0_9

van den Hoven van Genderen, R. (2018). Do we need new legal personhood in the age of robots and AI? In *Perspectives in Law, Business and Innovation* (pp. 185–206). Springer Nature. https://doi.org/10.1007/978-981-13-2874-9_2

Vladeck, D. C. (2014). Machines without principals: Liability rules and artificial intelligence. *Washington Law Review*, *89*(1), 117–150.

Wallach, W., & Marchant, G. E. (2019). Toward the agile and comprehensive international governance of AI and robotics. *Proceedings of the IEEE*, *107*(3), 505–508. https://doi.org/10.1109/jproc.2019.2899422

Wolfert, P., Robinson, N., & Belpaeme, T. (2022). A review of evaluation practices of gesture generation in embodied conversational agents. *IEEE Transactions on Human-Machine Systems*, *52*(3), 379–389. https://doi.org/10.1109/THMS.2022.3149173

Wu, H., & Zhang, W. (2023). Digital identity, privacy security, and their legal safeguards in the Metaverse. *Security and Safety*, *2*, 2023011. https://doi.org/10.1051/sands/2023011

Yanisky-Ravid, S., & Velez-Hernandez, L. A. (2018). Copyrightability of artworks produced by creative robots, driven by artificial intelligence systems and the concept of originality: The formality-objective model. *Minnesota Journal of Law, Science & Technology*, *19*(1), 1–53. https://doi.org/10.2139/ssrn.2943778

Yayman, D. (2023). Taxation in Virtual Worlds: Analysis Under United States of America and Turkish Tax Regulations. *Sosyoekonomi*, *31*(55), 211–231. https://doi.org/10.17233/sosyoekonomi.2023.01.11

Zimmermann, D., Wehler, A., & Kaspar, K. (2023). Self-representation through avatars in digital environments. *Current Psychology*, *42*, 21775-21789. https://doi.org/10.1007/s12144-022-03232-6

Сведения об авторе

Бен Честер Чонг – магистр права (Кембридж), преподаватель права, Школа права, Сингапурский университет общественных наук; исследователь, Кембриджский центр по изучению управления окружающей средой, энергетикой и природными ресурсами, кафедра экономики землепользования, Кембриджский университет
Адрес: Сингапур, 599494, г. Сингапур, Клементи Роуд, 463; Великобритания, CB2 3QZ, г. Кембридж, Пемброк Стрит, Девид Аттенборо Билдинг
E-mail: benchestercheong@suss.edu.sg
ORCID ID: https://orcid.org/0000-0002-1026-8292
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57226145674
WoS Researcher ID: https://www.webofscience.com/wos/author/record/3646618
Google Scholar ID: https://scholar.google.com/citations?user=bVHXJt0AAAAJ

Конфликт интересов

Автор сообщает об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.07.45 / Право и научно-технический прогресс
Специальность ВАК: 5.1.3 / Частно-правовые (цивилистические) науки

История статьи

Дата поступления – 31 мая 2024 г.
Дата одобрения после рецензирования – 14 июня 2024 г.
Дата принятия к опубликованию – 13 декабря 2024 г.
Дата онлайн-размещения – 20 декабря 2024 г.

Research article
UDC 34:004:34.096:347.211:004.8
EDN: https://elibrary.ru/shduef
DOI: https://doi.org/10.21202/jdtl.2024.43

The Evolving Role of Copyright Law in the Age of AI-Generated Works

James Hutson
Lindenwood University, Saint Charles, United States

Keywords

artificial intelligence,
copyright,
copyright protection,
digital technologies,
generative artificial intelligence,
intellectual property right,
law,
machine learning technologies,
prompt engineering,
work of art

Abstract

Objective: to identify the prospects and directions of copyright law development associated with the increasing use of generative artificial intelligence.

Methods: the study is based on the formal-legal, comparative, historical methods, doctrinal analysis, legal forecasting and modeling.

Results: the article states that the emergence of generative artificial intelligence makes one rethink the processes occurring in the field of creative activity and the traditional copyright system, which becomes inadequate to modern realities. The author substantiates the necessity of legal reassessment of copyright and emphasizes the urgent need for updated means of copyright protection. Unlike previous digital tools, which expanded human creativity by improving original works, generative artificial intelligence creates content through complex algorithmic processes, blurring the boundaries of authorship and originality. The research shows limitations of existing intellectual property law, as courts deny copyright in works created by artificial intelligence and insist on the need for "human authorship". Such decisions emphasize the contradiction between existing laws and the reality of co-creation involving artificial intelligence. It is argued that taking into account the creative potential of generative artificial intelligence will facilitate the evolution of copyright law towards hybrid approaches, with artificial intelligence as an integral, albeit secondary, tool. It seems promising to create flexible intellectual property standards that give artists the opportunity to restrict or authorize the use of their works as training data for artificial

© Hutson J., 2024

This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (CC BY 4.0) (https://creativecommons.org/licenses/by/4.0), which permits unrestricted re-use, distribution and reproduction, provided the original article is properly cited.

intelligence, as well as ensure that authors retain control over their works included in datasets for training artificial intelligence, in case copyright metadata is integrated into digital works, etc.

Scientific novelty: based on the analysis of the latest judicial precedents, modern international regulations and evolving institutional practices, the author proposes a balanced adaptive approach to copyright reform to ensure the ethical integration of generative artificial intelligence into the creative ecosystem and to develop flexible copyright protection measures that correspond to the rapid technological progress.

Practical significance: the proposed combined approach will allow generative AI tools to become part of the human creative process in the same way that previous generations used digital tools. At the same time, it will contribute to the creation of an environment where the autonomy of authors is respected. This will not only protect the creators of creative content, but also broaden the understanding of creativity as a collaboration with generative artificial intelligence, where artificial intelligence is positioned as a force that complements but not replaces humans in creativity.

For citation

Hutson, J. (2024). The Evolving Role of Copyright Law in the Age of AI-Generated Works. *Journal of Digital Technologies and Law, 2*(4), 886–914. https://doi.org/10.21202/jdtl.2024.43

Content

Introduction
1. Copyright Protection for AI-Generated Works
   1.1. Human Authorship Requirement
   1.2. The Role of Foundational Cases in Establishing Human Input
   1.3. Originality and Fixation in Visual Artworks
   1.4. AI-Assisted Works and Human Creativity
2. Use of Copyrighted Material in AI Training
   2.1. Training Data and Copyright Infringement Concerns
   2.2. Derivative Works and AI-Generated Content
   2.3. International Approaches and Text and Data Mining Exceptions
3. Challenges and Policy Developments
   3.1. Litigation and Legal Precedents
   3.2. International Policy Approaches

4. Towards a Revised Copyright Framework for Generative AI
4.1. Creating Flexible IP Standards
4.2. Reimagining Authorship in AI Co-Creation
Conclusion
References

Introduction

Artificial intelligence (AI) has disrupted creative industries more quickly than any previous emergent technology, providing tools that enable unprecedented levels of content generation and artistic innovation. For instance, ChatGPT, launched by OpenAI in late 2022, quickly set a record as the fastest-adopted technology in history by reaching one million users in just five days, followed by over 100 million monthly active users by January 2023[1]. From generating music and visual art to drafting written content, generative AI (GAI) technologies like Claude, Stable Diffusion, and Runway have expanded the creative landscape, offering both opportunities and legal challenges. Such technologies work by employing machine learning (ML) models that produce new content based on patterns learned from vast datasets (Feuerriegel et al., 2024; Kretschmer et al., 2024). Unlike more traditional tools like cameras or Photoshop, which require direct human input to capture or edit existing content, GAI models are trained on extensive datasets, often containing text, images, and other media, to learn structures, styles, and elements within these media. As such, the «generative» in AI refers to the ability of the model to create entirely new content by combining learned elements in ways that simulate human creativity, rather than simply modifying existing content (Epstein et al., 2023).

For example, Stable Diffusion and Runway generate images by using neural networks trained on large collections of images, where they learn to reproduce certain visual patterns. Given a textual description or prompt, these models can generate new images that match the prompt's specifications. This process, based on diffusion models or transformers, is able to synthesize new visual or text content that might look like a human-made piece but is derived from algorithmic understanding rather than human-originated design or manipulation (Fig. 1) (Moreno et al., 2023). At the same time, creators can use prompt engineering to achieve creative output that more closely aligns to what is intended. The level of control over these tools is thus variable and dependent upon human input in terms of a textual prompt, image, video, or sound clip to generate a new output.

[1] Gordon, C. (2023, February 2) ChatGPT Is The Fastest Growing App In The History Of Web Applications. Forbes. https://clck.ru/3ELfZi

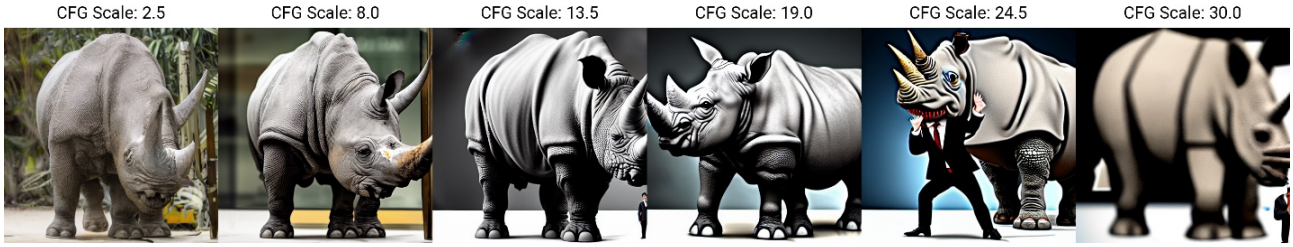


Figure 1. Rhino XY Plot with Different CFG Scale, Stable Diffusion. December 12, 2022. (CC 0)

The variability in human involvement in the creative process is what makes GAI stand apart from other creative tools in that it can function without needing a direct creative act from the user, like taking a photo or designing an image from scratch. Tools like cameras and Photoshop have come to be seen as serving as extensions of human creativity; they depend on the direct actions and decisions of a human. A camera captures real-world images, Photoshop enhances or modifies them, and digital imaging tools edit or create elements from scratch based on user input. But even in these examples, there are levels of human involvement in the creative process. For instance, photography involves deciding what to take a photograph of, perhaps even framing and lighting it and selecting a particular lens. At that point, the tool records and assists in converting (as in the case of digital photography) the captured light into a digital file for output. Additional creative input would then be carried out postproduction in software like Photoshop to further alter the image the machine produced. These and other digital imaging tools can slightly alter the photograph, such as changing the lighting, cropping the image, as well as introduce major alterations like removing subjects or creating new ones before final output physically or digitally for distribution and public consumption (Aaland, 2006; Kelby, 2020).

The levels of human involvement in creation are what is highly contested with GAI, as it is seen to autonomously interpret prompts to output new, algorithmically created content, leveraging its learned representations without replicating specific pieces from its training data (Risi & Togelius, 2020). This ability to create entirely new content – often indistinguishable from human-made works—introduces both opportunities and challenges. While it enables rapid content generation across industries, it also raises legal questions about authorship, copyright, and originality, as AI-generated content often lacks the direct, personal authorship traditionally required for copyright protection (Kibirige, 2024). This disruption of conventional copyright frameworks is primarily due to the historical focus of copyright law on human authorship as essential for intellectual property protection (Ploman & Hamilton, 2024). Given this, traditional copyright structures, rooted in principles of originality and intentional creativity, are struggling

to accommodate works produced or heavily influenced by AI systems, which operate through data-driven algorithms rather than conscious creativity.

A recent example illustrating the copyright complexities in AI use comes from August 12, 2024 in Andersen et al. v. Stability AI Ltd., a case where artists accused Stability AI and other GAI companies of infringing on copyrights by training their models with billions of images sourced online without explicit permission. This lawsuit, currently proceeding through the California courts, represents another example of copyright law grappling with how these tools are trained and produce content. Central to the case are questions around whether these datasets, composed of copyrighted images, can be considered infringing works and, if so, how culpability might be assigned to the companies developing and deploying these AI models (No. 23-cv-00201-WHO (N.D. Cal. Aug. 12, 2024). This development highlights the challenging position of current copyright law, which was not designed to handle data-driven processes like AI. As these platforms rely on vast amounts of data to generate creative outputs, the courts must determine whether the process of using copyrighted works to "train" an AI model constitutes infringement, or, as these companies claim "fair use" given how they were sourced and that the models do not output the works exactly. This case, alongside others involving companies like Meta and OpenAI, underscores the pressing need for updated legal frameworks that can balance intellectual property protections with the rapid advancement of technology (Spica, 2024).

While human creations were initially necessary to train these large models, the involvement of human creators in their output is questioned, especially with regard to medium. The primary issue lies in copyright's foundational requirement for originality, which implies a degree of human intention and creative decision-making. Historically, copyright law, as defined under 17 U.S.C. § 102, requires a "human author" for works to be eligible for copyright, a standard that AI-generated content challenges as these creations lack direct human authorship (Abbott & Rothman, 2023). Recent legal cases, such as Allen v. U.S. Copyright Office (2024) (1:24-cv-2665), further illustrate the legal difficulty in assigning authorship and protection to works that are perceived to have minimal human involvement. In this case, Jason Allen, an artist, sought copyright for his AI-assisted artwork, Théâtre D'opéra Spatial (2022) (Fig. 2), which was created using the GAI tool Midjourney. The U.S. Copyright Office rejected the application, citing insufficient human authorship, a core requirement under U.S. copyright law. Allen argued that his extensive use of prompts constituted a creative process, making him the rightful author. However, the Copyright Office maintained that authorship

and copyright protections require direct human creativity rather than merely guiding an algorithm[2].

Figure 2. Jason M. Allen, Théâtre D'opéra Spatial, 2022. Midjourney (CC 0)

This decision aligns with other recent rulings, such as Thaler v. Perlmutter, where the court ruled that “autonomous creations” by AI are ineligible for copyright since they lack human authorship. The dispute began in August 2019 with A Recent Entrance to Paradise (Fig. 3), an image created autonomously, according to artist Stephen Thaler, using the Creativity Machine. Because the artist maintained that the true author of the work was the machine, he was denied copyright, even though he argued that he owned the device[3]. The case illustrates the difficulties in categorizing AI-generated works under traditional copyright frameworks and signals a need for clear guidelines on the level of human involvement required for copyright eligibility, especially as AI continues to play a more prominent role in creative processes. Moreover, a better understanding

2 Brittain, B. (2024, September 26). Artist sues after US rejects copyright for AI-generated image. Reuters. https://clck.ru/3ELfmr

3 Mathur, A. (2023, December 11). Case Review: Thaler v. Perlmutter (2023). Center for Art Law. https://clck.ru/3ELfnX

of the processes used by creatives when creating content with these tools on the part of lawmakers will inevitably lead to a more nuanced understanding of "autonomous creations."

Figure 3. Stephen Thaler, A Recent Entrance to Paradise, 2023. Creativity Machine (CC 0)

Given these ambiguities, this review article explores how copyright law might evolve to better address the complexities of AI-assisted and AI-generated works, with the goal of supporting both human creators and the burgeoning field of AI innovation. Although the technology can autonomously generate creative content, there are nuanced considerations. First, even with the lack of human authorship in processes with minimal prompting, these tools and resultant content necessitates a re-examination of copyright protections, particularly as they relate to ownership, fair use in training datasets, and authorship rights (Jiang et al., 2023). Second, creatives using AI-assisted technologies should be able to copyright their work given record or demonstration of "significant human contributions". Many artists have met these criteria by documenting their process, showing that they used their own works for training their own models, and continue to mold the final appearance of works post-production (Hutson et al., 2023).

Therefore, a revised copyright framework would include flexible standards for AI-assisted works and AI-generated content that acknowledges both the rights of authors and artists to opt out of their works being used for training, which currently exists, as well as those of the creatives using the AI tools for creative output. Such an approach offers a balanced solution that encourages innovation while respecting traditional notions of creativity and authorship. Ultimately, as creative industries increasingly integrate AI, a legal reevaluation of copyright is essential to ensure that this technology supports human creativity without undermining established intellectual property rights. The task ahead is not only to accommodate the role of AI within copyright law but also to develop protections that respect the distinct contributions of human creators within AI-driven processes. Balancing innovation with intellectual property protections may pave the way for a fair and sustainable future in which AI serves as a tool for human expression rather than as a replacement for it.

1. Copyright Protection for AI-Generated Works

1.1. Human Authorship Requirement

The foundation of copyright law in the United States is human authorship, as specified under 17 U.S.C. § 102. This legal standard requires that works are the result of human creativity, a criterion applied consistently across digital and analog mediums. The legal framework is built on the premise that copyright incentivizes human creators, who possess the originality and personal input necessary to claim ownership. Recent cases such as Allen v. U.S. Copyright Office illustrate the complexity of applying this standard to AI-generated content, where courts have ruled that works created solely by AI lack the human element required for copyright (Kasap, 2021; Bridy, 2016). This requirement reflects the essential "human touch" in copyright, mandating that creative works contain elements of independent, original input, a notion that has remained central to U.S. copyright law despite advancements in technology.

1.2. The Role of Foundational Cases in Establishing Human Input

Landmark cases such as Bridgeman Art Library v. Corel Corp. and Meshwerks, Inc. v. Toyota Motor Sales, U.S.A., Inc. have further reinforced that copyright protection requires human input, particularly in the digital domain. These cases highlighted that digital reproductions or works without substantial human intervention lack originality and are ineligible for copyright. In Bridgeman v. Corel, the court ruled that photographic reproductions of public domain artworks were mere mechanical copies, with insufficient

creative input to warrant copyright protection (Kasap, 2021). This ruling underscores that digital reproductions or AI outputs are not automatically granted copyright unless there is meaningful human creativity involved. These precedents emphasize the need for tangible human input, a standard that AI-generated works challenge due to their reliance on machine learning algorithms that operate with limited human oversight (Burylo, 2022).

Another critical case is Meshwerks v. Toyota, 528 F.3d 1258 (10th Cir. 2008), which involved the creation of digital wireframe models of Toyota vehicles. Meshwerks, a digital design company, created these models for Toyota's marketing materials, but Toyota used them beyond the scope of their agreement, leading to a copyright dispute. The court ruled that Meshwerks' digital wireframe models were not eligible for copyright protection because they were faithful representations of Toyota's cars without any additional creative input or originality. The Meshwerks decision is significant for digital media artists and those using AI tools, as it highlights that mere technical skill in using software to replicate existing objects or works does not meet the standard for copyright protection. Like the earlier Bridgeman case, Meshwerks shows that originality in digital works must come from the creative choices of the human, not the operation of the tool alone.

1.3. Originality and Fixation in Visual Artworks

Visual artworks eligible for copyright protection must meet two criteria: originality and fixation. Originality requires the work to be independently created with minimal creativity, while fixation mandates that it be captured in a tangible medium, as specified by 17 U.S.C. § 102(a). Originality was clarified in cases like Feist Publications, Inc. v. Rural Telephone Service Co., where the U.S. Supreme Court ruled that only a minimal degree of creativity is needed, but mere mechanical processes do not fulfill this requirement (Yu, 2017). This dual requirement for originality and fixation presents challenges for AI-generated works, as the creative role of the human operator is often limited to inputting prompts rather than actively shaping the final output. As a result, purely AI-generated works without sufficient human creative input do not meet these legal thresholds, a standard currently upheld in U.S. copyright law (Hedrick, 2018).

While AI systems are capable of generating visual works, those works must still be fixed in a tangible medium, as required by 17 U.S.C. § 102(a). This fixation may occur in digital formats, such as a file stored on a computer, or in physical formats, such as a printed image. However, fixation alone does not satisfy the requirements for copyright protection; there must be demonstrable human creativity involved in the work's creation. In instances where human and AI collaboration occurs, copyright law may recognize

the human as the sole author, provided the human's input significantly shapes the creative outcome. For example, if a human artist uses AI to generate preliminary designs and then substantially modifies or curates the results, the final work may be considered a product of human authorship, as the artist exercises creative control over the AI-generated content. The Compendium states that if a human "selected or arranged the elements in a sufficiently creative way," the resulting work may be copyrightable (Compendium, § 906.1).

1.4. AI-Assisted Works and Human Creativity

Under U.S. copyright law, AI-assisted works that involve substantial human input may qualify for copyright protection. Copyright law permits protection for human-authored portions of a work, which might include prompt design, selection, and post-processing, while excluding purely machine-generated content. Foundational cases, like Feist Publications, Inc. v. Rural Telephone Service Co., have established that copyright requires a minimal level of creativity, such as arranging factual data in an original way, thus underscoring the necessity of human choice in establishing copyrightable originality (Kasap, 2021). In this regard, human involvement is pivotal: for instance, applying a Photoshop filter alone lacks originality for copyright, but creative decisions about composition, tone, or visual message may cross the threshold into copyrightable material (Burylo, 2022).

The principle of human creativity as a determinant in copyright has also been supported in cases like Mannion v. Coors Brewing Co., which emphasized that copyright requires distinctive creative choices that reflect an author's personal expression. In AI-assisted work, these human decisions could include not only initial prompt design but also subsequent choices about refining or altering generated content, as outlined in recent U.S. Copyright Office guidelines (Horzyk, 2023). These guidelines suggest that, while copyright may apply to AI-assisted works, it will not cover parts that were generated without human-led creative decisions.

Human input continues to serve as the critical factor in copyright eligibility, especially in works generated with AI assistance. The Copyright Office has clarified that AI outputs can be protected if they involve significant human contribution, such as stylistic or structural decisions that shape the final output. Without such human guidance, however, the content is unlikely to meet copyright's originality requirement, as emphasized in the Zarya of the Dawn decision, where AI-generated images were deemed unprotectable without human creativity embedded in the process (Iaia, 2022). Human input can manifest in various forms throughout an AI-aided creative process, from curating datasets to defining prompts and refining outputs. This nuanced distinction between using AI as a mere tool and exercising creative control is critical in determining copyright protection for AI-assisted works (Dimitrova, 2023).

2. Use of Copyrighted Material in AI Training

2.1. Training Data and Copyright Infringement Concerns

GAI models rely on extensive datasets, often incidentally incorporating copyrighted works as part of the training process, to produce high-quality outputs. The practice has raised significant legal questions, as the use of such copyrighted materials may constitute infringement. In the case of Andersen v. Stability AI, artists filed suit, alleging that their work was incorporated into training datasets without permission, thus infringing upon their copyrights. This and similar cases highlight the potential for unauthorized use of copyrighted materials in AI training and have led to calls for clearer legal standards to govern how these systems use copyrighted content (Sobel, 2021).

The widespread adoption of these models has made the legality of using copyrighted material in training datasets a central issue. Legal experts argue that the lack of transparency around the sources used in training could lead to inadvertent violations of copyright, as copyrighted material is often scraped from the internet without explicit authorization. This has prompted both creators and legislators to advocate for frameworks that protect intellectual property without stifling AI innovation (Lucchi, 2023).

In the United States, some argue that the “fair use doctrine” could provide a legal basis for using copyrighted works in training under limited conditions. Fair use generally permits limited use of copyrighted material without permission, particularly when the use is transformative or serves a public benefit. However, critics contend that use of copyrighted datasets is not inherently transformative since the models often replicate stylistic elements from these works rather than creating original content. Courts have yet to fully address whether fair use applies to training datasets, leaving developers to face uncertainty regarding potential liability (Torrance & Tomlinson, 2023). In response to these challenges, some developers have begun entering into licensing agreements with rights holders to avoid infringement claims. Licensing provides a pathway to lawfully use copyrighted materials for AI training, ensuring that creators are compensated and their rights are respected. The approach reflects a broader trend toward regulated use of copyrighted data, with the goal of establishing clearer standards for the industry while protecting the interests of original creators (Samuelson, 2023).

2.2. Derivative Works and AI-Generated Content

Under 17 U.S.C. § 101, a derivative work is one that is based on or transforms existing works into a new creation. In the context of AI, this concept is highly relevant, especially when AI-generated content closely resembles the original training data. When a human artist makes significant modifications to an AI-generated output, such as adding new elements or altering its style, the resulting work may qualify as a derivative under copyright law. This status would grant the modified work copyright protection, contingent on the originality introduced by human intervention (Gervais, 2022).

The notion of derivative works emphasizes the importance of human creativity in copyright law. If an AI system generates a piece based on copyrighted material and a human creatively adapts or transforms this output, the final product may attain copyright protection for the human-authored elements. This distinction is key for AI users seeking copyright for modified AI outputs, as it requires the human to make substantial, original contributions beyond the AI's initial generation (Henderson et al., 2023).

For copyright protection to apply to an AI-assisted derivative work, the human contribution must meet the originality standard. This threshold, as defined in Feist Publications, Inc. v. Rural Telephone Service Co., demands a minimal degree of creativity, sufficient to distinguish the work from mere reproduction. In AI contexts, this could mean selecting unique outputs, modifying them to convey distinct messages, or incorporating personal style elements. This threshold underscores that originality is a fundamental requirement for copyright, ensuring that only works with human input are eligible (Wagh et al., 2023).

2.3. International Approaches and Text and Data Mining Exceptions

In Europe, the text and data mining exception under the EU Directive on Copyright in the Digital Single Market offers a distinct approach, allowing copyrighted materials to be used in AI training for research and non-commercial purposes, provided certain conditions are met. This exception enables AI developers to use copyrighted materials without infringing, as long as rights holders have not explicitly opted out. This approach contrasts with the U.S. reliance on fair use and highlights how international copyright standards can vary widely, creating challenges for AI systems that operate across borders (Sobel, 2021).

Ongoing litigation, such as in the Andersen v. Stability AI case, has the potential to reshape copyright law as it applies to AI. A decision requiring developers to obtain explicit licenses for training data could impose substantial financial and logistical burdens on AI companies, potentially slowing the field's growth. Conversely, rulings favoring fair use for AI training data could diminish the protections afforded to copyrighted works, raising concerns among creators about lost revenue and unlicensed usage. The outcomes of these cases will likely influence legislative efforts to refine copyright law in relation to AI and generative models (McCann, 2021). The debate over AI's use of copyrighted data brings into focus the tension between protecting creators' rights and fostering technological innovation. Legal scholars argue that copyright law should evolve to accommodate the unique needs of AI without compromising the intellectual property rights of original creators. Proposals include establishing clearer standards for derivative works, creating specific AI licensing frameworks, and revisiting fair use to ensure it addresses the challenges posed by AI-driven content generation (Elkin-Koren et al., 2023).

3. Challenges and Policy Developments

3.1. Litigation and Legal Precedents

Active litigation surrounding the use of copyrighted material by models illustrates the rising legal challenges in GAI and copyright law. For instance, class-action lawsuits such as Andersen v. Stability AI have brought attention to the unlicensed use of copyrighted materials in training datasets, where plaintiffs allege that AI companies exploited artist work without permission. These cases could set important precedents, as they involve large datasets often scraped from the internet, raising questions about ownership and licensing requirements for training purposes. As courts examine these issues, the rulings could shape future guidelines on permissible training practices in terms of copyright (Samuelson, 2023).

Legal precedent plays a significant role in setting standards for how AI may engage with copyrighted content. Court decisions in cases like Allen v. U.S. Copyright Office and Bridgeman v. Corel emphasize the necessity of human authorship for copyright eligibility, framing this requirement as essential in AI-generated works. These cases demonstrate that, without substantive human input, copyright protections cannot be extended to AI-created content. This legal approach reinforces the originality requirement in copyright law and highlights the limitations of protecting works that emerge solely from automated processes (James, 2024).

The outcomes of these lawsuits are already influencing legislative discussions on the need for transparency in model training and data usage. For example, transparency measures are being proposed to require developers to disclose data sources used in training, which would enhance accountability and provide creators with greater control over their works. Some lawmakers suggest that clearer guidelines are needed to protect both creator rights and support innovation, highlighting the delicate balance policymakers must strike to address these complex issues (Mensah, 2023).

Further, the emphasis of the courts on human creativity as essential for copyright has encouraged proposals to create specific regulations for AI-generated works that involve minimal human input. These proposals aim to distinguish between fully AI-generated content and AI-assisted works where human decisions significantly shape the output. If adopted, such guidelines would provide clearer boundaries, helping creators, AI developers, and copyright authorities navigate copyright claims more effectively. As legal decisions continue to accumulate, they serve as a basis for creating more definitive copyright policies around AI's role in creative processes (Atilla, 2024).

3.2. International Policy Approaches

The approach to AI and copyright varies widely across jurisdictions, reflecting different legal traditions and attitudes toward intellectual property. The European Union has adopted a text and data mining exception in its Copyright Directive, permitting the use of copyrighted content for AI training in specific, mainly non-commercial, contexts. This approach contrasts with that of the United States, where fair use provides the primary legal avenue for developers to access copyrighted materials, albeit with ongoing debates about its adequacy. These differences highlight the complexities of establishing a unified global framework for AI and copyright (Kretschmer et al., 2024). Moreover, United Kingdom copyright law has not embraced the U.S. model of fair use and instead follows a fair dealing approach, which limits the scope of copyright exceptions. Recent discussions in the U.K. have suggested a potential shift toward a more flexible system that could accommodate AI innovations, similar to the EU's text and data mining provisions. Such an adaptation would align the U.K. more closely with EU policies, offering a balanced framework that allows limited AI access to copyrighted content under regulated circumstances (Ploman & Hamilton, 2024).

For creators, international disparities in copyright policy present significant challenges in protecting rights across different jurisdictions. As these systems operate globally, the lack of consistent copyright standards creates uncertainties, with works potentially being protected in one country but vulnerable to unlicensed use in another. Creators

face the task of navigating these cross-border legal discrepancies, often relying on local licensing strategies or technology-based solutions like blockchain to monitor the use of their works internationally (Mia et al., 2023). Blockchain technology is one solution that has been proposed to facilitate international copyright protection for digital content. By creating immutable records of ownership and licensing terms, blockchain could provide creators with a means of tracking their works across borders. While this technology holds promise, it requires substantial legal adjustments to become viable on a large scale, as copyright policies in many jurisdictions do not yet support blockchain-based protections (Bonnet & Teuteberg, 2023).

Moving forward, policymakers face the challenge of balancing copyright protections with the need for innovation in AI and digital content. The discussions in regions like the EU, U.S., and U.K. highlight the need for policy frameworks that can adapt to evolving technologies while respecting creators' rights. As applications continue to expand, policy developments must address issues such as transparency, fair compensation, and international cooperation to establish effective copyright protections in a digital age. These ongoing policy discussions and legislative updates signal an incremental approach to copyright reform, one that aims to establish adaptable protections that keep pace with rapid technological advancements.

4. Towards a Revised Copyright Framework for Generative AI

4.1. Creating Flexible IP Standards

With the rapid integration of AI in creative fields, the need for flexible intellectual property (IP) standards has become increasingly evident. Creative Commons (CC) licensing is a flexible copyright framework that allows creators to grant permission to others to use, share, and build upon their work while retaining some rights. Originally developed to encourage the open sharing of knowledge and creativity, CC licenses offer a range of options for creators who want to maintain control over how their works are used without the need for traditional copyright restrictions. CC licenses range from the most permissive, which allows users to freely distribute and modify the work, to more restrictive options, which limit usage, distribution, and adaptation (Longpre et al., 2023).

The key feature of CC licensing is its adaptability; it allows creators to customize the level of protection and freedom associated with their works. The licenses typically include several core components:

1. Attribution (BY): This requires users to credit the creator when sharing or using the work.

2. Non-Commercial (NC): This restricts the work's use to non-commercial purposes only, protecting the creator's right to monetize their work in other contexts.

3. No Derivatives (ND): This prohibits users from modifying the work, ensuring that it remains in its original form.

4. Share Alike (SA): This allows users to distribute adaptations of the work under the same license terms as the original, encouraging a similar level of openness for any derivative works.

These modular options provide creators with a clear way to communicate how their work can be used, reducing legal ambiguity. Each CC license option is straightforward and legally binding, and the licenses are globally recognized, making them effective across borders.

In the context of AI, a Creative Commons-style licensing model for training data could introduce an «opt-in» or «opt-out» feature that allows creators to specify whether their work can be used to train models. This proposed framework could help address copyright issues by establishing clear permissions for datasets. For instance, a creator could apply a "Non-Commercial" restriction to prevent their work from being used for profit-generating AI applications or require "Attribution" to maintain recognition for their contribution. By providing AI developers with unambiguous permissions through this standardized system, CC-style licensing could help mitigate risks of unauthorized use, ensuring that the rights of creators are respected in an AI-driven environment.

Another potential solution to the copyright issues facing creatives is the use of metadata. Metadata, often described as «data about data,» consists of descriptive information embedded within digital files to convey details about their content, ownership, and usage rights. Metadata typically includes fields such as the creator's name, date of creation, copyright status, licensing terms, and permissible uses, making it a powerful tool for copyright management (Majumdar et al., 2023). This embedded information travels with the digital work across various platforms, providing a persistent record that can inform users—and even automated systems – about the work's legal and usage status.

In digital rights management (DRM) and content distribution, metadata plays an essential role in making copyright and licensing terms transparent and enforceable. By embedding copyright data directly in files, creators and rights holders can establish the boundaries of usage without relying solely on external copyright notices. For example, when someone opens or attempts to modify a digitally protected work, metadata can serve as a built-in reference to the terms under which the content can be used or modified. This system of rights metadata is already widely applied in industries like publishing and photography, where tracking rights across multiple formats, platforms, and users is critical (Pellegrini, 2023).

In the context of AI, embedding rights metadata could serve as a powerful tool for regulating the use of copyrighted content within training datasets. Since AI models often learn from vast datasets that include text, images, or audio, metadata can function as a safeguard, informing the AI system of specific limitations. For instance, metadata within an image file could include a restriction against commercial use, signaling to AI developers or end-users that the content cannot be monetized without additional permissions. If standardized across datasets, this rights metadata could be integrated into AI training workflows, where algorithms could detect metadata fields and filter out restricted content, reducing the risk of unauthorized use.

Applying metadata to AI would ideally involve a standardized metadata schema designed for content used in AI systems. Such a schema could include fields specifically for AI usage, such as «Permitted for AI Training» or «Not for Derivative AI Works,» enabling creators to specify whether and how their work may contribute to AI-generated content. This would provide transparency and accountability in AI data curation, allowing creators to choose how their works contribute to AI training while preserving the integrity of copyright laws. Furthermore, metadata could support traceability in AI outputs, where systems could flag content generated from datasets with specific usage rights, ensuring that any derivative works respect the original terms. This approach would be beneficial in legal contexts, as it enables compliance with copyright standards while supporting a responsible AI development model that acknowledges and respects intellectual property rights.

4.2. Reimagining Authorship in AI Co-Creation

The Zarya of the Dawn (2022) (Fig. 5) case offers a critical illustration of the evolving stance of copyright law on AI-generated content and the importance of human input in determining copyright eligibility. This AI-assisted graphic novel, created by Kris Kashtanova, initially faced rejection by the U.S. Copyright Office, which argued that the images generated through MidJourney lacked sufficient human creativity to qualify for copyright. However, copyright protection was granted for the human-authored narrative and the comic's overall structure, highlighting the distinction between purely AI-generated components and human-crafted elements. The Copyright Office emphasized that copyright law, as per 17 U.S.C. § 102, requires original authorship, which AI alone cannot fulfill. This decision demonstrates the Office's commitment to preserving human creativity as central to copyright, underscoring that meaningful human input is essential for legal recognition (Klukosky & Kohel, 2024).

Figure 5. Kris Kashtanova, Zarya of the Dawn Cover, Comic Book, 2022. (CC 0).

Given the current state of copyright and that GAI tools, like MidJourney and DALL-E, provide unprecedented capabilities for producing artwork, the fact that human-guided prompts and creative direction are required for the creation of copyrightable work should be foregrounded. These tools operate by synthesizing outputs based on vast datasets and algorithmic patterns, which means that, legally, they function as extensions of human intention rather than independent creators. This approach aligns with past legal precedents, such as Feist Publications and Meshwerks, which established that originality stems from human creative effort, not mechanical reproduction. Consequently, the level of human involvement in guiding the output is crucial to determining the copyright eligibility of AI-assisted works (Militsyna, 2023).

Therefore, establishing copyright for AI-generated works hinges on various types of human input that demonstrate originality and creative decision-making, essential components in copyright law (Table 1). The design of prompts, for example, is a critical and foundational element of human involvement in the creation of AI-generated art. Through detailed instructions that specify style, composition, and thematic focus, the human creator provides a conceptual framework that the AI tool then executes. This process aligns with the principles illustrated in Mannion v. Coors Brewing Co., where the court recognized that creative choices, such as lighting and framing, imbue photographs with the originality necessary for copyright. Similarly, a thoughtfully crafted prompt reflects the unique creative vision of the human user, positioning the output for copyright eligibility by showcasing the human's contribution to the artistic process (Burylo, 2022).

Type of Human Input	Description	Legal Parallel
Creative Prompt Design	Human input in designing detailed prompts (e.g., artistic style, composition, theme) provides the conceptual framework for AI outputs, reflecting human creativity and intention.	Mannion v. Coors Brewing Co.: The court recognized that creative choices like lighting and framing can imbue works with originality.
Selection and Curation of Outputs	Selecting specific AI-generated outputs from multiple options involves subjective choice, aligning with the creator's artistic vision, akin to a photographer's decision in choosing final shots.	Garcia v. Google, Inc.: Emphasized control over the final work as essential for authorship.
Post-Processing and Refinement	Enhancing or modifying AI-generated images by adjusting colors, altering compositions, or adding elements introduces a unique creative layer, transforming the output into a derivative work that reflects human creativity.	Meshwerks, Inc. v. Toyota Motor Sales, U.S.A., Inc.: Found that substantial alterations can imbue reproductions with originality.
Conceptual Framework and Artistic Intent	The overarching artistic vision and themes (e.g., social commentary, aesthetics) introduced by the human creator shape the essence of the final work, signifying originality.	Feist Publications, Inc. v. Rural Telephone Service Co.: Reinforced the originality requirement, emphasizing creativity and intent.
Human Authorship Threshold	The extent of human involvement, including textual and narrative elements, determines copyright eligibility, as shown in cases where AI-generated content alone was deemed insufficient.	Zarya of the Dawn decision by the U.S. Copyright Office: Granted copyright for human-authored narrative but not AI-generated images lacking human intervention.
Derivative Work Creation	Transforming AI outputs through creative adjustments aligns with the principles of originality, as copyright protection can extend to derivative works if human contributions are substantial.	17 U.S.C. § 101: Defines derivative works as those that transform or build upon preexisting materials through creative additions.

The process of selecting and curating outputs from multiple AI-generated options is another key indicator of human authorship. Much like photographers who sift through numerous shots to find those that best align with their artistic intent, the act of choosing specific AI outputs from a set of generated possibilities adds an additional layer of creative discretion. This curatorial decision-making is integral to shaping the final work and represents the creator's unique artistic vision, further substantiating a claim for copyright. By selecting one version over another, the creator exercises subjective judgment, aligning the work with a particular vision and highlighting the indispensable role of human choice (Wan & Lu, 2021).

Moreover, post-processing and refinement contribute significantly to establishing copyright eligibility. When creators modify AI-generated images by enhancing elements, adjusting color schemes, or altering compositions, they introduce new creative dimensions that elevate the work beyond a simple automated output. This form of human intervention parallels the precedent set in Meshwerks, where the court noted that substantial alterations could imbue digital reproductions with originality. In the context of AI,

extensive post-processing transforms the generated content into a derivative work that bears the imprint of human creativity, justifying copyright protection and emphasizing the human's essential role in the creative transformation (Geiger, 2024).

Beyond these technical inputs, the overarching conceptual framework and artistic intent that guide the use of AI tools are fundamental to establishing authorship. Whether AI tools are employed to explore complex social themes, convey specific messages, or embody particular aesthetic philosophies, it is the human creator's vision that ultimately shapes the work's essence. This concept aligns closely with the insights from Mannion, where the court recognized the photographer's creative decisions as key to the work's copyrightability. In AI-generated art, the human's intent and philosophical direction help align the work with the originality requirement in copyright law, reinforcing the idea that AI is a tool serving the human creator's broader artistic purpose (Kasap, 2021).

Each of these types of human input reflects a spectrum of creative involvement that distinguishes AI-assisted works from mere algorithmic outputs. From the specificity of prompts to selective curation, extensive post-processing, and thematic direction, these elements underscore that meaningful human creativity remains central to copyright claims in the age of AI. As AI technology becomes more sophisticated, the consistent need for substantial human input will continue to be the cornerstone of copyright eligibility, maintaining a balance between technological innovation and the recognition of human authorship.

These diverse types of human input suggest that AI should be understood as a tool extending, rather than replacing, human creativity. As the Compendium of U.S. Copyright Office Practices indicates, human intervention must be significant to meet the originality standard required by copyright law. This principle reinforces the Copyright Office's stance in Zarya of the Dawn and aligns with 17 U.S.C. § 102, which stresses human authorship. The future of copyright in AI contexts will likely continue emphasizing whether the human's input is creatively substantial enough to meet the threshold of originality (Fenwick & Jurcys, 2023).

For artists using AI tools, certain best practices can strengthen copyright claims. First, detailed prompt design that showcases originality and creativity can establish human authorship. Second, curating and selecting outputs from AI-generated options reflects artistic judgment, further supporting copyright eligibility. Third, engaging in significant post-processing transforms the AI's output into a derivative work, emphasizing human contribution. Lastly, ensuring a coherent conceptual framework guided by the artist's intent further reinforces copyright eligibility, establishing that the AI is simply a sophisticated tool rather than an independent creator. With these considerations,

a potential revision to copyright frameworks could establish a new category recognizing AI-assisted works as co-creations. By defining AI as a contributory tool, rather than an autonomous creator, copyright law could adapt to acknowledge both the artist's and the AI's role. This approach respects human creativity while allowing room for AI's capabilities, ensuring that copyright law remains relevant in an increasingly AI-integrated creative landscape.

Conclusion

As the presence of AI across creative domains expands, a new legal framework is needed to balance innovation with the protection of human authorship. Current copyright structures, largely designed around traditional concepts of human creativity, face challenges in addressing AI-generated works. A revised legal framework could potentially accommodate the unique capabilities of AI while upholding core principles of copyright, emphasizing that human creativity remains essential for authorship. Proposals suggest an adaptive model of copyright that allows AI to support human creativity without granting AI itself copyright protection (Geiger, 2024). In shaping this framework, policymakers must navigate the delicate balance between fostering technological innovation and ensuring creators retain control over their intellectual property. As AI systems become increasingly autonomous, the need for transparency, ethical standards, and rights protections will grow. A balanced approach could involve creating a legal category for human-AI collaborative works, acknowledging AI as a tool while protecting the human's central role in creative direction.

For future human-AI collaborations, evolving AI capabilities suggest a gradual shift in the amount and type of human input required to achieve copyright protection. AI technology may continue to automate aspects of creative production, yet the legal framework will likely emphasize human contribution as fundamental to originality. Recognizing AI as a co-creator under strict guidelines may help define a new model of authorship where AI assists but does not replace human innovation. Practical implications for copyright law involve reinforcing the human element in creative processes. AI may generate complex outputs, but copyright eligibility should rely on demonstrable human input. Adopting criteria for meaningful human input, such as creative prompts or post-processing, may serve as a foundation for determining authorship and protecting artists' rights in an AI-integrated world.

This evolving legal landscape also carries ethical implications. Embracing AI as a creative tool promotes a model of sustainable co-creation, wherein AI extends human creativity rather than competes with it. By embedding transparency and fairness

into copyright policies, lawmakers can protect individual rights while encouraging responsible AI use in creative fields. Ultimately, balancing protection and innovation in the AI era requires both flexibility and consistency in legal standards. Copyright law must evolve to reflect the transformative potential of AI while reinforcing the human-centered principles at its core. Through legal reforms, the creative industry can benefit from AI advancements without undermining the foundational role of human authorship.

References

Aaland, M. (2006). *Photoshop Elements 3 Solutions: The Art of Digital Photography*. John Wiley & Sons.

Abbott, R., & Rothman, E. (2023). Disrupting creativity: Copyright law in the age of generative artificial intelligence. *Florida Law Review*, *75*, 1141–1201.

Atilla, S. (2024). Dealing with AI-generated works: lessons from the CDPA section 9 (3). *Journal of Intellectual Property Law and Practice*, *19*(1), 43–54. https://doi.org/10.1093/jiplp/jpad102

Bonnet, S., & Teuteberg, F. (2023). Impact of blockchain and distributed ledger technology for the management of the intellectual property life cycle: A multiple case study analysis. *Computers in Industry*, *144*, 103789. https://doi.org/10.1016/j.compind.2022.103789

Bridy, A. (2016). The Evolution of Authorship: Work Made by Code. *Columbia Journal of Law and the Arts*, *39*, 395–401. https://doi.org/10.7916/D8CV4J6W

Burylo, Y. (2022). AI generated works and copyright protection. *Entrepreneurship, Economy and Law*, *3*, 7–13. https://doi.org/10.32849/2663-5313/2022.3.01

Dimitrova, R. (2023). Are AI-Assisted Works Copyrightable? In *2023 International Scientific Conference on Computer Science (COMSCI)*, Sozopol, Bulgaria (pp. 1–4). https://doi.org/10.1109/COMSCI59259.2023.10315917

Elkin-Koren, N., Hacohen, U., Livni, R., & Moran, S. (2023). Can Copyright be Reduced to Privacy? ArXiv, 2305.14822. https://doi.org/10.48550/arXiv.2305.14822

Epstein, Z., Hertzmann, A., Akten, M., Farid, H., Fjeld, J., Frank, M. R., Groh, M., Herman, L., Leach, N., Mahari, R., Pentland, A. "Sandy", Russakovsky, O., Schroeder, H., & Smith, A. (2023). Art and the science of generative AI. *Science*, *380*(6650), 1110–1111. https://doi.org/10.1126/science.adh4451

Fenwick, M., & Jurcys, P. (2023, February 11). *Originality and the future of copyright in an age of generative AI*.

Feuerriegel, S., Hartmann, J., Janiesch, C., & Zschech, P. (2024). Generative AI. *Business & Information Systems Engineering*, *66*(1), 111–126. https://doi.org/10.1007/s12599-023-00834-7

Geiger, C. (2024). Elaborating a Human Rights friendly Copyright Framework for Generative AI. *International Review for Intellectual Property and Competition Law*, *55*(7), 1129–1165. https://doi.org/10.2139/ssrn.4634992

Gervais, D. (2022). AI Derivatives: the Application to the Derivative Work Right to Literary and Artistic Productions of AI Machines. *Seton Hall Law Review*, *53*. 1111–1136. https://doi.org/10.2139/ssrn.4022665

Hedrick, S. F. (2018). I "think," therefore I create: claiming copyright in the outputs of algorithms. *NYU Journal of Intellectual Property & Entreprenurial Law*, 8(2), 324–375.

Henderson, P., Li, X., Jurafsky, D., Hashimoto, T., Lemley, M., & Liang, P. (2023). Foundation Models and Fair Use. ArXiv, 2303.15715. https://doi.org/10.48550/arXiv.2303.15715

Horzyk, A. (2023). How AI Affects Our Understanding of Musical Works That Should Be Protected by Copyright. In *2023 International Joint Conference on Neural Networks (IJCNN)*, Gold Coast, Australia (pp. 1–8). https://doi.org/10.1109/IJCNN54540.2023.10191524

Hutson, J., Lively, J., Robertson, B., Cotroneo, P., & Lang, M. (2023). Expanding Horizons: AI Tools and Workflows in Art Practice. In *Creative Convergence: The AI Renaissance in Art and Design* (pp. 101–132). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-45127-0_5

Iaia, V. (2022). To Be, or Not to Be … Original Under Copyright Law, That Is (One of) the Main Questions Concerning AI-Produced Works. *GRUR International*, *71*(9), 793–812. https://doi.org/10.1093/grurint/ikac087

James, T. B. (2024). Artificial Intelligence, Copyright Registration, and the Rule of Doubt. *Texas A&M Law Review Arguendo*, *12*(1), 20–31. https://doi.org/10.37419/lr.v12.arg.2

Jiang, H. H., Brown, L., Cheng, J., Khan, M., Gupta, A., Workman, D., & Gebru, T. (2023). AI Art and its Impact on Artists. In Proceedings of the 2023 AAAI/ACM Conference on AI, Ethics, and Society (pp. 363–374). https://doi.org/10.1145/3600211.3604681

Kasap, A. (2021). Copyright and creative artificial intelligence (AI) systems: A twenty-first century approach to authorship of AI-generated works in the United States. *Wake Forest Journal of Business & Intellectual Property Law*, *19*(4), 335–380. https://doi.org/10.31235/osf.io/gnyha

Kelby, S. (2020). *The digital photography book. Rocky Nook*. Inc.

Kibirige, H. (2024). The delving conundrum of intellectual property rights in the transformative era of artificial intelligence. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4841535

Klukosky, F. P., & Kohel, M. D. (2024). An Update on the State of Play with Generative Artificial Intelligence and Intellectual Property Issues. *Intellectual Property Litigation*, *34*(1), 10–17.

Kretschmer, M., Margoni, T., & Oruç, P. (2024). Copyright law and the lifecycle of machine learning models. IIC-International Review of Intellectual Property and Competition Law, 55(1), 110–138. https://doi.org/10.1007/s40319-023-01419-3

Longpre, S., Mahari, R., Chen, A., Obeng-Marnu, N., Sileo, D., Brannon, W., Muennighoff, N., Khazam, N., Kabbara, J., Perisetla, K., Wu, X., Shippole, E., Bollacker, K., Wu, T., Villa, L., Pentland, S., & Hooker, S. (2023). The data provenance initiative: A large scale audit of dataset licensing & attribution in AI. arXiv, 2310.16787. https://doi.org/10.48550/arXiv.2310.16787

Lucchi, N. (2023). ChatGPT: A Case Study on Copyright Challenges for Generative Artificial Intelligence Systems. *European Journal of Risk Regulation*. https://doi.org/10.1017/err.2023.59

Majumdar, S., Paul, S., Paul, D., Bandyopadhyay, A., Chattopadhyay, S., Das, P. P., & Majumder, P. (2023). Generative AI for software metadata: Overview of the information retrieval in software engineering track at FIRE 2023. arXiv, 2311.03374. https://doi.org/10.48550/arXiv.2311.03374

McCann, S. (2021). Copyright Throughout a Creative AI Pipeline. *Canadian JL & Tech*, *19*(1), 109–139. https://doi.org/10.2139/ssrn.3893972

Mensah, G. B. (2023). *Artificial intelligence and ethics: a comprehensive review of bias mitigation, transparency, and accountability in AI Systems*. Preprint, November, 10. https://doi.org/10.13140/RG.2.2.23381.19685/1

Mia, M., Wessels, J., & Adam, S. (2023). The Use of Blockchain Technology to Improve Transfer-Pricing Compliance and Administration in South Africa. In *ICABR Conference* (pp. 357–378). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-46177-4_20

Militsyna, K. (2023). Human Creative Contribution to AI-Based Output – One Just Can('t) Get Enough. *GRUR International*, *72*(10), 939–949. https://doi.org/10.1093/grurint/ikad075

Moreno, H., Gómez, A., Altares-López, S., Ribeiro, A., & Andújar, D. (2023). Analysis of Stable Diffusion-derived fake weeds performance for training Convolutional Neural Networks. *Computers and Electronics in Agriculture*, *214*, 108324. https://doi.org/10.1016/j.compag.2023.108324

Pellegrini, T. (2023). Digital Rights Management – Technologies, Application Areas, and Governance. In *Handbook of Media and Communication Economics: A European Perspective* (pp. 1–17). Wiesbaden: Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-34048-3_79-2

Ploman, E. W., & Hamilton, L. C. (2024). *Copyright: Intellectual property in the information age*. Taylor & Francis. https://doi.org/10.4324/9781003519973

Risi, S., & Togelius, J. (2020). Increasing generality in machine learning through procedural content generation. *Nature Machine Intelligence*, *2*(8), 428–436. https://doi.org/10.1038/s42256-020-0208-z

Samuelson, P. (2023). Generative AI meets copyright. *Science*, *381*(6654), 158–161. https://doi.org/10.1126/science.adi0656

Sobel, B. (2021). A Taxonomy of Training Data. In R. Hilty, J.-A. Lee, & K.-Ch. Liu (Eds.). *Artificial Intelligence and Intellectual Property*. Oxford University Press. https://doi.org/10.1093/oso/9780198870944.003.0011

Spica, E. (2024). Public Interest, the True Soul: Copyright's Fair Use Doctrine and the Use of Copyrighted Works to Train Generative AI Tools. *Texas Intellectual Property Law Journal*, *33*(1), 67–91.

Torrance, A., & Tomlinson, B. (2023). Training Is Everything: Artificial Intelligence, Copyright, and Fair Training. ArXiv, 2305.03720. https://doi.org/10.48550/arXiv.2305.03720

Wagh, S., Peerzada, D., & Rote, P. (2023). AI And Copyright. *Tuijin Jishu/Journal of Propulsion Technology*, *44*(3), 3431–3439. https://doi.org/10.52783/tjjpt.v44.i3.2053

Wan, Y., & Lu, H. (2021). Copyright protection for AI-generated outputs: The experience from China. *Computer Law & Security Review*, 42, 105581. https://doi.org/10.1016/J.CLSR.2021.105581

Yu, R. (2017). The Machine Author: What Level of Copyright Protection Is Appropriate for Fully Independent Computer-Generated Works? *University of Pennsylvania Law Review*, *165*, 1245–1270.

Author information

James Hutson – Ph.D., Lead XR Disruptor; Professor and Department Head of Art History, AI, and Visual Culture, College of Arts and Humanities, Lindenwood University
Address: 209 S. Kingshighway St, MO 63301, Saint Charles, United States
E-mail: jhutson@lindenwood.edu
ORCID ID: https://orcid.org/0000-0002-0578-6052
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57797793000
WoS Researcher ID: https://www.webofscience.com/wos/author/record/38589773
Google Scholar ID: https://scholar.google.com/citations?user=CaXrV38AAAAJ

Conflict of interests

The author declare no conflict of interests.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law
PASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – October 29, 2024
Date of approval – November 10, 2024
Date of acceptance – December 13, 2024
Date of online placement – December 20, 2024

Научная статья
УДК 34:004:34.096:347.211:004.8
EDN: https://elibrary.ru/shduef
DOI: https://doi.org/10.21202/jdtl.2024.43

Эволюция роли авторского права в эпоху произведений, созданных искусственным интеллектом

Джеймс Хатсон

Линденвудский университет, Сент-Чарльз, США

Ключевые слова

авторское право,
генеративный,
искусственный интеллект,
защита авторских прав,
искусственный интеллект,
право,
право интеллектуальной собственности,
произведение,
промпт-инжиниринг,
технологии машинного обучения,
цифровые технологии

Аннотация

Цель: выявить перспективы и направления развития авторского права, сопряженного с расширяющимся использованием генеративного искусственного интеллекта.

Методы: исследование базируется на применении формально-юридического, компаративного, исторического методов, доктринального анализа, юридического прогнозирования и моделирования.

Результаты: в статье отмечено, что появление генеративного искусственного интеллекта заставляет переосмыслить процессы, происходящие в области творческой деятельности, и традиционную систему авторского права, которая становится неадекватной современным реалиям. Обосновывается необходимость юридической переоценки авторского права. Подчеркивается острая необходимость в обновленных средствах защиты авторских прав. В отличие от прежних цифровых инструментов, которые расширяли творческие возможности человека посредством улучшения его авторских произведений, генеративный искусственный интеллект создает контент с помощью сложных алгоритмических процессов, размывая границы авторства и оригинальности. Показана ограниченность существующего законодательства об интеллектуальной собственности, поскольку суды отказывают в авторских правах на произведения, созданные искусственным интеллектом, и настаивают на необходимости «авторства человека». Такие решения подчеркивают противоречие между существующими законами и реальностью совместного творчества с участием искусственного интеллекта. Утверждается, что учет творческого потенциала генеративного искусственного интеллекта будет способствовать эволюционированию авторского права в сторону комбинированных подходов, когда искусственный интеллект выступает в качестве неотъемлемого, хотя и второстепенного, инструмента. Перспективным видится создание гибких стандартов интеллектуальной собственности, которые предоставляют творческим работникам возможность ограничить или разрешить

© Хатсон Дж., 2024

Статья находится в открытом доступе и распространяется в соответствии с лицензией Creative Commons «Attribution» («Атрибуция») 4.0 Всемирная (CC BY 4.0) (https://creativecommons.org/licenses/by/4.0/deed.ru), позволяющей неограниченно использовать, распространять и воспроизводить материал при условии, что оригинальная работа упомянута с соблюдением правил цитирования.

использование своих работ в качестве обучающих данных для искусственного интеллекта, а также обеспечивают авторам сохранение контроля над своими работами, включенными в базы данных для обучения искусственного интеллекта, в случае если метаданные о наличии авторских прав интегрированы в цифровые произведения, и др.

Научная новизна: на основе анализа новейших судебных прецедентов, современного опыта международного регулирования и развивающейся институциональной практики предлагается сбалансированный адаптивный подход к реформированию авторского права, обеспечивающий этическую интеграцию генеративного искусственного интеллекта в творческую экосистему и направленный на выработку гибких мер защиты авторского права, соответствующих быстрому прогрессу технологий.

Практическая значимость: предложенный комбинированный подход позволит инструментам генеративного искусственного интеллекта стать частью творческого процесса человека подобно тому, как предыдущие поколения использовали цифровые инструменты. Одновременно это будет способствовать созданию среды, где соблюдается автономия авторов. Таким образом будет не только обеспечена защита создателей творческого контента, но и расширено понимание творчества как процесса, совместного с генеративным искусственным интеллектом, где искусственный интеллект позиционируется как сила, дополняющая человека в творческом процессе, а не заменяющая его.

Для цитирования

Хатсон, Дж. (2024). Эволюция роли авторского права в эпоху произведений, созданных искусственным интеллектом. *Journal of Digital Technologies and Law*, *2*(4), 886–914. https://doi.org/10.21202/jdtl.2024.43

Список литературы

Aaland, M. (2006). *Photoshop Elements 3 Solutions: The Art of Digital Photography*. John Wiley & Sons.

Abbott, R., & Rothman, E. (2023). Disrupting creativity: Copyright law in the age of generative artificial intelligence. *Florida Law Review*, *75*, 1141–1201.

Atilla, S. (2024). Dealing with AI-generated works: lessons from the CDPA section 9 (3). *Journal of Intellectual Property Law and Practice*, *19*(1), 43–54. https://doi.org/10.1093/jiplp/jpad102

Bonnet, S., & Teuteberg, F. (2023). Impact of blockchain and distributed ledger technology for the management of the intellectual property life cycle: A multiple case study analysis. *Computers in Industry*, *144*, 103789. https://doi.org/10.1016/j.compind.2022.103789

Bridy, A. (2016). The Evolution of Authorship: Work Made by Code. *Columbia Journal of Law and the Arts*, *39*, 395–401. https://doi.org/10.7916/D8CV4J6W

Burylo, Y. (2022). AI generated works and copyright protection. *Entrepreneurship, Economy and Law*, *3*, 7–13. https://doi.org/10.32849/2663-5313/2022.3.01

Dimitrova, R. (2023). Are AI-Assisted Works Copyrightable? In *2023 International Scientific Conference on Computer Science (COMSCI)*, Sozopol, Bulgaria (pp. 1–4). https://doi.org/10.1109/COMSCI59259.2023.10315917

Elkin-Koren, N., Hacohen, U., Livni, R., & Moran, S. (2023). Can Copyright be Reduced to Privacy? ArXiv, 2305.14822. https://doi.org/10.48550/arXiv.2305.14822

Epstein, Z., Hertzmann, A., Akten, M., Farid, H., Fjeld, J., Frank, M. R., Groh, M., Herman, L., Leach, N., Mahari, R., Pentland, A. "Sandy", Russakovsky, O., Schroeder, H., & Smith, A. (2023). Art and the science of generative AI. *Science*, *380*(6650), 1110–1111. https://doi.org/10.1126/science.adh4451

Fenwick, M., & Jurcys, P. (2023, February 11). *Originality and the future of copyright in an age of generative AI.*

Feuerriegel, S., Hartmann, J., Janiesch, C., & Zschech, P. (2024). Generative AI. *Business & Information Systems Engineering*, *66*(1), 111–126. https://doi.org/10.1007/s12599-023-00834-7

Geiger, C. (2024). Elaborating a Human Rights friendly Copyright Framework for Generative AI. *International Review for Intellectual Property and Competition Law*, *55*(7), 1129–1165. https://doi.org/10.2139/ssrn.4634992

Gervais, D. (2022). AI Derivatives: the Application to the Derivative Work Right to Literary and Artistic Productions of AI Machines. *Seton Hall Law Review*, *53*. 1111–1136. https://doi.org/10.2139/ssrn.4022665

Hedrick, S. F. (2018). I "think," therefore I create: claiming copyright in the outputs of algorithms. *NYU Journal of Intellectual Property & Entreprenurial Law*, 8(2), 324–375.

Henderson, P., Li, X., Jurafsky, D., Hashimoto, T., Lemley, M., & Liang, P. (2023). Foundation Models and Fair Use. ArXiv, 2303.15715. https://doi.org/10.48550/arXiv.2303.15715

Horzyk, A. (2023). How AI Affects Our Understanding of Musical Works That Should Be Protected by Copyright. In *2023 International Joint Conference on Neural Networks (IJCNN)*, Gold Coast, Australia (pp. 1–8). https://doi.org/10.1109/IJCNN54540.2023.10191524

Hutson, J., Lively, J., Robertson, B., Cotroneo, P., & Lang, M. (2023). Expanding Horizons: AI Tools and Workflows in Art Practice. In *Creative Convergence: The AI Renaissance in Art and Design* (pp. 101–132). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-45127-0_5

Iaia, V. (2022). To Be, or Not to Be … Original Under Copyright Law, That Is (One of) the Main Questions Concerning AI-Produced Works. *GRUR International*, *71*(9), 793–812. https://doi.org/10.1093/grurint/ikac087

James, T. B. (2024). Artificial Intelligence, Copyright Registration, and the Rule of Doubt. *Texas A&M Law Review Arguendo*, *12*(1), 20–31. https://doi.org/10.37419/lr.v12.arg.2

Jiang, H. H., Brown, L., Cheng, J., Khan, M., Gupta, A., Workman, D., & Gebru, T. (2023). AI Art and its Impact on Artists. In Proceedings of the 2023 AAAI/ACM Conference on AI, Ethics, and Society (pp. 363–374). https://doi.org/10.1145/3600211.3604681

Kasap, A. (2021). Copyright and creative artificial intelligence (AI) systems: A twenty-first century approach to authorship of AI-generated works in the United States. *Wake Forest Journal of Business & Intellectual Property Law*, *19*(4), 335–380. https://doi.org/10.31235/osf.io/gnyha

Kelby, S. (2020). *The digital photography book. Rocky Nook*. Inc.

Kibirige, H. (2024). The delving conundrum of intellectual property rights in the transformative era of artificial intelligence. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4841535

Klukosky, F. P., & Kohel, M. D. (2024). An Update on the State of Play with Generative Artificial Intelligence and Intellectual Property Issues. *Intellectual Property Litigation*, *34*(1), 10–17.

Kretschmer, M., Margoni, T., & Oruç, P. (2024). Copyright law and the lifecycle of machine learning models. IIC-International Review of Intellectual Property and Competition Law, 55(1), 110–138. https://doi.org/10.1007/s40319-023-01419-3

Longpre, S., Mahari, R., Chen, A., Obeng-Marnu, N., Sileo, D., Brannon, W., Muennighoff, N., Khazam, N., Kabbara, J., Perisetla, K., Wu, X., Shippole, E., Bollacker, K., Wu, T., Villa, L., Pentland, S., & Hooker, S. (2023). The data provenance initiative: A large scale audit of dataset licensing & attribution in AI. arXiv, 2310.16787. https://doi.org/10.48550/arXiv.2310.16787

Lucchi, N. (2023). ChatGPT: A Case Study on Copyright Challenges for Generative Artificial Intelligence Systems. *European Journal of Risk Regulation*. https://doi.org/10.1017/err.2023.59

Majumdar, S., Paul, S., Paul, D., Bandyopadhyay, A., Chattopadhyay, S., Das, P. P., & Majumder, P. (2023). Generative AI for software metadata: Overview of the information retrieval in software engineering track at FIRE 2023. arXiv, 2311.03374. https://doi.org/10.48550/arXiv.2311.03374

McCann, S. (2021). Copyright Throughout a Creative AI Pipeline. *Canadian JL & Tech*, *19*(1), 109–139. https://doi.org/10.2139/ssrn.3893972

Mensah, G. B. (2023). *Artificial intelligence and ethics: a comprehensive review of bias mitigation, transparency, and accountability in AI Systems*. Preprint, November, 10. https://doi.org/10.13140/RG.2.2.23381.19685/1

Mia, M., Wessels, J., & Adam, S. (2023). The Use of Blockchain Technology to Improve Transfer-Pricing Compliance and Administration in South Africa. In *ICABR Conference* (pp. 357–378). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-46177-4_20

Militsyna, K. (2023). Human Creative Contribution to AI-Based Output – One Just Can('t) Get Enough. *GRUR International*, *72*(10), 939–949. https://doi.org/10.1093/grurint/ikad075

Moreno, H., Gómez, A., Altares-López, S., Ribeiro, A., & Andújar, D. (2023). Analysis of Stable Diffusion-derived fake weeds performance for training Convolutional Neural Networks. *Computers and Electronics in Agriculture*, *214*, 108324. https://doi.org/10.1016/j.compag.2023.108324

Pellegrini, T. (2023). Digital Rights Management – Technologies, Application Areas, and Governance. In *Handbook of Media and Communication Economics: A European Perspective* (pp. 1–17). Wiesbaden: Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-34048-3_79-2

Ploman, E. W., & Hamilton, L. C. (2024). *Copyright: Intellectual property in the information age*. Taylor & Francis. https://doi.org/10.4324/9781003519973

Risi, S., & Togelius, J. (2020). Increasing generality in machine learning through procedural content generation. *Nature Machine Intelligence*, *2*(8), 428–436. https://doi.org/10.1038/s42256-020-0208-z

Samuelson, P. (2023). Generative AI meets copyright. *Science*, *381*(6654), 158–161. https://doi.org/10.1126/science.adi0656

Sobel, B. (2021). A Taxonomy of Training Data. In R. Hilty, J.-A. Lee, & K.-Ch. Liu (Eds.). *Artificial Intelligence and Intellectual Property*. Oxford University Press. https://doi.org/10.1093/oso/9780198870944.003.0011

Spica, E. (2024). Public Interest, the True Soul: Copyright's Fair Use Doctrine and the Use of Copyrighted Works to Train Generative AI Tools. *Texas Intellectual Property Law Journal*, *33*(1), 67–91.

Torrance, A., & Tomlinson, B. (2023). Training Is Everything: Artificial Intelligence, Copyright, and Fair Training. ArXiv, 2305.03720. https://doi.org/10.48550/arXiv.2305.03720

Wagh, S., Peerzada, D., & Rote, P. (2023). AI And Copyright. *Tuijin Jishu/Journal of Propulsion Technology*, *44*(3), 3431–3439. https://doi.org/10.52783/tjjpt.v44.i3.2053

Wan, Y., & Lu, H. (2021). Copyright protection for AI-generated outputs: The experience from China. *Computer Law & Security Review*, 42, 105581. https://doi.org/10.1016/J.CLSR.2021.105581

Yu, R. (2017). The Machine Author: What Level of Copyright Protection Is Appropriate for Fully Independent Computer-Generated Works? *University of Pennsylvania Law Review*, *165*, 1245–1270.

Сведения об авторе

Джеймс Хатсон – PhD, ведущий специалист в области дополненной реальности; профессор, заведующий кафедрой истории искусств, искусственного интеллекта и визуальной культуры; факультет искусств и гуманитарных дисциплин, Линденвудский университет
Адрес: МО 63301, США, г. Сент Чарльз, ул. С. Кингзхайвей, 209
E-mail: jhutson@lindenwood.edu
ORCID ID: https://orcid.org/0000-0002-0578-6052
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57797793000
WoS Researcher ID: https://www.webofscience.com/wos/author/record/38589773
Google Scholar ID: https://scholar.google.com/citations?user=CaXrV38AAAAJ

Конфликт интересов

Автор сообщает об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.07.45 / Право и научно-технический прогресс
Специальность ВАК: 5.1.3 / Частно-правовые (цивилистические) науки

История статьи

Дата поступления – 29 октября 2024 г.
Дата одобрения после рецензирования – 10 ноября 2024 г.
Дата принятия к опубликованию – 13 декабря 2024 г.
Дата онлайн-размещения – 20 декабря 2024 г.

Research article
UDC 34:004:343.9:004.8
EDN: https://elibrary.ru/jvglrh
DOI: https://doi.org/10.21202/jdtl.2024.44

Sociological and Criminological Research of Victimization Issues: Preliminary Stage and New Sphere of Cybercrime Categorization

Aminu Muhammad Auwal
University of Jos, Jos, Nigeria

Suleman Lazarus ✉
London School of Economics and Political Science, London, United Kingdom
University of Surrey, Guildford, United Kingdom
University of Portsmouth, Portsmouth, United Kingdom

Keywords

cybercrime victim,
cybercrime,
cybercriminology,
cyber-espionage,
digital criminology,
digital technologies,
legal policy,
online fraud,
victimization,
victimology

Abstract

Objective: to identify the main issues of victimization as a result of cybercrime growth in the world in general and in Nigerian society in particular from the standpoint of sociological approaches, using a Tripartite Cybercrime Framework (TCF), which comprises geopolitical, psychosocial and socio-economic categories of cybercrime.

Methods: the methodology is based on the sociological research method. The data collection included the distribution of a questionnaire among 896 participants from the academic environment, including students and university staff, and the analysis of the responses. The presented data were analyzed using descriptive statistics, with special attention to the issues of gender inequality, socio-economic factors, the impact of educational level on vulnerability to online fraud and victimization as a result of cybercrime through the prism of the ideal victim concept and the socio-economic gap between North and South.

Results: the article presents an analysis of the Tripartite Cybercrime Framework. The survey showed that 65.20% of the participants had been victims of cybercrime. There were more men among the victims (64.69%). The authors found patterns in the distribution of cybercrimes. All cybercrimes against the respondent were socio-economic ones, which underlines the

✉ Corresponding author
© Auwal A. M., & Lazarus S., 2024

This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (CC BY 4.0) (https://creativecommons.org/licenses/by/4.0), which permits unrestricted re-use, distribution and reproduction, provided the original article is properly cited.

high frequency of cybercrime and the relevance of countering it in Nigerian society. Special attention was paid to the issues of gender inequality, socio-economic factors, and the impact of education on vulnerability to cybercrime. The article considers from the viewpoint of the ideal victim concept. The study results provide an idea of the prevalence and distribution of specific types of cybercrime in the socio-economic category among the studied population.

Scientific novelty: For the first time, the study uses the Tripartite Cybercrime Framework (TCF) to study victimization as a result of cybercrime in Nigerian society. The research novelty is also due to the fact that the conceptual foundations of countering cybercrime that have developed in the global North are not fully applicable in Nigeria.

Practical significance: the results obtained demonstrate the need to apply carefully calibrated gender-based, inclusive and contextual approaches to the development of a national legal policy to combat cybercrime. The results can be used to justify the law-making decisions which are being developed in the field of preventing and countering manifestations of cybercrime, as well as to form the basis for legal measures to protect cybercrime victims.

For citation

Auwal, A. M., & Lazarus, S. (2024). Sociological and Criminological Research of Victimization Issues: Preliminary Stage and New Sphere of Cybercrime Categorization. *Journal of Digital Technologies and Law, 2*(4), 915–942. https://doi.org/10.21202/jdtl.2024.44

Content

Introduction
1. Literature Review
  1.1. Cybercrime and Cyber Criminology
  1.2. Tripartite Cybercrime Framework (TCF)
    1.2.1. Geopolitical Cybercrime
    1.2.2. Psychosocial Cybercrime
    1.2.3. Socioeconomic Cybercrime
  1.3. Complexities and Challenges of Cybercrime in Nigeria
  1.4. The Rise of Economic Cybercrime in Nigeria
  1.5. Victims-Oriented Studies
  1.6. Cybercriminals in a Nigerian society (Yahoo Boys)
  1.7. Convergence and Divergence in Prior Research
  1.8. Novelty of Current Work

2. Methods and materials
2.1. Data Analysis
3. Results
3.1. Gender Dimension
3.2. Educational Level
3.3. Confirmed Negative Experience of Cybercrime
3.4. Type of Cybercrime
3.5. Reported Incidents
3.6. Stolen Money Reversed/Suitable Action Taken
4. Discussion
4.1. Gender Dimension of Online Fraud Victimization
4.2. The centrality of Socioeconomic Dynamics of Cybercrime
4.3. Educational Attainment and Online Fraud Victimizations
4.4. Cybercrime Victimization, Ideal Victims, and the North-South Divide
Conclusion
References

Introduction

While cybercrime is a global issue, spatial characteristics influence local human behavior and can be revealed or hidden by spatial elements (Hall & Yarwood, 2024; Lazarus & Button, 2022). This article aims to shed light on the reported cybercrime experiences and provide empirical evidence through quantitative analysis. Cybercrime has emerged as a significant societal concern in Nigeria, and its prevalence has increased in recent years (Ibrahim, 2016a; Idem & Olarinde, 2023). Many scholars have examined victims of cybercrime in various contexts, such as Australia (Cross, 2020; Drew & Webster, 2024), China (Wang, 2023), Portugal (Murça et al., 2024), the United Kingdom (Lazarus et al., 2022b) and Russia (Timofeyev & Dremova, 2022). Only a few studies have investigated the victims of cybercrime in Nigeria. Unlike in many nations, especially such as Australia (Cross, 2020; Drew & Websters, 2024; Meikle & Cross, 2024) and the United Kingdom (Button et al., 2014, 2015; 2021), victims of cybercrime in Nigeria are under-researched.

For instance, Aborisade et al. (2024) conducted a study through interpretative phenomenological analysis and one-on-one semi-structured video interviews; ten victims of Nigerian romance fraudsters from six different nations were examined. In addition, Tade and Adeniyi (2017) examined data generated through in-depth interviews with ATM fraud victims, revealing that victims suffered post-fraud trauma and often relied on friends, parents, and relatives to cope with the aftermath. However, none of these studies utilized quantitative methods to explore respondents' demographic

characteristics and experiences of cybercrime. This study aims to address this gap by investigating the demographic characteristics and experiences of respondents regarding cybercrime. Specifically, it sought to examine the prevalence, characteristics, and reporting dynamics of cybercrime experiences among respondents. To achieve this, the study aims to contribute to the under-researched topic of cybercrime victimization in Nigerian society using data collected via a distributed survey.

1. Literature Review

1.1. Cybercrime and Cyber Criminology

The idea that the division between the physical and digital worlds hinders the understanding of offline social cues, which also affect the digital realm, has been explored by various scholars (Jaishankar, 2007; Ibrahim, 2016a; Powell et al., 2018). While researchers have emphasized the connection between offline and online life, they have used different terms to convey this concept. For instance, McGerty (2000) stated that «nobody lives only in cyberspace," Jaishankar (2007, 2011, 2018) introduced the concept of «cyber criminology,» while Powell et al. (2018) rebranded it «digital criminology». These variations in terminology reflect the contestation of ownership within scholarly discourse on this topic.

The concept of «cybercrime» encompasses unlawful activities conducted via the Internet and Information Communication Technology (ICT), including «cyber-dependent» and «cyber-enabled crimes» (Button et al., 2023; Ibrahim, 2016a; Hall & Yarwood, 2024; Musotto & Wall, 2022). While often used interchangeably to refer to all online unlawful activities, it is common for security agencies, researchers, and the media to group various digital offenses under «cybercrime,» ignoring their unique attributes (Lazarus, 2019). Cyber-dependent offenses occur even without digital technology or networks, while cyber-enabled crimes are amplified by networks. We focus on cyber-enabled crimes. However, the conflation of «cyber-enabled crimes»[1] and «people-centric cybercrimes» (Gordon & Ford, 2006) makes it difficult to differentiate financially motivated crimes like «online fraud» from psychologically motivated ones like «revenge pornography» (Ibrahim, 2016a; Lazarus, 2019). We now utilize Nigerian-oriented frameworks and perspectives on cybercrime, particularly Ibrahim (2016a), to contribute to ongoing discussions on online fraud victimization, addressing the oversight of Nigerian scholars' insights, as Cross (2018a) pointed out.

[1] McGuire, M., & Dowling, S. (2013, October). Cybercrime: a review of the evidence: Research Report 75. https://clck.ru/3F25c7

1.2. Tripartite Cybercrime Framework (TCF)

Empirical literature (De Kimpe et al., 2020; Lazarus et al., 2022b) has utilized the Tripartite Cybercrime Framework (TCF) to distinguish between cybercrimes driven by psychology (psychosocial cybercrime), economics (socioeconomic category), and geopolitics, as illustrated in Fig. 1, derived from Ibrahim's (2016a) original formulation. Ibrahim (2016a) specifically clarifies that while cybercrimes in a Nigerian context are primarily financially driven, not all cyber-enabled crimes, such as revenge pornography, possess this attribute. Drawing from these classifications, we highlight the unique characteristics of cybercrimes in Nigeria as a subset of offenses. Cybercrime is indeed a global crime. However, it also exhibits spatial characteristics, influencing human behavior in specific regions and manifesting in spatial elements that may be concealed or revealed (Hall & Yawood, 2024; Lazarus & Button, 2022).

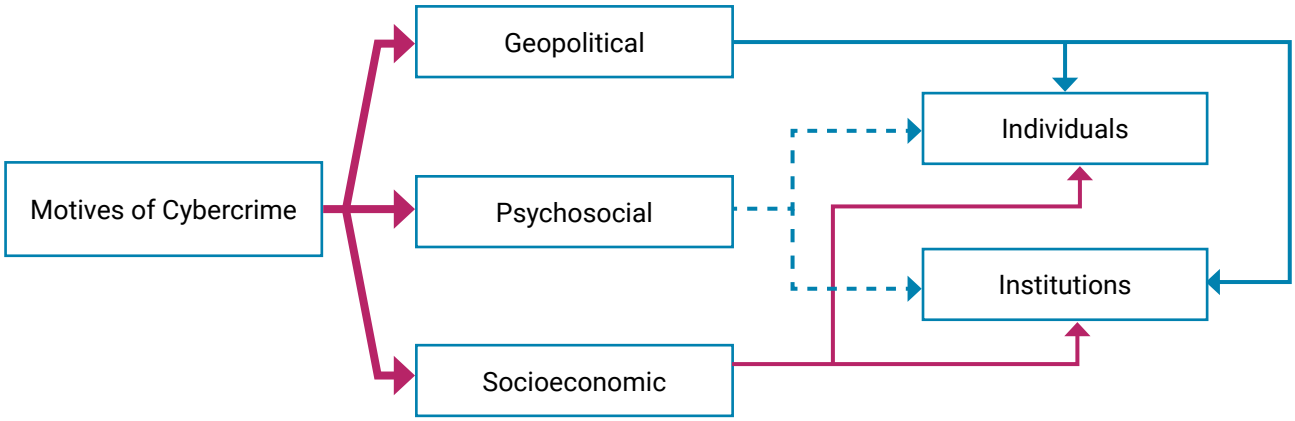


Figure 1. Tripartite Cybercrime Framework (TCF)

1.2.1. Geopolitical Cybercrime

Geopolitical cybercrime involves cybercrimes driven by political motives, often involving state actors, non-state activists, or their representatives (Ibrahim, 2016a; Lazarus, 2019). These activities may include cyber espionage or attacks on critical infrastructure. However, cybercrime originating from Nigeria rarely falls into this category, unlike other nations such as the United States and China (Ibrahim, 2016a). For instance, state-sponsored hacking groups may target foreign government agencies to gather intelligence for political advantages in diplomatic negotiations or military strategies (Akoto, 2021; Makridis et al., 2024). The primary motivation for geopolitical cybercrime is political, aligned with the geopolitical category of TCF (Ibrahim, 2016a).

1.2.2. Psychosocial Cybercrime

Psychosocial cybercrime involves digital offences primarily driven by psychological motivations, intending to cause distress, anguish, or harm to individuals (Ibrahim, 2016a; Lazarus, 2019). Monetary gain is not the primary objective in such cases. Examples include cyberstalking, cyberbullying, and online abuse, targeting victims on social media platforms to harm them psychologically and undermine their credibility. Perpetrators derive satisfaction from causing distress, emphasizing the psychosocial nature of these crimes (Ibrahim, 2016a; Lazarus, 2019). While revenge pornography offenders often blame and humiliate victims, this is not the primary motive for fraud, which is money.

1.2.3. Socioeconomic Cybercrime

Socioeconomic cybercrime involves the pursuit of financial gains through deceptive practices facilitated by computers or internet technologies. This encompasses illegal activities such as online fraud, romance scams, copyright theft, and illegal downloads of digital content (Ibrahim, 2016a). Nigeria is particularly vulnerable to practices within this category, which include prevalence, impersonation, manipulation, counterfeiting, forgery, and fraudulent misrepresentation. Notable examples include online romances (Drew & Webster, 2024; Lazarus et al., 2023) and pig butchering fraud (Wang, 2023; Whittaker et al., 2024). These fraudulent schemes are primarily motivated by financial gain.

However, the geopolitical, psychosocial, and socioeconomic categories are not rigidly defined, and instances of overlap can occur. For example, hacktivists may release stolen personal information to convey political messages, which has psychological and geopolitical implications. Nonetheless, the TCF serves as a useful tool for categorizing the distinct characteristics of various cybercrimes in Nigeria and beyond. Nigeria lacks substantial documentation of other types of cyber offences, such as cyber espionage, cyberstalking, and revenge porn, which are more prevalent in countries such as Belgium, Canada and the United Kingdom (Ibrahim, 2016a). Therefore, the conceptual framework of the cybercrime framework in the Global North may not fully apply in Nigeria, representing Africa south of the Sahara (Ibrahim, 2016a). The complexities of cybercrime in Nigeria are worth noting.

1.3. Complexities and Challenges of Cybercrime in Nigeria

Recent conference papers shed light on various aspects of cybercrime prosecution, regulation, and its impact on Nigeria. Idem et al. (2023a) identified key challenges hindering cybercriminal prosecution in Nigeria, including the lack of robust legislation,

ineffective law enforcement, slow legal processes, and limited forensic analysis capabilities. Building on this, Idem et al. (2023b) emphasize the urgent need for reform within cybercrime regulatory agencies to protect Nigeria from its status as one of the top three countries with the highest growth of cybercrime. Similarly, Idem (2023) suggests that Nigeria's Cybercrimes Law has played a significant role in regulating and deterring various forms of cybercrime, safeguarding online businesses, and promoting internet enterprises. These three related studies collectively spotlight the multifaceted challenges posed by cybercrime in Nigeria and emphasize the importance of legislative, regulatory, and socioeconomic interventions to address them.

Furthermore, while Ojolo and Adewumi (2020) and Lazarus et al. (2023) illuminate the normalization of cybercrime within Nigerian society, highlighting factors such as economic instability, corruption, and peer influence as significant drivers of its prevalence, Lazarus et al. (2022a) draws parallels between internet scammers (Yahoo Boys) and Nigerian corrupt politicians ("Yahoo Men"). Similarly, Olaiya, Lamidi, and Bello (2020), Monsurat (2020), and Adeduntan (2022) emphasize the influence of political corruption, peer pressure, economic hardship, and inadequate social support systems. Additionally, Ojolo and Singh (2023) and Aransiola and Asindemade (2011) uncovered the lucrative nature of this activity and the complicity of corrupt law enforcement officers and asserted that financial incentives intersect with institutional vulnerabilities to sustain illicit practices online. Collectively, the above studies suggest that cybercrime is a complex phenomenon rooted in socioeconomic disparities, institutional deficiencies, and cultural influences. Nonetheless, there is a clear pattern that incidents of cybercrime have risen in recent years.

1.4. The Rise of Economic Cybercrime in Nigeria

The Rise of Economic Cybercrime in Nigeria has become a concern for various stakeholders. Idem and Olarinde (2023) highlight the negative effects of cybercrime on youth development, the economy, and governance in Nigeria. They identify unemployment, poverty, corruption, and ineffective governance as primary drivers of youth involvement in cybercriminal activities and offer recommendations to combat these issues. According to the analysis of cybercrime and cybersecurity incident reports posted by the Economic and Financial Crimes Commission (EFCC) from 2019 to 2022, online fraud has been on a sharp rise[2]. This is how this information is summarised to give the idea of cybercrime incidence in Nigeria, when the number of sentences dramatically increased in four years of observation.

[2] EFCC. (2022). https://goo.su/TJjHS

For example, between 2019 and 2022, the EFCC witnessed a substantial surge in reported cybercrime incidents. In 2019, 877 individuals reported cybercrime incidents, which escalated to 1890 incidents in 2020, representing a 115.5 % increase compared to the previous year. By 2021, reported incidents further rose to 2400, reflecting a staggering 173.7 % increase compared to the baseline of 2019. Projections for 2022 indicated a continued upward trend, with 2900 reported incidents comprising a substantial 230.7 % increase compared to the initial figures of 2019. These statistics highlight the exponential growth of online scams and underscore the exigency for scholarly inquiry into victimization patterns within the country. Our analysis reveals a marked surge in cybercrime activities, substantiated by the escalating number of convicted cybercrime incidents reported by the EFCC. These findings spotlight a significant uptick in cybercrime within Nigeria over the specified timeframe, emblematic of the activities of cybercriminal entities, predominantly recognized as Yahoo Boys (Aborisade, 2023; Lazarus & Okolorie, 2019; Ogunleye et al., 2019; Ojedokun & Eraye, 2012).

1.5. Victims-Oriented Studies

The actions of Yahoo Boys have global repercussions, prompting an increase in research focused on victims of online fraud. Many studies have been conducted on the topic of victimization, but most of them have focused on Western societies and Asian nations like China. A few studies have looked into African nations like Nigeria, but they are relatively uncommon. For instance, studies by Button et al. (2014), Meikle and Cross (2024), Drew and Websters (2024), Cross (2020), Cross (2018b), and Whitty (2019) primarily concentrate on victims from Western societies and Asian nations like China (Tao, 2022; Wang, 2023; Wang & Topalli, 2024), while only a few researchers such as Aborisade et al. (2024) have studied victimization in African nations like Nigeria. This imbalance could be stemming from the Western media's exclusive coverage of victims from Western countries, as well as priorities of research funding allocation. Such tendencies perpetuate and inadvertently marginalize victims from a Nigerian context. This study seeks to address this disparity by emphasizing that the detrimental impact of Yahoo Boys extends beyond local boundaries to the global arena. By shedding light on the experiences of victims in African nations like Nigeria, we aim to challenge the prevailing Western-centric narrative and highlight the universality of the issue. Through an inclusive approach, we endeavor to contribute to a deeper understanding of online fraud and its impact on victims worldwide.

1.6. Cybercriminals in a Nigerian society (Yahoo Boys)

Several qualitative investigations have investigated Nigerian cybercriminals both within Nigeria (Aransiola & Asindemade, 2011; Lazarus & Okolorie, 2019; Ogunleye et al., 2019; Ojedokun & Eraye, 2012) and outside Nigeria (Lazarus, 2024), thereby providing insights into the diverse facets of these offenders. The empirical literature cited above consistently

indicates that men (and boys) are the primary perpetrators of cybercrime. These individuals fundamentally coordinate socioeconomic digital crimes on the internet, as shown in Figure 1. In contrast to their male counterparts, according to testimonials, female undergraduates who commit online fraud mostly do so from subordinate positions to their male-dominated superior positions (Ogunleye et al., 2019). Although the research above findings specifically pertained to Nigerian society' emphasizing that males are the predominant perpetrators of these cybercriminal activities, only a limited number of studies, including Aborisade et al. (2024), have investigated the experiences of cybercrime victims in Nigeria.

1.7. Convergence and Divergence in Prior Research

In the Nigerian context, many research endeavors have produced convergent findings using a variety of data sources. These include interviews with frontline law enforcement officers (Lazarus & Okolorie, 2019), analysis of scam emails (Genc et al., 2021; Rich, 2018), examination of music lyrics (Adeduntan, 2022; Lazarus et al., 2023), interviews with Nigerian parents (Aborisade, 2023; Ibrahim, 2016b), interviews with online fraudsters (Aransiola & Asindemade, 2011; Lazarus, 2024; Ojedokun & Eraye, 2012; Ogunleye et al., 2019), exploration of tweets (Lazarus & Button, 2022), and consistency and concurrence among these studies substantially enhance the credibility of empirical research as a whole, thereby reaffirming the fundamental understanding about characteristics of online offenders and they category of cybercrimes they commit. Furthermore, studies not based on empirical evidence support the empirical literature (Idem et al., 2023a, 2023b). This verifies these attributes and brings together evidence from diverse research methodologies. Only a limited number of studies have been conducted on victims of cybercrime in Nigeria, notably Aborisade et al. (2024), Mba et al. (2017), and Tade and Adeniyi (2017).

1.8. Novelty of Current Work

This study is distinct from previous research in several respects. Although previous studies have investigated cybercrime victims in Nigeria (Aborisade et al., 2024; Mba et al., 2017; Tade & Adeniyi, 2017), no distributed questionnaires have been employed. Previous approaches, such as those by Aborisade et al. (2024) and Tade and Adeniyi (2017), relied on qualitative methods, whereas Mba et al. (2017) sourced data from a Nigerian forum hosted at www.topix.com, supplemented by Web engine searches to identify similar online and active scam posts. While empirical literature such as De Kimpe et al.'s (2020) study in Belgium has used the TCF as a reference point, none has ever examined cybercrime by explicitly considering the Tripartite Cybercrime Framework (TCF) excerpt for Lazarus et al. (2022b) study which merge the TCF and feminist epistemology of crime. While Lazarus et al. (2022b) explored perceptions of cybercrimes aligned with the TCF categories in the United Kingdom, our study aims to address this gap by examining cybercrime victimization in Nigeria through the lens of the TCF classifications. We will use «the Socioeconomic Theory of Nigerian Cybercriminals» proposed by Ibrahim (2016a) as a framework for our research.

2. Methods and materials

We employed a distributed survey approach to collect data from a diverse cohort of students, staff, and workers from various sectors. Our questionnaire explores Ibrahim's (2016a) framework, which categorizes cybercrime into socioeconomic, geopolitical, and psychosocial dimensions, to expose the nuances and particularities of cybercrime types in Nigeria. The survey targeted voluntary participants with diverse demographic backgrounds to contribute to the understanding of cybercrime experiences. While participants' responses were anonymized and kept confidential, ethical approval was obtained from one of the universities in Nigeria to ensure academic and research guidelines adherence. The survey was meticulously designed and distributed through established survey platforms to ensure its efficiency and broad reach. Participants provided informed consent before participation, and stringent measures were implemented to safeguard their anonymity and confidentiality throughout the data collection process.

2.1. Data Analysis

We conducted a nearest-neighbor analysis to identify the geographical clusters and sectors most affected by cybercrime. By employing a combination of simple statistical methods and advanced spatial statistics, data analysis yielded valuable insights into the prevalence and characteristics of cybercrime in the studied population. Moreover, statistical analysis was employed to discern trends and patterns in cybercrime occurrence rates over a specified period. Descriptive statistics such as means and medians were computed using Excel spreadsheets to facilitate the calculation of relevant counts and percentages. While this method has its limitations, however, we offer the following justifications for this approach:

1. Exploratory Analysis. Descriptive statistics serve as a valuable tool for conducting exploratory analysis, enabling researchers to gain an initial understanding of the data by summarizing key characteristics like central tendency and variability. Since this is a preliminary study, this approach allows for the identification of basic patterns in cybercrime experiences among participants without assuming underlying relationships, which may not be misleading, given the complex sociocultural fabric of Nigerian society.

2. Data Presentation. Descriptive statistics are crucial for presenting critical findings in a clear and concise manner, making them accessible to a broad audience, including undergraduate students from various disciplines. Given that the study focuses on cybercrime experiences among university students and workers in Nigeria, descriptive statistics provide a straightforward way to communicate important findings about the prevalence and characteristics of cybercrime in this population.

3. Simple Data Structures. The investigation tool used in the study has a relatively simple structure with few variables and straightforward relationships. As such, descriptive statistics are well-suited to address the research question and objectives

of this preliminary inquiry. More complex analytical techniques may not be necessary. They could introduce unnecessary complexity, making descriptive statistics an efficient way to analyze and summarize data, providing valuable insights into cybercrime victimization experiences among the study population.

3. Results

This section presents the findings from the quantitative analysis of 896 responses, delineating the frequencies and percentages associated with each category identified in the study as illustrated in Table 1. Almost all participants (99.78 %) provided informed consent, indicating a high level of willingness to participate in the study. Only a small fraction (0.76 %) chose not to provide consent, suggesting that most participants were willing to participate.

Table 1. Summary of Our Findings

Item	Type	Frequency	Percentage
Informed consent response	Yes	896	99.78
	No	7	0.76
Gender of the respondents	Male	584	64.69
	Female	312	34.52
Educational level	Masters' Students	522	57.80
	Doctoral Candidates	21	2.36
	Teachers and Admin Staff	12	1.35
Experience of cybercrime as victims	Yes	588	65.20
	No	301	33.40
Gender of cybercrime victims	Male Victims	303	51.53
	Female Victims	285	48.47
Type of Cybercrime	E-Banking/Payment-Card Fraud	554	61.45
	Identity Theft	67	7.43
	Others	295	32.68
Reported?	Yes	322	35.74
	No	577	63.94
Stolen Money reversed/Suitable Action Taken?	Yes	54	5.99
	No	835	92.61

3.1. Gender Dimension

The findings of this study shed light on the gender dynamics within cybercrime victimization, revealing a notable disparity in the experiences of men and women. Data analysis indicates that among individuals affected by cybercrime, 303 men (51.53 %) and 285 women (48.47 %) reported adverse outcomes. This disparity is further underscored by the overall distribution of cybercrime victims, with 64.69 % male and 34.52 % female. These figures suggest a gendered pattern in cybercrime

victimization, with a higher proportion of men experiencing negative consequences compared to women. The data also highlights the need for gender-sensitive approaches in addressing cybercrime and implementing interventions to mitigate its impact on both male and female victims. Additionally, the relatively balanced distribution between male and female victims underscores the importance of considering gender dynamics in understanding and responding to cybercrime phenomena.

3.2. Educational Level

The participants had a diverse range of educational backgrounds. 37.80 % were undergraduates, 57.80 % were master's students, 2.36 % were doctoral candidates, and 1.35 % were teachers and admin staff. This diversity in educational level enriches the sample's heterogeneity and makes the findings more generalizable.

3.3. Confirmed Negative Experience of Cybercrime

A significant proportion of participants (65.20 %) reported experiencing adverse incidents related to cybercrime, highlighting its pervasive impact on the study population. Conversely, 33.40 % indicated that they had not experienced any cybercrime incidents, revealing a subset of individuals unaffected by this type of crime.

3.4. Type of Cybercrime

The study found distinct prevalence patterns in cybercrime incidents. E-Banking/ Payment-Card Fraud was the most common type, accounting for 61.45 % of reported incidents. Identity Theft accounted for 7.43 % of incidents, while other forms collectively constituted 32.68 % of cases, such as online job scams. These findings provide insights into the prevalence and distribution of specific cybercrime types among the study population: the socioeconomic types.

3.5. Reported Incidents

The study found that 35.74 % of participants reported cybercrime incidents to relevant authorities or entities, indicating a moderate engagement with reporting mechanisms. In contrast, the majority (63.94 %) did not report any incidents, suggesting potential underreporting and areas for improvement in reporting practices.

3.6. Stolen Money Reversed/Suitable Action Taken

Among participants who reported cybercrime incidents, only a minority (5.99 %) indicated that stolen funds were reversed or appropriate actions were taken in response. Conversely, the vast majority (92.61 %) reported no remedial actions, suggesting

challenges in achieving restitution or resolution following cybercrime victimization. While these findings provide valuable insights into cybercrime prevalence, characteristics, and reporting dynamics among participants, further exploration is warranted to compare with prior empirical literature and to discern implications for policy, practice, and future research endeavors.

4. Discussion

In the discussion section, we build upon insights garnered through a distributed survey approach to advance understanding cybercrime victimization across diverse demographic spectra. This section discusses four primary themes: (1) Disparities in Cybercrime Experiences based on gender; (2) the pivotal role of Socioeconomic pertaining to Cybercrime in Nigeria; (3) the correlation between Educational Attainment and vulnerability to online fraud; and (4) an exploration of Cybercrime Victimization through the lens of ideal victimization, juxtaposed with the North-South socioeconomic Divide.

4.1. Gender Dimension of Online Fraud Victimization

Our study's analysis of gender disparities in cybercrime victimization (Table 1, section 3.4 of the article) both aligns with and diverges from findings in prior research. For example, Lazarus et al. (2022b) assert that while women tend to perceive psychosocial cybercrimes, such as revenge pornography, as more severe than men, no discernible gender disparities exist in socio-economic cybercrimes like credit card online fraud. Notably, unlike the above authors, our study does not explicitly explore perceptions of cybercrime and shows a gender difference in socioeconomic cybercrime victimization, contributing to the discourse. Moreover, numerous studies have delved into the intricate dynamics of cybercrime victimization, shedding light on various influencing factors (Näsi et al., 2023). Kadoya et al. (2021) research in Japan identified gender and marital status as potential determinants of victimization, indicating that males and married individuals are more susceptible to fictitious billing fraud. Similarly, Whitty's (2019) study in the United Kingdom underscores gender variations in cybercrime, particularly evident in romance fraud, where women are disproportionately victimized. Although our study did not specifically inquire about marital status or romance scams, our findings resonate with those of Kadoya et al. (2021) and Whitty (2019), corroborating the significance of gender in cybercrime victimization.

The variability in gender disparities across different contexts is further illuminated by studies conducted in Finland (Näsi et al., 2023) and the Netherlands (Weijer et al., 2020). While Finnish research found no statistically significant gender differences, a Dutch study revealed that females were likelier to report traditional crimes to the police, while

males exhibited greater proactivity in reporting cybercrime incidents (Näsi et al., 2023; Weijer et al., 2020). Consequently, it is plausible to assert that the gender differences identified in our study may be attributed, in part, to disparities in crime reporting behavior. This underscores the multifaceted nature of cyber victimization reporting, often leading to cybercrimes being reported to organizations other than the police. Furthermore, gender differences significantly impact susceptibility to online fraud, with psychological traits such as risk-taking and low self-control further contributing to vulnerability (Norris et al., 2019). Although our study did not investigate psychological traits and their association with online fraud victimization, our findings agree that gender differences significantly influence susceptibility to online fraud. Despite these gender-related nuances, gender alone plays only a partial role in predicting cyber victimization, with other factors such as fraudster motivation and target vulnerability exerting considerable influence as well.

4.2. The centrality of Socioeconomic Dynamics of Cybercrime

Our research has identified clear prevalence trends in cybercrime incidents (Table 1), notably highlighting E-Banking/Payment-Card Fraud as the most dominant type, comprising 61.45 % of reported cases. Identity Theft comprised 7.43 % of incidents, while various other scams, including online job scams and phishing schemes, collectively accounted for 32.68 % of cases, all falling within the socioeconomic category of cybercrime (Table 1). It reinforces that cybercrime exhibits spatial characteristics as it traverses and manifests in various regions, exerting an impact on human conduct within particular localities while also being capable of being obscured or revealed by spatial elements (Hall & Yawood, 2024; Lazarus & Button, 2022). The Tripartite Cybercrime Framework (TCF) delineates cybercrimes into three principal motivational components – socioeconomic, psychological, and geopolitical – underscoring the distinction between socioeconomic and psychosocial cyber offenses (Ibrahim, 2016a; Lazarus, 2019; Lazarus et al., 2022b).

Unlike countries like Canada, Russia, China, and the United Kingdom, Nigeria lacks substantial documentation of other cybercrime categories, notably geopolitical, such as cyber espionage, and psychosocial, such as revenge pornography (Ibrahim, 2016a). The geopolitical and sociocultural contexts of different nations significantly shape their behavior in cyberspace. For instance, while revenge pornography is prevalent in Western nations like Portugal (Murça et al., 2024), the United Kingdom, Canada, etc. (Harper et al., 2023), it may not be as pronounced in Nigeria. Furthermore, unlike Nigeria, countries like the United States, Russia, China, and the United Kingdom confront significant challenges with nation-sponsored cyber espionage (Akoto, 2021, 2024; Markridis et al., 2024). These social and contextual nuances challenge the notion

of cyberspace and physical space as distinct entities with clear boundaries, as highlighted by Jaishankar (2007, 2011, 2018). As a result, the conceptual frameworks commonly utilized in "the Global North" may not entirely apply in Nigeria, representing Africa south of the Sahara (Ibrahim, 2016a). The complexities of cybercrime in Nigeria are notable. Although our survey data originated from a single institution, the findings offer insights into the prevalence and distribution of cybercrime types within the socioeconomic classification.

However, while Nigeria may lack substantial documentation of certain cybercrime categories, it does not necessarily mean that psychosocial cybercrimes, such as cyberstalking and cyberbullying, are non-existent or negligible. One possible explanation is that the sociocultural fabric of Nigerian society prioritizes socioeconomic cybercrime types, such as online scams. This emphasis is evident in the exclusive focus on financial crimes reported by the EFCC, the elite enforcement agency in Nigeria. Additionally, the lack of documentation could stem from other factors, such as limited resources or infrastructure for detecting and reporting such cybercrime types. Furthermore, while sociocultural and geopolitical contexts influence cyberspace behavior, it is essential to acknowledge that geopolitical cybercrime types often do not affect ordinary citizens like the students and teachers we studied in this research. As a result, our inquiry did not cover geopolitical entities, leading to potential oversight in our findings.

4.3. Educational Attainment and Online Fraud Victimizations

One significant discovery from our research pertains to the educational backgrounds of the participants. While over 99 % of them possessed or were in the process of obtaining a university degree, the distribution across educational levels varied considerably. In particular, among the participants, 37.80 % were undergraduates, 57.80 % were master's students, 2.36 % were pursuing doctoral degrees, and 1.35 % were educators and admin staff (Section 3.4 of the article). Despite this educational diversity, over 65 % of all participants reported being victims of cybercrime, a finding that both align with and diverges from prior studies.

Existing research indicates that the likelihood of falling victim to online fraud is influenced by several factors, among which educational attainment plays a significant role. Studies have demonstrated that individuals with lower levels of education are more susceptible to consumer fraud (Whitty, 2018). However, research also suggests a nuanced relationship between education level and fraud victimization. For instance, individuals at the extreme ends of educational attainment, such as those with no high school degree or graduate degree, are less likely to become victims of fraud (Schoepfer & Piquero, 2009), indicating a U-shaped pattern in this relationship.

Moreover, individuals who have completed higher education and spend more time online are found to be at greater risk of being targeted by fraudsters (Paek & Nalla, 2015). This association underscores the impact of routine online activities on victimization risk, highlighting the role of online interactions in cybercrime vulnerability. Additionally, older individuals, who typically have higher levels of education, are identified as particularly vulnerable to cyber-fraud victimization (Whitty, 2019). This demographic often exhibits traits such as high impulsivity, engagement in risky online behaviors, and addictive tendencies, all of which heighten their susceptibility to online scams.

4.4. Cybercrime Victimization, Ideal Victims, and the North-South Divide

The outcomes of our investigation underscore the pervasive impact of cybercrime in Nigeria, with a notable majority of participants (65.20 %) reporting personal victimization experiences (Aborisade et al., 2024). This prevalence underscores the widespread nature of cybercrime and its substantial effect on the study population. Conversely, 33.40 % of respondents indicated no encounters with cybercrime incidents, revealing a subset of individuals within Nigeria unaffected by this criminal activity. This contrast initiates discussions surrounding ideal victimization and the interplay between the Global North and West Africa (Nigeria), a subject rarely explored in online fraud literature.

The operations of groups like the Yahoo Boys, originating in Nigeria but impacting globally, have garnered increased attention to victims of online fraud. However, existing research predominantly centers on victims from Western societies (Button et al., 2014, 2015; Cross, 2020; Drew & Webster, 2024) and some non-Western contexts like China (Tao, 2022; Wang, 2023), with limited studies dedicated to West African nations such as Nigeria (Aborisade et al., 2024). It is plausible that the unequal distribution of research attention on certain issues is due to the tendency of Western media to focus on high-profile victims from Western countries. Additionally, research funding often prioritizes Western-centric perspectives, resulting in a lack of attention and resources for other regions, including West African nations such as Nigeria (Mosbah-Natanson & Gingras, 2014). These biases perpetuate assumptions and inadvertently marginalize victims from non-Western contexts, thus highlighting the concept of «ideal victims» where ce rtain victims may be considered more “ideal victims” than others. Online fraud victims in Western societies such as the United States, the United Kingdom, and Australia are no less significant than their counterparts in Nigeria.

Building upon Christie’s (1986) seminal work on ideal victims, which delineates the traits of an ideal victim, our study investigated the dynamics of online fraud

victimization within the Nigerian context. Christie (1986) posits that ideal victims are perceived to embody specific traits aligning with societal norms of innocence, vulnerability, and lack of culpability, eliciting positive societal reactions. This public response could potentially prevent crimes against potential victims or bring criminal actors to justice. Other scholars have utilized this concept to examine facets of cybercrime (Hock & Button, 2023; Loyens & Paraciani, 2023). Utilizing this concept, we explore not only the dynamics of scams targeting Nigerians but also global societal responses, including research funding allocations, to crimes affecting Nigerians as victims. We argue that power dynamics between the Global North and South, alongside the structure of the global economy, shape victim perception, with victims from the West perceived as more deserving of «ideal victim» status than Nigerians, thus influencing both regional and global responses to crimes perpetrated against Nigerians. Given the significant rise in online fraud victimization in Nigeria, for example, from 2019 to 2022, the issue is deeply concerning.

However, it is worth noting that the power dynamics and economic structures that shape victim perception are complex and multifaceted and should not be oversimplified or reduced to a single factor. Also, regional agencies and Nigerian authorities are primarily responsible for their citizens rather than shifting local responsibilities to external bodies and international communities (e.g., Western nations) to support victims of online fraud within Nigerian society. Finally, while online fraud victimization is indeed a serious issue in Nigeria, the phenomenon is not unique to the country and occurs in many other parts of the world as well.

Conclusion

Our study, derived from 896 participants, has presented insights into cybercrime victimization, focusing on gender disparities, socioeconomic factors, educational attainment's influence on online fraud vulnerability, and cybercrime victimization through the lens of ideal victimization juxtaposed with the North-South socioeconomic divide. Our analysis has highlighted gender differences in cybercrime victimization experiences, with a higher proportion of men experiencing negative consequences, aligning with prior research like Kadoya et al. (2021). We have offered fresh insights into this discourse, emphasizing the variability in gender disparities across contexts and the need for gender-sensitive approaches in addressing cybercrime. Secondly, our study has emphasized socioeconomic factors' pivotal role in cybercrime prevalence, particularly in Nigeria. The prevalence patterns of cybercrime incidents, especially E-Banking/ Payment-Card Fraud, have underscored socioeconomic dynamics in cybercrime perpetration in Nigeria, highlighting the centrality of the socioeconomic cybercrimes

category in Nigeria. Thirdly, we have shed light on the correlation between educational attainment and vulnerability to online fraud. While over 99 % of our participants were university-educated, the distribution across educational levels has varied, impacting susceptibility to cybercrime. Our findings align with existing research (Whitty, 2018), underscoring the nuanced relationship between education level and fraud victimization. Last but not least, considering the North-South socioeconomic divide, we have explored cybercrime victimization through the ideal victimization lens. Drawing upon Christie's (1986) ground-breaking work, we have delved into online fraud victimization dynamics within Nigeria, highlighting disparities in research attention and global responses to cybercrime affecting non-Western contexts. Our findings have emphasized the need for gender, inclusive, and contextual, sensitive approaches to cybercrime research and policymaking in Nigeria and beyond, given the global power dynamics discussed. These insights have informed the development of multidimensional and contextually sensitive approaches to address cybercrime and mitigate its impact on vulnerable populations worldwide.

References

Aborisade, R. A. (2023). Yahoo boys, yahoo parents? An explorative and qualitative study of parents' disposition towards children's involvement in cybercrimes. *Deviant Behavior*, *44*(7), 1102–1120. https://doi.org/10.1080/01639625.2022.2144779

Aborisade, R. A., Ocheja, A., & Okuneye, B. A. (2024). Emotional and financial costs of online dating scam: A phenomenological narrative of the experiences of victims of Nigerian romance fraudsters. *Journal of Economic Criminology*, *3*, 100044. https://doi.org/10.1016/j.jeconc.2023.100044

Adeduntan, A. (2022). Rhyme, reason, rogue: Yoruba popular music and the hip hop amoral turn. *Journal of Popular Music Studies*, *34*(1), 44–67. https://doi.org/10.1525/jpms.2022.34.1.44

Akoto, W. (2021). International trade and cyber conflict: Decomposing the effect of trade on state-sponsored cyber attacks. *Journal of Peace Research*, *58*(5), 1083–1097. https://doi.org/10.1177/0022343320964549

Akoto, W. (2024). Who spies on whom? Unravelling the puzzle of state-sponsored cyber economic espionage. *Journal of Peace Research*, *61*(1), 59–71. https://doi.org/10.1177/00223433231214417

Aransiola, J. O., & Asindemade, S. O. (2011). Understanding cybercrime perpetrators and the strategies they employ in Nigeria. *Cyberpsychology, Behavior, and Social Networking*, 14(12), 759–763. https://doi.org/10.1089/cyber.2010.0307

Button, M., Hock, B., Shepherd, D., & Gilmour, P. (2023). Understanding the rise of fraud in England and Wales through field theory: Blip or flip? *Journal of Economic Criminology*, *1*, 100012. https://doi.org/10.1016/j.jeconc.2023.100012

Button, M., Nicholls, C. M, Kerr, J., & Owen, R. (2015). Online Fraud Victims in England and Wales: Victims' Views on Sentencing and the Opportunity for Restorative Justice? *The Howard Journal of Criminal Justice*, *54*(2), 193–211. https://doi.org/10.1111/hojo.12123

Button, M., Nicholls, C. M., Kerr, J., & Owen, R. (2014). Online frauds: Learning from victims why they fall for these scams. *Australian & New Zealand Journal of Criminology*, *47*(3), 391–408. https://doi.org/10.1177/0004865814521224

Button, M., Blackbourn, D., Sugiura, L., Shepherd, D., Kapend, R., & Wang, V. (2021). From feeling like rape to a minor inconvenience: Victims' accounts of the impact of computer misuse crime in the United Kingdom. *Telematics and Informatics*, *64*, 101675. https://doi.org/10.1016/j.tele.2021.101675

Christie, N. (1986). The ideal victim. In E. A. Fattah (Ed.), *From crime policy to victim policy* (pp. 17–30). Palgrave Macmillan. https://doi.org/10.1007/978-1-349-08305-3_2

Cross, C. (2018a). Marginalized voices: The absence of Nigerian scholars in global examinations of online fraud. In K. Carrington, R. Hogg, J. Scott, & M. Sozzo (Eds.), *The Palgrave Handbook of Criminology and the Global South* (pp. 261–280). Palgrave Macmillan. https://doi.org/10.1007/978-3-319-65021-0_14

Cross, C. (2018b). Expectations vs reality: Responding to online fraud across the fraud justice network. *International Journal of Law, Crime and Justice*, *55*, 1–12. https://doi.org/10.1016/j.ijlcj.2018.08.001

Cross, C. (2020). 'Oh we can't actually do anything about that': The problematic nature of jurisdiction for online fraud victims. *Criminology & Criminal Justice*, *20*(3), 358–375. https://doi.org/10.1177/1748895819835910

De Kimpe, L., Ponnet, K., Walrave, M., Snaphaan, T., Pauwels, L., & Hardyns, W. (2020). Help, I need somebody: Examining the antecedents of social support seeking among cybercrime victims. *Computers in Human Behavior*, *108*, 106310. https://doi.org/10.1016/j.chb.2020.106310

Drew, J. M., & Webster, J. (2024). The victimology of online fraud: A focus on romance fraud victimisation. *Journal of Economic Criminology*, *3*, 100053. https://doi.org/10.1016/j.jeconc.2024.100053

Genc, Y., Kour, H., Arslan, H. T., & Chen, L. C. (2021). Understanding Nigerian e-mail scams: A computational content analysis approach. *Information Security Journal: A Global Perspective*, *30*(2), 88–99. https://doi.org/10.1080/19393555.2020.1804647

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology*, *2*, 13–20. https://doi.org/10.1007/s11416-006-0015-z

Hall, T., & Yarwood, R. (2024). New geographies of crime? Cybercrime, southern criminology and diversifying research agendas. *Progress in Human Geography*, *48*(4), 437–457. https://doi.org/10.1177/03091325241246015

Harper, C. A., Smith, L., Leach, J., Daruwala, N. A., & Fido, D. (2023). Development and Validation of the Beliefs About Revenge Pornography Questionnaire. *Sexual Abuse*, *35*(6), 748–783. https://doi.org/10.1177/10790632221082663

Hock, B., & Button, M. (2023). Non-ideal victims or offenders? The curious case of pyramid scheme participants. *Victims and Offenders*, *18*(7), 1311–1334. https://doi.org/10.1080/15564886.2023.2186996

Ibrahim, S. (2016a). Social and contextual taxonomy of cybercrime: Socioeconomic theory of Nigerian cybercriminals. *International Journal of Law, Crime and Justice*, *47*, 44–57. https://doi.org/10.1016/j.ijlcj.2016.07.002

Ibrahim, S. (2016b). Causes of socioeconomic cybercrime in Nigeria. In *IEEE International Conference on Cybercrime and Computer Forensic (ICCCF)*, Vancouver, BC, Canada (pp. 1–9). IEEE. https://doi.org/10.1109/icccf.2016.7740439

Idem, U. J. (2023). The Legal Approach for Fighting Cybercrimes in Nigeria: Some Lessons from the United States and the United Kingdom. In *2023 International Conference On Cyber Management And Engineering (CyMaEn)* (pp. 191–198). IEEE. https://doi.org/10.1109/cymaen57228.2023.10050983

Idem, U. J., & Olarinde, E. S. (2023). Cybercrime and its Negative Effects on Youth's Development, the Economy and Nigeria. In *2023 International Conference On Cyber Management And Engineering (CyMaEn)* (pp. 199–204). IEEE. https://doi.org/10.1109/cymaen57228.2023.10051047

Idem, U. J., Olarinde, E. S., Anwana, E. O., Ogundele, A. T., Awodiran, M. A., & Omomen, M. A. (2023a). The Prosecution of Cybercrimes in Nigeria: Challenges and Prospects. In *2023 International Conference On Cyber Management And Engineering (CyMaEn)* (pp. 178–183). IEEE. https://doi.org/10.1109/cymaen57228.2023.10050896

Idem, U. J., Olarinde, E. S., Ikpeze, N. G., Emem, O., Ogundele, A. T., & Awodiran, M. A. (2023b). Cybercrime Regulatory Agencies need urgent Reform to Protect Nigeria. In *2023 International Conference On Cyber Management And Engineering (CyMaEn)* (pp. 184–190). IEEE. https://doi.org/10.1109/cymaen57228.2023.10050994

Jaishankar, K. (2011). Introduction: Expanding Cyber Criminology with an Avant-Garde Anthology. In *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior* (pp. xxvii–xxxv). Boca Raton: CRC Press.

Jaishankar, K. (2007). Cyber criminology: Evolving a novel discipline with a new journal. *International Journal of Cyber Criminology*, *1*(1), 1–6. https://doi.org/10.5281/zenodo.18276

Jaishankar, K. (2018). Cyber criminology as an academic discipline: history, contribution and impact. *International Journal of Cyber Criminology*, *12*(1), 1–8. https://doi.org/10.5281/zenodo.1467308

Kadoya, Y., Khan, M. S. R., Narumoto, J., & Watanabe, S. (2021). Who is next? A study on victims of financial fraud in Japan. *Frontiers in Psychology*, *12*, 649565. https://doi.org/10.3389/fpsyg.2021.649565

Lazarus, S. (2019). Where is the Money? The Intersectionality of the Spirit World and the Acquisition of Wealth. *Religions*, *10*(3), 146. https://doi.org/10.3390/rel10030146

Lazarus, S. (2024). Cybercriminal Networks and Operational Dynamics of Business Email Compromise (BEC) Scammers: Insights from the «Black Axe» Confraternity. *Deviant Behavior*, 1–25. https://doi.org/10.1080/01639625.2024.2352049

Lazarus, S., & Button, M. (2022). Tweets and Reactions: Revealing the Geographies of Cybercrime Perpetrators and the North-South Divide. *Cyberpsychology, Behavior, and Social Networking*, *25*(8), 504–511. https://doi.org/10.1089/cyber.2021.0332

Lazarus, S., & Okolorie, G. U. (2019). The Bifurcation of the Nigerian Cybercriminals: Narratives of the Economic and Financial Crimes Commission (EFCC) Agents. *Telematics and Informatics*, *40*, 14–26. https://doi.org/10.1016/j.tele.2019.04.009

Lazarus, S., Button, M., & Adogame, A. (2022a). Advantageous Comparison: Using Twitter Responses to Understand Similarities between Cybercriminals ("Yahoo Boys") and Politicians ("Yahoo men"). *Heliyon*, *8*(11), e11142. https://doi.org/10.1016/j.heliyon.2022.e11142

Lazarus, S., Button, M., & Kapend, R. (2022b). Exploring the value of feminist theory in understanding digital crimes: Gender and cybercrime types. *The Howard Journal of Crime and Justice*, *61*(3), 381–398. https://doi.org/10.1111/hojo.12485

Lazarus, S., Olaigbe, O., Adeduntan, A., Dibiana, E. T., & Okolorie, G. U. (2023). Cheques or Dating Scams? Online Fraud Themes in Hip-Hop Songs Across Popular Music Apps. *Journal of Economic Criminology*, *2*, 100033. https://doi.org/10.1016/j.jeconc.2023.100033

Loyens, K., & Paraciani, R. (2023). Who is the ("Ideal") Victim of Labor Exploitation? Two Qualitative Vignette Studies on Labor Inspectors' Discretion. *The Sociological Quarterly*, *64*(1), 27–45. https://doi.org/10.1080/00380253.2021.1974321

Makridis, C., Maschmeyer, L., & Smeets, M. (2024). If it bleeps it leads? Media coverage on cyber conflict and misperception. *Journal of Peace Research*, *61*(1), 72–86. https://doi.org/10.1177/00223433231220264

Mba, G., Onaolapo, J., Stringhini, G., & Cavallaro, L. (2017, April). Flipping 419 cybercrime scams: Targeting the weak and the vulnerable. In *Proceedings of the 26th International Conference on World Wide Web Companion* (pp. 1301–1310). https://doi.org/10.1145/3041021.3053892

McGerty, L. J. (2000). «Nobody lives only in cyberspace»: Gendered subjectivities and domestic use of the Internet. *CyberPsychology & Behavior*, *3*(5), 895–899. https://doi.org/10.1089/10949310050191863

Meikle, W., & Cross, C. (2024). "What action should I take?": Help-seeking behaviours of those targeted by romance fraud. *Journal of Economic Criminology*, *3*, 100054. https://doi.org/10.1016/j.jeconc.2024.100054

Monsurat, I. (2020). African insurance (spiritualism) and the success rate of cybercriminals in Nigeria: a study of the Yahoo Boys in Ilorin, Nigeria. *International Journal of Cyber Criminology*, *14*(1), 300–315. https://doi.org/10.5281/zenodo.3755848

Mosbah-Natanson, S., & Gingras, Y. (2014). The globalization of social sciences? Evidence from a quantitative analysis of 30 years of production, collaboration and citations in the social sciences (1980–2009). *Current Sociology*, *62*(5), 626–646. https://doi.org/10.1177/0011392113498866

Murça, A., Cunha, O., & Almeida, T. C. (2024). Prevalence and Impact of Revenge Pornography on a Sample of Portuguese Women. *Sexuality & Culture*, *28*(1), 96–112. https://doi.org/10.1007/s12119-023-10100-3

Musotto, R., & Wall, D. S. (2020). More Amazon than Mafia: analysing a DDoS stresser service as organised cybercrime. *Trends in Organized Crime*, *25*, 173–191. https://doi.org/10.1007/s12117-020-09397-5

Näsi, M., Danielsson, P., & Kaakinen, M. (2023). Cybercrime Victimisation and Polyvictimisation in Finland – Prevalence and Risk Factors. *European Journal on Criminal Policy and Research*, *29*, 283–301. https://doi.org/10.1007/s10610-021-09497-0

Norris, G., Brookes, A., & Dowell, D. (2019). The Psychology of Internet Fraud Victimisation: a Systematic Review. *Journal of Police and Criminal Psychology*, *34*, 231–245. https://doi.org/10.1007/s11896-019-09334-5

Ogunleye, Y. O., Ojedokun, U. A., & Aderinto, A. A. (2019). Pathways and Motivations for Cyber Fraud Involvement among Female Undergraduates of Selected Universities in South-West Nigeria. *International Journal of Cyber Criminology*, *13*(2). https://doi.org/10.5281/zenodo.3702333

Ojedokun, U. A., & Eraye, M. C. (2012). Socioeconomic lifestyles of the yahoo-boys: A study of perceptions of university students in Nigeria. *International Journal of Cyber Criminology*, *6*(2), 1001–1013.

Ojolo, T. L., & Singh, S. B. (2023). Interrogating the Yahoo-Yahoo Menace: An Analysis of Moral Decadence, Poverty, and Unemployment In Nigeria. *Journal of African Films and Diaspora Studies*, *6*(1), 55. https://doi.org/10.31920/2516-2713/2023/6n1a4

Ojolo, T., & Adewumi, S. A. (2020). Understanding youths' perception and factors advancing cybercrime (yahoo-yahoo) in Ado-Ekiti, Ekiti State, Nigeria. *African Journal of Gender, Society & Development*, *9*(4), 243. https://doi.org/10.31920/2634-3622/2020/v9n4a11

Okpa, J. T., Ajah, B. O., Nzeakor, O. F., Eshiotse, E., & Abang, T. A. (2023). Business e-mail compromise scam, cyber victimization, and economic sustainability of corporate organizations in Nigeria. *Security Journal*, *36*(2), 350–372. https://doi.org/10.1057/s41284-022-00342-5

Olaiya, T. A., Lamidi, K. O., & Bello, M. A. (2020). Narrative of illicit money: 'Yahoo'Boy (Format) of cyber scams and governance challenges in Africa. *Global Journal of Interdisciplinary Social Sciences*, *9*(2), 003.

Paek, S. Y., & Nalla, M. K. (2015). The relationship between receiving phishing attempt and identity theft victimization in South Korea. International Journal of Law, Crime and Justice, 43(4), 626–642. https://doi.org/10.1016/j.ijlcj.2015.02.003

Powell, A., Stratton, G., & Cameron, R. (2018). *Digital criminology: Crime and justice in digital society*. New Delhi: Routledge. https://doi.org/10.4324/9781315205786

Rich, T. (2018). You can trust me: A multimethod analysis of the Nigerian email scam. *Security Journal*, *31*, 208–225. https://doi.org/10.1057/s41284-017-0095-0

Schoepfer, A., & Piquero, N. L. (2009). Studying the correlates of fraud victimization and reporting. *Journal of Criminal Justice*, *37*(2), 209–215. https://doi.org/10.1016/j.jcrimjus.2009.02.003

Tade, O., & Adeniyi, O. (2017). 'They withdrew all I was worth': Automated teller machine fraud and victims' life chances in Nigeria. *International Review of Victimology*, *23*(3), 313–324. https://doi.org/10.1177/0269758017704330

Tao, H. (2022). Loving strangers, avoiding risks: Online dating practices and scams among Chinese lesbian (lala) women. Media, Culture & Society, 44(6), 1199–1214. https://doi.org/10.1177/01634437221088952

Timofeyev, Y., & Dremova, O. (2022). Insurers' responses to cyber crime: evidence from Russia. *International Journal of Law, Crime and Justice*, *68*, 100520. https://doi.org/10.1016/j.ijlcj.2021.100520

Wang, F. (2023). Sentencing Disparity and Focal Concern: An Assessment of Judicial Decisions on Sha Zhu Pan Cases Collected From China Judgements Online. *Crime & Delinquency*, *0*(0). https://doi.org/10.1177/00111287231158571

Wang, F., & Topalli, V. (2024). Understanding romance scammers through the lens of their victims: qualitative modeling of risk and protective factors in the online context. *American Journal of Criminal Justice*, *49*(1), 145–181. https://doi.org/10.1007/s12103-022-09706-4

Weijer van de, S., Leukfeldt, R., & Van der Zee, S. (2020). Reporting cybercrime victimization: determinants, motives, and previous experiences. *Policing: An International Journal*, *43*(1), 17–34. https://doi.org/10.1108/PIJPSM-07-2019-0122

Whittaker, J. M., Lazarus, S., & Corcoran, T. (2024). Are fraud victims nothing more than animals? Critiquing the propagation of "pig butchering" (Sha Zhu Pan, 杀猪盘). *Journal of Economic Criminology*, *3*, 100052. https://doi.org/10.1016/j.jeconc.2024.100052

Whitty, M. (2018). Do you love me? Psychological characteristics of Romance scam victims. *Cyberpsychology Behavior and Social Networking*, *21*(2), 105–109. https://doi.org/10.1089/cyber.2016.0729

Whitty, M. T. (2019). Predicting susceptibility to cyber-fraud victimhood. *Journal of Financial Crime*, *26*(1), 277–292. https://doi.org/10.1108/jfc-10-2017-0095

Authors information

Aminu Muhammad Auwal – Bachelor of Science in Information Technology, IT Specialist, University of Jos
Address: PMB 2084, Jos, Plateau State, Nigeria
E-mail: i.elameenu@gmail.com
ORCID ID: https://orcid.org/0009-0005-1799-7876
WoS Researcher ID: https://www.webofscience.com/wos/author/record/JFS-7098-2023
Google Scholar ID: https://scholar.google.com/citations?user=RDxPEr4AAAAJ

Suleman Lazarus – PhD in Cybercrime and Criminology, Visiting Fellow at the Mannheim Centre for Criminology, London School of Economics and Political Science; Fellow at the Centre of Excellence on Ageing, University of Surrey; Honorary Lecturer at the Centre for Cybercrime and Economic Crime, University of Portsmouth.
Address: Houghton Street, London, WC2A 2AE, United Kingdom; Stag Hill, Guildford, GU2 7XH, United Kingdom; St. George's Building, Portsmouth, PO1 2HY, United Kingdom.
E-mail: suleman.lazarus@gmail.com
ORCID ID: https://orcid.org/0000-0003-1721-8519
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57205679641
WoS ResearcherID: https://www.webofscience.com/wos/author/record/629543
Google Scholar ID: https://scholar.google.com/citations?user=Em8EXqcAAAAJ

Authors' contributions

The authors have contributed equally into the concept and methodology elaboration, validation, formal analysis, research, selection of sources, text writing and editing, project guidance and management.

Conflict of interest

The authors declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law
PASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – May 16, 2024
Date of approval – May 28, 2024
Date of acceptance – December 13, 2024
Date of online placement – December 20, 2024

Научная статья
УДК 34:004:343.9:004.8
EDN: https://elibrary.ru/jvglrh
DOI: https://doi.org/10.21202/jdtl.2024.44

Социолого-криминологическое исследование проблем виктимизации: предварительный этап и новая область категоризации киберпреступности

Амину Мухаммад Аувал

Университет Джоса, Джос, Нигерия

Сулеман Лазарус ✉

Лондонская школа экономики и политических наук, Лондон, Великобритания
Университет Суррея, Гилфорд, Великобритания
Портсмутский университет, Портсмут, Великобритания

Ключевые слова

виктимизация,
виктимология,
жертва киберпреступления,
киберкриминология,
киберпреступность,
кибершпионаж,
онлайн-мошенничество,
правовая политика,
цифровая криминология,
цифровые технологии

Аннотация

Цель: выявление основных проблем виктимизации в результате роста киберпреступности в мире в целом и в нигерийском обществе в частности с позиций социологических подходов и с помощью трехчастной концепции киберпреступности (Tripartite Cybercrime Framework, TCF), состоящей из геополитических, психосоциальных и социально-экономических категорий киберпреступности.

Методы: основу методологии составили социологический метод исследования. Процесс сбора данных включал распространение опросника среди 896 участников из академической среды, в том числе студентов и сотрудников университета, и анализ ответов респондентов. Представленные данные анализировались с помощью описательной статистики, особое внимание при этом было уделено вопросам гендерного неравенства, социально-экономическим факторам, влиянию уровня образования на уязвимость к онлайн-мошенничеству и виктимизации в результате киберпреступлений через призму концепции идеальной жертвы и социально-экономического разрыва между Севером и Югом.

Результаты: в статье представлен анализ трехчастной концепции киберпреступности. На основе изучения данных, полученных в ходе анкетирования, установлено, что 65,20% участников опроса когда-либо становились жертвами киберпреступников. Выявлен гендерный перекос среди жертв киберпреступлений в сторону мужчин (64,69%).

✉ Корреспондирующий автор
© Аувал А. М., Лазарус С., 2024

Статья находится в открытом доступе и распространяется в соответствии с лицензией Creative Commons «Attribution» («Атрибуция») 4.0 Всемирная (CC BY 4.0) (https://creativecommons.org/licenses/by/4.0/deed.ru), позволяющей неограниченно использовать, распространять и воспроизводить материал при условии, что оригинальная работа упомянута с соблюдением правил цитирования.

Установлены закономерности в распределении киберпреступлений. Все киберпреступления против опрошенных лиц относились к категории социально-экономических, что подчеркивает распространенность киберпреступности и актуальность противодействия ей в нигерийском социуме. Особое внимание уделено вопросам гендерного неравенства, социально-экономическим факторам, влиянию уровня образования на уязвимость к киберпреступлениям. Проблема виктимизации рассмотрена с точки зрения концепции идеальной жертвы. **Результаты** исследования позволяют получить представление о распространенности и распределении конкретных видов киберпреступности социально-экономической категории среди исследуемой группы населения.

Научная новизна: в исследовании впервые используется подход трехчастной концепции киберпреступности (TCF) для изучения виктимизации в результате киберпреступлений в нигерийском обществе. Новизна представленного исследования обусловлена еще и тем, что сложившиеся на глобальном Севере концептуальные основы противодействия киберпреступности не вполне применимы в Нигерии.

Практическая значимость: полученные результаты демонстрируют необходимость применения тщательно выверенных гендерных, инклюзивных и контекстуальных подходов к разработке национальной правовой политики борьбы с киберпреступностью, могут быть положены в обоснование разрабатываемых правотворческих решений в области предупреждения и противодействия проявлениям киберпреступности, а также в основу правовых мер защиты жертв киберпреступлений.

Для цитирования

Аувал, А. М., Лазарус, С. (2024). Социолого-криминологическое исследование проблем виктимизации: предварительный этап и новая область категоризации киберпреступности. *Journal of Digital Technologies and Law*, *2*(4), 915–942. https://doi.org/10.21202/jdtl.2024.44

Список литературы

Aborisade, R. A. (2023). Yahoo boys, yahoo parents? An explorative and qualitative study of parents' disposition towards children's involvement in cybercrimes. *Deviant Behavior*, *44*(7), 1102–1120. https://doi.org/10.1080/01639625.2022.2144779

Aborisade, R. A., Ocheja, A., & Okuneye, B. A. (2024). Emotional and financial costs of online dating scam: A phenomenological narrative of the experiences of victims of Nigerian romance fraudsters. *Journal of Economic Criminology*, *3*, 100044. https://doi.org/10.1016/j.jeconc.2023.100044

Adeduntan, A. (2022). Rhyme, reason, rogue: Yoruba popular music and the hip hop amoral turn. *Journal of Popular Music Studies*, *34*(1), 44–67. https://doi.org/10.1525/jpms.2022.34.1.44

Akoto, W. (2021). International trade and cyber conflict: Decomposing the effect of trade on state-sponsored cyber attacks. *Journal of Peace Research*, *58*(5), 1083–1097. https://doi.org/10.1177/0022343320964549

Akoto, W. (2024). Who spies on whom? Unravelling the puzzle of state-sponsored cyber economic espionage. *Journal of Peace Research*, *61*(1), 59–71. https://doi.org/10.1177/00223433231214417

Aransiola, J. O., & Asindemade, S. O. (2011). Understanding cybercrime perpetrators and the strategies they employ in Nigeria. *Cyberpsychology, Behavior, and Social Networking*, 14(12), 759–763. https://doi.org/10.1089/cyber.2010.0307

Button, M., Hock, B., Shepherd, D., & Gilmour, P. (2023). Understanding the rise of fraud in England and Wales through field theory: Blip or flip? *Journal of Economic Criminology*, *1*, 100012. https://doi.org/10.1016/j.jeconc.2023.100012

Button, M., Nicholls, C. M, Kerr, J., & Owen, R. (2015). Online Fraud Victims in England and Wales: Victims' Views on Sentencing and the Opportunity for Restorative Justice? *The Howard Journal of Criminal Justice*, *54*(2), 193–211. https://doi.org/10.1111/hojo.12123

Button, M., Nicholls, C. M., Kerr, J., & Owen, R. (2014). Online frauds: Learning from victims why they fall for these scams. *Australian & New Zealand Journal of Criminology*, *47*(3), 391–408. https://doi.org/10.1177/0004865814521224

Button, M., Blackbourn, D., Sugiura, L., Shepherd, D., Kapend, R., & Wang, V. (2021). From feeling like rape to a minor inconvenience: Victims' accounts of the impact of computer misuse crime in the United Kingdom. *Telematics and Informatics*, *64*, 101675. https://doi.org/10.1016/j.tele.2021.101675

Christie, N. (1986). The ideal victim. In E. A. Fattah (Ed.), *From crime policy to victim policy* (pp. 17–30). Palgrave Macmillan. https://doi.org/10.1007/978-1-349-08305-3_2

Cross, C. (2018a). Marginalized voices: The absence of Nigerian scholars in global examinations of online fraud. In K. Carrington, R. Hogg, J. Scott, & M. Sozzo (Eds.), *The Palgrave Handbook of Criminology and the Global South* (pp. 261–280). Palgrave Macmillan. https://doi.org/10.1007/978-3-319-65021-0_14

Cross, C. (2018b). Expectations vs reality: Responding to online fraud across the fraud justice network. *International Journal of Law, Crime and Justice*, *55*, 1–12. https://doi.org/10.1016/j.ijlcj.2018.08.001

Cross, C. (2020). 'Oh we can't actually do anything about that': The problematic nature of jurisdiction for online fraud victims. *Criminology & Criminal Justice*, *20*(3), 358–375. https://doi.org/10.1177/1748895819835910

De Kimpe, L., Ponnet, K., Walrave, M., Snaphaan, T., Pauwels, L., & Hardyns, W. (2020). Help, I need somebody: Examining the antecedents of social support seeking among cybercrime victims. *Computers in Human Behavior*, *108*, 106310. https://doi.org/10.1016/j.chb.2020.106310

Drew, J. M., & Webster, J. (2024). The victimology of online fraud: A focus on romance fraud victimisation. *Journal of Economic Criminology*, *3*, 100053. https://doi.org/10.1016/j.jeconc.2024.100053

Genc, Y., Kour, H., Arslan, H. T., & Chen, L. C. (2021). Understanding Nigerian e-mail scams: A computational content analysis approach. *Information Security Journal: A Global Perspective*, *30*(2), 88–99. https://doi.org/10.1080/19393555.2020.1804647

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology*, *2*, 13–20. https://doi.org/10.1007/s11416-006-0015-z

Hall, T., & Yarwood, R. (2024). New geographies of crime? Cybercrime, southern criminology and diversifying research agendas. *Progress in Human Geography*, *48*(4), 437–457. https://doi.org/10.1177/03091325241246015

Harper, C. A., Smith, L., Leach, J., Daruwala, N. A., & Fido, D. (2023). Development and Validation of the Beliefs About Revenge Pornography Questionnaire. *Sexual Abuse*, *35*(6), 748–783. https://doi.org/10.1177/10790632221082663

Hock, B., & Button, M. (2023). Non-ideal victims or offenders? The curious case of pyramid scheme participants. *Victims and Offenders*, *18*(7), 1311–1334. https://doi.org/10.1080/15564886.2023.2186996

Ibrahim, S. (2016a). Social and contextual taxonomy of cybercrime: Socioeconomic theory of Nigerian cybercriminals. *International Journal of Law, Crime and Justice*, *47*, 44–57. https://doi.org/10.1016/j.ijlcj.2016.07.002

Ibrahim, S. (2016b). Causes of socioeconomic cybercrime in Nigeria. In *IEEE International Conference on Cybercrime and Computer Forensic (ICCCF)*, Vancouver, BC, Canada (pp. 1–9). IEEE. https://doi.org/10.1109/icccf.2016.7740439

Idem, U. J. (2023). The Legal Approach for Fighting Cybercrimes in Nigeria: Some Lessons from the United States and the United Kingdom. In *2023 International Conference On Cyber Management And Engineering (CyMaEn)* (pp. 191–198). IEEE. https://doi.org/10.1109/cymaen57228.2023.10050983

Idem, U. J., & Olarinde, E. S. (2023). Cybercrime and its Negative Effects on Youth's Development, the Economy and Nigeria. In *2023 International Conference On Cyber Management And Engineering (CyMaEn)* (pp. 199–204). IEEE. https://doi.org/10.1109/cymaen57228.2023.10051047

Idem, U. J., Olarinde, E. S., Anwana, E. O., Ogundele, A. T., Awodiran, M. A., & Omomen, M. A. (2023a). The Prosecution of Cybercrimes in Nigeria: Challenges and Prospects. In *2023 International Conference On Cyber Management And Engineering (CyMaEn)* (pp. 178–183). IEEE. https://doi.org/10.1109/cymaen57228.2023.10050896

Idem, U. J., Olarinde, E. S., Ikpeze, N. G., Emem, O., Ogundele, A. T., & Awodiran, M. A. (2023b). Cybercrime Regulatory Agencies need urgent Reform to Protect Nigeria. In *2023 International Conference On Cyber Management And Engineering (CyMaEn)* (pp. 184–190). IEEE. https://doi.org/10.1109/cymaen57228.2023.10050994

Jaishankar, K. (2011). Introduction: Expanding Cyber Criminology with an Avant-Garde Anthology. In *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior* (pp. xxvii–xxxv). Boca Raton: CRC Press.

Jaishankar, K. (2007). Cyber criminology: Evolving a novel discipline with a new journal. *International Journal of Cyber Criminology*, *1*(1), 1–6. https://doi.org/10.5281/zenodo.18276

Jaishankar, K. (2018). Cyber criminology as an academic discipline: history, contribution and impact. *International Journal of Cyber Criminology*, *12*(1), 1–8. https://doi.org/10.5281/zenodo.1467308

Kadoya, Y., Khan, M. S. R., Narumoto, J., & Watanabe, S. (2021). Who is next? A study on victims of financial fraud in Japan. *Frontiers in Psychology*, *12*, 649565. https://doi.org/10.3389/fpsyg.2021.649565

Lazarus, S. (2019). Where is the Money? The Intersectionality of the Spirit World and the Acquisition of Wealth. *Religions*, *10*(3), 146. https://doi.org/10.3390/rel10030146

Lazarus, S. (2024). Cybercriminal Networks and Operational Dynamics of Business Email Compromise (BEC) Scammers: Insights from the «Black Axe» Confraternity. *Deviant Behavior*, 1–25. https://doi.org/10.1080/01639625.2024.2352049

Lazarus, S., & Button, M. (2022). Tweets and Reactions: Revealing the Geographies of Cybercrime Perpetrators and the North-South Divide. *Cyberpsychology, Behavior, and Social Networking*, *25*(8), 504–511. https://doi.org/10.1089/cyber.2021.0332

Lazarus, S., & Okolorie, G. U. (2019). The Bifurcation of the Nigerian Cybercriminals: Narratives of the Economic and Financial Crimes Commission (EFCC) Agents. *Telematics and Informatics*, *40*, 14–26. https://doi.org/10.1016/j.tele.2019.04.009

Lazarus, S., Button, M., & Adogame, A. (2022a). Advantageous Comparison: Using Twitter Responses to Understand Similarities between Cybercriminals ("Yahoo Boys") and Politicians ("Yahoo men"). *Heliyon*, *8*(11), e11142. https://doi.org/10.1016/j.heliyon.2022.e11142

Lazarus, S., Button, M., & Kapend, R. (2022b). Exploring the value of feminist theory in understanding digital crimes: Gender and cybercrime types. *The Howard Journal of Crime and Justice*, *61*(3), 381–398. https://doi.org/10.1111/hojo.12485

Lazarus, S., Olaigbe, O., Adeduntan, A., Dibiana, E. T., & Okolorie, G. U. (2023). Cheques or Dating Scams? Online Fraud Themes in Hip-Hop Songs Across Popular Music Apps. *Journal of Economic Criminology*, *2*, 100033. https://doi.org/10.1016/j.jeconc.2023.100033

Loyens, K., & Paraciani, R. (2023). Who is the ("Ideal") Victim of Labor Exploitation? Two Qualitative Vignette Studies on Labor Inspectors' Discretion. *The Sociological Quarterly*, *64*(1), 27–45. https://doi.org/10.1080/00380253.2021.1974321

Makridis, C., Maschmeyer, L., & Smeets, M. (2024). If it bleeps it leads? Media coverage on cyber conflict and misperception. *Journal of Peace Research*, *61*(1), 72–86. https://doi.org/10.1177/00223433231220264

Mba, G., Onaolapo, J., Stringhini, G., & Cavallaro, L. (2017, April). Flipping 419 cybercrime scams: Targeting the weak and the vulnerable. In *Proceedings of the 26th International Conference on World Wide Web Companion* (pp. 1301–1310). https://doi.org/10.1145/3041021.3053892

McGerty, L. J. (2000). «Nobody lives only in cyberspace»: Gendered subjectivities and domestic use of the Internet. *CyberPsychology & Behavior*, *3*(5), 895–899. https://doi.org/10.1089/10949310050191863

Meikle, W., & Cross, C. (2024). "What action should I take?": Help-seeking behaviours of those targeted by romance fraud. *Journal of Economic Criminology*, *3*, 100054. https://doi.org/10.1016/j.jeconc.2024.100054

Monsurat, I. (2020). African insurance (spiritualism) and the success rate of cybercriminals in Nigeria: a study of the Yahoo Boys in Ilorin, Nigeria. *International Journal of Cyber Criminology*, *14*(1), 300–315. https://doi.org/10.5281/zenodo.3755848

Mosbah-Natanson, S., & Gingras, Y. (2014). The globalization of social sciences? Evidence from a quantitative analysis of 30 years of production, collaboration and citations in the social sciences (1980–2009). *Current Sociology*, *62*(5), 626–646. https://doi.org/10.1177/0011392113498866

Murça, A., Cunha, O., & Almeida, T. C. (2024). Prevalence and Impact of Revenge Pornography on a Sample of Portuguese Women. *Sexuality & Culture*, *28*(1), 96–112. https://doi.org/10.1007/s12119-023-10100-3

Musotto, R., & Wall, D. S. (2020). More Amazon than Mafia: analysing a DDoS stresser service as organised cybercrime. *Trends in Organized Crime*, *25*, 173–191. https://doi.org/10.1007/s12117-020-09397-5

Näsi, M., Danielsson, P., & Kaakinen, M. (2023). Cybercrime Victimisation and Polyvictimisation in Finland – Prevalence and Risk Factors. *European Journal on Criminal Policy and Research*, *29*, 283–301. https://doi.org/10.1007/s10610-021-09497-0

Norris, G., Brookes, A., & Dowell, D. (2019). The Psychology of Internet Fraud Victimisation: a Systematic Review. *Journal of Police and Criminal Psychology*, *34*, 231–245. https://doi.org/10.1007/s11896-019-09334-5

Ogunleye, Y. O., Ojedokun, U. A., & Aderinto, A. A. (2019). Pathways and Motivations for Cyber Fraud Involvement among Female Undergraduates of Selected Universities in South-West Nigeria. *International Journal of Cyber Criminology*, *13*(2). https://doi.org/10.5281/zenodo.3702333

Ojedokun, U. A., & Eraye, M. C. (2012). Socioeconomic lifestyles of the yahoo-boys: A study of perceptions of university students in Nigeria. *International Journal of Cyber Criminology*, *6*(2), 1001–1013.

Ojolo, T. L., & Singh, S. B. (2023). Interrogating the Yahoo-Yahoo Menace: An Analysis of Moral Decadence, Poverty, and Unemployment In Nigeria. *Journal of African Films and Diaspora Studies*, *6*(1), 55. https://doi.org/10.31920/2516-2713/2023/6n1a4

Ojolo, T., & Adewumi, S. A. (2020). Understanding youths' perception and factors advancing cybercrime (yahoo-yahoo) in Ado-Ekiti, Ekiti State, Nigeria. *African Journal of Gender, Society & Development*, *9*(4), 243. https://doi.org/10.31920/2634-3622/2020/v9n4a11

Okpa, J. T., Ajah, B. O., Nzeakor, O. F., Eshiotse, E., & Abang, T. A. (2023). Business e-mail compromise scam, cyber victimization, and economic sustainability of corporate organizations in Nigeria. *Security Journal*, *36*(2), 350–372. https://doi.org/10.1057/s41284-022-00342-5

Olaiya, T. A., Lamidi, K. O., & Bello, M. A. (2020). Narrative of illicit money: 'Yahoo'Boy (Format) of cyber scams and governance challenges in Africa. *Global Journal of Interdisciplinary Social Sciences*, *9*(2), 003.

Paek, S. Y., & Nalla, M. K. (2015). The relationship between receiving phishing attempt and identity theft victimization in South Korea. International Journal of Law, Crime and Justice, 43(4), 626–642. https://doi.org/10.1016/j.ijlcj.2015.02.003

Powell, A., Stratton, G., & Cameron, R. (2018). *Digital criminology: Crime and justice in digital society*. New Delhi: Routledge. https://doi.org/10.4324/9781315205786

Rich, T. (2018). You can trust me: A multimethod analysis of the Nigerian email scam. *Security Journal*, *31*, 208–225. https://doi.org/10.1057/s41284-017-0095-0

Schoepfer, A., & Piquero, N. L. (2009). Studying the correlates of fraud victimization and reporting. *Journal of Criminal Justice*, *37*(2), 209–215. https://doi.org/10.1016/j.jcrimjus.2009.02.003

Tade, O., & Adeniyi, O. (2017). 'They withdrew all I was worth': Automated teller machine fraud and victims' life chances in Nigeria. *International Review of Victimology*, *23*(3), 313–324. https://doi.org/10.1177/0269758017704330

Tao, H. (2022). Loving strangers, avoiding risks: Online dating practices and scams among Chinese lesbian (lala) women. Media, Culture & Society, 44(6), 1199–1214. https://doi.org/10.1177/01634437221088952

Timofeyev, Y., & Dremova, O. (2022). Insurers' responses to cyber crime: evidence from Russia. *International Journal of Law, Crime and Justice*, *68*, 100520. https://doi.org/10.1016/j.ijlcj.2021.100520

Wang, F. (2023). Sentencing Disparity and Focal Concern: An Assessment of Judicial Decisions on Sha Zhu Pan Cases Collected From China Judgements Online. *Crime & Delinquency*, *0*(0). https://doi.org/10.1177/00111287231158571

Wang, F., & Topalli, V. (2024). Understanding romance scammers through the lens of their victims: qualitative modeling of risk and protective factors in the online context. *American Journal of Criminal Justice*, *49*(1), 145–181. https://doi.org/10.1007/s12103-022-09706-4

Weijer van de, S., Leukfeldt, R., & Van der Zee, S. (2020). Reporting cybercrime victimization: determinants, motives, and previous experiences. *Policing: An International Journal*, *43*(1), 17–34. https://doi.org/10.1108/PIJPSM-07-2019-0122

Whittaker, J. M., Lazarus, S., & Corcoran, T. (2024). Are fraud victims nothing more than animals? Critiquing the propagation of "pig butchering" (Sha Zhu Pan, 杀猪盘). *Journal of Economic Criminology*, *3*, 100052. https://doi.org/10.1016/j.jeconc.2024.100052

Whitty, M. (2018). Do you love me? Psychological characteristics of Romance scam victims. *Cyberpsychology Behavior and Social Networking*, *21*(2), 105–109. https://doi.org/10.1089/cyber.2016.0729

Whitty, M. T. (2019). Predicting susceptibility to cyber-fraud victimhood. *Journal of Financial Crime*, *26*(1), 277–292. https://doi.org/10.1108/jfc-10-2017-0095

Сведения об авторах

Амину Мухаммад Аувал – бакалавр в области информационных технологий, специалист в области информационных технологий, Университет Джоса
Адрес: Нигерия, PMB 2084, штат Плато, г. Джос
E-mail: i.elameenu@gmail.com
ORCID ID: https://orcid.org/0009-0005-1799-7876
WoS Researcher ID: https://www.webofscience.com/wos/author/record/JFS-7098-2023
Google Scholar ID: https://scholar.google.com/citations?user=RDxPEr4AAAAJ

Сулеман Лазарус – PhD в области киберпреступности и криминологии, приглашенный специалист Центра криминологии им. Маннхайма, Лондонская школа экономики и политических наук; сотрудник Центра изучения старения населения, университет Суррея; почетный преподаватель Центра по изучению киберпреступности и экономической преступности, Портсмутский университет
Адрес: Великобритания, WC2A 2AE, г. Лондон, Хьютон Стрит; Великобритания GU2 7XH, г. Гилфорд, Стэг Хилл; Великобритания, PO1 2HY, г. Портсмут, Сент-Джордж Билдинг.
E-mail: suleman.lazarus@gmail.com
ORCID ID: https://orcid.org/0000-0003-1721-8519
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57205679641
WoS Researcher ID: https://www.webofscience.com/wos/author/record/629543
Google Scholar ID: https://scholar.google.com/citations?user=Em8EXqcAAAAJ

Вклад авторов

Авторы внесли равный вклад в разработку концепции, методологии, валидацию, формальный анализ, проведение исследования, подбор источников, написание и редактирование текста, руководство и управление проектом.

Конфликт интересов

Авторы сообщают об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.27.41 / Сделки
Специальность ВАК: 5.1.3 / Частно-правовые (цивилистические) науки

История статьи

Дата поступления – 16 мая 2024 г.
Дата одобрения после рецензирования – 28 мая 2024 г.
Дата принятия к опубликованию – 13 декабря 2024 г.
Дата онлайн-размещения – 20 декабря 2024 г.

Research article
UDC 34:004:343.721:004.8
EDN: https://elibrary.ru/mjuigd
DOI: https://doi.org/10.21202/jdtl.2024.45

Overcoming Illegal Cross-border Transfer of Personal Data

Dmitry V. Bakhteev ✉
Ural State Law University named after V. F. Yakovlev, Yekaterinburg, Russia

Anna M. Sosnovikova
Ural State Law University named after V. F. Yakovlev, Yekaterinburg, Russia

Evgeniy V. Kazenas
Ural Federal University named after the first President of Russia B. N. Yeltsin, Yekaterinburg, Russia

Keywords

communications,
computer network,
cross-border data transfer,
digital technologies,
incident,
information security,
information,
law,
legislation,
personal data

Abstract

Objective: to form of a comprehensive interdisciplinary legal and technological risk management model in the field of illegal cross-border transfer of personal data by eliminating legislative gaps and creating a system for automated control of outgoing information flows, as well as expert response to identified incidents.

Methods: in addition to general dialectical and general scientific methods, special legal and cybernetic methods were used. For example, based on comparative legal analysis, the authors reveal differences between national and international regulation of cross-border flows of personal data. In the second section, the modeling method allows forming an algorithm for identifying information security incidents in the field of cross-border transfer of personal data and responding to them.

Results: the article formulates proposals to optimize legislation in the field under study by introducing specialized protective norms for violating the rules of cross-border transfer of personal data and stipulating the operator's obligation to notify personal data subjects of the intention to transfer the information abroad. The second section describes the concept of a software package designed to detect information security incidents in the field under consideration, as well as a model of action of an authorized representative of the operator after receiving a signal from the automated system.

✉ Corresponding author
© Bakhteev D. V., Sosnovikova A. M., Kazenas E. V., 2024

This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (CC BY 4.0) (https://creativecommons.org/licenses/by/4.0), which permits unrestricted re-use, distribution and reproduction, provided the original article is properly cited.

Scientific novelty: to solve the set problem, the work combines the knowledge and competencies of legal scientists and specialists in the field of information security, which allows an interdisciplinary approach. At the same time, it is stated that the issues of illegal cross-border transfer of personal data have not received proper coverage in science today, since Russian legislation in this area has changed recently. The authors propose not so much to strengthen the sanction for legislation violation in this area, as to ensure the punishment of persons who commit cyberattacks, and to equip personal data operators with an effective tool to minimize the risks of information leakage.

Practical significance: the research results can be used to improve legislation in the field of cross-border transfer of personal data and the organization of activities of authorized employees of the personal data operator for risk management in this area.

For citation

Bakhteev, D. V., Sosnovikova, A. M., Kazenas, E. V. (2024). Overcoming Illegal Cross-border Transfer of Personal Data. *Journal of Digital Technologies and Law, 2*(4), 943–972. https://doi.org/10.21202/jdtl.2024.45

Contents

Introduction
1. Legal aspects of cross-border transfer of personal data
   1.1. History of the legal relations in the sphere of cross-border transfer of personal data
   1.2. Regulation of cross-border transfer of personal data by the legislation of the Russian Federation and international laws
2. Technical and technological aspects of cross-border data transfer
   2.1. Main technical communication channels through which the cross-border transfer of personal data is carried out
   2.2. Model for identifying the facts of illegal cross-border transfer of personal data through technical means and responding to them
Conclusions
References

Introduction

The rapid development of technology and society as a whole has led to the blurring of borders between countries in the virtual space. This phenomenon entails many positive consequences: the possibility of international communication, the availability of foreign education, the ability to buy goods from abroad, etc. However, it is not without

negative manifestations, one of which is the illegal cross-border transfer of personal data.

Today, Russia has fairly strict rules for such transfers, as a result of which personal data operators are not always able to accurately comply with them. In addition, more and more malicious attacks are carried out every year; as a result, personal data of a wide range of people become publicly available on foreign servers, which violates the constitutional rights of citizens, undermines the national security of the state and results in significant fines for legal entities.

In this regard, our goal was to propose an optimal comprehensive legal and technological model for minimizing the risks of illegal cross-border transfer of personal data, while maintaining a balance of interests of all parties. To achieve this goal, we have solved the following tasks: studied the history of the relations in this area; analyzed the current national and international regulations governing the cross-border transfer of personal data; formulated proposals to optimize these standards; established the main channels through which personal data can be transferred abroad; established the nodes through which it is possible to prevent unauthorized flows; and proposed an algorithm for identifying information security incidents in this area and responding to them.

We believe that the practical implementation of the proposals outlined in this paper and the focus on the issues raised will not only be of interest to the scientific community, but will also reduce illegal cross-border flows of personal data.

1. Legal aspects of cross-border transfer of personal data

1.1. History of the legal relations in the sphere of cross-border transfer of personal data

Today, personal data is a priori associated with “sensitive” information (Ji et al., 2023), the unauthorized access of which by third parties is extremely undesirable. However, this was not always the case: for a long time, the world was dominated by an order in which, on the one hand, the rights of an individual did not matter; on the other hand, there were no globalization phenomena generating active international interaction at the private level. In this regard, the phenomenon of personal data did not refer to legal regulation, and there was no cross-border transfer of such information in principle. Personal data could only get to another state together with the person or their imminent arrival in that state (for example, when traveling or as part of sending diplomatic representatives from one country to another). At the same time, if the “identity” of someone was stolen and illegally used abroad, this fact did not affect the life of the one whose data turned out to be in the possession of the attackers.

At the same time, the development of society gradually led to systemic changes in the field of personal data: for example, during the Great French Revolution, the question of respect for the individual and their freedoms, including the right to personal privacy, was raised.

In the Russian Empire, such rights were legalized on the initiative of the Emperor: Alexander II adopted Postal and Telegraphic Statutes, which enshrined the inviolability of private life and the secrecy of correspondence. The Criminal Code also provided for sanctions for violation of these norms (Balashkina, 2007). Such a guarantee of privacy was excluded from the legal sphere after the Great October Revolution; however, provisions of the inviolability of the person and the secrecy of correspondence reappeared in the USSR Constitution in 1936[1].

However, in a strict sense, the concept of personal human rights was still very far from the well-established understanding of personal data and their protection regime today. The first relevant phenomenon that approximates modern realities was the theory of American legal scientists S. Warren and L. Brandeis, who in 1890 formulated the concept of privacy as the right to "be left alone" (Balashkina, 2007). About half a century later, a judicial interpretation of this category was given, from which it follows that privacy means the inviolability of personal data and this principle follows from the first amendments to the US Constitution.

The concept of personal data was widely developed only in the second half of the 20th century. At about the same time, against the background of incipient digitalization and intensifying globalization, the phenomenon of cross-border transfer of such information arose.

We must make a reservation that by cross-border data transfer we mean the situation when a specific person (operator) transferred data, including without notifying the subject, from the state in which the subject voluntarily provided the operator with certain information that allows identifying them (unambiguously establishing their identity) to another state, and provided access to the information to third parties. Thus, we do not consider the situation when a subject of information independently communicates their data to representatives of another state, for example, in the case of traveling abroad, when a person provides her passport when checking in and her data is entered into the foreign hotel database. The same applies to legislative norms, which will be discussed below.

The international community's interest in the described phenomenon took shape only after the beginning of the "computer age" (Romansky Noninska, 2020; Zheng, 2021), since at that time many risks associated with the lack of uniform standards for interstate turnover of personal data and their protection in the process of such turnover became apparent.

On the one hand, obtaining various rights and privileges and implementation of the natural interests of people in the era of widespread Internet is almost impossible without cross-border flows of various personal data (Fuentes, 2020). This is due to the development of international business, when a founder is located in one state, and

[1] Glushkova, S. I. (2002). Human rights in Russia: theory, history, practice: tutorial. Yekaterinburg.

its branches and representative offices operate in many countries. Other examples include remote registration of foreign business trips by an internal personnel service; the referral of a seriously ill person to another state for treatment and many other, often quite routine situations (Artemova, 2023). Separately, it is necessary to describe the practice that was widespread in Russia before 2015 and related to the use of foreign databases located outside the Russian Federation for storing personal data obtained by domestic companies. Such use of third-party resources was due to their cheapness and existence as such (Smolensky & Levshin, 2016), since earlier in Russia, there was no demand for its own reliable and accessible databases of various sizes capable of processing significant amounts of information and withstanding malicious attacks. Similar problems are also considered in foreign publications (Abdulrauf et al., 2023).

On the other hand, personal data is a very valuable resource in the modern world. Their legal processing allows commercial companies to produce products more adapted to the interests of the target audience, create targeted advertising, attracting new customers and increasing profits. For states, personal data is necessary in order to combat crime and various kinds of offenses (using cameras with automatic face recognition, conducting genomic and fingerprint identification, etc.), aggregate statistical data on the population (health status, standard of living, etc.), forecast political decisions that will receive support of the population, etc. At the same time, personal data is also of interest for intruders, since they enable them to perform various kinds of theft, discredit a specific person in the media space, encrypt their own identity when carrying out illegal actions, etc.

Thus, a multilateral conflict of interests is formed even within one state: citizens advocate for the inviolability and secrecy of their own personal data (Abramova, 2020); commercial organizations seek to increase the profitability of their business by using customer information; intruders try to steal personal data in order to facilitate or ensure commitment of criminal acts; and the state strives for sole control over the maximum amount of information about its citizens.

The situation is aggravated if we add a cross-border factor, since the subjects of personal data have significantly reduced control over information about themselves. In the commercial sector, competition increases which means the increased demand for large amounts of personal data of potential consumers. It becomes easier for attackers to remain unpunished and unidentified if they distribute various stages of criminal activity in different countries with different legal regimes, conditions for the protection of personal data and rules for the extradition of criminals. States, on the other hand, lose some control over the personal data of their citizens and at the same time acquire the potential ability to obtain relevant information about residents of other countries, which can become an instrument in international counteraction and political pressure.

Legislative and international norms are designed to find a balance between the private interests of individual freedom, the commercial interests of companies and the desire of states to ensure security. It seems that modern legal norms fully provide a compromise in these relations, but they are based on the presumption of good faith of all parties to interaction; hence, the criminal element is omitted. At the same time, the greatest threat to the natural rights of citizens, to the commercial interest of organizations, and to the national security of states is the malicious theft of personal data or violation of their secrecy, as a result of which information about people gets into an open network.

For example, in 2023 alone, 168 leaks of personal data were identified, the largest of which were:

– from the Sberbank "Spasibo" loyalty program – 52.5 million entries;
– from the "Sportmaster" sportswear sales network – 46 million entries;
– from the zdravcity.ru online pharmacy – 8.9 million records;
– from the "Kassy.ru" service – 4.5 million records;
– from the "Zoloto585" jewelry store – 9.9 million records;
– from the "Sogaz" insurance company – 8.3 million records.

The situation of obtaining unauthorized access to the personal data of 1,000,000 MTS Bank users deserves special attention. In total, three files with personal information of clients were unlawfully made public. The first one included a million lines with names, phone numbers, gender, INN, and citizenship. The second one had three million records with types, part of the 16-digit card numbers and their release dates. The third file included 1.8 million phone numbers, 50 thousand e-mails and user IDs[2].

One of the most large-scale incidents occurred in the summer of 2024, when information processed by the Moscow Department of Information Technology, as of September 2023, became publicly available. The published file contains 13,462,446 lines with the following information about Muscovites and guests of the capital who used digital services:

– last name, first name, patronymic;
– phone number (7.2 million unique numbers);
– email address (4.8 million unique addresses, more than 16 thousand of which are on the @mos.ru domain);
– address of registration and actual place of residence;
– date of birth;
– series, number of passport or birth certificate;
– place of birth;
– number of a Muscovite's social card;
– number of the compulsory health insurance policy[3].

---

2 Talash, A. Leakage of personal data: high-profile scandals, who was fined last year and how will they be punished in 2024? Rosco. https://clck.ru/3EmK8s

3 Nefedova, M. The Moscow Department of Information Technology stated that the data published by hackers is a compilation. Khaker. https://clck.ru/3EmK9J

We point out that, at the time of writing, the Moscow Government does not confirm the fact of leakage, reporting the compilation of data freely available on the network due to the fault of the citizens or as a result of a security breach by other operators.

In all the described situations, the personal data of Russians also got to the information resources of foreign countries, i.e. there was an obvious illegal cross-border data transfer based on the broken dam principle. However, the covert transmission of this kind of information abroad is no less dangerous[4].

In total, in 2023, more than 300 million records with personal data of Russian citizens became publicly available, which resulted in fines for businesses totaling over 4.6 million rubles[5]. These are statistics for the Russian Federation only, whereas the problem is global (Jurcys et al., 2022). However, it seems that tightening the liability of legal entities for ongoing violations of the confidentiality of users' personal data is not an optimal measure, since it is aimed at resolving symptoms, but not combating the root cause – hackers carrying out cyberattacks. This situation is connected, in our opinion, with the difficulty of detecting leaks when confidentiality has already been violated, but the data has not yet become widely available, as well as with the fact that criminals belong to other states and use high-tech means of encrypting their own identity and actions. In this regard, it seems necessary, on the one hand, to develop international and national legislation in terms of punishing those really guilty of violating the inviolability of personal data, and on the other hand, to create and implement special technological means of detecting and blocking illegal cross-border transfer of personal data into the activities of the Russsian Federal Service for Supervision of Communications, Information Technology, and Mass Media (Roskomnadzor). This work is devoted to analyzing the current legislation in the field under consideration and describing the models of such technological solutions.

1.2. Regulation of cross-border transfer of personal data by the legislation of the Russian Federation and international laws

In the Russian Federation, the basic provision defining the procedure for the cross-border transfer of personal data is Article 12 of Federal Law No. 152-FZ of July 27, 2006 "On personal data"[6] (hereinafter – 152-FZ), which has undergone four revisions since 2006. Initially, it had only three parts; today, with the latest amendments of July 14, 2022, it consists of 15 parts. This clearly confirms the trends, on the one hand, towards the

[4] Explanatory note to the draft Federal Law "On amendments to the Federal Law 'On personal data' and other legislative acts of the Russian Federation on the protection of the rights of personal data subjects". System of ensuring legislative activity (SOZD). https://clck.ru/3EmKC8

[5] Roskomnadzor recorded 168 data leaks in 2023. Право.ru. https://clck.ru/3EmKCx

[6] On personal data. No. 152-FZ of 27.07.2006. (July 31, 2006). Collection of legislation of the Russian Federation, No. 31 (part I), Art. 3451.

intensification of globalization processes, and on the other hand, towards an increase in cases of such cross-border data transfer, which, without being directly prohibited by law, violates the legitimate rights and freedoms of citizens and the interests of the state as a whole. We will not delve into the historical comparison, focusing on the current regulation of the issue.

The modern edition of the Article regulates in detail the procedure for the cross-border transfer of personal data, according to which:

1. The list of states to which personal data may be transferred from Russia is conditionally limited to those countries that are either members of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, or provide high standards of personal data protection under national legislation.

2. This rule is not absolute, since in extreme cases it is possible to transfer personal data to other states.

3. Any operator of personal data is obliged to send to the authorized body – Roskomnadzor[7] – a separate motivated notification of the intention to transfer personal data abroad, indicating the purpose of the transfer, the country and specific recipients of this information.

4. Roskomnadzor may decide to ban the transfer of personal data to a certain state or in a certain situation.

5. This possibility is not absolute, but the range of grounds is very wide, including:

– protection of the constitutional system of Russia, morality, health, rights and legitimate interests of citizens;

– ensuring the country's defense and state security;

– protection of the economic and financial interests of the Russian Federation;

– ensuring diplomatic and international-legal means of protecting the rights, freedoms and interests of citizens of the Russian Federation, sovereignty, security, territorial integrity of the Russian Federation and its other interests in the international arena.

6. If a decision is made on the inadmissibility of the personal data transfer when such transfer has already taken place, then the transferred personal data must be destroyed, for which the original operator is responsible.

It should also be noted that Article 12 of 152-FZ provides that the cross-border transfer of personal data is carried out in accordance with the above-mentioned Federal Law and international treaties of the Russian Federation, which, under the Russian Constitution, cannot be adopted if their provisions or interpretation contradicts the Constitution. In this regard, when analyzing international acts, we consider it advisable to focus only on documents ratified in the Russian Federation.

---

7 Resolution of the Government of the Russian Federation No. 228 of 16.03.2009. https://clck.ru/3EmKGN

The central international treaty applied to solve the issues of cross-border transfer of personal data is the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[8] (further – Convention). This convention was adopted in 1981 and slightly modernized in 2018 (there were included norms regulating the use of systems based on artificial intelligence technology for automated processing of personal data). Initially, 44 states signed the document; today 55 states are its members on an equal basis with Russia: Albania, Andorra, Argentina, Armenia, Austria, Azerbaijan, Belgium, Bosnia and Herzegovina, Bulgaria, Burkina Faso, Cape Verde, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Great Britain, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Mauritius, Mexico, Moldova, Monaco, Montenegro, Morocco, Netherlands, North Macedonia, Norway, Poland, Portugal, Romania, San Marino, Senegal, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Tunisia, Turkey, Ukraine, and Uruguay.

This act regulates the relations arising from the storage of personal data, i.e. any information about a certain or identifiable natural person: the implementation of logical and/or arithmetic operations with this data, their modification, destruction, search or dissemination, if these actions are carried out in whole or in part using automated means. In general terms, the Convention provisions are similar to the norms and guarantees enshrined in 152-FZ, since it was on the basis of the Convention that the Russian law was adopted. However, as is natural for international agreements, the Convention has a more dispositive character, leaving wide scope for the discretion of the contracting parties. We will not dwell on the review of this Convention, but will highlight only the norm that directly relates to the topic of this study.

Article 12 of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regulates the specifics of cross-border transfer of personal data, establishing as a general rule that the Parties may not prohibit or restrict cross-border flows of personal data between themselves only for the reason of protecting privacy. However, there are two exceptions to this rule – in the following situations, the Parties are free to prohibit or restrict the transfer:

1) the legislative regulation of the processing of a particular category of personal data on the side of the outcome differs from similar norms in the receiving state;

2) personal data will be transferred from the territory of the receiving state to a country that is not a Party to the Convention.

Thus, despite the seemingly strict rule guaranteeing the free transfer of personal data between the Parties to the Convention, there are two rather broad exceptions to it.

[8] Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ETS No. 108 (Strasbourg, January 28, 1981). (February 3, 2014). Collection of legislation of the Russian Federation, No. 5, Art. 419.

Moreover, it is not as strict as it may seem upon a superficial analysis. While prohibiting restrictions based on the privacy protection, the provision in question does not prohibit states from using other grounds for such restrictions. For example, in Russia it is stipulated that cross-border data transfer may be restricted or prohibited in order to ensure national security and for other equally valid and weighty reasons. From this one may conclude that the provisions of Article of 152-FZ and Article 12 of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data do not contradict each other; national legislation only regulates issues in more detail, providing greater protection for the personal data of its citizens.

We believe this approach to be correct, because, as it was shown above and noted by researchers, personal data is sensitive information, the access of which by intruders can significantly harm both a particular citizen and society as a whole (Akulin et al., 2020). However, the current normative and organizational regulation of cross-border transfer of personal data is far from perfect. There is an opinion that the most correct model is free transfer of personal data between countries, while conditional or prohibitive regulation negatively affects the processes of international interaction (Ferracane van der Marel, 2024). However, in our opinion, this viewpoint focuses exclusively on the interests of business and ignores the issues of human rights, national security and the risks of criminal activity in this area. Therefore, it is necessary to develop a more consensual protective model.

First of all, it should be noted that, as is known, a rule of law should consist of three elements: a hypothesis (describing public relations subject to regulation), a disposition (indicating required or prohibited behavior in these public relations) and a sanction (providing punishment for violation of requirements (prohibitions) to behavior). If any of these parts is missing, then the norm is "dead" and will not actually be applied, losing its regulatory force. In this regard, for the strict rules for the cross-border transfer of personal data established by Article 12 of 152-FZ to be observed, a liability for their violation should be provided. The situation with latter is not so clear. Article 13.11 of the Administrative Code of the Russian Federation, consisting of nine parts, provides for liability for various violations of the legislation on personal data. However, there is no special rule regarding the cross-border transfer of such information; hence, it is necessary to turn to the general part.

Part 1 of Article 13.11 of the Administrative Code of the Russian Federation says that "processing of personal data in cases not provided for by the legislation of the Russian Federation in the field of personal data, or processing of personal data incompatible with the purposes of collecting personal data, entails the imposition of an administrative fine on citizens in the amount of 2,000 to 6,000 rubles; on officials – from 10,000 to 20,000 rubles; on legal entities – from 60,000 to 100,000 rubles"[9].

[9] Administrative Code of the Russian Federation of December 30, 2001, No. 195-FZ. (January 7, 2002). Collection of legislation of the Russian Federation, No. 1 (part I), Art. 1.

However, the application of this rule seems difficult due to the very vague wording of the disposition. On the one hand, almost any operator's action may fall under cases not provided for by law or incompatible purposes; on the other hand, one may easily imagine a situation when formally legal, but in fact illegal cross-border transfer of personal data is carried out. In addition, the sanction of this norm, if imposed on the situation of illegal cross-border transfer of personal data, turns out to be very insignificant, because the profit from these illegal actions can exceed the amount of fines by tens or even hundreds of times.

At the same time, Roskomnadzor's practice follows a different path: for such violations organizations involved are suited under Part 9 of Article 13.11, which provides that "the failure of the operator collecting personal data, including via the Internet information and telecommunications network, to fulfil the obligation provided for by the legislation of the Russian Federation in the field of personal data to ensure the recording, systematization, accumulation, storage, clarification (updating, modification) or extraction of personal data of citizens of the Russian Federation using databases located on the territory of the Russian Federation, entails the imposition of an administrative fine on citizens in the amount of 30,000 to 50,000 rubles; on officials – from 100,000 to 200,000 rubles; on legal entities – from 1,000,000 to 6,000,000 rubles"[10].

Undoubtedly, the sanction in this case is much more significant, but formally, the cited norm introduces liability only for one particular case of illegal cross-border transfer of personal data – non-use of domestic databases, which violates the rule introduced in 2015. However, this regulation appeared only in 2019. A similar situation can be observed today – introduced in 2022, the complicated procedure for the cross-border transfer of personal data is currently not provided with a sanction for violating its rules, which negatively affects the regulatory mechanism. We believe that there is an urgent need to elaborate and adopt a special protective norm aimed at preventing illegal cross-border transfer of personal data. At the same time, we believe that the disposition of such a rule should fix an intentional form of guilt so that personal data operators are not subject to punishment for a cyberattack committed on them. This will reduce the latency of such incidents, ensure the cooperation of operators with law enforcement agencies and the implementation of the sanction fairness principle, as it will be directed against the really guilty persons. Simultaneously, especially in an unfriendly international atmosphere, we consider it necessary to introduce an additional qualifying feature in Articles 272, 273, and 274.1 of the Criminal Code of the Russian Federation, for them to enshrine the consequences in the form of obtaining unlawful access to legally protected computer information by persons located outside the Russian Federation.

[10] Administrative Code of the Russian Federation No. 195-FZ of 30.12.2001 (ed. of 23.11.2024). (2024). SPS KonsultantPlyus. https://clck.ru/3ExqcF

The next problem is related to the requirement of Article 12 of 152-FZ, according to which, if Roskomnadzor decides to ban or restrict the cross-border transfer of personal data, "the operator is obliged to ensure the destruction by a foreign state authority, a foreign individual, or a foreign legal entity of the personal data previously transferred to them"[11]. It seems unlikely that the government of a foreign, especially unfriendly, state will delete personal data previously received from Russia on the instructions of any commercial company from our state. There is no mechanism by which this requirement can be implemented. Thus, taking into account the notification procedure for the cross-border transfer of personal data to states that are Parties to the Council of Europe Convention or provide an adequate level of personal data protection (34 more states)[12], as well as the possibility in exceptional cases to carry out cross-border transfer to other states, there appears a very significant risk of leakage of personal data of Russians and their abandonment on hostile territory, after Roskomnadzor decides that the transfer should not have taken place.

Apart from special norms, we can identify another possibility for citizens to protect their personal data from cross-border transfer. As enshrined in paragraph 8, part 7 of Article 14 of 152-FZ, the subject of personal data has the right to receive information about the implemented or proposed cross-border transfer of their data. The systematic interpretation of Part 2 of Article 9 and Part 1 of Article 14 of 152-FZ provides that the subject of personal data may at any time withdraw their consent to their processing and may require the operator to delete their personal data. If a person does not agree with the cross-border transfer of their personal data, they may prohibit the operator from carrying out such actions. However, all the described processes must be initiated by the subject, as the operator is not obliged to report on the planned or ongoing cross-border transfer of personal data until a request for the relevant information is received from the subject. At the same time, most citizens, not having a properly developed legal culture, may not be aware of these features, and therefore they are unable to protect their interests in practice. In addition, even being aware of the above legal provisions, a person is not able to track down all operators potentially carrying out or planning to carry out cross-border transfer of her personal data, since there are many such operators per one subject.

In this regard, we consider it necessary to supplement Article 12 of 152-FZ with a rule providing for mandatory notification of the personal data subject of the intention to make a cross-border transfer of information referring to them, as well as to provide them with the opportunity to limit such transfer to a certain state or in specific situations.

---

11 On personal data. No. 152-FZ of 27.07.2006 (ed. of 08.08.2024). (2024). SPS KonsultantPlyus. https://clck.ru/3Exr2K

12 Order of the Federal Agency for Supervision of Communications, Information Technology and Mass Communications No. 128 of 05.08.2022. https://clck.ru/3EmKNQ

Despite all of the above, it should be recognized that comprehensive measures are being taken in Russia to ensure maximum protection of personal data of persons residing in the state. For example, one has to mention the Federal Law "On amendments to certain legislative acts of the Russian Federation in terms of clarifying the procedure for processing personal data in information and telecommunications networks" dated July 21, 2014, No. 242-FZ (the so-called Localization Law). It amended 152-FZ, stipulating that the recording, systematization, accumulation, storage, clarification (updating, modification), and extraction of personal data of the Russian Federation citizens must be carried out using databases located on the territory of the Russian Federation[13].

This requirement seems to be very effective for protecting the personal data of the Russians, minimizing the risks of information leaks, ensuring state control over information about their citizens, and eliminating the risk of situations where the personal data of Russian citizens will be inaccessible to domestic companies and the state due to blocking of certain foreign services or disconnecting Russian users from foreign databases, or will be used to commit crimes. However, not everyone adheres to this position – for example, in 2015, when the described norm was just coming into force, scenarios were developed to circumvent it in order to minimize business losses (Veselitsky, 2015). In this regard, today we can expect a wide spread of shadow schemes that actually allow storing personal data of Russian citizens abroad.

From all of the above, we can conclude that the regulation of the issue under study cannot adequately protect the personal data of Russians. However, preventing cases of illegal cross-border transfer is a fundamental task of the Russian state, on which the security the country's population and the stability of state power rely. In this regard, it is necessary not only to improve legislation, but also to develop technological mechanisms that would effectively identify and block suspicious flows of personal data outside the territory of the Russian Federation until all the circumstances are clarified and a qualified decision is made.

2. Technical and technological aspects of cross-border data transfer

2.1. Main technical communication channels through which the cross-border transfer of personal data is carried out

Before we describe the technical means of preventing illegal cross-border transfer of personal data, it is necessary to identify the channels of potential information leakage. Currently, the transfer of personal data, which may pose a threat, is carried

[13] On amendments to certain legislative acts of the Russian Federation in terms of clarifying the procedure for processing personal data in information and telecommunications networks. No. 242-FZ of 21.07.2014. (2014). https://clck.ru/3EmKSW

out via computer networks. Certainly, many companies keep paper personal files of employees, for example. However, it seems unrealistic that identifiable information, entirely in analog form, will be obtained from them in large quantities, stored, transferred across the border and published to be accessible to a wide range of people, including for the purpose of their subsequent criminal use. That is why we will consider the technical communication channels represented by computer networks.

To predict the level of threat from illegal access to information, as well as to determine the possibilities of minimizing cyberattacks and leaks, it is important to accurately determine the territory within which the communication channel operates. The following can be distinguished:

Global networks. The most famous of them is the Internet; they encircle the whole world. Global networks also include intra-national networks operating within a particular country or region. It is almost impossible to ensure full protection of information in such networks due to the principle of openness and accessibility underlying their operation.

2. City networks. It is obvious from the name that they exist within a city. However, more often this level includes only networks serving megacities or urban agglomerations. It was at the level of city networks that the special Web software was initially organized.

3. Corporate networks (networks of organizations and enterprises). Networks of this level, on the one hand, are smaller than city ones, since they are aimed at servicing enterprises; but, on the other hand, such networks operate cross-border, i.e. they connect branches and divisions located in different cities, regions and countries.

It should be noted that corporate networks are the most vulnerable from the viewpoint of information security and protection from cyberattacks. The reason is, they cover a significant territory, but are serviced by the private sector, which is limited in resources for constant updating of security protocols and is not bound by strict information protection rules, like state-owned enterprises.

At the same time, departmental communication channels also belong to corporate networks. Their security level is the highest, since they transmit restricted information.

4. Local networks are concentrated in a small area (usually within a radius of 1-2 km). They operate on the territory of one enterprise (factory, hospital, educational institution, etc.). Usually such networks are well protected, as they are organized in a sector where the turnover of legally protected information is carried out in a limited area and through identified terminal equipment, with sufficient resources to set up and maintain security systems.

5. Personal networks are designed for the interaction of devices belonging to the same owner (family members), at a short distance (usually up to 10 m). Despite their low territorial distribution, an individual may not pay enough attention to compliance with the rules of information security and digital hygiene, which puts this infrastructure at risk.

As is obvious from the above classification, cross-border transfer of personal data can be carried out exclusively via global and corporate networks. However, in the latter case, such information is protected and, if an incident occurs, security is violated, then the information is transmitted to global networks, where it becomes available to a wide range of people, including representatives of other states. In this regard, an intermediate conclusion can be drawn that the control of illegal cross-border transfer of personal data is most effective at the border of a secure communication channel and a global network. This approach minimizes the risks of false positive errors when legal internal flows (between government agencies, between divisions of a legal entity, between devices of the same user) are blocked.

To substantiate this thesis, it is necessary to focus in more detail on the characteristics of global computer networks. Their main characteristic feature is that they have a decentralized architecture, are distributed across continents, countries, and can physically be located not only on the Earth's surface, but also above it or underwater – anywhere. Some segments of global networks can be duplicated, including via satellite communications. This, together with the previously mentioned fundamental principle of open access, allows creating a system in which any device with access to the global network can interact with any other connected equipment.

Most often, global computer networks rely on dedicated lines, at one end of which a router is connected to the local network, and at the other end a switch is connected to the rest of the global network. These elements will be discussed in more detail later, as they are important for identifying the facts of unauthorized transfer of personal data.

Note that modern computer networks have inherited a lot from their predecessors – telephone lines. The main technological innovation that the former brought was the rejection of the principle of channel switching, in which interaction requires the physical connection of two devices and allocation of a separate channel for their communication. It was replaced by the technology of multi-level packet switching, when information is divided into small blocks that are transmitted to the addressee along different routes.

Due to such structure of global computer systems, it is impossible to control the flow of information (including personal data) when they are inside the system (Ivanova et al., 2010). Therefore, all measures to block the data transmission channel must be carried out at the local level, amenable to centralized administration.

For the issue of preventing unauthorized flows of personal data, it is important to determine, besides the network level, the media through which information is transmitted. It can be:

– optical fiber;
– copper wires;
– infrared channel;
– radio channel (Wi-Fi, LTE, Bluetooth, etc.).

It is the easiest to intercept, and therefore block, information transmitted through material media – optical fiber and copper wires. In this case, as will be shown below, a technical device that detects unauthorized flows of personal data can be installed directly on the channel. However, in this case, it is very difficult to determine the type of data being transmitted – for this, it is necessary to decrypt them, which requires additional time and special equipment. Therefore, it is much more useful to have access to the so-called infrastructure nodes – local network equipment, which can be active or passive.

Active equipment is the devices directly connected to networks and therefore providing data transmission and routing. They allow a full cycle of data processing: receiving, systematizing, storing, managing, and transmitting. For this purpose, such devices are equipped with their own processor and RAM.

Passive equipment can be called auxiliary: it is characterized by the absence of its own power source and therefore cannot have any effect on the passing data streams. One can draw a metaphorical analogy with a bridge over a river, when traffic lights and signs regulating the order of movement are installed on both sides of it, but the bridge itself is only a section of road on which it is impossible to obtain new information and modernize behavior under its influence. Similarly, passive equipment only creates an environment for data transmission, without managing traffic or processing data. Passive equipment includes, in particular:

– cables (e.g. twisted pair or fiber optic cable) used to connect devices and transfer data between them;

– connectors, patch panels and cross fields used to connect cables and devices;

– splitters or splice boxes used to separate or unite fiber-optic communication lines.

Thus, the role of passive network equipment is reduced to ensuring more efficient and reliable network operation; therefore, it is difficult to block the flow of personal data on it.

Active network equipment is very diverse and performs a variety of functions:

– distribution of traffic between networks;

– connecting local networks at different levels (from intra-organizational to global);

– providing wireless communication between devices within a local network;

– determining the target direction of data packets.

The latter is of particular interest for this study, since in this way it is possible to establish that certain sensitive data is being sent abroad (to a device whose MAC address is registered abroad).

Based on the above features, it follows that in order to effectively prevent unauthorized cross-border flows of sensitive information, minimize the risks of false

positive and false negative errors in determining the direction of information movement, it is necessary to use specialized technical devices to influence active network equipment.

At the same time, there are many different types of network devices, each with its unique features, characteristics and purpose. Therefore, we will give just a brief description of those that should be influenced in order to prevent unauthorized cross-border flows of personal data.

1. A switchboard. This device, which has temporary (intermediate) memory, connects a finite number of devices into a single network. The number of devices that a switchboard can connect depends on the number of ports it has.

The general principle of its operation can be represented as follows: at the first stage, the switchboard receives data that is transmitted to all ports, while the sender's MAC address is identified and assigned to one specific port. Further, if packets are received intended for a device with an identified MAC address, they are transmitted only to the port assigned to it. Otherwise, the data is transmitted to all ports. Over time, all devices interacting on the network are identified.

In terms of the risks of unauthorized cross-border transmission, the switchboard can be useful for detecting their source (i.e. determining the guilty employee), as well as for identifying the very fact of the personal data transfer.

Similar functions, but on a different, broader scale, are performed by hubs, which differ from switchboards by being more vulnerable to information security threats due to less "intelligence".

2. A router is designed to transfer data packets between different computer networks. To do this, it uses a routing table that contains the MAC addresses of the end devices and the communication paths to them. The router matches the MAC address of the recipient specified in the data packet with the specified table and transmits the information to the recipient. At the same time, the router is a moderated system that operates according to the rules set by the administrator, who can indicate the need for traffic filtering, encryption (decryption) of certain data, and other processing.

Thus, it is best to detect incidents of unauthorized cross-border data transmission at the router level, automating this process by introducing several additional rules at the stage of its installation and configuration. However, the router is not specifically designed for such control, unlike the next element of the network infrastructure.

3. Firewall is a software or hardware-software complex that specifically functions to protect a computer network from unauthorized access, malicious attacks, data theft and other threats from the external environment. The main tasks solved by the firewall are as follows:

– traffic filtering;

– blocking attempts to log into the network from unknown or untrusted sources;

– blocking the transmission (reception) of certain types of traffic (for example, traffic with malicious content or personal data), etc.

Undoubtedly, any of the described devices can be used to detect personal data flows, prevent or at least detect not only their free transfer abroad, but also malicious theft. However, such measures will be most effective when they are applied on routers and firewalls. In the next section, we will consider a somewhat generalized scenario of these protective measures.

2.2. Model for identifying the facts of illegal cross-border transfer of personal data through technical means and responding to them

Before proceeding to the description of the proposed model, we make a reservation that this part of the study will be objectively limited to actions within a legal entity or government agency that serve as personal data operators. Also, we will not consider methods of preventing attacks aimed at stealing personal data, as they are generally reduced to constant updating of security protocols and equipment, compliance with all requirements of technical regulations and Roskomnadzor in this area, and using certified and licensed software. However, these measures do not safeguard against any malicious attacks. Hence, we consider it important to create a mechanism for detecting illegal cross-border flows of personal data, regardless of the reason for which they occurred: as a result of an external breakthrough of the security circuit or as a result of illegal (or erroneous) actions on the part of the operator. This said, since the main problem today is centered on large personal data operators represented by corporations and government agencies, we will focus specifically on detecting flows from local, city and corporate networks, which will be generically referred to as local networks for simplification.

We would like to point out that the basic measure to detect and prevent unauthorized cross-border transfer of personal data is control. Assumingly, it should not only be provided for in local acts and instructions as an obligatory element of network management, but also consist of joint efforts of technical, including automated, devices and humans.

Control of network operation is usually divided into two stages: monitoring and analysis. However, preliminary preparation is of great importance, which implies the development of local acts of the organization, the normative consolidation of the procedure for identifying and processing information about information security incidents and responding to them (Rowe, 2003).

At the monitoring stage, primary data is collected, which will be necessary in the future to analyze the situation and make an informed decision (Pascual et al., 2024). Monitoring, especially in large personal data operators, can (and rather must) be carried out using

technical means. Moreover, we consider it necessary to develop a hardware-software module that can be integrated into the equipment of a specific organization, government agency, adapted to the specifics of the operator's activities and its technical and technological resources, ensuring the effective accumulation of all relevant information. Such a device should work according to the following algorithm:

1. Registering the fact that (any) data is flowing out of the local network.
2. Filtering personal data flows (their detention).
3. Determining the direction of these flows.
   3.1. If the stream is directed abroad, it is blocked.
   3.2. If the flow is internal, it is skipped.
4. Informing the authorized person of the operator about the identified flow, transmitting all the accompanying information (time, source, direction, etc.) to this employee.

At the same time, one can use a software solution, similar to the one that has already proven effective in identifying and processing digital traces of the user (Daniela Amélie, 2022). It should also be noted that, if necessary, such a device can be configured to block any flows of personal data or other information before their preliminary verification by an authorized person.

Next, the authorized employee performs an analysis – comprehension of the information collected at the monitoring stage, comparing it with profile (target) templates and subsequent management decision-making. At this stage, a person should evaluate the following in terms of cross-border flows of personal data:

1) whether they are transferred to a state that is a Party to the European Convention or provides adequate protection of personal data;

2) whether the operator is authorized to carry out cross-border transfer of personal data;

3) whether the notification of this transfer was sent to Roskomnadzor;

4) whether the information specified in the notification correspond to the circumstances and content of the personal data being transferred;

5) whether there is a ban or restriction on the transfer of this personal data to a particular state under existing conditions;

6) whether there was any objection from the personal data subject to transfer their information abroad;

7) whether the purposes of the personal data transfer violate the legislation of the Russian Federation;

8) who is the initiator of the personal data transfer (employees of the organization or an external entity that violated the security of the local network).

After answering all these questions, the authorized person decides whether to allow the cross-border transfer of personal data or inform the head (or law enforcement agencies) about the identified and timely prevented information security incident.

The described model is shown in a general form in Fig. 1.

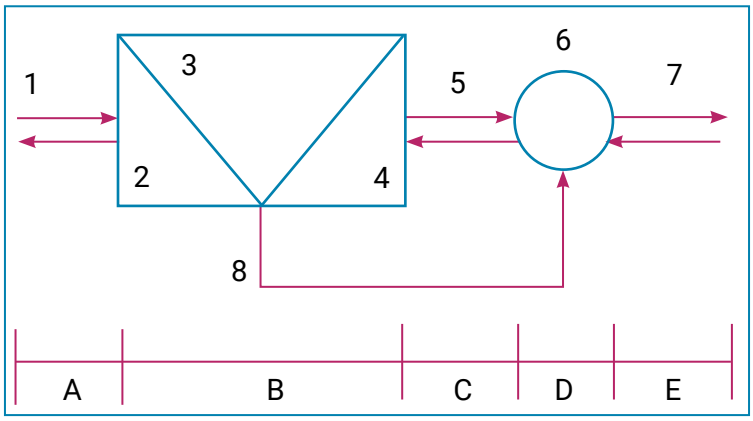


Fig. 1. Graphical representation of the model for identifying the fact of cross-border transfer of personal data and making a managerial decision

In section A, the number 1 shows incoming and outgoing data flows of the physical, network, channel, transport, session, representative, and application levels. Obtaining information from all seven levels of the ISO/OSI model in simple, hierarchical, route, aggregate and other forms for subsequent analysis is necessary, as incoming data, including personal data, may have other than textual representation.

In section B, module 2 shows the identification of the information recipient by analyzing their IP address, domain name, and other similar information and comparing it with official data on the registration of these IP addresses.

Information about the IP address belonging to a geographical (country) location and to a legal entity or individual can be obtained from the official resources of domain name registrars[14]. Obviously, in the model under consideration, the highest priority of trust will belong to domain name registrars operating in Russia (due to the norms of current legislation and regulatory norms of the Federal Service for Technical and Expert Control, the Federal Security Service of the Russian Federation, the Federal Agency for Supervision of Communications, Information Technology and Mass Communications, etc.).

If the recipient is located within the Russian Federation, then no further analysis of the package is performed and it is passed unchanged to section D of module 6. If the recipient is located outside the Russian Federation, then the package is further processed by module 3.

In section B, module 3 collects and normalizes the information (data) intended for recipients outside the country. It is here that the work of an authorized employee of the organization (state body) is supposed to take place.

The data normalization consists of software and mathematical transformations (including, but not limited to: TLS/SSL, HTTPS, HTTPX, E1/T1, ATM and others) of any data representations into text form.

[14] Coordination center for domain names.RU/.РФ. https://clck.ru/3EmLBZ

In section B, module 4 analyzes the normalized data for compliance with the attributive and substantive features of the personal data that fall under the definition.

To do this, the organization must define a list of processed personal data at the level of a local act or instruction and develop appropriate templates (for example, regular expressions), according to which the procedure for detecting target information is carried out. We point out that, depending on the specific tasks of the personal data operator, module 4 may be located before module 3, i.e., precede human analysis.

If the analyzed traffic contains matches with patterns of information that is unacceptable for transmission, then a control action (element 8) is sent to the section D of module 6 about the destruction (discarding) of a specific packet and logging of this event. In the considered model, such command can be submitted by an authorized employee; however, the fully automated operation of the proposed software module is not excluded.

In section D, module 6 is a corporate firewall, which, in addition to its main functions, decides on destroying (discarding) a specific package and logging an information protection event when a control action (command) comes from section B.

Elements 5 and 7 are standard information flows within the local network and the module for automated processing of outgoing data flows.

Similar algorithms were also proposed by foreign research teams (Liu et al., 2024; Pascual et al., 2024; Guaman et al., 2021; Yan et al., 2023). Therefore, we consider it useful to establish international cooperation in this area in order to most effectively achieve the goals of protecting sensitive information.

We have to make a reservation that the monitoring and analysis we have considered are only parts of a more detailed algorithm, which includes related organizational measures (creation of local acts in the field of information security, cooperation with regulatory authorities, implementation of general and private prevention, etc.). However, this study does not claim to be complete and exhaustive, and therefore we consider it sufficient to highlight only those stages of management within which specialized technical means can be involved, as it was initially stated.

Conclusions

Summarizing the above, we would like to emphasize the following.

1. Relations in the sphere of cross-border transfer of personal data could develop only in the digital age, when global information flows beyond the borders of any state became commonplace, and therefore the legal and political regulation of this area is just being formed.

2. Personal data are a valuable resource: they contain information about personal life that a person wants to keep secret; they are necessary for business development; they are required for effective fight against crimes and offenses; they are an important component

of criminal and other illegal activities; they can be a factor in interstate and inter-political struggle.

3. Illegal cross-border flows of personal data pose a serious threat to individual rights, national security and financial well-being of organizations; however, current national and international legal norms do not provide a mechanism sufficient to prevent them.

4. To resolve this problem, it is necessary to introduce a special prosition for violating the established procedure for the cross-border transfer of personal data to the Administrative Code of the Russian Federation; to supplement the qualifying signs in the Articles of the Criminal Code of the Russian Federation devoted to the violation of the security of computer information; to oblige the operator of personal data to inform their subject of their intention to carry out cross-border transfer of such information.

5. Simultaneously with the legislation optimization, it is necessary to introduce specialized technical means for detecting unauthorized cross-border flows of personal data into the information security systems of organizations and government agencies acting as personal data operators.

6. The use of these tools should be carried out according to the following algorithm: constant automated background control of all outgoing information flows, determination of their direction; identification of flows moving abroad; attribution of information in this flow to personal data; blocking of the flow corresponding to the two above-specified signs; notification of an authorized employee of the organization (state body) about the identified flow; human assessment of the permissibility of cross-border data transmission; decision-making on skipping or final blocking of the stream; in the latter case, informing about an identified and prevented information security incident.

We believe that the implementation of the described algorithm, as well as the improvement of legal regulation in the field of cross-border transfer of personal data, will reduce the number of thefts and unintentional leaks of such sensitive information. This will help to protect the rights of citizens, ensure the political stability of the Russian Federation, reduce the number of crimes using other people's personal data, and achieve financial well-being for commercial organizations.

References

Abdulrauf, L., Adaji, A., & Ojibara, H. (2023). Clarifying the legal requirement for cross-border sharing of health data in POPIA: Recommendations on the draft Code of Conduct for Research. *South African Journal of Bioethics and Law*, *17*(1), 44–48. https://doi.org/10.7196/sajbl.2024.v17i1.1969

Abramova, A. G. (2020). Contemporary issues of personal data protection in the network: fundamental principles of personal data protection. *Region i mir*, *11*(4), 21–25. (In Russ.).

Akulin, I. M., Chesnokova, E. A., Guryanova, N. E., Presnyakov, R. A., & Letova, A. D. (2020). Possibility of transboundary transfer of health-personal data within the EAEU: reality, prospects. *Menedzher Zdravookhranenia*, *7*, 65–73. (In Russ.). https://doi.org/10.37690/1811-0185-2020-7-65-73

Artemova, A. N. (2023). Legal regulation of cross-border personal data transfer. *Yuridicheskaya nauka i praktika*, *19*(3), 9–16. (In Russ.). https://doi.org/10.25205/2542-0410-2023-19-3-9-16

Balashkina, I. V. (2007). Features of the constitutional regulation of the right to privacy in the Russian Federation. *Pravo i politika*, *7*, 92–105. (In Russ.).

Daniela, V., & Amélie, M. (2022). A Frequency-Based Learning-To-Rank Approach for Personal Digital Traces. *Proceedings of the 55th Hawaii International Conference on System Sciences*, 2920–2929. https://doi.org/10.24251/hicss.2022.361

Ferracane, M., & Van der Marel, E. (2024). Governing personal data and trade in digital services. *Review of International Economics*. https://doi.org/10.1111/roie.12735

Fuentes, I. T. (2020). Legal Recognition of the Digital Trade in Personal Data. *Mexican Law Review*, *12*(2), 87–117. https://doi.org/10.22201/iij.24485306e.2020.2.14173

Guaman, D., Del Alamo, J., & Caiza, J. (2021). GDPR Compliance Assessment for Cross-Border Personal Data Transfers in Android Apps. *IEEE Access*, *9*, 15961–15982. https://doi.org/10.1109/ACCESS.2021.3053130

Ivanova, O. V., Ivanov, P. V., & Smelov, M. N. (2010). Problems and algorithms of information retrieval in global computer networks. *T-Comm*, *4*(3), 23–2. (In Russ.).

Ji, P., Shan, F., Li, F., Sun, H., Wang, M., & Shan, D. (2023). Adaptive Sensitive Information Recognition Based on Multimodal Information Inference in Social Networks. *Security and Communication Networks*, *2023*(1), 5627246. https://doi.org/10.1155/2023/5627246

Jurcys, P., Corrales, M. C., & Fenwick, M. (2022). The future of international data transfers: Managing legal risk with a 'user-held' data model. *Computer Law & Security Review*, *46*, 105691. https://doi.org/10.1016/j.clsr.2022.105691

Liu, Y., Yang, C., Liu, Q., Xu, M., Zhang, C., Cheng, L., & Wang, W. (2024). PDPHE: Personal Data Protection for Trans-Border Transmission Based on Homomorphic Encryption. *Electronics*, *13*(10), 1–23. https://doi.org/10.3390/electronics13101959

Pascual, H. A., Del Alamo, J., Rodríguez, D. T., & Dueñas, J. (2024). Hunter: Tracing anycast communications to uncover cross-border personal data transfers. *Computers & Security*, *141*, 103823. https://doi.org/10.1016/j.cose.2024.103823

Romansky, R. P., & Noninska, I. S. (2020). Challenges of the digital age for privacy and personal data protection. *Math Biosci Eng*, *17*(5), 5288–5303. https://doi.org/10.3934/mbe.2020286

Rowe, H. (2003). Data transfer to third countries: Transfers of personal data to third countries: the role of binding corporate rules. *Computer Law & Security Review*, *19*(6), 490–496. https://doi.org/10.1016/S0267-3649(03)00609-5

Smolenskij, M. B., & Levshin, N. S. (2016). Localization of personal data of Russian citizens as a component of Russia's economic and national security. *Nauka i obrazovanie: khozyajstvo i ekonomika, predprinimatelstvo, pravo i upravlenie*, *2*(69), 111–114. (In Russ.).

Veseliczky, O. I. (2015). Issues of cross-border transfer of personal data in accordance with the requirements of 242-FZ. *Collections of conferences of the Sotsiosfera SIC*, *53*, 275–279. (In Russ.).

Yan, S., Odom, P., Pasunuri, R., Kersting, K., & Natarajan, S. (2023). Learning with privileged and sensitive information: a gradient-boosting approach. *Frontiers in Artificial Intelligence*, *6*, 1260583. https://doi.org/10.3389/frai.2023.1260583

Zheng, G. (2021). Trilemma and tripartition: The regulatory paradigms of cross-border personal data transfer in the EU, the U.S. and China. *Computer Law & Security Review*, *43*, 105610. https://doi.org/10.1016/j.clsr.2021.105610

Authors information

Dmitriy V. Bakhteev – Dr. Sci. (Law), Professor, Department of Criminalistic named after I. F. Gerasimov, Head of Laboratory of Digital Technologies in Criminalistic, Ural State Law University named after V. F. Yakovlev
Address: 21 Komsomolskaya Str., 620066, Yekaterinburg, Russia
E-mail: ae@crimlib.info
ORCID ID: https://orcid.org/0000-0002-0869-601X
ScopusAuthorID:https://www.scopus.com/authid/detail.uri?authorId=57208909117
WoS Researcher ID: https://www.webofscience.com/wos/author/record/ABA-1494-2020
Google Scholar ID: https://scholar.google.ru/citations?user=h0zOOdcAAAAJ
РИНЦ Author ID: https://elibrary.ru/author_items.asp?authorid=762765

Anna M. Sosnovikova – probation researcher of the Laboratory for digital technologies in Criminalistic, Ural State Law University named after V. F. Yakovlev
Address: 21 Komsomolskaya Str., 620066, Yekaterinburg, Russia
E-mail: at@crimlib.info
ORCID ID: https://orcid.org/0000-0002-1631-9265
WoS Researcher ID: https://www.webofscience.com/wos/author/record/KDP-3525-2024
Google Scholar ID: https://scholar.google.ru/citations?user=BLBhZHMAAAAJ
RSCI Author ID: https://elibrary.ru/author_items.asp?authorid=1196069

Evgeniy V. Kazenas – student, Ural Federal University named after the first President of Russia B. N. Yeltsin
Address: 19 Mira Str., 620002, Yekaterinburg, Russia
E-mail: kazenas03@mail.ru
ORCID ID: https://orcid.org/0009-0002-3301-9720

Authors' contributions

The authors have contributed equally into the concept and methodology elaboration, validation, formal analysis, research, selection of sources, text writing and editing, project guidance and management.

Conflict of interests

The authors declare no conflict of interests.

Financial disclosure

The research was funded by Russian Science Foundation, grant No. 23-78-10011, https://rscf.ru/project/23-78-10011/

Thematic rubrics

OECD: 5.05 / Law
PASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – June 28, 2024
Date of approval – July 12, 2024
Date of acceptance – December 13, 2024
Date of online placement – December 20, 2024

Научная статья
УДК 34:004:343.721:004.8
EDN: https://elibrary.ru/mjuigd
DOI: https://doi.org/10.21202/jdtl.2024.45

Преодоление нелегальной трансграничной передачи персональных данных

Дмитрий Валерьевич Бахтеев ✉
Уральский государственный юридический университет имени В. Ф. Яковлева, Екатеринбург, Россия

Анна Михайловна Сосновикова
Уральский государственный юридический университет имени В. Ф. Яковлева, Екатеринбург, Россия

Евгений Владимирович Казенас
Уральский федеральный университет имени первого Президента России Б. Н. Ельцина, Екатеринбург, Россия

Ключевые слова

законодательство,
информационная безопасность,
информация,
инцидент,
компьютерная сеть,
персональные данные,
право,
связь,
трансграничная передача данных,
цифровые технологии

Аннотация

Цель: формирование комплексной междисциплинарной юридико-технологической модели управления рисками в сфере незаконной трансграничной передачи персональных данных посредством ликвидации законодательных лакун и создания системы автоматизированного контроля исходящих потоков информации, а также экспертного реагирования на выявленные инциденты.

Методы: в работе, помимо всеобщего диалектического и общенаучных, используются специально-юридические и кибернетические методы. Так, на основе сравнительно-правового анализа выявляются различия между национальным и международным регулированием трансграничных потоков персональных данных, а метод моделирования, положенный в основу второго раздела исследования, позволяет сформировать алгоритм выявления инцидентов информационной безопасности в сфере трансграничной передачи персональных данных и реагирования на них.

Результаты: сформулированы предложения по оптимизации законодательства в рассматриваемой сфере посредством введения специализированных охранительных норм за нарушение правил трансграничной передачи персональных данных, закрепления обязанности оператора уведомлять субъектов персональных данных о намерении осуществить передачу информации за рубеж. Во второй части работы описана концепция программного комплекса, предназначенного для детекции инцидентов информационной безопасности в рассматриваемой области, а также модель действия уполномоченного представителя оператора после получения сигнала от автоматизированной системы.

✉ Корреспондирующий автор
© Бахтеев Д. В., Сосновикова А. М., Казенас Е. В., 2024

Статья находится в открытом доступе и распространяется в соответствии с лицензией Creative Commons «Attribution» («Атрибуция») 4.0 Всемирная (CC BY 4.0) (https://creativecommons.org/licenses/by/4.0/deed.ru), позволяющей неограниченно использовать, распространять и воспроизводить материал при условии, что оригинальная работа упомянута с соблюдением правил цитирования.

Научная новизна: для решения заявленной проблемы в работе объединяются знания и компетенции ученых-юристов и специалистов в сфере информационной безопасности, что позволяет предложить междисциплинарный подход. Одновременно с этим вопросы незаконной трансграничной передачи персональных данных на сегодняшний день не получили должного освещения в науке, поскольку российское законодательство в данной сфере изменилось не так давно. Авторы настоящей работы предлагают не столько усилить санкцию за нарушение законодательства в рассматриваемой сфере, сколько обеспечить наказание лиц, совершающих кибератаки, и вооружить операторов персональных данных действенным инструментом минимизации рисков утечки информации.

Практическая значимость: результаты исследования могут быть использованы для совершенствования законодательства в сфере трансграничной передачи персональных данных и организации деятельности уполномоченных сотрудников оператора персональных данных по управлению рисками в рассматриваемой сфере.

Для цитирования

Бахтеев, Д. В., Сосновикова, А. М., Казенас, Е. В. (2024). Преодоление нелегальной трансграничной передачи персональных данных. *Journal of Digital Technologies and Law*, *2*(4), 943–972. https://doi.org/10.21202/jdtl.2024.45

Список литературы

Абрамова, А. Г. (2020). Современные проблемы осуществления защиты персональных данных в сети: Основополагающие принципы защиты персональных данных. *Регион и мир*, *11*(4), 21–25. https://www.elibrary.ru/eveayh

Акулин, И. М., Чеснокова, Е. А., Гурьянова, Н. Е., Пресняков, Р. А., Летова А. Д. (2020). Возможность трансграничной передачи связанных со здоровьем персональных данных в рамках ЕАЭС: реальность, перспективы. *Менеджер здравоохранения*, *7*, 65–73. https://doi.org/10.37690/1811-0185-2020-7-65-73

Артемова, А. Н. (2023). Правовое регулирование трансграничной передачи персональных данных. *Юридическая наука и практика*, *19*, 3, 9–16. EDN: https://www.elibrary.ru/cgfugw. DOI: https://doi.org/10.25205/2542-0410-2023-19-3-9-16

Балашкина, И. В. (2007). Особенности конституционного регулирования права на неприкосновенность частной жизни в Российской Федерации. *Право и политика*, *7*, 92–105. https://www.elibrary.ru/hzyhnn

Веселицкий, О. И. (2015). Вопросы трансграничной передачи персональных данных в соответствии с требованиями 242-ФЗ. *Сборники конференций НИЦ Социосфера*, *53*, 275–279. https://www.elibrary.ru/vbvgev

Иванова, О. В., Иванов, П. В., Смелов, М. Н. (2010). Проблемы и алгоритмы поиска информации в глобальных компьютерных сетях. *T-Comm: Телекоммуникации и транспорт*, *4*(3), 23–25. https://www.elibrary.ru/ophpnz

Смоленский, М. Б., Левшин, Н. С. (2016). Локализация персональных данных граждан РФ как составляющая экономической и национальной безопасности России. *Наука и образование: хозяйство и экономика, предпринимательство, право и управление*, *2*(69), 111–114. https://elibrary.ru/item.asp?id=25423352

Abdulrauf, L., Adaji, A., & Ojibara, H. (2023). Clarifying the legal requirement for cross-border sharing of health data in POPIA: Recommendations on the draft Code of Conduct for Research. *South African Journal of Bioethics and Law*, *17*(1), 44–48. https://doi.org/10.7196/sajbl.2024.v17i1.1969

Daniela, V., & Amélie, M. (2022). A Frequency-Based Learning-To-Rank Approach for Personal Digital Traces. *Proceedings of the 55th Hawaii International Conference on System Sciences*, 2920–2929. https://doi.org/10.24251/hicss.2022.361

Ferracane, M., & Van der Marel, E. (2024). Governing personal data and trade in digital services. *Review of International Economics*. https://doi.org/10.1111/roie.12735

Fuentes, I. T. (2020). Legal Recognition of the Digital Trade in Personal Data. *Mexican Law Review*, *12*(2), 87–117. https://doi.org/10.22201/iij.24485306e.2020.2.14173

Guaman, D., Del Alamo, J., & Caiza, J. (2021). GDPR Compliance Assessment for Cross-Border Personal Data Transfers in Android Apps. *IEEE Access*, *9*, 15961–15982. https://doi.org/10.1109/ACCESS.2021.3053130

Ji, P., Shan, F., Li, F., Sun, H., Wang, M., & Shan, D. (2023). Adaptive Sensitive Information Recognition Based on Multimodal Information Inference in Social Networks. *Security and Communication Networks*, *2023*(1), 5627246. https://doi.org/10.1155/2023/5627246

Jurcys, P., Corrales, M. C., & Fenwick, M. (2022). The future of international data transfers: Managing legal risk with a 'user-held' data model. *Computer Law & Security Review*, *46*, 105691. https://doi.org/10.1016/j.clsr.2022.105691

Liu, Y., Yang, C., Liu, Q., Xu, M., Zhang, C., Cheng, L., & Wang, W. (2024). PDPHE: Personal Data Protection for Trans-Border Transmission Based on Homomorphic Encryption. *Electronics*, *13*(10), 1–23. https://doi.org/10.3390/electronics13101959

Pascual, H. A., Del Alamo, J., Rodríguez, D. T., & Dueñas, J. (2024). Hunter: Tracing anycast communications to uncover cross-border personal data transfers. *Computers & Security*, *141*, 103823. https://doi.org/10.1016/j.cose.2024.103823

Romansky, R. P., & Noninska, I. S. (2020). Challenges of the digital age for privacy and personal data protection. *Math Biosci Eng*, *17*(5), 5288–5303. https://doi.org/10.3934/mbe.2020286

Rowe, H. (2003). Data transfer to third countries: Transfers of personal data to third countries: the role of binding corporate rules. *Computer Law & Security Review*, *19*(6), 490–496. https://doi.org/10.1016/S0267-3649(03)00609-5

Yan, S., Odom, P., Pasunuri, R., Kersting, K., & Natarajan, S. (2023). Learning with privileged and sensitive information: a gradient-boosting approach. *Frontiers in Artificial Intelligence*, *6*, 1260583. https://doi.org/10.3389/frai.2023.1260583

Zheng, G. (2021). Trilemma and tripartition: The regulatory paradigms of cross-border personal data transfer in the EU, the U.S. and China. *Computer Law & Security Review*, *43*, 105610. https://doi.org/10.1016/j.clsr.2021.105610

Сведения об авторах

Бахтеев Дмитрий Валерьевич – доктор юридических наук, доцент, профессор кафедры криминалистики имени И. Ф. Герасимова, заведующий лабораторией цифровых технологий в криминалистике, Уральский государственный юридический университет имени В. Ф. Яковлева
Адрес: 620066, Россия Федерация, г. Екатеринбург, ул. Комсомольская, 21
E-mail: ae@crimlib.info
ORCID ID: https://orcid.org/0000-0002-0869-601X
ScopusAuthorID:https://www.scopus.com/authid/detail.uri?authorId=57208909117
WoS Researcher ID: https://www.webofscience.com/wos/author/record/ABA-1494-2020
Google Scholar ID: https://scholar.google.ru/citations?user=h0zOOdcAAAAJ
РИНЦ Author ID: https://elibrary.ru/author_items.asp?authorid=762765

Сосновикова Анна Михайловна – стажер-исследователь лаборатории цифровых технологий в криминалистике, Уральский государственный юридический университет имени В. Ф. Яковлева
Адрес: 620066, Россия, г. Екатеринбург, ул. Комсомольская, 21
E-mail: at@crimlib.info
ORCID ID: https://orcid.org/0000-0002-1631-9265
WoS Researcher ID: https://www.webofscience.com/wos/author/record/KDP-3525-2024
Google Scholar ID: https://scholar.google.ru/citations?user=BLBhZHMAAAAJ
РИНЦ Author ID: https://elibrary.ru/author_items.asp?authorid=1196069

Казенас Евгений Владимирович – студент, Уральский федеральный университет имени первого Президента России Б. Н. Ельцина
Адрес: 620002, Россия, г. Екатеринбург, ул. Мира, 19
E-mail: kazenas03@mail.ru
ORCID ID: https://orcid.org/0009-0002-3301-9720

Вклад авторов

Авторы внесли равный вклад в разработку концепции, методологии, валидацию, формальный анализ, проведение исследования, подбор источников, написание и редактирование текста, руководство и управление проектом.

Конфликт интересов

Авторы сообщают об отсутствии конфликта интересов.

Финансирование

Исследование выполнено за счет гранта Российского научного фонда № 23-78-10011, https://rscf.ru/project/23-78-10011/

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.77 / Уголовное право
Специальность ВАК: 5.1.4 / Уголовно-правовые науки

История статьи

Дата поступления – 28 июня 2024 г.
Дата одобрения после рецензирования – 12 июля 2024 г.
Дата принятия к опубликованию – 13 декабря 2024 г.
Дата онлайн-размещения – 20 декабря 2024 г.

Research article
UDC 34:004:341.4:004.8
EDN: https://elibrary.ru/nnftqi
DOI: https://doi.org/10.21202/jdtl.2024.46

Countering Cyberattacks: Gaps in International Law and Prospects for Overcoming them

Mohammad Minhazur Rahman ✉
State University of Bangladesh, Dhaka, Bangladesh

Tapos Kumar Das
Jahangirnagar University, Dhaka, Bangladesh
City University of Hong Kong, Hong Kong

Keywords

cyberattack,
cybercrime,
digital technologies,
human rights,
international convention,
international law,
law,
legal liability,
principle of due diligence,
principle of proportionality,
principles of international law

Abstract

Objective: to categorize cyber attacks in the national and international legal sytems and to define legal measures to counter them at the international level.

Methods: include doctrinal legal analysis, formal legal, comparative legal methods, synthesis, induction, deduction, as well as methods of legal forecasting and modeling. International legal documents and acts of national legislation, judicial precedents, and doctrinal sources were studied.

Results: the article defines the legal consequences of cyberattacks, identifies difficulties in determining and holding individuals and organizations accountable for their commission, identifies national measures to counter cyberattacks based on the principle of proportionality, and systematizes the international legal framework for responding to cyberattacks. The main focus is on the urgent problems of identifying and verifying cyber weapons, establishing international standards for their use, developing methods of disarmament or limiting offensive cyber capabilities. The authors raise the issue of ensuring humanitarian activities, protecting critical infrastructure and the population through cybersecurity measures in wartime. The legal framework is analyzed; gaps and other defects are identified in the current regulation of exercising jurisdiction in such areas of cyber activity as international transactions, data localization and extraterritorial enforcement of national legislation. The parameters were developed and described within

✉ Corresponding author
© Rahman M. M., & Das T. K., 2024

This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (CC BY 4.0) (https://creativecommons.org/licenses/by/4.0), which permits unrestricted re-use, distribution and reproduction, provided the original article is properly cited.

which states may conduct proactive cyber operations to prevent or deter cyberattacks (cyber countermeasures). The main parameters are due diligence, legal decisions on using cyber countermeasures, proportionality of protection measures to the consequences of illegal actions.

Scientific novelty: this is due to the progressive solutions in the field of international legal regulation of cyber countermeasures by states responding to cybercrime. The solutions are formulated taking into account the impact of the countermeasures on human and civil rights and freedoms, including the right to privacy and freedom of speech.

Practical significance: the research results can be used to develop and improve international legal instruments in the field of combating cyberattacks and ensuring cybersecurity, and can serve as a model for national legislators when designing law-making solutions to counter cybercrime.

For citation

Rahman, M. M., & Das, T. K. (2024). Countering Cyberattacks: Gaps in International Law and Prospects for Overcoming them. *Journal of Digital Technologies and Law, 2*(4), 973–1002. https://doi.org/10.21202/jdtl.2024.46

Content

Introduction
1. Challenges Relating to Legality or Illegality of Cyberattacks
   1.1. Attribution Conundrum of Cyberattacks
   1.2. Accountability Challenges of Non-State Entities
   1.3. Cooperation Imperative in Cyberterrorism
   1.4. Human Rights Concerns in Cyberattacks
2. Scopes and Limitations of Countermeasures against Cyberattacks
   2.1. Proportionality Calibration in Cyber Operations
   2.2. Obstacles of Global Collaboration
   2.3. Legal Labyrinth of Anticipatory Self Defence
3. Instrumentalising International Law and Institutions to Address Cyberattacks
   3.1. Confronting the Lacuna in International Cybersecurity Norms
   3.2. Need for Translating Legal Standards to the Cyberspace
   3.3. The Inadequacy of Traditional Warfare Principles in Cyberspace
   3.4. Complex Landscape beyond Sovereign Borders
Conclusion
References

Introduction

The increased frequency of cyberattacks in today's world poses serious threats to the safety and security of nations. As nations try to figure out how to defend themselves from cyberattacks, the legal implications of cyberwarfare and countermeasures have become important fields of study. This research sheds light on numerous areas of international law by exploring the legal implications and issues involved with various parts of countermeasures in cyberwarfare. Identifying the people or organisations responsible for cyberattacks is a major obstacle to resolving the problem (Etzioni & Rice, 2015). Correctly attributing cyberattacks is essential for developing efficient countermeasures. But attribution of it is difficult because of the nature of the internet, which allows for anonymity and the adoption of sophisticated tactics to conceal identities. This research revisits the existing legal frameworks and proposes techniques to establishing responsibility when it comes to attributing cyberattacks in the context of countermeasures.

Proportionality as it relates to defences against cyberwarfare is another important topic covered in this research. The application of proportionality in evaluating the extent and severity of countermeasures is becoming increasingly important as nations respond to cyberattacks. Given the asymmetric nature of cyber operations and the broad collateral harm they can do, the legal rules for establishing the proportionality of countermeasures need to be carefully examined (Roscini, 2014). Existing legal standards and concepts are examined in this research, as well as their relevance to cyber countermeasures. International collaboration is essential in the face of increasingly complex and transnational cyber threats. This research looks at the legal structures and procedures that promote international collaboration in the face of cyberattacks. The exchange of information, coordination of actions, and development of effective measures to counteract cyber threats all need cooperation between governments.

This research also examines the advantages and disadvantages of international cooperation in the field of cyber countermeasures by examining existing international legal instruments and cooperative channels. While states are the dominant participants in cyberwarfare, cybercriminals and hacktivist organisations have emerged as significant players as well (Buchan, 2012). That's why this research evaluates the difficulties of holding non-state actors accountable for cyberattacks and examines the legal remedies accessible to nations for responding within the bounds of international law. Concerns about the possible violation of fundamental human rights, such as the right to privacy and freedom of speech, emerge as nations engage in defensive or offensive cyber operations. To find a middle ground between national security concerns and the preservation of individual rights, this research investigates the legal frameworks and concepts regulating the junction of cyber countermeasures and human rights. In addition, this research analyses the parameters within which nations may legitimately conduct pre-emptive cyber operations to either prevent or discourage cyberattacks (Hollis & Finnemore, 2016).

This research investigates the limits and policies of pre-emptive cyber countermeasures by examining the current rules of anticipatory self-defence and their relevance in the cyber countermeasure. The research also investigates the necessity of due diligence as a criterion for governmental accountability in cyber countermeasures and examines the norms and duties imposed on nations for deciding the legitimacy of their cyber countermeasures, and sheds light on the potential repercussions and remedies for governments that engage in illegal cyber activities. The difficulties of defining, verifying, and regulating cyber weapons are also explored in this research and it looks at the standards for using cyber weapons in the context of countermeasures, as well as the legal frameworks and prospective procedures for disarming or limiting offensive cyber capabilities (Liivoja & Väljataga, 2021). Additionally, the legal frameworks governing intelligence actions in cyberspace are investigated, along with the bounds of acceptable espionage, the range of legitimate state interests, and the possible influence on international relations. This research argues that understanding of legal implications and difficulties of cyber intelligence collection can be improved by this approach (Putman & Albright, 2018).

In addition, this research investigates how cybersecurity safeguards might aid in the safety of populations, vital infrastructure, and humanitarian efforts in times of war. By doing so, it sheds insight on the possible roles and duties of states and non-state actors in preserving cyberspace during wars by investigating the legal requirements of states and the potential synergies between cybersecurity and international humanitarian law. Finally, the research looks into the difficulties and legal precedents of asserting jurisdiction over illegal cyber actions. Examining the jurisdictional challenges that arise from cross-border cyber operations, data localisation, and the extraterritorial implementation of national laws, this research finally examines the possibilities for international legal collaboration (Andrew & Bernard, 2021). This research intends to further the establishment of legal frameworks and norms governing countermeasures in cyberwarfare by exploring these many and under-researched areas of international law aspiring to deal with the difficulties and ambiguities of cyber threats and to further the knowledge of the legal consequences of this changing landscape (Knowles & Thomas, 2016).

Three significant research questions will be explored in this research. Firstly, the author will investigate how the legality and illegality of cyberattacks are classified under international law and treaties, and will compare and contrast how these classifications are used in various jurisdictions and settings. Secondly, existing legal frameworks and techniques used by governments and international organizations to respond to and mitigate cyberattacks will be examined, and potential limits of the approaches of cyber countermeasures as well as self-defence strategies will be identified and explored from an international law perspective. Thirdly, given the dynamic nature of the global digital ecosystem, this research will seek to explore ways in which international law and institutions could be better leveraged or altered to meet the growing problem of cyberattacks.

Furthermore, this research concerns unexplored questions relevant to the legal consequences of cyber countermeasures that are complex and multidimensional, necessitating an all-encompassing research technique to answer them. To give a thorough examination of the topic, this research will combine qualitative research methodologies with doctrinal approaches. Scholarly publications, books, legal texts, case law, and international legal instruments will all be reviewed as part of this research (Wren & Wren, 1986). Insight into the various cyber countermeasures' legal frameworks, philosophies, and arguments will be gained from these sources. The legal implications of countermeasures, attribution difficulties, and particular cases of cyberattacks will all be examined through case studies. There will be an examination of how various legal systems and international cooperation mechanisms deal with cyberattacks (Van Hoecke, 2011). To determine what works and what may be improved, this research will compare and contrast key international treaties, agreements, and cooperative approaches taken so far. To clarify the legal standards, norms, and principles controlling the many components of cyber countermeasures, the author will perform a doctrinal study of international legal instruments such as treaties, customary international law, and pertinent legal principles (Watkins & Burton, 2013).

To answer the research questions, this research will also need the interpretation and application of legal rules and precedents. The focus of this research has been narrowed to the difficulties and legal implications of developing responses against cyberattacks. The author's knowledge and experience in this continuously developing field are the primary limitations on the research (Tyler, 2017). Despite these limitations, it is expected that this research will make a significant addition to the knowledge of the legal consequences and difficulties of cyber warfare countermeasures.

1. Challenges Relating to Legality or Illegality of Cyberattacks

1.1. Attribution Conundrum of Cyberattacks

Since cyberattacks frequently leave no evidence, attribution of these offences may be a challenging and time-consuming operation (Tsagourias & Farrell, 2020). Attribution refers to the steps used to identify a cyberattack's origin. According to Michael Schmitt, cyberattack attribution is a difficult and complicated problem. Responsibility for cyberattacks cannot be determined by the legal system. However, there are a variety of legal frameworks and innovative approaches that can help in attributing cyber attacks. Adopting these models and procedures can help states deal with cyber threats more effectively. According to Michael Schmitt, it is difficult to establish liability in the event of a cyberattack due to the absence of a uniform legal framework. However, using innovative techniques and legal frameworks can improve nations' abilities to identify cyber assaults and develop effective countermeasures (Schmitt, 2013). This indicates that juridical instruments currently exist that can aid with attribution in the event of cyber

emergencies. James A. Lewis argues that identifying the perpetrators of a cyberattacks is a crucial first step in responding to a catastrophic event in cyberspace. Taking appropriate legal, diplomatic, or military response is difficult if the perpetrators cannot be identified. The anonymity of the internet and the difficulties of acquiring proof make it difficult to pin down who is behind cyberattacks. However, several options exist for improving the attribution of cyberattacks. States may strengthen their defences against cyber threats by employing these methods and resources (Lewis, 2018). This suggests that there are viable approaches to enhancing attribution processes, notwithstanding the difficulties.

Similarly, Gabriella Blum (Wittes & Blum, 2016) highlights that cyberattack attribution is an important topic in international law. It is challenging to hold nations accountable for conduct in cyberspace without attribution. The principles of state responsibility, due diligence, and proportionality are only a few of the legal frameworks that might be used to the problem of attributing attacks via the internet. However, these models are intricate and tricky to put into action. More definition and agreement are needed on the legal principles for assigning blame for cyberattacks. Blum stresses the necessity to make nations accountable for their acts in cyberspace and the importance of attribution for international law. Some of the legal principles she discusses that can be applied to attributing cyberattacks include state responsibility, due diligence, and proportionality (Wittes & Blum, 2016). The intricacy and real-world challenges of implementing these systems are also acknowledged by Blum. She stresses the importance of better defining and agreeing upon the legal norms that regulate attribution. Attributing a cyberattack to a specific attacker may not always be easy. Attribution has far-reaching legal implications. If one country can prove that another is responsible for a cyberattack, it may be able to sue the offending nation in court. But it may be impossible for a state to take legal action in the event of a cyberattack if it cannot determine who was responsible for it (Ohlin et al., 2015).

There are other innovative methods that may be utilised to attribute cyberattacks in addition to the existing legal frameworks. Collecting and analysing digital evidence left behind by cyberattacks is known as cyber forensics. This data can be utilised to pin down the perpetrators of cyber operations. The attribution of cyberattacks can be strengthened by international collaboration. The investigation into cyberattacks can be aided by states sharing information and resources. The attribution of cyberattacks may be further strengthened through public-private collaborations. Cyberattack data from private entities can be shared with government agencies. Governments can utilise this data to better understand and attribute cyber threats (Klimburg, 2018). As cyberattack attribution is a difficult and convoluted problem, domestic legal systems cannot be relied upon to assign responsibility for cyberattacks. Attributing cyber assaults, however, can be aided by a number of legal frameworks and creative methods. States can better respond to cyber threats by adopting these frameworks and methods.

1.2. Accountability Challenges of Non-State Entities

Non-state entities evading responsibility for cyberattacks present substantial difficulties in the contemporary international law framework. International law scholars acknowledge the difficulties in prosecuting non-state actors for cyber assaults. However, within the framework of international law, governments have a number of legal tools to respond to such attacks. State accountability, legal countermeasures, cyber operations with specific targets, and international cooperation are all viable solutions (Buchanan, 2017). To meet their international legal commitments, governments must give careful consideration to the legality and proportionality of their actions.

According to Michael N. Schmitt (1999), cyber operations carried out by non-state actors are subject to the same traditional rules of international law as those carried out by states, such as the concept of state accountability and the avoidance of intervention. Schmitt emphasises that conventional norms of international law might still apply to non-state entities participating in cyber assaults. A state can be held liable for the activities of a non-state actor by invoking the principle of state responsibility. When non-state actors conduct cyber operations from one state against another, the ban of involvement may also apply. According to him, one of the biggest obstacles to holding non-state actors responsible for their acts is the lack of a clear legal framework controlling the attribution of cyberattacks to non-state actors. To guarantee that their actions are legitimate and successful, states must collaborate to build a shared understanding of the legal standards regulating cyber operations (Schmitt, 1999). Michael Schmitt draws attention to the difficulty and absence of a clear legal framework in attributing cyberattacks to non-state actors. The term attribution describes the procedure of pinpointing the origin of a cyberattack. It is difficult to hold non-state actors accountable for their conduct in the absence of a defined legal framework. Schmitt contends that governments must work together to establish uniform legal norms for cyber activities. States' responses to cyber threats can be successful and compliant with the law if they are based on a shared understanding.

Tallinn Manual 2.0 also suggests that legal solutions available to states for dealing with cyber activities carried out by non-state actors include diplomatic, economic, and legal sanctions. According to the Tallinn Manual 2.0, governments have a wide range of options for responding to cyberattacks by non-state actors. These forms of repercussions might be either diplomatic or economic or even legal in nature, according to the nature of the offence and the circumstances. Similarly, according to Matthew C. Waxman, targeted cyber operations have been employed by states against non-state actors to impede their operations, weaken their capabilities, and make them pay the price for their hostility. Waxman encourages the use of targeted cyber operations by nations to stop the operations and resources of non-state entities doing hostile action. Such actions can be used

to dissuade future cyberattacks by imposing penalties on the attackers (Waxman, 2011). However, international law should be used to evaluate the legitimacy and proportionality of such measures.

1.3. Cooperation Imperative in Cyberterrorism

According to the U.N. General Assembly Resolution 71/256, states should work together to ensure that all efforts to prevent and defeat the threat of cyberterrorism are lawful under all applicable international treaties. The resolution passed by the General Assembly also highlights the significance of governments working together to combat terrorism, particularly cyberterrorism, while adhering to their respective commitments under international law (Mačák, 2016). Therefore, while reacting to cyber assaults by non-state actors, nations should think about international legal frameworks. According to Gabriella Blum, in any endeavour to hold non-state actors responsible, the lack of collaboration from other nations is a fundamental challenge that must be addressed. The effectiveness of state responses depends on states working together to establish cooperative mechanisms. Gabriella Blum argues that attempts to hold non-state actors responsible for cyberattacks are hindered by a lack of cooperation from other nations. When dealing with cyber threats from non-state actors, cooperation among governments is essential for gathering and sharing information, exchanging knowledge, and coordinating operations. Blum asserts that, in order to effectively respond to cyber threats, nations need to establish structures for collaboration (Lewis et al., 2019). Agreements to share data, conduct combined research, and coordinate responses are all examples of such systems. States' ability to respond to non-state actors participating in cyberattacks can be strengthened by encouraging collaboration. As discussed above, attributing cyberattacks to non-state actors is not governed by any clear international law framework. This ambiguity makes it more challenging for governments when holding non-state actors responsible for their acts. It might be challenging to track down and identify non-state actors. Even if non-state actors have been effectively ascribed to an assault, this challenge might make it hard for states to take measures against them.

For several reasons, including political concerns and fear of retaliation, nations may be hesitant to collaborate with other states in examining and punishing non-state actors. The inability to work together can make it hard for governments to hold non-state actors responsible for their behaviour. Although difficult, nations can have legal recourse when reacting to cyber assaults from non-state actors. The issue with the non-state actor or the state that is suspected of harbouring the non-state actor can be resolved diplomatically by the state involved (Mazanec, 2015). Economic sanctions can be imposed by states on either the non-state actor or the state that is allegedly providing safe haven to the

non-state actor. When responding to cyber assaults by non-state actors, states have the option to employ military action. However, this choice should be made only when all other options have been exhausted, as it might have serious repercussions, including an increase in aggression.

1.4. Human Rights Concerns in Cyberattacks

Human rights may also be adversely affected by cyberattacks. Cyberattacks may be used for many various purposes, including data collection without authorization, speech censorship, and system disruptions. Journalists, activists, and members of marginalised communities are especially susceptible to these effects. In the context of cyber countermeasures, there are a number of legal mechanisms that control the trade-off between national security objectives and human rights considerations (Kulesza & Balleste, 2015). The right to privacy and the ability to express oneself are just two of the many rights guaranteed by international human rights law. Even in the sake of national security, nations must uphold these freedoms. The law of armed conflict, often known as international humanitarian law, governs all armed conflicts. This law regulates the employment of physical and virtual weapons of destruction. Human rights may be afforded more protection at the national level, or the application of cyber countermeasures may be restricted under specific conditions. There are a variety of measures states may take to guarantee that their cyber activities are in line with universal human rights principles. The right to privacy and the freedom of speech are two human rights that states must uphold in the setting of cyber countermeasures.

Cyber countermeasures taken by states must be appropriate to the severity of the cyber threat. States may use any cyber countermeasures they see appropriate to accomplish this (Watt, 2021). When employing cyber countermeasures against any state or non-state actors, states must take every possible safety measure to ensure no civilians or civilian properties are harmed. Any damage caused by a state's cyber actions must be paid for. UN Human Rights Council in their Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression expressed that human rights must be included in the design and implementation of cybersecurity policies and procedures. It stresses the need of adhering to human rights standards while implementing cybersecurity measures and countermeasures. The measures must be lawful, necessary, proportionate, and non-discriminatory, and they must not single out or discriminate against any particular persons or groups. In the Case of Delfi AS v. Estonia, the ECtHR has repeatedly affirmed that the right to freely disseminate and discuss any and all ideas, regardless of how well they are accepted or whether they are considered objectionable, is a cornerstone of a democratic society. The importance of free speech in a democratic society is underscored by this case (Wagner et al., 2019). It stresses that the scope of this freedom includes not just

generally well-liked but also potentially contentious information and opinions. Therefore, even when dealing with controversial material, cyber defences should make sure this right is protected.

Also, article 19 of the ICCPR states that everyone has the right to express themselves in any way they see fit, whether verbally, in writing or print, in art, or through any other medium of their choosing; this includes the freedom to seek for, receive, and disseminate information and ideas of any type, across any and all borders. This legal provision emphasises the expansive nature of this right, which encompasses the freedom to access, consume, and distribute information and ideas in any media. The freedom of expression and information in the digital sphere must be protected from infringement by governments. To ensure that cyber operations are conducted in accordance with international human rights norms, a clear and comprehensive legislative framework is required (Mihr, 2017). The accountability, monitoring, and judicial review aspects of this system are essential. Before launching any kind of cyber operation, states must first complete extensive human rights impact assessments. They have to analyse how any limits could affect rights like privacy and freedom of speech, and make sure they aren't more severe than is absolutely required to achieve the legitimate goals at hand. Safeguards for due process, effective remedies for suspected violations, and independent and open methods of supervision must be implemented. Without jeopardising legitimate security concerns, states should tell the public on the goals, scope, and effect of cyber activities to foster openness and public accountability. They need to work together on a global scale to create guidelines for safeguarding human rights online (Mihr, 2016). The creation of all-encompassing norms and regulations is facilitated by working together with other governments, international organisations, and the general public. States can find a middle ground between human rights and national security concerns by ensuring that their cyber activities are in line with international human rights norms.

2. Scopes and Limitations of Countermeasures against Cyberattacks

2.1. Proportionality Calibration in Cyber Operations

One of the cornerstones of international law is the concept of proportionality, which forbids the use of force that is disproportionate to the severity of the threats. The same rule applies to cyber operations as it does to any other type of military combat. A countermeasure's proportionality must be evaluated in light of the specifics of the attack it is designed to repel. A retaliatory tactic that causes more damage than the first assault is likely to be deemed disproportionate. The countermeasure ought to be exactly what is needed to stop the cyberattack. A disproportionate response is one that goes beyond what is required to stop the attack. The countermeasure should not backfire and generate more problems than it solves. If the negative effects of the countermeasure are out of proportion to the benefits,

then the countermeasure is unfair. Applying the idea of proportionality to cyber operations might be challenging due to the unique nature of cyber activities (Dwan et al., 2022). For instance, cyber activities might have unforeseen consequences and very hard to be traced. Cyber operations pose a unique set of challenges when it comes to determining the proportionality of countermeasures, which necessitates taking into account the specific features of cyberattacks and their consequences for the concept of proportionality. Many scholars of international law have shed light on the relevance of current proportionality principles to cyber operations. According to Michael N. Schmitt, states must evaluate the potential collateral damage to civilian objects and measure it against the potential military advantage in order to meet the proportionality standard. Schmitt stresses the necessity to weigh the military advantage obtained from cyber operations against the predicted harm to civilian objects. Cyber strikes fall under this concept of proportionality, where governments should weigh the possible military benefit against any collateral harm to civilian infrastructure like crucial systems or important services (Schmitt, 2012).

According to the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, cyber operations that cause severe damage to essential infrastructure or casualties might be deemed an act of war. This suggests that while weighing the potential outcomes of such cyber operations, the criterion of proportionality must be employed. Damage to important infrastructure, loss of life, or injuries to individuals are all indicators that a cyber-operation has crossed the line into an act of war. Similarly, according to Marco Roscini (2014), a State Party to a Conflict must not undertake a cyberattack against a civilian object if the predicted civilian damage or accidental injury would be disproportionate to the expected military advantage, according to the principle of proportionality. Roscini emphasises the significance of limiting cyber assaults' effects on innocent people. When conducting a cyberoperation, the predicted harm to civilian objects or persons must not exceed the projected military gain. This idea still holds water in the realm of cyberwarfare (Roscini, 2014). Again, according to Christopher C. Joyner (2011), cyberwarfare must be governed by the concept of proportionality, which states that a combatant may not utilise force greater than the danger posed by the armed forces of the state being attacked. According to Joyner, the use of force in cyberwarfare should be limited to what is both required and commensurate to the danger posed by the military capabilities of the targeted state. That means cyber operations shouldn't do more damage than is absolutely essential to stop the current threat.

Proportionality in cyber operations is determined by evaluating the projected military advantage against the anticipated harm to civilian objects, according to legal academics (Frowe, 2022). Cyberattacks are unlike any other type of attack and must be carefully considered within the context of proportionality due to their potential to cause damage to key infrastructure or result in civilian harm. The propriety and legality of cyber operations in light of the probable effects can be evaluated using the current legal

norms and principles relevant to proportionality in armed engagements. States with far fewer resources than their targets are able to undertake cyberattacks. The attacker's capabilities may be unknown or hard to predict, making it difficult to determine whether or not a countermeasure is proportionate. Complexity and unpredictability are two hallmarks of cyber operations (Schmitt, 2011).

Due to the difficulty in anticipating all of the potential outcomes, it can be challenging to determine whether or not a countermeasure is proportionate. It can be challenging to identify the origin of cyber assaults because they might be launched from anywhere. Because of this, it may be difficult to zero in on the right target for a countermeasure. Cyberattacks might be trickier to assess in terms of their scope and severity. Cyber assaults can inflict a lot of harm, but it can be hard to tell how much because of their anonymity and complexity. This might make it hard to judge if a response is appropriate given the severity of the attack. Cyber countermeasures may be more challenging to justify. With so many potential ways to respond to cyber threats, deciding whether or not to take protective action can be challenging. It is also challenging to determine the likelihood that a response may be deemed excessive increases under certain circumstances. Cyber countermeasures may make it harder to foresee potential outcomes.

2.2. Obstacles of Global Collaboration

There are a variety of obstacles that prevent governments from working together to create legitimate cyber countermeasures. Cyber activities are not governed by any universally accepted set of laws. This ambiguity might hinder state cooperation in creating efficient countermeasures. Attributing cyberattacks to a specific attacker is often challenging. Since nations may be unsure about whom to target in the event of a cyberattack, this challenge can complicate responses to such strikes (Friis & Ringsmose, 2016). There can be a broad variety of intentional and unforeseen consequences from cyberattacks. But working together as nations to create legitimate and effective cyber defences is essential. Both the difficulties and the potential solutions have been pointed out by legal experts. For example, according to Duncan Hollis (Hollis & Finnemore, 2016), the interconnectedness of cyberattacks and vulnerabilities necessitates international collaboration to solve the issue, since no one state can do so successfully on its own. Hollis highlights the realisation that no one state can adequately confront cyber dangers alone and the underlying interconnectivity in cyberspace. This emphasises the need for governments to work together to exchange knowledge, skills, and resources in order to strengthen their cyber defences.

Again, according to Christopher S. Yoo, the costs of information gathering, coordination, and enforcement can be reduced, and the success rate of cybersecurity activities can be increased by the widespread dissemination of relevant data on behalf of the states. Yoo stresses the need of sharing knowledge in the field of cybersecurity. State-to-state information sharing procedures can improve cybersecurity while cutting

expenses related with data collection and coordination. More effective defences against cyberattacks may be achieved through the exchange of threat intelligence, best practises, and technical skills (Yoo & Blanchette, 2015). The United States International Strategy for Cyberspace mandates that together with other countries, the United States will strengthen cyber standards based on respect for human rights and endeavour to lessen the likelihood of conflict caused by the spread and use of information and communication technologies. It emphasises cooperative efforts across country boundaries to spread best practises in cybersecurity and encourage accountable behaviour. By working together, nations may more easily create and execute standards and guidelines that protect human rights while also making the internet safer for everyone.

Tallinn Manual 2.0 also suggests the same approach by stating that cyber defence agreements between states might lay out the precise cooperation steps that can be taken to aid one another in the event of a cyberattack. When it comes to cyber countermeasures, the Tallinn Manual 2.0 also recommends bilateral agreements between nations. Such agreements can lay the groundwork for sharing information and resources in the event of a cyber crisis or attack. Mutual trust is fostered and cyber security initiatives may be tackled more efficiently through bilateral agreements (Tsagourias, 2012). Furthermore, UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security recommends that to improve all nations' abilities to avoid, investigate, respond to, and recover from ICT-related incidents, governments must collaborate in designing and implementing capacity-building measures, including aid and collaboration. To improve all governments' abilities to respond to ICT-related incidents, the UN GGE stresses the necessity of collaboration in capacity building, including aid and cooperation. Collaboration and coordination among nations is greatly aided by international organisations like the United Nations (Henriksen, 2019).

Scholars of the international law have noted the benefits and drawbacks of international cooperation in the development of legitimate and efficient defences against cyber threats. Cyberspace's interconnectedness makes it imperative for nations to work together, share data, and increase their collective preparedness. While multilateral institutions like the United Nations can help coordinate efforts and provide assistance for the creation of standards and capacity-building programmes, bilateral agreements can define particular cooperation actions. Collectively, state governments may strengthen their cybersecurity capabilities and respond to cyberattacks by using these tools. Despite the difficulties, there are several openings for international cooperation on the creation of legitimate yet efficient cyber defences (Katagiri, 2021). It is possible for international organisations like the United Nations to facilitate cooperation between governments in order to create efficient countermeasures. These groups can serve as a meeting place for countries to collaborate on strategies for countering cyber threats. Effective countermeasure development can also benefit from bilateral agreements between governments. These pacts can serve as a basis for governments to coordinate their responses to cyber threats and share information about them.

The Global Information Sharing and Analysis Centre (GISAC) is another structure that can help encourage cooperation between governments in order to create more effective responses (Faga, 2017). These tools can help nations coordinate their reactions to cyber threats and share information about them. Significant obstacles exist for international cooperation in the development of effective and legal defences against cyber threats. On the other hand, there are a lot of ways in which people could work together. Cybersecurity is a shared responsibility, and governmental cooperation can lead to more robust measures of defence.

2.3. Legal Labyrinth of Anticipatory Self Defence

Pre-emptive cyber operations by nations to prevent or deter impending cyber assaults are a topic of continuous discussion, as are the conditions under which such operations can be legally conducted. Existing conventions and legal frameworks concerning anticipatory self-defence are not always relevant in the cyberattacks, and there is insufficient agreement on this matter. The UN Charter, the ICJ's Nicaragua judgement, and customary international law are the most important rules and legal frameworks pertaining to anticipatory self-defence (Dean, 2013). The use of force against the sovereignty or territorial integrity of a state is explicitly forbidden under the United Nations Charter. To counter this, Article 51 of the UN Charter permits nations to use force in self-defence if they feel they are being attacked. The International Court of Justice ruled in Nicaragua Case that a person has the right to use force in self-defence even if an assault has not yet happened. Nonetheless, the ICJ emphasised that the risk of attack had to be instant, overwhelming, and leaving no choice of means, and no moment for deliberation. The right to self-defence is also recognised under customary international law. Customary international law provides guidance in self-defense situations, although its content is not always crystal apparent. Some legal scholars maintain that nations must use every available diplomatic route to settle a conflict before resorting to force. However, there are many who argue that governments have the right to employ force in self-defence in the face of an assault, even if diplomatic solutions to the conflict are still possible.

There is continuous discussion over whether or not current norms and legal frameworks pertaining to anticipatory self-defence apply in the cyberattacks (Lucas, 2016). Experts are divided on whether or not self-defence concepts can be applied to the cyber world, with some saying they can and others saying they can't because of the special nature of cyber assaults. The difficulty of attributing attacks is a major obstacle to self-defence strategies in the cyber world. In the real world, identifying the perpetrator of an assault is usually not too difficult. However, tracing the origin of an assault in the cyber realm can be tricky. This complicates the ability of nations to assess threats and exercise self-defence rights. Another issue in bringing traditional concepts of self-defence into the cyberspace is determining how close an assault actually is. In the real world, it's usually easy to tell if an assault is going to happen soon. However, gauging the imminent threat of an assault

in the cyber sphere can be challenging. This complicates the question for governments of whether or not they have the right to exercise self-defence in the face of an imminent threat (Levite & Perkovich, 2017).

Pre-emptive cyber operations, in which a state proactively takes action to stop or discourage an assault, are a contentious topic of discussion among experts. Existing norms and legal frameworks relating to anticipatory self-defence are not always obvious or appropriate in the cyber sphere, and there is no clear consensus on this topic. According to the judgement of Nicaragua v. United States of America (1986), a case adjudicated by the International Court of Justice (ICJ), in the event of an invasion or other armed attack, every sovereign state has the right to employ military action to defend its territory. It reaffirms the inherent right to self-defence. The ICJ ruled that the right to self-defence includes the ability to take action in the face of an immediate threat of violence (Travis, 2016). The ICJ also ruled that self-defence actions including the use of force have to be justified.

According to Michael Schmitt, to be justified in using force in anticipatory self-defense, it must be necessary, proportional, and used in response to an imminent, unlawful armed attack. He suggests that anticipatory self-defence is only justified in cases when the use of force is necessary and appropriate, the threat of an armed assault is imminent, and there are no legitimate alternatives to the use of force[1]. Similarly, Bruce Schneier asserts that states must avoid engaging in pre-emptive cyber operations as they are potentially devastating and unstable. It will be harder for nations to work together to address cyber security concerns if these tensions intensify. He foresees that pre-emptive cyber operations will lead to greater disputes and make it harder for nations to work together to address cyber security threats (Schneier, 2013). Altogether these assertions by international law scholars highlights that pre-emptive cyber operations are controversial and the law is still being worked out on. The legislation is still developing, and there is no unanimous agreement on the topic. But the imminence of the threat, the need of the use of force, the proportionality of the use of force, and the differentiation between combatants and civilians are all criteria that legal academics have highlighted as crucial to the legitimacy of pre-emptive cyber operations.

The dangers and rewards of conducting pre-emptive cyber operations must be weighed against these legal constraints. Pre-emptive cyber actions carry the danger of sparking a wider war (Ossoff, 2021). They may backfire if they harm international ties and make it harder for governments to work together on cyber security. Pre-emptive cyber operations are controversial, and the choice to use them must be taken on a case-by-case basis. The legal, strategic, and political implications of such operations must be carefully considered by states before they are carried out.

[1] Schmitt, M. (2022, 24 May). The United Kingdom on International Law in Cyberspace. EJIL: Talk! https://clck.ru/3F3MMo

3. Instrumentalising International Law and Institutions to Address Cyberattacks

3.1. Confronting the Lacuna in International Cybersecurity Norms

The existing state of international organisations is unable to deal with the complexity and fluidity of cyber threats. The United Nations Group of Governmental Experts (GGE) is another example of it. The GGE's efforts to build voluntary, normative frameworks are hampered by the fact that they are consensus-based, making them slower to evolve and sometimes leading to impasse as a result of competing national interests and geopolitical conflicts. The inability of existing international law to judge and execute penalties against governments that commit or assist cyberattacks is another serious problem. Because existing enforcement procedures are mostly based on conventional conceptions of war, there is a vacuum in institutional protections for governments that conduct hostile cyber operations. This highlights the need for a new International Convention to define illicit cyber actions more precisely and provide efficient mechanisms for adjudication and enforcement. Due to the ever-evolving nature of technology, a new International Convention is also required.

Current technological advancements are outstripping the ability of existing international law and institutions to respond effectively. For instance, the emergence of quantum computing and cyberattacks driven by artificial intelligence presents new issues that are not yet accounted for by existing frameworks. A Convention with an eye on the future can be of assistance by being built with adaptability and flexibility from the ground up, so that it can grow and change in tandem with technology development. Moreover, the idea of global collaboration highlights the importance of a new International Convention (Gow et al., 2019). Cybersecurity is an international issue that calls for concerted effort. Different national interests and a lack of confidence have made it difficult for existing international entities to create considerable global collaboration. Fostering collaboration, boosting trust, and guaranteeing collective cybersecurity can all be facilitated by a globally agreed-upon framework provided by an international convention. It is encouraging that existing international bodies have tried to tackle the problem of cyberattacks. However, due to the ever-changing nature of cyber dangers and the limitations of existing international legal and institutional frameworks, the response to these risks has been inadequate thus far. A new international convention aimed at countering cyber dangers has great promise. This framework has the potential to be transparent, all-encompassing, and flexible in order to facilitate international collaboration, define criminal actions, and establish enforcement procedures.

A major step toward a more secure and safe internet would be the adoption of such a convention. When it comes to settling disputes and interpreting international law, the International Court of Justice (ICJ) and other international judicial authorities have been at the forefront (Harrison Dinniss, 2012). However, there are several obstacles to their

efficiency and compatibility in dealing with cyberattacks. The ICJ must have jurisdiction over a matter to rule on it, and this is normally accomplished with the cooperation of the participating governments. However, it is challenging to establish the people involved and acquire their agreement in cyberattacks since their origins are often unknown and they can be organized from various jurisdictions. In making their decisions, the ICJ and other comparable tribunals frequently look to precedent and established principles of international law. Since cyberwarfare is still in its infancy, few examples may serve as guides. Given the complexity and novelty of cyber warfare, it may be challenging for the court to apply existing legal rules (Bucci, 2018).

Cases heard by international courts might take years to resolve due to the complexity of the law involved. However, cyberattacks happen at breakneck speed and require fast response and resolution. It is difficult for these organizations to adequately resolve cyber conflicts due to a mismatch between the pace of judicial proceedings and the fast expanding cyber scene. There is no agreement on how sovereignty, non-intervention, and the use of force under traditional international law are to be interpreted in the context of cyber operations. In 2018, UK Attorney General Jeremy Wright gave a lecture in which he argued that a country's cyber infrastructure should be considered part of its sovereign territory[2]. Because of these discrepancies, international courts may issue decisions that are at odds with one another. The United Nations Charter, the Geneva Conventions, and a few other non-binding, normative rules form the backbone of international law's determination of what is and is not permissible. The problems of attribution, non-physical injury, and governmental accountability in cyberspace are not easily addressed by these laws because they were written for a time before the Internet. The ease with which cyberattacks may be routed across numerous countries makes, for instance, tracking them back to a state actor challenging when they occur. The legal evaluation of such operations is further complicated by the lack of clarity on what constitutes an 'armed attack' in cyberspace.

Introducing clear definitions, standards, and norms that are tailored to the digital realm can be made possible by a new International Convention (Nissenbaum, 2015). Existing legal frameworks present major obstacles to enacting countermeasures against cyberattacks. It is debatable whether or not governments have the right to self-defence against cyberattacks under Article 51 of the United Nations Charter. And unlike traditional combat, there is no consensus on whether or not such actions are necessary or proportionate in cyberspace (Cornish, 2021). Clearer standards for countermeasures might be established with the creation of a new International Convention that incorporates concepts of proportionality, need, and differentiation specific to cyberspace. The United Nations and other already-existing international organizations have taken some important

[2] Schmitt, M. (2022, 24 May). The United Kingdom on International Law in Cyberspace. EJIL: Talk! https://clck.ru/3F3MMo

steps in combating cybercrime. However, they are not always successful because of things like conflicting laws and jurisdictional issues. To properly deal with cyberattacks, international law and institutions must be instrumentalised. To do so, however, would need extensive changes to adapt to the ever-changing nature of cyber threats and circumvent the challenges presented by the digital realm. The frequency and severity of cyberattacks can be mitigated by the adoption of new international conventions that define, standardize, and enforce countermeasures.

3.2. Need for Translating Legal Standards to the Cyberspace

Due to the unconventional nature of cyber operations, it might be difficult to apply traditional legal standards like distinction, proportionality, and military necessity in case of cyberattacks and cyber countermeasures. For example, combatants and civilians must be treated differently, and only legitimate military targets should be attacked, according to the concept of distinction. Because of the anonymity and attribution issues inherent in cyberspace, determining the origin and type of an attack is a major difficulty in cyberwarfare. Distinction in cyberspace has serious difficulties because to the overlap between military and civilian computer systems, networks, and infrastructure. Again, according to the concept of proportionality, an attack can only be launched if the anticipated military benefit justifies the risk to people and civilian infrastructure. Accurately assessing the probable implications of an attack and estimating the collateral damage it may create is difficult in the context of cyber warfare. A cyber operation's unforeseen secondary implications and cascade impacts can be hard to foresee due to the interrelated structure of computer systems and networks. Moreover, to achieve legitimate military objectives, force may be used, however using excessive force is forbidden under the concept of military necessity (Singer & Friedman, 2014). The definition of a legitimate military aim in cyberwarfare is problematic and complicated. In addition to conventional military targets, key infrastructure, economic systems, and information networks are common cyber operations. Since the impacts of cyber operations may reach well beyond traditional military objectives, determining when they become unnecessary is a significant difficulty.

According to Michael Schmitt (2013), the same distinction, proportionality, and military necessity rules that apply to conventional conflict also apply to cyber warfare. He says that sides to a fight must tell the difference between civilians and combatants and aim their strikes solely at the former. Parties to a conflict are bound by the concept of proportionality to employ only the level of force that is both necessary and proportional to their expected military advantage. The parties to a war are bound by the concept of military necessity to employ no more force than is strictly required to accomplish an aim that can be justified by the use of force. Cyberwarfare may be viewed through the same lens as conventional warfare, according to Michael Schmitt, who stresses the need of using the concepts of difference, proportionality, and military necessity. He contends that in the event of a cyberattack, the parties involved should

still identify fighters from civilians and focus their attacks on the former. The principle of proportionality dictates that only a reasonable scale of force should be employed to achieve a particular military objective. According to the principle of military necessity, force should only be used when absolutely necessary to achieve a legitimate military objective. Schmitt argues that these guidelines can let nations engage in cyber operations while remaining compliant with international norms (Schmitt, 2013).

Similarly, according to Professor Cordula Droege (2012), the peculiarities of cyber operations make it impossible to apply the traditional criteria of distinction, proportionality, and military necessity to cyber conflict. Cyber activities, he says, can have unforeseen implications and are sometimes hard to identify. According to Droege, nations must find novel approaches of applying the criteria of difference, proportionality, and military necessity to cyberwarfare. He argues that distinction, proportionality, and military necessity might be difficult to apply to cyber operations due to their specific nature. Droege agrees that determining responsibility for the effects of cyber operations may be challenging. Therefore, nations, in his view, need to innovate in order to adapt these ideas to cyber warfare (Droege, 2012). The complexity of cyber operations necessitates novel approaches and concepts. Furthermore, according to Russel Buchan (Buchan, 2012), they must be interpreted in a way that takes into account the special nature of cyber operations. The impacts of cyber operations can be both physical and non-physical, he explains. According to Buchan, governments must exercise caution while conducting cyber operations so as not to contravene these values. Buchan suggests bringing distinction, proportionality, and military necessity to cyber conflicts as a means of striking a fair balance. However, he does note that these notions need to be interpreted with the specifics of cyber operations in mind. Cyber operations may have several concrete and intangible implications, as Buchan acknowledges. Therefore, he warns against straying from the norms of caution and responsibility when conducting cyber operations (Buchan, 2012).

3.3. The Inadequacy of Traditional Warfare Principles in Cyberspace

One of the biggest problems with creating cyber warfare principles that are in line with traditional combat is attribution. Cyberattacks can be difficult to trace back to their source (Denardis, 2020). This is due to the fact that tracing the initiation of a cyberattack might be tricky in some cases. This makes it harder to hold governments responsible for their actions and discourage attacks before they happen. When adapting traditional methods of conflict to the digital domain, it might be difficult to rule out unintended consequences. Cyberattacks can have a wide variety of physical and non-physical effects. An assault on a government's computer network, for instance, may have the unintended consequence of bringing down essential services like the electricity grid or the water supply. This complicates the task of ensuring that cyber activities are reasonable and appropriate. Cyber operations are intricate and not always easy to grasp (Winterfeld & Andress, 2013).

Because of this, it is hard to apply the concepts of proportionality, differentiation, and military necessity. It may be difficult to tell if a cyber operation is aimed against a military target or a civilian population. Assessing the possible physical and non-physical implications of a cyberattacks can be challenging as well.

There are a number of problems that must be solved before the traditional principles of armed conflict can be adapted to cyber warfare. Cyberwarfare is difficult to define precisely because of this. Because of this, it's hard to establish universally accepted principles for conducting cyber warfare on a global scale. Cyber security lacks a worldwide regulatory framework. This hinders the ability of nations to work together to combat cyber threats (Whyte & Mazanec, 2018). The rate of technical development in the cyber sphere is really quick. This makes it challenging to adopt new laws and norms to manage emerging cyber dangers in a timely manner. Despite the obstacles, efforts should be made to modify the norms of conventional combat to apply to cyber battle. Rules and conventions to control cyberwarfare are necessary due to the increasing danger posed by it.

3.4. Complex Landscape beyond Sovereign Borders

The legal foundations defining jurisdiction over cyber actions are complicated and developing, according to Michael Schmitt (2012). States have considerable leeway in selecting how they will exercise jurisdiction over cyber operations, and there is no one international convention that tackles this issue directly, as he points out. Schmitt asserts that nations may be directed by a variety of overarching principles, such as the concepts of territoriality, nationality, and universality (Schmitt M. N., 2012). A nation-state's ability to regulate online behaviour inside its borders is grounded on the idea of territoriality. This implies that even if the victims of a cybercrime are situated in another country, the perpetrators can be brought to justice by the state in which the crime was committed (Schmitt, 2014). Nationality principle holds that a country is liable for the criminal acts of its residents wherever in the whole world, including when they are committed through the internet. Therefore, regardless of the location of the victims, a state can seek charges against its own nationals who commit cybercrimes. The concept of universality states that any cybercrime that satisfies the definition of a crime under international law can be prosecuted by any state, regardless of where the crime was done or by whom. It is possible to prosecute cybercriminals in a state even though they are not residents of that state if their conduct amount to crimes under international law and their victims are located in a different country (Shackelford, 2014).

But Thomas J. Holt et al. (2015) argues that there are major challenges in establishing jurisdiction over conduct performed in cyberspace. He points out the challenges of tracing the origin of cyber actions and the worldwide impact they might have. Holt highlights that, in order for nations to exert authority over cyber activities, they need to innovate new forms of cooperation. This is because it is sometimes difficult to determine the origin of a cyberattack when one is started. As a result, it

becomes more challenging to hold governments accountable for their conduct and to dissuade potential assaults. The possibility of unforeseen effects is another difficulty in establishing jurisdiction over cyber activity. The impacts of cyber assaults, both physical and otherwise, can be rather diverse. An assault on a government's computer network, for instance, may have the unintended consequence of bringing down essential services like the electricity grid or the water supply (Shackelford, 2012). This complicates the task of ensuring that cyber activities are reasonable and appropriate. As the usage of cyber activities grows, the difficulties in establishing and enforcing jurisdiction over them are only going to increase, according to Peter M. Shane (Shane & Hunker, 2013). According to him, states need to get creative in order to deal with the difficulties of enforcing their authority over online activity. It is expected that the difficulties of exercising jurisdiction over cyber operations would increase as cyber technology develops further. To meet these difficulties, states will need to innovate new forms of cooperation and coordination (Shane & Hunker, 2013). They'll also have to write up some brand-new rules for controlling online behaviour.

Jurisdictional problems over cyber operations are complicated and constantly developing. Since cyber activities are not addressed by a single international convention, individual governments have considerable leeway in establishing the scope of their own jurisdiction. However, there are a number of broad principles that may be used to govern the behaviour of nations. These concepts include territoriality, nationality, and universality. There are substantial difficulties in enforcing jurisdiction over cyber activity (Roscini, 2010). The perpetrators of cyberattacks are not always obvious, and their effects can be felt all around the world. The successful exercise of jurisdiction over cyber activities requires new forms of cooperation between states. As the usage of cyber activities increases, the difficulties in exercising jurisdiction over them are likely to persist. The difficulties of asserting state authority over online activity require states to take proactive measures. Cyber security lacks a worldwide regulatory framework. This hinders the ability of nations to work together to combat cyber threats. The rate of technical development in the cyber sphere is really quick (Gheciu & Wohlforth, 2018). This makes it challenging to adopt new laws and norms to manage emerging cyber dangers in a timely manner. Cyber security challenges are not being addressed with enough international collaboration. This complicates efforts to create and implement global standards for cyber behaviour.

Conclusion

The legal consequences and difficulties of cyberattacks and cyber countermeasures have been investigated in this research. It has been highlighted how difficult it is to pinpoint the origin of cyberattacks and how crucial it is to take proportionality into account when formulating cyber countermeasures. The research has also discussed the effect of cyber countermeasures on human rights, the legal consequences of countermeasures

against non-state actors, and the legal foundations for international cooperation. In addition, it has examined the legal parameters for pre-emptive cyber operations, the level of state accountability, the difficulties of defining and verifying cyber weapons, the regulatory structures for intelligence operations, the function of cybersecurity measures in safeguarding civilians and critical infrastructure, the difficulties of establishing jurisdiction over cyber activities, and the relationship between cybersecurity and the right to development. By incorporating these less explored issues of international law framework, the research hopes to contribute to the formation of legal frameworks and norms controlling countermeasures in cyber warfare, therefore promoting inclusive and sustainable growth while maintaining the preservation of individual rights and international cybersecurity. As the globe becomes more linked, cyber-related risks remain a pressing concern that makes national borders ineffective and challenges the limits of current international legal systems. The 'grey zone' of undefined legal principles that characterises the digital realm makes it difficult to determine whether or not cyberattacks are actually criminal. The lack of consensus on a generally enforceable definition of cyberattacks and on how conventional principles of international law apply to these modern difficulties is a significant lacuna in the legal system. An entirely separate International Convention is required to address the intricacies of the cyberspace. Existing frameworks have their limits and jurisdictional issues that a Convention similar to this may help clear up. The work is challenging, but it is necessary to maintain global stability in an era when wars are just as likely to be fought online as they are on the ground. International bodies have tried to tackle the problem of cyberattacks. However, a proper response has been elusive due to the ever-changing nature of cyber threats and the limitations of existing international law and institutional frameworks. There is hope in a new international convention that aims to deal with cyber dangers. This framework has the potential to be transparent, all-encompassing, and flexible in order to facilitate international collaboration, define criminal actions, and establish enforcement procedures. Such a Convention would be a huge step forward in making the internet a more secure and safe place. Therefore, it is essential to re-evaluate and adapt the current legal infrastructure, or to investigate the possibility of establishing a specific international agency, that can effectively respond to the peculiarities of cyber warfare.

References

Andrew, J., & Bernard, F. (Eds.) (2021). *Human Rights Responsibilities in the Digital Age: States, Companies, and Individuals*. Oxford: Hart Publishing. https://doi.org/10.5040/9781509938865

Bucci, S. (2018). Strategic Cyber Deterrence: The Active Cyber Defense Option by Scott Jasper. Rowman & Littlefield, 2017, 255 pp. *Strategic Studies Quarterly*, *12*(2), 134–135.

Buchan, R. (2012). Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions? *Journal of Conflict and Security Law*, *17*(2), 212–227. https://doi.org/10.1093/jcsl/krs014

Buchanan, B. (2017). *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations*. Oxford Academic. a

Cornish, P. (Ed.) (2021). *The Oxford Handbook of Cyber Security*. Oxford University Press. https://doi.org/10.1093/oxfordhb/9780198800682.001.0001
Dean, S. E. (2013). Cyber Defense: securing military systems and critical civilian infrastructure from an electronic. *HRISQ*, *XIII*(3), 911.
Denardis, L. (2020). *The Internet in Everything: Freedom and Security in a World with No off Switch*. Yale University Press. https://doi.org/10.2307/j.ctvt1sgc0
Droege, C. (2012). Get off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians. *International Review of the Red Cross*, *94*(886), 533–578. https://doi.org/10.1017/s1816383113000246
Dwan, J. H., Paige, T. P., & McLaughlin, R. (2022). Pirates of the Cyber Seas: Are State-Sponsored Hackers Modern-Day Privateers? *Law, Technology and Humans*, *3*, 52. https://doi.org/10.5204/lthj.1583
Etzioni, A., & Rice, C. J. (2015). *Privacy in a Cyber Age*. Springer. https://doi.org/10.1057/9781137513960
Faga, H. P. (2017). The Implications of Transnational Cyber Threats in International Humanitarian Law: Analysing the Distinction between Cybercrime, Cyber Attack, and Cyber Warfare in the 21st Century. *Baltic Journal of Law & Politics*, *10*, 27. https://doi.org/10.1515/bjlp-2017-0001
Friis, K., & Ringsmose, J. (Eds.) (2016). *Conflict in Cyber Space: Theoretical, Strategic and Legal Pespectives*. Routledge & CRC Press. https://doi.org/10.4324/9781315669878
Frowe, H. (2022). *The Ethics of War and Peace: An Introduction*. Routledge/Taylor & Francis Group. https://doi.org/10.4324/9781003275466
Gheciu, A., & Wohlforth, W. C. (2018). *The Oxford Handbook of International Security*. Oxford University Press. https://doi.org/10.1093/oxfordhb/9780198777854.001.0001
Gow, J., Dijxhoorn, E., Clare Kerr, R., & Verdirame, G. (Eds.) (2019). *Routledge Handbook of War, Law and Technology*. Routledge Taylor & Francis Group. https://doi.org/10.4324/9781315111759
Harrison Dinniss, H. (2012). *Cyber Warfare and the Laws of War*. Cambridge University Press. https://doi.org/10.1017/cbo9780511894527
Henriksen, A. (2019). The End of the Road for the UN GGE Process: The Future Regulation of Cyberspace. *Journal of Cybersecurity*, *5*(1), 3. https://doi.org/10.1093/cybsec/tyy009
Hollis, D. B., & Finnemore, M. (2016). Constructing Norms for Global Cybersecurity. *American Journal of International Law*, *110*(3), 425–479. https://doi.org/10.1017/s0002930000016894
Holt, T., Bossler, A., & Seigfried-Spellar, K. (2015). *Cybercrime and Digital Forensics: An Introduction*. Routledge. https://doi.org/10.4324/9781315777870
Joyner, C. C. (2011). United States foreign policy interests in the Antarctic. *The Polar Journal*, *1*(1), 17–35. https://doi.org/10.1080/2154896x.2011.569384
Katagiri, N. (2021). Why International Law and Norms Do Little in Preventing Non-State Cyber Attacks. *Journal of Cybersecurity*, *7*(1). https://doi.org/10.1093/cybsec/tyab009
Klimburg, A. (2018). *The Darkening Web: The War for Cyberspace*. Penguin Books.
Knowles, J., & Thomas, P. A. (2016). *Effective Legal Research*. Sweet & Maxwell.
Kulesza, J., & Balleste, R. (2015). *Cybersecurity and Human Rights in the Age of Cyberveillance*. Rowman & Littlefield.
Levite, A., & Perkovich, G. (2017). Understanding cyber conflict. Georgetown University Press. https://doi.org/10.1353/book62546
Lewis, D. A., Modirzadeh, N. K., & Blum, G. (2019). Quantum of Silence: Inaction and Jus Ad Bellum. *Harvard Law School Program on International Law and Armed Conflict*. https://doi.org/10.54813/azzk2231
Lewis, J. A. (2018). Rethinking Cybersecurity: Strategy, Mass Effect, and States. Center for Strategic & International Studies; Rowman & Littlefield.
Liivoja, R., & Väljataga, A. (Eds.) (2021). *Autonomous Cyber Capabilities under International Law*. NATO Cooperative Cyber Defence Centre Of Excellence 2021.
Lucas, G. (2016). *Ethics and Cyber Warfare: The Quest for Responsible Security in the Age of Digital Warfare*. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780190276522.001.0001
Mačák, K. (2016). Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors. *Journal of Conflict and Security Law*, *21*(3), 405–428. https://doi.org/10.1093/jcsl/krw014
Mazanec, B. M. (2015). *The Evolution of Cyber War: International Norms for Emerging-Technology Weapons*. University of Nebraska Press. https://doi.org/10.2307/j.ctt1d989jr
Mihr, A. (2017). *Cyber Justice : Human Rights and Good Governance for the Internet*. Springer.
Mihr, A. (2016). Cyber justice: cyber governance through human rights and a rule of law in the Internet. *US-China Law Review*, *13*(4). https://doi.org/10.17265/1548-6605/2016.04.002

Nissenbaum, D. (2015). *A Street Divided : Stories from Jerusalem's Alley of God*. St Martin's Press.
Ohlin, J. D., Govern, K., & Finkelstein, C. (Eds.) (2015). *Cyber War: Law and Ethics for Virtual Conflicts*. Oxford University Press.
Ossoff, W. (2021). Hacking the Domaine Réservé: The Rule of Non-Intervention and Political Interference in Cyberspace. *Harvard International Law Journal*, *62*(1), 298.
Putman, W. H., & Albright, J. R. (2018). *Legal Research, Analysis, and Writing*. Cengage Learning.
Roscini, M. (2010). World Wide Warfare – Jus Ad Bellum and the Use of Cyber Force. *Max Planck Yearbook of United Nations Law Online*, *14*(1), 85–130 https://doi.org/10.1163/18757413-90000050
Roscini, M. (2014). *Cyber Operations and the Use of Force in International Law*. Oxford University Press.
Schmitt, M. (2011). Cyber Operations and the Jus Ad Bellum Revisited. *Villanova Law Review*, *56*, 569.
Schmitt, M. (2012). International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed. *Harvard International Law Journal*, *54*, 13–37.
Schmitt, M. N. (1999). Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework. *Columbia Journal of Transnational Law*, *37*, 1998–1999.
Schmitt, M. N. (2012). "Attack" as a Term of Art in International Law: The Cyber Operations Context. In *4th International Conference on Cyber Conflict (CYCON 2012)*, Tallinn, Estonia (pp. 1–11).
Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge University Press. https://doi.org/10.1017/CBO9781139169288
Schmitt, M. N. (2014). Below the Threshold' Cyber Operations: The Countermeasures Response Option and International Law. *Virginia Journal of International Law*, *54*, 698.
Schneier, B. (2013). *Beyond Fear: Thinking Sensibly about Security in an Uncertain World*. Springer.
Shackelford, S. J. (2012). Toward Cyber Peace: Managing Cyber Attacks through Polycentric Governance. *American University Law Review*. https://doi.org/10.2139/ssrn.2132526
Shackelford, S. J. (2014). Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace. Cambridge University Press. https://doi.org/10.1017/cbo9781139021838
Shane, P. M., & Hunker, J. A. (Eds.) (2013). Cybersecurity : Shared Risks, Shared Responsibilities. Carolina Academic Press.
Singer, P. W., & Friedman, A. (2014). Cybersecurity and Cyberwar: What Everyone Needs to Know®. Oxford University Press. https://doi.org/10.1093/wentk/9780199918096.001.0001
Travis, P. (2016). We're Going to Nicaragua: The United States, Nicaragua, and Counterterrorism in Central America during the 1980s. *Journal of Terrorism Research*, *7*, 38. https://doi.org/10.15664/jtr.1217
Tsagourias, N. (2012). The Tallinn Manual on the International Law Applicable to Cyber Warfare: A Commentary on Chapter II — the Use of Force. In *Yearbook of International Humanitarian Law* (Vol. 15, pp. 19–43). https://doi.org/10.1007/978-90-6704-924-5_2
Tsagourias, N., & Farrell, M. (2020). Cyber Attribution: Technical and Legal Approaches and Challenges. *European Journal of International Law*, *31*(3), 941–967. https://doi.org/10.1093/ejil/chaa057
Tyler, T. R. (2017). Methodology in Legal Research. *Utrecht Law Review*, *13*(3), 130–141. https://doi.org/10.18352/ulr.410
Van Hoecke, M. (2011). *Methodologies of Legal Research*. Bloomsbury Publishing.
Wagner, B., Kettemann, M. C., & Vieth, K. (2019). *Research Handbook on Human Rights and Digital Technology: Global Politics, Law and International Relations*. Edward Elgar Publishing. https://doi.org/10.4337/9781785367724
Watkins, D., & Burton, M. (2013). *Research Methods in Law*. Routledge. https://doi.org/10.4324/9780203489352
Watt, E. (2021). State Sponsored Cyber Surveillance: The Right to Privacy of Communications and International Law. Elgar. https://doi.org/10.4337/9781789900101
Waxman, M. (2011). Cyber-Attacks as "Force" under UN Charter Article 2(4). *International Law Studies*, *43*.
Whyte, C., & Mazanec, B. (2018). *Understanding Cyber-Warfare: Politics, Policy and Strategy*. Routledge. https://doi.org/10.4324/9781315636504
Winterfeld, S., & Andress, J. (2013). *The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and Practice*. Elsevier.
Wittes, B., & Blum, G. (2016). *The Future of Violence – Robots and Germs, Hackers and Drones*. Basic Books.
Wren, C. G., & Wren, J. R. (1986). *The Legal Research Manual: A Game Plan for Legal Research and Analysis* (2nd ed.). A-R Editions.
Yoo, C. S., & Blanchette, J.-F. (2015). *Regulating the Cloud*. MIT Press. https://doi.org/10.7551/mitpress/9780262029407.001.0001

Authors information

Mohammad Minhazur Rahman – LLM, Lecturer, Department of Law, State University of Bangladesh
Address: South Purbachal, Kanchan, Dhaka-1461, Bangladesh
E-mail: sabitminhaz@gmail.com
ORCID ID: https://orcid.org/0009-0004-9764-5450

Tapos Kumar Das – LLM, Associate Professor, Department of Law & Justice, Jahangirnagar University; PhD Student, School of Law, City University of Hong Kong
Address: Savar, Dhaka-1342, Bangladesh; 83 Tat Chee Avenue, Kowloon Tong, Kowloon, Hong Kong
E-mail: taposlaw@juniv.edu
ORCID ID: https://orcid.org/0000-0002-3349-8947

Authors' contributions

The authors have contributed equally into the concept and methodology elaboration, validation, formal analysis, research, selection of sources, text writing and editing, project guidance and management.

Conflict of interests

The authors declare no conflict of interests.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law
PASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – April 1, 2024
Date of approval – April 18, 2024
Date of acceptance – December 13, 2024
Date of online placement – December 20, 2024

Научная статья
УДК 34:004:341.4:004.8
EDN: https://elibrary.ru/nnftqi
DOI: https://doi.org/10.21202/jdtl.2024.46

Противодействие кибератакам: пробелы международного права и перспективы их преодоления

Мохаммад Минхазур Рахман ✉

Государственный университет Бангладеш, Дакка, Бангладеш

Тапос Кумар Дас

Джахангирнагарский университет, Дакка, Бангладеш
Городской университет Гонконга, Гонконг

Ключевые слова

кибератака,
киберпреступность,
международная конвенция,
международное право,
права человека,
право,
принцип должной осмотрительности,
принцип соразмерности,
принципы международного права,
цифровые технологии

Аннотация

Цель: категорирование кибератак в национальном и международном правопорядках и определение юридических мер противодействия им на международном уровне.

Методы: представлены доктринальным юридическим анализом, формально-юридическим, сравнительно-правовым методами, синтезом, индукцией, дедукцией, а также методикой правового прогнозирования и моделирования. Исследованию подверглись международно-правовые документы и акты национального законодательства, судебные прецеденты, доктринальные источники.

Результаты: в статье определены юридические последствия кибератак, выявлены трудности определения и привлечения лиц и организаций к ответственности за их совершение, обозначены национальные меры противодействия кибератакам на основе принципа пропорциональности, систематизированы международно-правовые основы реагирования на кибератаки. Основное внимание в работе уделено актуальным проблемам выявления и проверки кибероружия, установления международных стандартов его использования, разработки методов разоружения или ограничения наступательных кибервозможностей. Поставлен вопрос обеспечения гуманитарной деятельности, защиты важнейших объектов инфраструктуры, а также населения с помощью мер кибербезопасности в военное время. Проанализированы правовые основы и выявлены пробелы и иные дефекты действующего регулирования в осуществлении юрисдикции в таких областях кибердеятельности, как международные операции, локализация данных и экстерриториальное исполнение национального законодательства.

✉ Корреспондирующий автор
© Рахман М. М., Дас Т. К., 2024

Статья находится в открытом доступе и распространяется в соответствии с лицензией Creative Commons «Attribution» («Атрибуция») 4.0 Всемирная (CC BY 4.0) (https://creativecommons.org/licenses/by/4.0/deed.ru), позволяющей неограниченно использовать, распространять и воспроизводить материал при условии, что оригинальная работа упомянута с соблюдением правил цитирования.

Разработаны и описаны параметры, в рамках которых государства вправе проводить упреждающие кибероперации для предотвращения или сдерживания кибератак (киберконтрмеры), основными из которых являются проявление должной осмотрительности, законность принятии решения о применении киберконтрмер, соразмерность защиты от последствий совершения противоправных действий.

Научная новизна: обусловлена представленными в статье прогрессивными решениями в области международно-правового регулирования принятия государствами киберконтрмер в ответ на киберпреступления, сформулированными с учетом влияния обозначенных мер противодействия на права и свободы человека и гражданина, в том числе такие как право на неприкосновенность частной жизни и свобода слова.

Практическая значимость: результаты проведенного исследования могут быть взяты за основу при разработке и совершенствовании международно-правовых инструментов в области борьбы с кибератаками и обеспечения кибербезопасности, а также могут послужить образцом для национального законодателя при проектировании правотворческих решений противодействия киберпреступлениям.

Для цитирования

Рахман, М. М., Дас, Т. К. (2024). Противодействие кибератакам: пробелы международного права и перспективы их преодоления. *Journal of Digital Technologies and Law*, *2*(4), 973–1002. https://doi.org/10.21202/jdtl.2024.46

Список литературы

Andrew, J., & Bernard, F. (Eds.) (2021). *Human Rights Responsibilities in the Digital Age: States, Companies, and Individuals*. Oxford: Hart Publishing. https://doi.org/10.5040/9781509938865

Bucci, S. (2018). Strategic Cyber Deterrence: The Active Cyber Defense Option by Scott Jasper. Rowman & Littlefield, 2017, 255 pp. *Strategic Studies Quarterly*, *12*(2), 134–135.

Buchan, R. (2012). Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions? *Journal of Conflict and Security Law*, *17*(2), 212–227. https://doi.org/10.1093/jcsl/krs014

Buchanan, B. (2017). *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations*. Oxford Academic. Cornish, P. (Ed.) (2021). *The Oxford Handbook of Cyber Security*. Oxford University Press. https://doi.org/10.1093/oxfordhb/9780198800682.001.0001

Dean, S. E. (2013). Cyber Defense: securing military systems and critical civilian infrastructure from an electronic. *HRISQ*, *XIII*(3), 911.

Denardis, L. (2020). *The Internet in Everything: Freedom and Security in a World with No off Switch*. Yale University Press. https://doi.org/10.2307/j.ctvt1sgc0

Droege, C. (2012). Get off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians. *International Review of the Red Cross*, *94*(886), 533–578. https://doi.org/10.1017/s1816383113000246

Dwan, J. H., Paige, T. P., & McLaughlin, R. (2022). Pirates of the Cyber Seas: Are State-Sponsored Hackers Modern-Day Privateers? *Law, Technology and Humans*, *3*, 52. https://doi.org/10.5204/lthj.1583

Etzioni, A., & Rice, C. J. (2015). *Privacy in a Cyber Age*. Springer. https://doi.org/10.1057/9781137513960

Faga, H. P. (2017). The Implications of Transnational Cyber Threats in International Humanitarian Law: Analysing the Distinction between Cybercrime, Cyber Attack, and Cyber Warfare in the 21st Century. *Baltic Journal of Law & Politics*, *10*, 27. https://doi.org/10.1515/bjlp-2017-0001

Friis, K., & Ringsmose, J. (Eds.) (2016). *Conflict in Cyber Space: Theoretical, Strategic and Legal Pespectives*. Routledge & CRC Press. https://doi.org/10.4324/9781315669878

Frowe, H. (2022). *The Ethics of War and Peace: An Introduction*. Routledge/Taylor & Francis Group. https://doi.org/10.4324/9781003275466

Gheciu, A., & Wohlforth, W. C. (2018). *The Oxford Handbook of International Security*. Oxford University Press. https://doi.org/10.1093/oxfordhb/9780198777854.001.0001
Gow, J., Dijxhoorn, E., Clare Kerr, R., & Verdirame, G. (Eds.) (2019). *Routledge Handbook of War, Law and Technology*. Routledge Taylor & Francis Group. https://doi.org/10.4324/9781315111759
Harrison Dinniss, H. (2012). *Cyber Warfare and the Laws of War*. Cambridge University Press. https://doi.org/10.1017/cbo9780511894527
Henriksen, A. (2019). The End of the Road for the UN GGE Process: The Future Regulation of Cyberspace. *Journal of Cybersecurity*, *5*(1), 3. https://doi.org/10.1093/cybsec/tyy009
Hollis, D. B., & Finnemore, M. (2016). Constructing Norms for Global Cybersecurity. *American Journal of International Law*, *110*(3), 425–479. https://doi.org/10.1017/s0002930000016894
Holt, T., Bossler, A., & Seigfried-Spellar, K. (2015). *Cybercrime and Digital Forensics: An Introduction*. Routledge. https://doi.org/10.4324/9781315777870
Joyner, C. C. (2011). United States foreign policy interests in the Antarctic. *The Polar Journal*, *1*(1), 17–35. https://doi.org/10.1080/2154896x.2011.569384
Katagiri, N. (2021). Why International Law and Norms Do Little in Preventing Non-State Cyber Attacks. *Journal of Cybersecurity*, *7*(1). https://doi.org/10.1093/cybsec/tyab009
Klimburg, A. (2018). *The Darkening Web: The War for Cyberspace*. Penguin Books.
Knowles, J., & Thomas, P. A. (2016). *Effective Legal Research*. Sweet & Maxwell.
Kulesza, J., & Balleste, R. (2015). *Cybersecurity and Human Rights in the Age of Cyberveillance*. Rowman & Littlefield.
Levite, A., & Perkovich, G. (2017). Understanding cyber conflict. Georgetown University Press. https://doi.org/10.1353/book62546
Lewis, D. A., Modirzadeh, N. K., & Blum, G. (2019). Quantum of Silence: Inaction and Jus Ad Bellum. *Harvard Law School Program on International Law and Armed Conflict*. https://doi.org/10.54813/azzk2231
Lewis, J. A. (2018). Rethinking Cybersecurity: Strategy, Mass Effect, and States. Center for Strategic & International Studies; Rowman & Littlefield.
Liivoja, R., & Väljataga, A. (Eds.) (2021). *Autonomous Cyber Capabilities under International Law*. NATO Cooperative Cyber Defence Centre Of Excellence 2021.
Lucas, G. (2016). *Ethics and Cyber Warfare: The Quest for Responsible Security in the Age of Digital Warfare*. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780190276522.001.0001
Mačák, K. (2016). Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors. *Journal of Conflict and Security Law*, *21*(3), 405–428. https://doi.org/10.1093/jcsl/krw014
Mazanec, B. M. (2015). *The Evolution of Cyber War: International Norms for Emerging-Technology Weapons*. University of Nebraska Press. https://doi.org/10.2307/j.ctt1d989jr
Mihr, A. (2017). *Cyber Justice : Human Rights and Good Governance for the Internet*. Springer.
Mihr, A. (2016). Cyber justice: cyber governance through human rights and a rule of law in the Internet. *US-China Law Review*, *13*(4). https://doi.org/10.17265/1548-6605/2016.04.002
Nissenbaum, D. (2015). *A Street Divided : Stories from Jerusalem's Alley of God*. St Martin's Press.
Ohlin, J. D., Govern, K., & Finkelstein, C. (Eds.) (2015). *Cyber War: Law and Ethics for Virtual Conflicts*. Oxford University Press.
Ossoff, W. (2021). Hacking the Domaine Réservé: The Rule of Non-Intervention and Political Interference in Cyberspace. *Harvard International Law Journal*, *62*(1), 298.
Putman, W. H., & Albright, J. R. (2018). *Legal Research, Analysis, and Writing*. Cengage Learning.
Roscini, M. (2010). World Wide Warfare – Jus Ad Bellum and the Use of Cyber Force. *Max Planck Yearbook of United Nations Law Online*, *14*(1), 85–130 https://doi.org/10.1163/18757413-90000050
Roscini, M. (2014). *Cyber Operations and the Use of Force in International Law*. Oxford University Press.
Schmitt, M. (2011). Cyber Operations and the Jus Ad Bellum Revisited. *Villanova Law Review*, *56*, 569.
Schmitt, M. (2012). International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed. *Harvard International Law Journal*, *54*, 13–37.
Schmitt, M. N. (1999). Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework. *Columbia Journal of Transnational Law*, *37*, 1998–1999.
Schmitt, M. N. (2012). "Attack" as a Term of Art in International Law: The Cyber Operations Context. In *4th International Conference on Cyber Conflict (CYCON 2012)*, Tallinn, Estonia (pp. 1–11).
Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge University Press. https://doi.org/10.1017/CBO9781139169288

Schmitt, M. N. (2014). Below the Threshold' Cyber Operations: The Countermeasures Response Option and International Law. *Virginia Journal of International Law*, *54*, 698.

Schneier, B. (2013). *Beyond Fear: Thinking Sensibly about Security in an Uncertain World*. Springer.

Shackelford, S. J. (2012). Toward Cyber Peace: Managing Cyber Attacks through Polycentric Governance. *American University Law Review*. https://doi.org/10.2139/ssrn.2132526

Shackelford, S. J. (2014). Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace. Cambridge University Press. https://doi.org/10.1017/cbo9781139021838

Shane, P. M., & Hunker, J. A. (Eds.) (2013). Cybersecurity : Shared Risks, Shared Responsibilities. Carolina Academic Press.

Singer, P. W., & Friedman, A. (2014). Cybersecurity and Cyberwar: What Everyone Needs to Know®. Oxford University Press. https://doi.org/10.1093/wentk/9780199918096.001.0001

Travis, P. (2016). We're Going to Nicaragua: The United States, Nicaragua, and Counterterrorism in Central America during the 1980s. *Journal of Terrorism Research*, *7*, 38. https://doi.org/10.15664/jtr.1217

Tsagourias, N. (2012). The Tallinn Manual on the International Law Applicable to Cyber Warfare: A Commentary on Chapter II — the Use of Force. In *Yearbook of International Humanitarian Law* (Vol. 15, pp. 19–43). https://doi.org/10.1007/978-90-6704-924-5_2

Tsagourias, N., & Farrell, M. (2020). Cyber Attribution: Technical and Legal Approaches and Challenges. *European Journal of International Law*, *31*(3), 941–967. https://doi.org/10.1093/ejil/chaa057

Tyler, T. R. (2017). Methodology in Legal Research. *Utrecht Law Review*, *13*(3), 130–141. https://doi.org/10.18352/ulr.410

Van Hoecke, M. (2011). *Methodologies of Legal Research*. Bloomsbury Publishing.

Wagner, B., Kettemann, M. C., & Vieth, K. (2019). *Research Handbook on Human Rights and Digital Technology: Global Politics, Law and International Relations*. Edward Elgar Publishing. https://doi.org/10.4337/9781785367724

Watkins, D., & Burton, M. (2013). *Research Methods in Law*. Routledge. https://doi.org/10.4324/9780203489352

Watt, E. (2021). State Sponsored Cyber Surveillance: The Right to Privacy of Communications and International Law. Elgar. https://doi.org/10.4337/9781789900101

Waxman, M. (2011). Cyber-Attacks as "Force" under UN Charter Article 2(4). *International Law Studies*, *43*.

Whyte, C., & Mazanec, B. (2018). *Understanding Cyber-Warfare: Politics, Policy and Strategy*. Routledge. https://doi.org/10.4324/9781315636504

Winterfeld, S., & Andress, J. (2013). *The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and Practice.* Elsevier.

Wittes, B., & Blum, G. (2016). *The Future of Violence – Robots and Germs, Hackers and Drones*. Basic Books.

Wren, C. G., & Wren, J. R. (1986). *The Legal Research Manual: A Game Plan for Legal Research and Analysis* (2nd ed.). A-R Editions.

Yoo, C. S., & Blanchette, J.-F. (2015). *Regulating the Cloud*. MIT Press. https://doi.org/10.7551/mitpress/9780262029407.001.0001

Сведения об авторах

Мохаммад Минхазур Рахман – магистр права, преподаватель, кафедра права, Государственный университет Бангладеш
Адрес: Бангладеш, 1461, г. Дакка, Канчан, Саут Пурбачал
E-mail: sabitminhaz@gmail.com
ORCID ID: https://orcid.org/0009-0004-9764-5450

Тапос Кумар Дас – магистр права, доцент, кафедра права и юстиции, Джахангирнагарский университет; кандидат на соискание степени PhD, Школа права, Городской университет Гонконга
Адрес: Бангладеш, 1342, г. Дакка, Савар; Гонконг, Коулун, Коулун Тонг, Тат Чи Авеню, 83
E-mail: taposlaw@juniv.edu
ORCID ID: https://orcid.org/0000-0002-3349-8947

Вклад авторов

Авторы внесли равный вклад в разработку концепции, методологии, валидацию, формальный анализ, проведение исследования, подбор источников, написание и редактирование текста, руководство и управление проектом.

Конфликт интересов

Авторы сообщают об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.87 / Международное право
Специальность ВАК: 5.1.5 / Международно-правовые науки

История статьи

Дата поступления – 1 апреля 2024 г.
Дата одобрения после рецензирования – 18 апреля 2024 г.
Дата принятия к опубликованию – 13 декабря 2024 г.
Дата онлайн-размещения – 20 декабря 2024 г.

Research article
UDC 34:004:341:004.4
EDN: https://elibrary.ru/ocdmla
DOI: https://doi.org/10.21202/jdtl.2024.47

International Cooperation in Overcoming Digital Inequality: Legal Frameworks, Barriers and Development Parameters

Ksenia M. Belikova
Kutafin Moscow State Law University, Moscow, Russia

Rafael Dias Martins
Intersystemas, Natal, Brazil

Evgeniy T. Kazanba
Kutafin Moscow State Law University, Moscow, Russia

Keywords

availability of technologies,
digital divide,
digital inequality,
digital space,
digital technologies,
international cooperation,
international law,
Internet,
law,
legislation

Abstract

Objective: based on a systematic analysis of the actual level of international cooperation in overcoming digital inequality, to determine the parameters of its further development, taking into account modern legal and other barriers and global challenges caused by the transition from the knowledge economy to the data economy.

Methods: the methodological basis of the research is represented by dialectics, comparative legal and historical legal approaches, and the method of system analysis.

Results: the problem of digital inequality was considered in the following key aspects: access to the Internet; differences in the level of digital literacy; features of technology use and the versatility of digital inequality. It is noted that access to the Internet and digital technologies should become one of the fundamental human rights in order to ensure equal opportunities for all segments of society, since initially the crystallization of clearly expressed digital differences is based on the existing offline social differences. It was established that, in order to successfully overcome digital inequality, the key global task is to develop digital skills and literacy among the population. It is also important to stimulate the rational use

Corresponding author
© Belikova K. M., Dias Martins R., Kazanba E. T. , 2024

This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (CC BY 4.0) (https://creativecommons.org/licenses/by/4.0), which permits unrestricted re-use, distribution and reproduction, provided the original article is properly cited.

of technologies and ensure people's understanding of working with both the technologies and the data obtained through them. The authors propose to expand and deepen cooperation between developed and developing countries so that the latter can produce more data that may serve as a metric and a basis for creating development strategies. At the same time, greater transparency should be ensured by providing effective and accessible means so that the data owner can clearly understand who and why processes their personal data. The article argues that the transition from the knowledge economy to the data economy requires the adaptation of international cooperation strategies to ensure equitable access to both data and their processing. This may accelerate scientific discoveries and support inclusive economic development. The issues of fragmentation and defragmentation of international law are analyzed.

Scientific novelty: it is due to the current lack of scientific results concerning the level of international cooperation achieved so far in overcoming digital inequality given the parameters of its systemic development and the main (legal and other) barriers.

Practical significance: the study results can be used to improve the legal framework and strategies for international cooperation in overcoming digital inequality to ensure equitable access to data and their processing.

For citation

Belikova, K. M., Dias Martins, R., Kazanba, E. T. (2024). International Cooperation in Overcoming Digital Inequality: Legal Frameworks, Barriers and Development Parameters. *Journal of Digital Technologies and Law, 2*(4), 1003–1030. https://doi.org/10.21202/jdtl.2024.47

Contents

Introduction
1. Parameters of the development of international cooperation in overcoming digital inequality
   1.1. General context
   1.2. Internet access: practical implementations and barriers
   1.3. The global North–South digital divide and ways to overcome it
   1.4. Delocalization of the digital space as a mechanism of international cooperation: examples of approaches
2. Cooperation in overcoming digital inequality at the regional level
   2.1. Fragmentation of international law and network partnership
   2.2. Digital skills of users: a barrier and a development parameter
   2.3. Obstacles to the full implementation of the digital technologies' potential: the example of Brazil and the experience of the USSR

2.4. Data inequality: the new challenge of the data economy and the use of personal data
Conclusions
References

Introduction

Legal and other sciences have always aimed to address a variety of societal problems, including (un)equality issues. Attempts by countries to reduce social inequalities have not always been successful, and scientific research on these issues began long after these attempts had been implemented[1]. Probably, it is high time to find solutions to digital inequality/divide/gap, and not to miss out the inequalities that are beginning to grow more and more rapidly to become social ones: in the digitalization era, social inequalities are often transferred to the digital space, which is becoming increasingly important in people's lives. This is especially true given the fact that achieving and respecting digital equality during digitalization can be an effective tool to combat social inequalities.

1. Parameters of the development of international cooperation in overcoming digital inequality

1.1. General context

Talking about parameters of the development of international cooperation in overcoming the digital divide as input data, we can see the following. In 2008, the UN Secretary-General convened the High-level Panel on Digital Cooperation[2] to promote proposals to strengthen cooperation in the digital space between governments, the private sector, civil society, international organizations, technical and academic communities, and other relevant or interested parties. The panel is expected to raise awareness of the transformative impact of digital technologies on societies and economies and contribute to a broader public debate on how to ensure a secure and inclusive digital future for all, taking into account the relevant human rights' standards. One of the Panel's results was the 2019 report "The Age of Digital Interdependence" [3] (co-chaired by the famous Melinda Gates and Jack Ma), which argues that "digital dividends coexist with digital divides"[4].

---

1 Kiseleva, E. V., Markelova, M. N. (2022). UNO integrated approach to the protection of human rights by the example of children-refugees. In A. Ku. Abashidze (ed.), International law: manual for post-graduate students (pp. 300–329). Moscow: RUDN.

2 Secretary-General's High-level Panel on Digital Cooperation. https://clck.ru/3EYpgr

3 The Age of Digital Interdependence. Report of the UN Secretary-General's High-level Panel on Digital Cooperation. (2019, June 10). https://clck.ru/3EYpiU

4 Ibid. P. 6.

Probably, this is why the traditional pattern of analyzing digital divide includes three key aspects, which we will also consider both as parameters for the development of international digital cooperation in this sphere and as its barriers. These are: 1) unequal access to the Internet (access...as the 'first-level digital divide'); 2) differences in the level of digital literacy among users of both the Internet and various digital products, technologies and services (skills/usage...as the 'second-level digital divide'); 3) the multifaceted nature of the digital divide, emphasizing the importance of users' motivation and the specifics of technology use to achieve the desired benefits (benefits/outcomes... as the 'third-level digital divide') (Li et al., 2024, Gladkova et al., 2019, Cinnamon, 2019; Du & Wang, 2024; Kuo-Hsun, 2022)[5].

Although today one cannot speak of digital inequality only in relation to access (lack of access) to the Internet, all other levels are simply irrelevant without such access. Hence, these three levels (parameters, barriers) have received sufficient attention both in the above-mentioned report "The Age of Digital Interdependence" and in the UN Secretary-General's Report "Roadmap for Digital Cooperation"[6]. The latter, referring to the 2019 Panel Report, indicates five recommendations for the international community to work together to optimize the use of digital technologies and reduce risks. The first recommendation is to build an inclusive digital economy and society (others are to develop human and institutional potential; to protect human rights and strengthen human rights organizations; to build digital trust, security and stability; and to promote global digital cooperation). This indicates that focusing on access to the Internet and digital technologies is a necessary, but not sufficient step. It is necessary to ensure that technologies are used inclusively[7]. It is also argued that human rights are realized both on and off the Web, especially with regard to security and privacy.

1.2. Internet access: practical implementations and barriers

Starting with the issue of Internet access, it is worth noting that in practical terms, Starlink project of Space X, for example, is a unique initiative aimed at promoting digital equality around the world. Starlink is a global satellite Internet network developed and provided by SpaceX, a company founded by Elon Musk[8]. Its slogan is "Connect at home or on the go". The technology was supposed to be available worldwide, but this is currently not the case due to restrictions in some countries, which vary and are related to various motivations, including radio frequency regulation, data privacy,

5 Ibid. Pp. 4, 6, 7–9, 11–13, 32.

6 Roadmap for Digital Cooperation. Report of the Secretary-General. (2020, June). https://clck.ru/3EYpsV

7 Ibid. P. 4.

8 High-speed internet around the world. https://clck.ru/3EYpuN

security, etc. [9] However, the essence of the restrictions is not so much the presence or absence of equipment (for example, according to recent open media information, Starlink equipment can again be bought in Russia[10]) or low-orbit satellites violating the territorial borders of various countries. It is more in the approaches to ensuring the information security of states[11]. Concern about this issue is reflected in various acts and their drafts. For example, earlier the Russian Ministry of Communications and Mass Media proposed to introduce into the Russian Code of Administrative Offenses an article stipulating a fine for misusing satellite communication networks under foreign jurisdiction located in the Russian territory[12]. One should also mention the Decree of the Russian Government of October 20, 2021 No. 1800 "On the order of registration of radio electronic means and high-frequency devices" [13]. It established a list and rules of registration of such means and devices. This approach is based on the concept of digital sovereignty[14] and the Decree of the Russian President "On approval of the information security doctrine of the Russian Federation"[15]. It is worth mentioning that Starlink satellites have long been somewhat of a nuisance to astronomers, and recently a group of experts from China have published a study in the Radio Engineering peer-reviewed scientific journal, accusing SpaceX of its Starlink satellites violating safety rules, as this may lead to a disaster in orbit by them not keeping a distance between each other[16]. Specifically, on June 30, 2022, two Starlink satellites approached each other by only 4.9 km, while the generally accepted minimum distance is 10 km. According to this study, the extreme proximity was not an accident, but the result of a complex SpaceX scheme aimed at maximizing the performance of the laser communication system.

9 See, e.g.: Starlink network will not operate in Russia, China, Belarus and Iran. (September 19, 2022). https://clck.ru/3EYpvS

10 See: Starlink terminals are on sale again in Russia. Where and how can they be used? (February 6, 2024). clck.ru/3EYpwA

11 See, e.g.: Starlink and OneWeb cannot operate in Russia due to the priority of the Russian application for frequencies. (December 15, 2022). https://clck.ru/3EYpya; Decree of the Russian Government No. 1194 of November 14, 2014 (November 24, 2014). Collection of the legislation of the Russian Federation. No. 47, Art. 6554.

12 The Ministry of Communications proposes to penalize the use of foreign satellite networks in Russia. (June 11, 2019). https://clck.ru/3EYpzQ

13 Collection of the legislation of the Russian Federation. (November 1, 2021), No. 44 (Part III), Art. 7411.

14 Zinovieva, E., Yajie, B. (May 29, 2023). Digital Sovereignty in Russia and China. clck.ru/3EYq26

15 Decree of the Russian President No. 646 of 05.12.2016. (December 12, 2016). Collection of the legislation of the Russian Federation. No. 50, Art. 7074.

16 The source not specifying that, the Chinese scientists are referring to Kessler syndrome, a theoretical situation of the domino principle on a near-Earth scale, for example, when space debris resulting from the collision of two satellites, collides with other satellites to form more and more debris, making the entire orbit unusable for spacecraft in the shortest possible time. See: Is SpaceX with its Starlink satellites threatening the entire space industry? Chinese scientists urged the company to stick to the rules. (November 30, 2022). https://clck.ru/3EYq4q

The said case was allegedly not the only one. Prior to that, in 2021, China filed a complaint against Starlink with the UNO. It claimed that during 2021, a Chinese space station had to perform evasive maneuvers twice to avoid collision with Elon Musk's satellites[17].

The complaint is based on the Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies[18]. Its Article V reads: "States Parties to the Treaty shall immediately inform other States Parties to the Treaty or the Secretary-General of the United Nations of phenomena in outer space, including the Moon and other celestial bodies, which they have identified and which could constitute a danger to the life or health of astronauts". According to its Article VI, "the States Parties to the Treaty bear international responsibility for national activities in outer space, including the Moon and other celestial bodies, regardless of whether they are carried out by governmental bodies or non-governmental legal entities, and for ensuring that national activities are carried out in accordance with the provisions contained in this Treaty...".

Despite such positions, one cannot deny that satellite Internet technology and its legal regime can play an important role in solving the problem of digital inequality at the level of access to digital technologies in both developed and developing countries (Rabbani, 2024). For example, on June 5, 2024, at the round table on eliminating digital inequality in Russia, held at the Federation Council Committee on Economic Policy, A. Volin, Director General of "Space Communications", noted that this enterprise closely cooperates with the Ministry of Digital Development for connecting small settlements. "In Russia, there are 13.8 thousand settlements with 50 to 100 inhabitants and another 20 thousand settlements with 11 to 25 inhabitants. These are territories where optical fiber will never come. We calculated that it would take 50 years to take cable communications and the Internet to all these places, and the price would be about 600 thousand rubles per subscriber." Although the satellite may offer lower speeds, the time and cost of connecting consumers in this case will be significantly smaller[19].

Researchers note that the Internet, a prominent representative of digital technologies, was created as a means of transferring data between universities, and its purpose was to create open access to knowledge (Pool et al., 1999). However, even one of the oldest global packet-switched networks, ARPANET, was created by the DARPA agency (at that time – ARPA), who signed a software development contract with Bolt, Beranek and Newman from Cambridge, Massachusetts, in late 1968. Physically, ARPANET consisted

---

17 China has filed a complaint with the UNO against Starlink over threats to its space station. (December 29, 2021). Miltroen. https://clck.ru/3EYq5m

18 Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies [Russian, English] Adopted by General Assembly resolution 2222 (XXI) of December 19, 1966 Signed in Washington, London, Moscow. (January 27, 1967). https://clck.ru/3EYq6h and https://clck.ru/3EYq8V

19 Digital equality and satellite fraternity. (June 11, 2024). https://clck.ru/3EYqBJ

of approximately 50 C30 and C300 minicomputers of BBN Corporation, called Packet Switching Nodes (PSN). Point-to-point data lines, leased from firms providing global communications, connected PSNs together, forming a network. For example, a leased line connected the PSN, located at Purdue University, to the PSN at Carnegie Mellon and to the PSN at the University of Wisconsin[20]. Actually, they were located at universities, but DARPA[21] is the Advanced Defense Research Projects Agency of the US Department of Defense (Advanced Research Projects, with the word "defense" appearing and disappearing)[22]. Did it really imply openness from the beginning? The answer depends on the purpose of its creation (and now its functioning), and not intermediate testing in the university infrastructure.

An analysis of other national acts on electronic communication networks, electronic government and services, for example, of Austria, Denmark, the Netherlands[23], the European Union as a whole[24], shows that the purpose of legal regulation is double-sided. On the one hand, it is to ensure equality of citizens and other subjects of regulated relations (for example, people with disabilities and others); on the other hand, it is to impose responsibilities on service providers (for example, public authorities). It shows the lack of holistic regulation and high fragmentation even at the level of national legislation. This situation can be eliminated in Russia with the adoption of the digital code, the idea of which does not cease to be discussed.

1.3. The global North–South digital divide and ways to overcome it

At the same time, the said problem of access to technologies acquires a new color from the perspective of the digital divide between the global North and the global South, the inequality of access to digital infrastructure between developed and developing countries, between rich and poor (the so-called inequality of technological opportunities) (Cinnamon, 2019; Gallardo & Whitacre, 2024; Wang & Zhang, 2024). The term "digital neocolonialism" is not uncommon already. It is caused by an imbalance in the resources available to developed and developing countries. Expensive technological solutions

---

20 Global information resources. Theme 2. Review of information networks under operation. https://clck.ru/3EYqC8

21 DARPA. https://clck.ru/3EYqDF

22 See: DARPA: how the agency that created the Internet was born out of sales of household chemicals and fear of Sputnik. (December 17, 2022). Erwinmal. RUVDS.com. https://clck.ru/3EYqE2

23 Danilov, N. A. (2013). Legal regulation of e-government in foreign countries: abstract of Cand. Sci. (Law) thesis. Moscow: HSE; Danilov, N. A. (2012). Social justice in the information society: the problem of digital equality. Informatsionnoye pravo, 2(29), 5–6 and others.

24 Directive (EU) 2016/2102 of the European Parliament and of the Council of 26 October 2016 on the accessibility of the websites and mobile applications of public sector bodies. (2016, December 2). OJ L, 327, 1–15. https://clck.ru/3EYqFk; Directive (EU) 2019/882 of the European Parliament and of the Council of 17 April 2019 on the accessibility requirements for products and services. (2019, June 7), OJ L, 151, 70–115. https://clck.ru/3EYqHA

caused by the non-application of the strategy of open source patents[25] and open innovations (hereinafter referred to as OIs) for users create inequality – now OIs are used for the convenience and benefit of companies due to their lack of funds, specialists and other things to solve emerging issues alone. Multinational companies monopolize the market and do not contribute to the development of poor countries. As a result, poor countries remain dependent on the rich ones. At the same time, the actual monopolization of certain solutions, platforms and services is very common in the digital sphere.

The global digital divide may also be growing due to the allocation of resources for green transformation. Therefore, for example, the Program of the Indian Presidency of the G20 highlights digital equality as a priority. Without a fundamental change in worldview, it will be difficult to achieve equal access to digital infrastructure and sustainable development[26]. This idea developed in the theme of India's G20 presidency, "One Earth – One Family – One Future", aimed at achieving unanimity to collectively and effectively solve global problems[27].

Thus, we can draw the following scheme for the formation of digital inequality (Fig. 1), where digitalization is initially determined by access to technological opportunities (level 1), although there may be additional differences in technical skills and ways of using technology (level 2), as well as in who can benefit and get tangible results from using it (level 3).

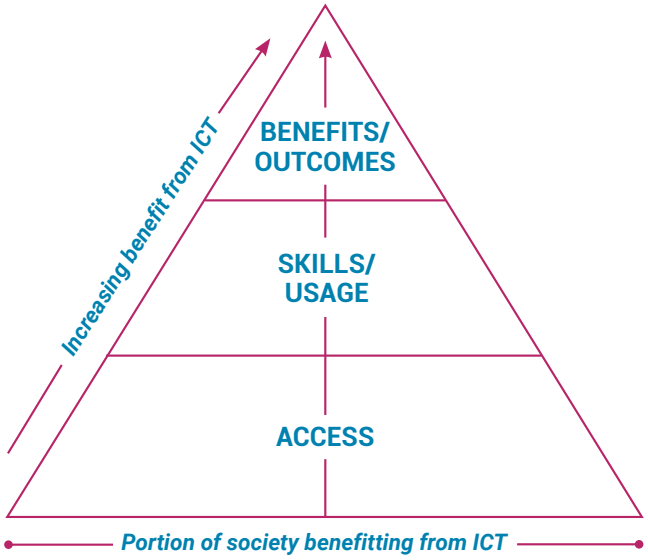


Fig. 1. Levels of digital inequality (Cinnamon, 2019)

25 Open Source Patents: Everything You Need to Know. Updated November 3, 2020 & February 01, 2023. https://clck.ru/3EYqHn

26 See in more detail: Barabanov, O. N. (March 14, 2023). Neocolonialism practices and global digital equality. https://clck.ru/3EYqLk

27 Konishi, T. (June 19, 2023). India's G20 Presidency: An Opportunity to Steer the World Toward Inclusive and Sustainable Growth. https://clck.ru/3EYqMe

As for the possible mechanisms to solve the problem of digital equality and the parameters for the development of international cooperation in the field under consideration, the lack of funding and imbalance in wealth between developed and developing countries can be overcome similarly to climate policy. The latter assumes and promotes that developed countries can take on commitment to financial support for the green transition of developing countries (Gritsenko, 2023; Liu et al., 2024). Similarly, it is proposed to adhere to the principle that developed countries should help poor countries with digital transformation and access to digital services[28]. In this regard, it seems that the willingness of developed countries to fund developing countries for a green transition is explained by the fact that one of its elements, inter alia (renewable energy sources, environmentally friendly transport, green financing, and ESG standards) is the economy "decarbonization" (Polyakov et al., 2022). For example, the foundry industry requires sufficient supplies of environmentally friendly hydrogen and energy from renewable sources at competitive prices, and their production even in Europe still needs to be established; at the same time, large-scale electrolysis for the production of "green" hydrogen requires significant volume of electricity produced without fossil fuels, and this, in turn, requires increasing investments[29]. Thus, the example of developing countries shows that the green transition will require enormous investments and the destruction of the existing "carbonized" industry. This will apparently weaken these countries as competitors in the world market and is beneficial to those who want such a weakening. However, the idea of alternative energy sources in itself certainly deserves attention, approval at the conceptual level and development, and the idea of putting ICT at the service of decarbonization is being discussed (Wang et al., 2024). Whereas equality in the digital sphere, on the contrary, will serve to increase the competitiveness of these countries on the global stage. Whether this is desirable depends on the goal pursued by digitalization in general and its individual manifestations in particular, for example, mining[30]. The "cultivation", development and functioning of "strong artificial intelligence" will require more and more new data[31], which, in turn, objectively requires universal digitalization – provided that the emergence of artificial intelligence is an objective phenomenon, like the laws of nature (for example, water boils at 100 degrees, etc.), which naturally occurs with a certain course of events (like the invention of gunpowder, wheels, etc.), and not a subjective one (the pursuit of competitive advantages of companies, countries, etc.).

---

28 Barabanov, O. N. (March 14, 2023). Neocolonialism practices and global digital equality. https://clck.ru/3EYqPP

29 Ermolenko, G. (January 4, 2024). Decarbonization of metallurgy requires reducing the cost of "green" hydrogen – analysts. https://clck.ru/3EYqQj

30 Kolobova, M. (June 4, 2024). What are your codes: mining in the Russian Federation will soon become an economic activity. How will this change the cryptocurrency mining market and help the budget. https://clck.ru/3EYqSH. Compare, e.g., Arthur C. Clarke (1953). The Nine Billion Names of God. https://clck.ru/3EYqTP

31 A former OpenAI employee has published predictions about the future of AI (June 5, 2024). RBK Trends. https://clck.ru/3EYqVG

This idea did not appear yesterday. Before the 2nd World Summit on the Information Society in Tunis in 2005, UNO Secretary-General K. Annan called on the leading producers of modern knowledge-intensive and information-communication technologies to expand their activities, focusing on helping developing countries to develop innovations. He noted that the effectiveness and sustainability of the new economic model – the knowledge-based economy – can be achieved only through the universal dissemination of the principles of this model, meeting the needs of humanity in communication and information, as well as the interest of countries in achieving the Millennium Development Goals and respect for human rights. This call also served as the basis for the Tunisian Information Society Program, adopted on November 15, 2005. At the previous meeting in Geneva in 2003, the Declaration on shaping the information society as a global challenge in the new millennium was adopted on December 12, 2003, as well as the Action Plan for ensuring the development of the information society in a global perspective (Perfilieva, 2007).

In the same period, the author of the abovementioned strategy of open innovations H. Chesbrough published his works "Open Innovation: The New Imperative for Creating and Profiting from Technology" (Harvard Business School Press, Boston, MA, 2003) and "Open business models. How to thrive in the new innovation landscape" (Harvard Business School Press, Boston, MA, 2006).

1.4. Delocalization of the digital space as a mechanism of international cooperation: examples of approaches

There is also an opinion that the digital space should be separated from the domain of states' sovereignty. Instead, separate jurisdictions of international bodies should be created, based either on the existing supranational international institutions (such as the UN General Assembly and the UN Security Council), or on new ones working through coordinated efforts of various countries and organizations (like the International Council for Digital Equality, hereinafter – ICDE) and new legal frameworks and universal principles by which it would work. The basis for such a vision has long been established. The idea of the Internet as a sovereign digital territory and a separate jurisdiction has been put forward by many scholars. For example, in 1996, D. R. Johnson and D. G. Post considered the problems of jurisdiction in cyberspace and argued that traditional territorial principles of law are inapplicable to the Internet, proposing the concept of cyberspace as an independent legal space (Johnson & Post, 1996). In 1997, J. R. Reidenberg considered how technological solutions can shape legal norms in cyberspace and developed the concept of lex informatica, suggesting the idea of the Internet as an independent jurisdiction and arguing that it could be useful to centralize the legislative vector later (Reidenberg, 1997).

The ideas of delocalization now take various forms. For example, the idea of delocalized arbitration[32] is rooted in the concept of international commercial arbitration (ICA) autonomy from national legal systems. It says that ICA functions independently from national legal systems and forms its own autonomous legal environment, mainly at the procedural level, when it considers and resolves disputes, as issues of procedural and substantive nature should be resolved based on the rules chosen by the parties or agreed by them. At the same time, the seat of the arbitral tribunal should not influence its work, for example in determining its competence. This is because parties generally want to see neutral arbitrators and a convenient (also territorially in terms of accessibility) forum, so the resolution of these issues is largely not directly related to the essence of the dispute. Most ICA decisions are executed voluntarily, and a refusal to execute or vacation of a decision in one country does not mean that it cannot be enforced in another country (as the case below will show); hence, even the issue of mandatory enforcement of ICA decisions does not necessarily bind the arbitration to the national legal system.

The initiative to create a fundamentally new investment arbitration institute on the BRICS platform was taken by St. Petersburg University. The Dean of its Law Faculty said, "Most important is that we propose to create a permanent institution that will take into account not only the peculiarities of legal systems, but also the legal political culture of states, first of all, our BRICS partners, of course. The new institution will allow taking into account public interests in investment disputes, not always putting only the economic interests of investors first, but looking for a balanced approach that will ensure the interests of both sides in investment relations. In our opinion, this can be a serious incentive for investment development"[33].

An example of current arbitrations of this type is on-line arbitration (arbitration using electronic telecommunications networks), for example, the Internet courts of three Chinese cities – Beijing, Guangzhou, and Hangzhou.

Delocalization was implemented in the case of PT Putrabali Adyamulia v. Rena Holding[34]. According to the arbitration decision of April 10, 2001, the refusal of the French Rena Holding to pay for goods purchased from the Indonesian company Putrabali was recognized as legitimate. The latter appealed it to the High Court of London, which sent the case for reconsideration to the arbitration panel. On August 21, 2003 it issued a new decision obliging Rena Holding to pay $163,086 to Putrabali. In parallel, in September 2003 Rena Holding achieved recognition and enforcement of the 2001 arbitration decision in France. In turn, Putrabali achieved recognition and enforcement of the 2003 arbitration decision in France. On June 27, 2007, the French Court of Cassation stated that the 2001

---

32 See, e.g.: Scientists from St. Petersburg State University proposed making St. Petersburg the capital of international investment arbitration [for the BRICS states – author]. (May 8, 2024. https://clck.ru/3EYqWj

33 Ibid.

34 Enforcement of arbitration awards in France. (July 29, 2008). Reed Smith LLP. https://clck.ru/3EYqYB

arbitration decision recognized in France could not be changed by the 2003 decision, since it met the requirements of the French legal order, although it was subsequently changed by the court at the place of arbitration. The 2003 decision was overturned on the grounds that it was recognized in France later than the 2001 decision.

As can be seen from these examples, the understanding of arbitration delocalization differs both conceptually (as the transfer of dispute settlement from one country to another) and institutionally (as the operation of arbitration online). Hence, it is necessary to develop a clearer understanding of this concept in order to implement it as a way to overcome not only distrust of arbitrations (including investment ones), but also other problems related to the work of arbitrations.

Returning to the idea of delocalizing the legal regulation of the Internet, the key legal principle underlying the ICDE functioning could be to recognize the Internet as a global public good, in fact establishing the right to it as a (quasi?)human right accessible to all people, regardless of their race, social status or physical abilities (the idea of establishing digital inclusion as one of the basic human rights is now provided for by the Draft Constitutional Amendment of Article 5 of the Constitution[35]).

The International Council for Digital Equality could:

– establish a legal framework for the management of the Internet by developing and adopting international treaties (conventions) and other acts binding on all participants in the digital space, such as regulations, directives and decisions, which, in turn, would establish standards and norms for various aspects of Internet use and management. Thus, the proclaimed principle of equal access to the Internet would be enshrined in international acts ratified by the participating countries, becoming part of their national legal systems. The ICDE Internet jurisdiction could operate through a set of international treaties and national legislative acts, ensuring their unification and integration into national legal order. Special attention could be paid to the protection of user rights, including personal data protection and cybersecurity. In this area, the ICDE could develop international standards and protocols that all participants in the digital space would be required to comply with. These standards could include measures to prevent cybercrime, protect privacy and ensure the security of digital communications;

– establish legal mechanisms for monitoring and ensuring compliance with the regulations it would adopt. Such a system could include specialized oversight and control bodies entitled to conduct investigations, assess compliance with established standards and take measures to eliminate violations. In case of non-compliance with the requirements of international legislation, the ICDE would be entitled to apply sanctions, including fines and restrictions on access to Internet resources;

– initiate and support international programs and projects aimed at developing digital infrastructure and improving digital skills of the population. These programs

[35] Proposta de Emenda à Constituição n° 47, de 2021. https://clck.ru/3EYqZ4

could be funded through international funds and implemented in cooperation with national governments and the private sector and would be aimed at creating a fair, inclusive and secure digital environment. They could be secured through international treaties and cooperation agreements that would define the parties' obligations and the conditions for their implementation;

– within its jurisdiction, actively cooperate with other international organizations such as the United Nations, the World Bank and the World Health Organization to coordinate efforts and ensure an integrated approach to solving global problems of digital (in) equality. Such interaction would be based on international legal agreements and mechanisms (instruments) that would define mutual obligations and ways to coordinate actions.

Thus, the Internet, as an international jurisdiction under the management of the ICDE, would become a complex legal structure based on international treaties and national legislative acts aimed at ensuring equal access, user rights protection and sustainable development of the digital space.

This seems to be an ideal option for the future at the moment. Today, under the fragmentation of international law and economics (which will be discussed below), we surely can talk about a fragmented Internet of the future, for example, a unified Internet of several BRICS countries, or Russia – Iran – North Korea, etc.

Whereas today, due to the lack of comprehensive international legal sources, one may ask: is it at all possible to achieve digital equality with current legal regulation? After all, the above approaches and their embodiments are not enough to solve the issue of digital inequality, but they are a necessary step towards such solution.

2. Cooperation in overcoming digital inequality at the regional level

2.1. Fragmentation of international law and network partnership

At the same time, there exists the long-standing fragmentation of international law, which is facilitated by such factors as regionalization, specialization of international law, unification ideas that began to develop from a certain point in the past at the level of states (United States of Europe / EU, MERCOSUR, NAFTA), economies (APEC, ASEAN) and strategies (BRICS, etc.). They have contributed and are contributing, on the one hand, to regionalization and thus fragmentation (e.g., Montevideo Treaties of 1960 and 1980). On the other hand, they promote globalization and unification, working on (de) fragmentation by creating legal ways to overcome national borders when forming the global economy. By the example of existing associations and some of their member states and modern realities, they reveal special legal prohibitions that have survived to date, limits of the permissible, and restrictions. The fragmentation of international law results in the states transferring their efforts to ensure various issues on the international agenda to the level of regional and other integration associations. For example, clause 33 of the

Johannesburg II Declaration. BRICS and Africa: Partnership for Mutually Accelerated Growth, Sustainable Development and Inclusive Multilateralism[36] states the importance of the digital economy for global economic development from the perspective of the positive impact of trade and investment on promoting sustainable development, national and regional industrialization, and transition to sustainable models of consumption and production. It accentuates the challenges facing the BRICS countries in the digital age, including inequality in digital development and the need to overcome the problems associated with it. The participants supported the establishment of the BRICS Working Group on the Digital Economy and emphasize the role of openness, efficiency, stability and reliability in stimulating international trade and investments. They also welcome further partnership between BRICS countries to strengthen interconnections in supply chains and payment systems in order to promote trade and investment flows (Sandton, Gauteng, South Africa, August 23, 2023). Clause 74 states the desire to "strengthen skills exchange and cooperation among BRICS countries, to support the digital transformation in education and TVET space, as each BRICS country is domestically committed to ensure education accessibility and equity, and promote the development of quality education… share digital educational resources, build smart education systems, and jointly promote digital transformation of education in BRICS countries and to develop a sustainable education by strengthening the cooperation within BRICS Network University and other institution-to-institution initiatives in this area, including the BRICS University League… to expand membership of the BRICS Network University to include more universities from the BRICS countries… [to] share best practices on expanding access to holistic early childhood care and education to provide a better start in life for children within BRICS countries... to facilitate exchanges within BRICS countries on equipping learners with skills fit for the future through multiple learning pathways"[37]. Thus, we can see that at the BRICS level there is also an approach to recognizing (designating) and removing the second of the above-mentioned parameters (barriers) in overcoming digital inequality – user skills.

2.2. Digital skills of users: a barrier and a development parameter

Speaking of this second parameter (barrier), we should note that the issue of user skills will be resolved faster and more significantly among the younger population, who could provide assistance to other segments of the population (Ren & Zhu, 2024). In any case, of the three parameters (barriers), it seems that the issue of skills is not the most significant, as we

[36] Ministry of Foreign Affairs of the Russian Federation. (August 24, 2023). Johannesburg II Declaration. BRICS and Africa: Partnership for Mutually Accelerated Growth, Sustainable Development and Inclusive Multilateralism. https://clck.ru/3EYqaG

[37] Ibid.

see that technologies enter the lives of all people and they get used to them. On the other hand, it is worth bearing in mind the aspect already mentioned above in relation to the economy "decarbonization". It is similar to the one described in the 1963 fiction story "Turning Point" by Pol Anderson[38], in which one of the possible options for contact between Earthlings and aliens was discussed – the "domino effect"[39] in the technological development of the latter. The story, in particular, describes the characters' reflections on the alien civilization's technological development:

"Yes," Baldinger ruminated, "I always realized that our betters must exist. Didn't expect we'd run into them in my own lifetime, however. Not in this microscopic sliver of the galaxy that we've explored. And... well, I always imagined the Elders having machines, science, space travel."

"They will," I said.

"If we go away—" Lejeune began.

"Too late," I said. "We've already given them this shiny new toy, science. If we abandon them, they'll come looking for us in a couple of hundred years. At most."[40]

However, we are not arguing that the issue of digital skills is unimportant. Its importance is underlined by various regional initiatives at the European Union level, such as the Digital Skills and Jobs Coalition, which combats the digital skills deficit by bringing together member states, companies and organizations[41]; the European Skills Agenda, a five-year plan to help individuals and businesses develop more skills and put them into practice[42]. The Digital Opportunities Internship Program, an EU-funded training initiative, is aimed at helping manufacturing, banking, agriculture and healthcare companies to fill vacancies with candidates skilled in digital technologies for cybersecurity, data analytics, machine learning, as a computer-literate workforce is vital to maintain Europe's global competitiveness in a rapidly changing world[43]. With all this, we believe that the issue of mastering certain skills is simpler and easier to address than the third level parameter (barrier) – the multifaceted nature of the digital divide, that is, how people use technology and what benefits (or problems) they derive from it.

38 P. Anderson (1963). Turning Point. Libking. https://clck.ru/3EYqbD

39 The domino effect is a political theory that any change entails a linear series of other changes, similar to how dominoes fall in a row.

40 P. Anderson (1963). Turning Point. https://textarchive.ru/c-2199079-p25.html

41 European Commission. The Digital Skills and Jobs Coalition. https://clck.ru/3EYqgZ

42 European Commission. The European Skills Agenda. https://clck.ru/3EYqfE

43 Digital Opportunity Traineeships. ErasmusIntern.org. https://clck.ru/3EYqhL

2.3. Obstacles to the full implementation of the digital technologies' potential: the example of Brazil and the experience of the USSR

We know that the Internet opens up many opportunities, but it can also be disruptive to people's lives. There are casinos and other games on the Internet today that are not worth spending money on, but they can take up so much of a person's time that digital technology may become harmful. So, the third level, in our opinion, is the most difficult point.

The fact is that how consumers will use technology is mainly determined by various sociological factors. For example, in the comprehensive work "A Ralé Brasileira – Quem é e como vive" by a Brazilian researcher Jesse de Souza, it is shown that the transition from the lower to the middle class is an illusion, as this "transition" is only based on the money factor: a lot of people in Brazil started earning as middle class or higher in monetary terms, but people who come from poor (lower than middle) classes, who had never fit into the middle class, continue to not fit into it because their mentality and even that of their children is different.

While a traditional middle class representative thinks: "I will work and everything will be fine", a representative of the "new" middle class lived and continues to livewith the mentality of a poor person, despite the money. Hence, there is no mixing of representatives of the "new" middle class with those who traditionally were and continue to be its representatives. The same applies to their children – they are not confident in themselves, they are not prepared as leaders, they continue to think in the categories of the lower than middle class. In other words, even if people get money, mentally they do not become representatives of the middle class (Souza, 2018).

This approach is also evident in Brazil in the digital environment. Although there are no definitive studies on the topic, some data show that Internet access has increased among the poorest Brazilians, but its impact on people's lives remains uneven across classes. It suggests[44] that Internet use by people below the middle class will not give them a chance to develop. The initiatives at the international community level contain no measures to address this significant problem.

Assumingly, one may outline the contours of this problem in all societies where the gap between rich and poor is historically large. In our opinion, this is related to the initial level of upbringing and subsequent education received by people.

Obviously, well-grounded are the words "Give a man a fish, you feed him once. Teach him to catch fish, and he will be fed all his life", attributed either to Laozi, or to Confucius, or considered as mentioned in the ancient Chinese philosophical treatise 'Huainanzi' created during the early Han times[45].

---

[44] O portal Brasil61.com conversou com o ex-coordenador do Comitê Gestor da Internet no Brasil, Márcio Migon. Reportagem: Felipe Moura. 21 de Fevereiro de 2022, 22:35h, Atualizado em: 23 de Fevereiro de 2022, 22:46h. https://clck.ru/3EYqj5

[45] "Give a man a fish, you feed him once..." (June 10, 2020). https://clck.ru/3EYqkP; Today, let us consider a proverb that goes deep into Chinese history (January 10, 2023). VKontakte. https://clck.ru/3EYqn5, etc.

This problem was solved in the Soviet Union during the campaign to eliminate illiteracy – mass literacy training of adults and adolescents from 1919 to the early 1940s. That was the most large-scale social and educational project not only in the history of Russia, but also in Europe. It required hard work to create an extensive network of secondary schools, workers' faculties, technical schools and universities (Trubilin & Zolotukhina, 2022). Well-known is the poster "Knowledge will break the chains of slavery" by A. Radakov (1920, Petrograd)[46].

Also, when a person has a dream, it becomes a driving force for development. Take, for example, the so-called American dream, partly reflected in the movie "The Pursuit of Happyness" (2006, USA)[47], or the famous J. London's "Martin Eden". In the Indian epic "Mahabharata"[48], the irresistible urge of Karna, the son of Princess Kunti and the Sun God Surya, who was brought up in the family of a charioteer, made him an archer and a great warrior.

At the same time, the above ideas and their embodiments developed in the depths of the knowledge economy (Rodríguez et al., 2021). That is an economic system in which the production of goods and services is based mainly on knowledge-intensive activities that foster technical and scientific innovation, and in which a key element of value depends on human capital and intellectual property as a source of innovative ideas, information and practices. There is now a shift from a knowledge economy to a data economy[49], an inherently networked and customizable digital ecosystem. In it, data are collected by various actors, including the state, search engines, social networks, online and conventional stores, payment systems, software as a service (SaaS) providers and other companies using connected devices in the Internet of Things (IoT) (Ershova et al., 2024). The data are systematized and exchanged through a network of individuals (companies) and institutions to create digital value. Storage and protection of collected data, including personal data, is a significant part and a priority of such an economy.

2.4. Data inequality: the new challenge of the data economy and the use of personal data

Under these conditions, new problems of inequality are emerging, which traditionally are not covered by the concept of digital inequality. One of them is data inequality (Cinnamon, 2019). Personal data is often referred to as the new oil, since the modern economy is largely dependent on data, especially big data. On the one hand, all users with

46 Museum of Moscow. Exhibits. https://clck.ru/3EYqny

47 The Pursuit of Happyness, 2006, USA. https://clck.ru/3EYqpE

48 "Mahabharata" serial, 2013, India. https://clck.ru/3EYqqA

49 European Commission. (May 9, 2021). Results of the European Data Market study 2021–2023. https://clck.ru/3EYqru

Internet access produce such data; on the other hand, very few of them have the ability to process and capitalize on them.

For example, within the experimental legal regime established by the Federal Law of April 24, 2020 No. 123-FZ "On conducting an experiment to establish special regulation to create the necessary conditions for the development and implementation of artificial intelligence technologies in the subject of the Russian Federation – the city of federal significance Moscow and on amendments to Articles 6 and 10 of the Federal Law 'On personal data'"[50], anonymized personal data can be processed without the consent of the personal data subject – the citizen identified. This is claimed to be done in order to improve the efficiency of state or municipal administration, but it is unclear what is meant by improving such efficiency.

Analysts believe[51] that such data will be processed by the experiment participants based on an agreement with the authorized body (determined by the Moscow City Government). The said agreement will contain requirements for procedures for depersonalization of personal data received by the experiment participant and/or state and local authorities in compliance with the provisions of Roskomnadzor Order No. 996 of September 5, 2013 "On Approval of Requirements and Methods for Personal Data Depersonalization"[52] (Order No. 996). These processing techniques will also apply to data on health status (information on the presence or absence of disability, medical diagnosis, etc.). Previously the Federal Law of July 27, 2006 No. 152-FZ "On Personal Data"[53] did not contain provisions that the relevant information can be processed in an anonymized form without the consent of the personal data subject.

Questions are raised[54] that, with rare exceptions, data cannot be anonymized completely and the risk of back identification remains. For example, this is explicitly mentioned in paragraph 5 of Order No. 996, according to which anonymized data must have the characteristic of reversibility (prohibited in Brazil, for example). The latter is the possibility of transformation, reverse anonymization (de-anonymization). It allows bringing anonymized data to the original form, revealing the belonging of personal data to a particular subject, thus eliminating anonymity. The anonymization requirement may

---

50 On personal data. No. 152-FZ of July 27, 2006 (July 31, 2006). Collection of the legislation of the Russian Federation. No. 31 (Part I), Art. 3451.

51 Zaytsev, A., Mingazova, L. (June 10, 2020). #DigitalLaw. Review of the Federal Law on conducting an experiment in Moscow to create the necessary conditions for the development and implementation of artificial intelligence technologies. Part 1. Business Solutions and Technologies. Zakon.ru. https://clck.ru/3EYquM

52 Order on Approving the Requirements and Methods for Personal Data Depersonalization. (September 17, 2013). Rossiyskaya gazeta, 208.

53 On personal data. No. 152-FZ of 27.07.2006. (July 31, 2006). Collection of the legislation of the Russian Federation. No. 31 (Part I), Art. 3451.

54 Experiment over Moscow: The law on the introduction of artificial intelligence has come into force. (July 1, 2020). NK – Lawyers' stories! https://clck.ru/3EYqvR; (Cinnamon, 2019).

be new to many companies, so it is questionable how it will be implemented. If data is so valuable, why only large or select companies may have access and the ability to interpret it, leading to a sort of "digital proletariat" status for most users?

In Brazil, the situation is somewhat different, but the problems are the same. For example, the rules on informing personal data subjects about the purposes of processing their data are enshrined in the 2018 Act on Personal Data Protection[55], but they are ineffective. According to clause I of Article 6, an operator must process personal data in accordance with lawful, legitimate and predetermined purposes communicated to the personal data subject. According to clause VI of Article 6, the operator must guarantee to the data subject the quality of data in terms of guaranteeing their accuracy, clarity, relevance and topicality in accordance with the necessity that led to their collection and the purpose of their processing. Article 7 establishes the cases in which the processing of personal data is allowed, including the fulfillment of legal obligations or regulatory functions of the supervisory authority (e.g. clause II). According to Article 18, the personal data subject has the right to obtain from the supervisory authority, at any time and upon request, the following information in relation to the processed personal data: I – confirmation of the existence of processing; II – access to data; III – correction of incomplete, inaccurate or outdated data; IV – anonymization, blocking or deletion of unnecessary, excessive data or data processed not in accordance with the provisions of the 2018 Act; V – transfer of data to another service or product provider upon explicit request and in compliance with commercial and industrial secrecy in accordance with the rules applicable to the supervisory authority; VI – deletion of personal data processed with the consent of the controller, except in the case stipulated by Article 16 of the 2018 Act; VII – information on public and private persons with whom the supervisory authority has shared data; VIII – information on the possibility of not giving consent to data processing and the consequences of refusal; IX – withdrawal of consent pursuant to Article 8 § 5 of the 2018 Act.

However, these formulations often do not describe or convey to the data subject the correct representation of the path of their personal data on the data market. Whereas today, if a user does not want to provide their data, they often cannot use services. In addition, data production is uneven worldwide and one of the reasons is that there are about 1.1 billion people in the world without an official identity document; often basic data such as births, deaths, etc. are not captured, creating a mass of information-poor people (Cinnamon, 2019).

How, in such cases, do we even create a metric for development? If development is the goal of international endeavors, how can we measure the results of measures aimed at achieving this goal?

---

[55] Lei Geral de Proteção de Dados Pessoais (LGPD) Nº 13.709, de 14 de Agosto de 2018 (Redação dada pela Lei nº 13.853, de 2019 para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências). https://goo.su/tUZhUwC

It seems that international efforts should focus on 1) creating enforceable rules to ensure that data companies properly inform users of their purposes so that the user knows exactly what will be done with their data, and 2) creating enforceable rules for more flexibility in choosing the purposes of processing personal data (and data in general) and its use on the side of data subjects and other persons.

Conclusions

The above allow concluding as follows.

1. The future of the digital society depends on the joint efforts of the global community to create fair and equitable conditions of access to information resources and technologies. Therefore, access to the Internet and digital technologies should become a basic human right in order to ensure equal opportunities for all segments of society, since the initial crystallization of distinct digital differences is based on existing offline social differences.

2. Developing digital skills and literacy among the population is a crucial task to successfully overcome digital inequalities, along with encouraging the rational use of technologies to achieve all the potential benefits they offer and to ensure that people understand how big data works and how to use their personal data.

3. There is a need to broaden and deepen cooperation between developed and developing countries so that the latter can produce more data to serve as a metric for development and a basis for creating development strategies. At the same time, more transparency should be ensured by providing effective and accessible means so that a data owner can clearly understand who and for what purpose processes their personal data.

4. The transition from a knowledge economy to a data economy requires adapting international cooperation strategies to ensure equitable access to data and to their processing. As a consequence, information from big data processing should be more accessible to researchers and the general public, which will accelerate scientific discoveries and support inclusive economic development, including through policies of transnational access to research infrastructure or joint exploitation of research infrastructure facilities, e.g. in BRICS countries.

5. To achieve all this, all countries should be concerned with the development of the educational system in terms of improving the way in which people acquire thinking skills and develop their worldviews, taking into account the possibilities of utilizing the social and cultural resources of BRICS countries, such as linguistic diversity and educational traditions, to create quality and equitable education, considering open education as a model for the education of the future.

References

Cinnamon, J. (2019). Data inequalities and why they matter for development. *Information Technology for Development*, *26*(2), 214–233. https://doi.org/10.1080/02681102.2019.1650244

Du, Z., & Wang, Q. (2024). Digital infrastructure and innovation: Digital divide or digital dividend? *Journal of Innovation & Knowledge*, *9*(3), 100542. https://doi.org/10.1016/j.jik.2024.100542

Ershova, I. V., Laptev, V. A., Andreeva, L. V., Akhrem, T. P., Besedin, A. N., Belikova, K. M., Gabov, A. V., Galkin, S. S., Drueva, A. A., Elnikova, | E. V., Enkova, E. E., Kantor, N. E., Korotkova, O. V., Lebedev, A. V., Mikryukov, V. A., Petrakov, A. Yu., Sajdasheva, M. V., Svit, Yu. P. … Shherbakova, M. A. (2024). *Law and the real sector of the Russian economy*. Moscow: Prospekt. (In Russ.). https://doi.org/10.31085/9785392407354-2024-480

Gallardo, R., & Whitacre, B. (2024). An unexpected digital divide? A look at internet speeds and socioeconomic groups. *Telecommunications Policy*, *48*(6), 102777. https://doi.org/10.1016/j.telpol.2024.102777

Gladkova, A. A., Garifullin, V. Z., Ragnedda, M. (2019). Model of Three Levels of the Digital Divide: Current Advantages and Limitations (Exemplified by the Republic of Tatarstan). *Moscow University Journalism Bulletin*, *4*, 41–72. (In Russ.). https://doi.org/10.30547/vestnik.journ.4.2019.4172

Gritsenko, D. (2023). Advancing UN digital cooperation: Lessons from environmental policy and governance. *World Development*, *173*, 106392. https://doi.org/10.1016/j.worlddev.2023.106392

Johnson, D. R., & Post, D. G. (1996). Law and Borders: The Rise of Law in Cyberspace. *Stanford Law Review*, *48*(5), 1367–1402. https://doi.org/10.2307/1229390

Kuo-Hsun, J., Ma. (2022). *Digital learning divide. In International Encyclopedia of Education* (Fourth Ed., pp. 157–164). https://doi.org/10.1016/b978-0-12-818630-5.01013-7

Li, P., Li, Q., Li, X. (2024). The influence of three digital divide levels on financial advisor demand and engagement among Chinese residents: An investigation based on China. *Journal of Innovation & Knowledge*, *9*(2), 100488 https://doi.org/10.1016/j.jik.2024.100488

Liu, N., Qian, Y., Gu, X., & Li, G. (2024). Digital technology, e-commerce, and economic inequality: The case of China. *International Review of Economics & Finance*, *91*, 259–271. https://doi.org/10.1016/j.iref.2024.01.016

Perfilieva, O. V. (2007). Getting over Digital Divide: the international organizations contribution. *International Organisations Research Journal*, *2*(2), 34–49. (In Russ.).

Polyakov, L. V., Ankudinov, I. A., Egorov, V. Yu., Lyatsos, A. D., Ryzhkin, E. N. (2022). Green Russia of the future: economic problems and political prospects. *Biznes. Obshhestvo. Vlast*, 46, 87–116. (In Russ.).

Pool, H., Schuyler, T., Senf, T. M., & Moschovitis, Ch. J. P. (1999). *History of the Internet. A Chronology, 1843 to Present*. London: ABC-CLIO.

Rabbani, M. (2024). Internet price, speed, and disparity: The case of rural healthcare providers in the United States. *Telecommunications Policy*, *48*(2), 102674. https://doi.org/10.1016/j.telpol.2023.102674

Reidenberg, J. R. (1997). Lex Informatica: The Formulation of Information Policy Rules through Technology. *Texas Law Review*, *76*, 553.

Ren, W., & Zhu, X. (2024). The age-based digital divides in China: Trends and socioeconomic differentials (2010–2020). *Telecommunications Policy*, *48*(3), 102716. https://doi.org/10.1016/j.telpol.2024.102716

Rodríguez, A., Abraham, A., Voxi, O., Amavilah H. (2021). Using deep learning neural networks to predict the knowledge economy index for developing and emerging economies. *Expert Systems with Applications*, *184*, 115514 https://doi.org/10.1016/j.eswa.2021.115514

Souza, J. (2018). *Ralé brasileira: quem é e como vive*. Belo Horizonte: Editora UFMG. (in Portuguese).

Trubilin, A. G., Zolotukhina, A. D. (2022). The elimination of illiteracy is the largest social and educational project in the history of Russia. *International Journal of Humanities and Natural Sciences*, *12-5*(75), 16–21. (In Russ.).

Wang, Q., Hu, S., Li, R. (2024). Could information and communication technology (ICT) reduce carbon emissions? The role of trade openness and financial development. *Telecommunications Policy*, *48*(3), 102699. https://doi.org/10.1016/j.telpol.2023.102699

Wang, S., & Zhang, H. (2024). Inter-Organizational cooperation in digital green supply chains: a catalyst for Eco-Innovations and sustainable business practices. *Journal of Cleaner Production*, *472*, 143383. https://doi.org/10.1016/j.jclepro.2024.143383

Authors information

Ksenia M. Belikova – Dr. Sci. (Law), Professor, Department of Entrepreneurial and Corporate Law, Kutafin Moscow State Law University
Address: 9 Sadovo-Kudrinskaya Str., 125993 Moscow, Russia
E-mail: BelikovaKsenia@yandex.ru
ORCID ID: https://orcid.org/0000-0001-8068-1616
ScopusAuthorID:https://www.scopus.com/authid/detail.uri?authorId=57193239710
WoS Researcher ID: https://www.webofscience.com/wos/author/record/N-3126-2016
Google Scholar ID: https://scholar.google.ru/citations?user=H58vKS4AAAAJ&hl=ru
РИНЦ Author ID: https://elibrary.ru/author_items.asp?authorid=497601

Rafael Dias Martins– PhD (Law), software developer, Intersystemas, lawyer (OAB/RN 15.923)
Address: ave. Caiapos, 2885 - Pitimbu, Natal/PH, 59067-400, Brazil
E-mail: martins.rafael@mail.ru
ORCID ID: https://orcid.org/0009-0001-9397-8694

Evgeniy T. Kazanba – post-graduate student, Kutafin Moscow State Law University, Chief Legal Adviser of the Federal State Budgetary Institution «Central Territorial Administration of Property Relations» of the Ministry of Defense of the Russian Federation
Address: 9 Sadovo-Kudrinskaya Str., 125993 Moscow, Russia
E-mail: ekazanba@gmail.com
ORCID ID: https://orcid.org/0009-0006-6242-5735

Authors' contributions

The authors have contributed equally into the concept and methodology elaboration, validation, formal analysis, research, selection of sources, text writing and editing, project guidance and management.

Conflict of interest

The authors declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law
PASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – July 8, 2024
Date of approval – July 22, 2024
Date of acceptance – December 13, 2024
Date of online placement – December 20, 2024

Научная статья
УДК 34:004:341:004.4
EDN: https://elibrary.ru/ocdmla
DOI: https://doi.org/10.21202/jdtl.2024.47

Международное сотрудничество в преодолении цифрового неравенства: правовые основы, барьеры и параметры развития

Ксения Михайловна Беликова ✉

Московский государственный юридический университет имени О. Е. Кутафина (МГЮА), Москва, Россия

Диас Мартинс Рафаэл

Интерсистемас, Натал, Бразилия

Евгений Тенгизович Казанба

Московский государственный юридический университет имени О. Е. Кутафина (МГЮА), Москва, Россия

Ключевые слова

доступность технологий,
законодательство,
международное право,
международное сотрудничество,
право,
сеть Интернет,
цифровое неравенство,
цифровое пространство,
цифровой разрыв,
цифровые технологии

Аннотация

Цель: на основе системного анализа достигнутого уровня международного сотрудничества в преодолении цифрового неравенства определить параметры его дальнейшего развития с учетом современных правовых и иных барьеров и глобальных вызовов, обусловленных переходом от экономики знаний к экономике данных.

Методы: методологическая основа исследования представлена диалектикой, сравнительно-правовым и историко-правовым подходами, методом системного анализа.

Результаты: проблема цифрового неравенства рассмотрена по следующим ключевым аспектам: доступ к сети Интернет; различия в уровне цифровой грамотности; особенности использования технологий и многогранность цифрового неравенства. Отмечается, что доступ к сети Интернет и цифровым технологиям должен стать основным правом человека, чтобы обеспечить равные возможности для всех слоев общества, поскольку изначально кристаллизация отчетливо выраженных цифровых различий основывается на существующих офлайн социальных различиях. Установлено, что для успешного преодоления цифрового неравенства наряду со стимулированием рационального

✉ Контактное лицо

© Беликова К. М., Диас Мартинс Р., Казанба Е. Т., 2024

Статья находится в открытом доступе и распространяется в соответствии с лицензией Creative Commons «Attribution» («Атрибуция») 4.0 Всемирная (CC BY 4.0) (https://creativecommons.org/licenses/by/4.0/deed.ru), позволяющей неограниченно использовать, распространять и воспроизводить материал при условии, что оригинальная работа упомянута с соблюдением правил цитирования.

использования технологий и обеспечением понимания людьми работы с ними и получаемых посредством них данных развитие цифровых навыков и грамотности среди населения является важнейшей глобальной задачей в решении вопроса преодоления цифрового неравенства. Предлагается расширить и углубить сотрудничество развитых стран с менее развитыми, чтобы последние могли производить больше данных, которые будут служить метрикой и основой для создания стратегий развития; при этом следует обеспечить большую прозрачность, предоставляя эффективные и доступные средства, чтобы владелец данных мог ясно понять, кем и с какой целью обрабатывались его персональные данные. Утверждается, что переход от экономики знаний к экономике данных требует адаптации стратегий международного сотрудничества для обеспечения справедливого доступа к данным и их обработки, что позволит ускорить научные открытия и поддержать инклюзивное экономическое развитие. Проанализированы вопросы фрагментации и дефрагментации международного права.

Научная новизна: обусловлена отсутствием в настоящее время результатов научного анализа достигнутого на сегодня уровня международного сотрудничества в преодолении цифрового неравенства с позиции параметров его системного развития и основных (юридических и иных) барьеров.

Практическая значимость: результаты исследования могут найти применение при совершенствовании правовой основы и стратегий международного сотрудничества в преодолении цифрового неравенства для обеспечения справедливого доступа к данным и их обработки.

Для цитирования

Беликова, К. М., Диас Мартинс Р., Казанба, Е. Т. (2024). Международное сотрудничество в преодолении цифрового неравенства: правовые основы, барьеры и параметры развития. *Journal of Digital Technologies and Law*, *2*(4), 1003–1030. https://doi.org/10.21202/jdtl.2024.47

Список литературы

Гладкова, А. А., Гарифуллин, В. З., Рагнедда, М. (2019). Модель трех уровней цифрового неравенства: современные возможности и ограничения (на примере исследования Республики Татарстан). *Вестник Московского университета (Серия 10. Журналистика)*, *4*, 41–72. https://doi.org/10.30547/vestnik.journ.4.2019.4172

Ершова, И. В., Лаптев, В. А., Андреева, Л. В., Ахрем, Т. П., Беликова, К. М., Беседин, А. Н., Габов, А. В., Галкин, С. С., Друева, А. А., Ельникова, Е. В., Енькова, Е. Е., Кантор, Н. Е., Короткова, О. В., Лебедев, А. В., Микрюков, В. А., Микрюкова, Г. А., Петраков, А. Ю., Сайдашева, М. В., Свит, Ю. П. … Щербакова, М. А. (2024). *Право и реальный сектор экономики России*. Москва: Проспект. EDN: https://elibrary.ru/awgyzd. DOI: https://doi.org/10.31085/9785392407354-2024-480

Перфильева, О. В. (2007). Проблема цифрового разрыва и международные инициативы по ее преодолению. *Вестник международных организаций: образование, наука, новая экономика*, *2*(2), 34–49. https://elibrary.ru/jwnzzp

Поляков, Л. В., Анкудинов, И. А., Егоров, В. Ю., Ляцос, А. Д., Рыжкин, Е. Н. (2022). Зеленая Россия будущего: экономические проблемы и политические перспективы. *Бизнес. Общество. Власть*, 46, 87–116. https://www.elibrary.ru/wjuvwn

Трубилин, А. Г., Золотухина, А. Д. (2022). Ликвидация безграмотности – самый масштабный социальный и образовательный проект в истории России. *Международный журнал гуманитарных и естественных наук*, *12-5*(75), 16–21.

Cinnamon, J. (2019). Data inequalities and why they matter for development. *Information Technology for Development*, *26*(2), 214–233. https://doi.org/10.1080/02681102.2019.1650244

Du, Z., & Wang, Q. (2024). Digital infrastructure and innovation: Digital divide or digital dividend? *Journal of Innovation & Knowledge*, *9*(3), 100542. https://doi.org/10.1016/j.jik.2024.100542

Gallardo, R., & Whitacre, B. (2024). An unexpected digital divide? A look at internet speeds and socioeconomic groups. *Telecommunications Policy*, *48*(6), 102777. https://doi.org/10.1016/j.telpol.2024.102777

Gritsenko, D. (2023). Advancing UN digital cooperation: Lessons from environmental policy and governance. *World Development*, *173*, 106392. https://doi.org/10.1016/j.worlddev.2023.106392

Johnson, D. R., & Post, D. G. (1996). Law and Borders: The Rise of Law in Cyberspace. *Stanford Law Review*, *48*(5), 1367–1402. https://doi.org/10.2307/1229390

Kuo-Hsun, J., Ma. (2022). *Digital learning divide. In International Encyclopedia of Education* (Fourth Ed., pp. 157–164). https://doi.org/10.1016/b978-0-12-818630-5.01013-7

Li, P., Li, Q., Li, X. (2024). The influence of three digital divide levels on financial advisor demand and engagement among Chinese residents: An investigation based on China. *Journal of Innovation & Knowledge*, *9*(2), 100488 https://doi.org/10.1016/j.jik.2024.100488

Liu, N., Qian, Y., Gu, X., & Li, G. (2024). Digital technology, e-commerce, and economic inequality: The case of China. *International Review of Economics & Finance*, *91*, 259–271. https://doi.org/10.1016/j.iref.2024.01.016

Pool, H., Schuyler, T., Senf, T. M., & Moschovitis, Ch. J. P. (1999). *History of the Internet. A Chronology, 1843 to Present*. London: ABC-CLIO.

Rabbani, M. (2024). Internet price, speed, and disparity: The case of rural healthcare providers in the United States. *Telecommunications Policy*, *48*(2), 102674 https://doi.org/10.1016/j.telpol.2023.102674

Reidenberg, J. R. (1997). Lex Informatica: The Formulation of Information Policy Rules through Technology. *Texas Law Review*, *76*, 553.

Ren, W., & Zhu, X. (2024). The age-based digital divides in China: Trends and socioeconomic differentials (2010–2020). *Telecommunications Policy*, *48*(3), 102716. https://doi.org/10.1016/j.telpol.2024.102716

Rodríguez, A., Abraham, A., Voxi, O., Amavilah H. (2021). Using deep learning neural networks to predict the knowledge economy index for developing and emerging economies. *Expert Systems with Applications*, *184*, 115514 https://doi.org/10.1016/j.eswa.2021.115514

Souza, J. (2018). *Ralé brasileira: quem é e como vive*. Belo Horizonte: Editora UFMG.

Wang, Q., Hu, S., Li, R. (2024). Could information and communication technology (ICT) reduce carbon emissions? The role of trade openness and financial development. *Telecommunications Policy*, *48*(3), 102699. https://doi.org/10.1016/j.telpol.2023.102699

Wang, S., & Zhang, H. (2024). Inter-Organizational cooperation in digital green supply chains: a catalyst for Eco-Innovations and sustainable business practices. *Journal of Cleaner Production*, *472*, 143383. https://doi.org/10.1016/j.jclepro.2024.143383

Информация об авторах

Беликова Ксения Михайловна – доктор юридических наук, профессор, профессор кафедры предпринимательского и корпоративного права, Московского государственный юридический университет имени О.Е. Кутафина (МГЮА)
Адрес: 125993, Россия, г. Москва, ул. Садовая-Кудринская, 9
E-mail: BelikovaKsenia@yandex.ru
ORCID ID: https://orcid.org/0000-0001-8068-1616
ScopusAuthorID:https://www.scopus.com/authid/detail.uri?authorId=57193239710
WoS Researcher ID: https://www.webofscience.com/wos/author/record/N-3126-2016
Google Scholar ID: https://scholar.google.ru/citations?user=H58vKS4AAAAJ&hl=ru
РИНЦ Author ID: https://elibrary.ru/author_items.asp?authorid=497601

Диас Мартинс Рафаэл – кандидат юридических наук, разработчик программного обеспечения Интерсистемас, адвокат (OAB/RN 15.923)
Адрес: 9067-400, Бразилия, Натал/РН, 2885 – Питимбу, просп. Каиапос, 5
E-mail: martins.rafael@mail.ru
ORCID ID: https://orcid.org/0009-0001-9397-8694

Казанба Евгений Тенгизович – аспирант, Московского государственный юридический университет имени О. Е. Кутафина (МГЮА), Главный юрисконсульт ФГКУ «Центральное территориальное управление имущественных отношений» Министерства обороны России
Адрес: 125993, Россия, г. Москва, ул. Садовая-Кудринская, 9
E-mail: ekazanba@gmail.com
ORCID ID: https://orcid.org/0009-0006-6242-5735

Вклад авторов

Авторы внесли равный вклад в разработку концепции, методологии, валидацию, формальный анализ, проведение исследования, подбор источников, написание и редактирование текста, руководство и управление проектом.

Конфликт интересов

Авторы сообщают об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.87 / Международное право
Специальность ВАК: 5.1.5 / Международно-правовые науки

История статьи

Дата поступления – 8 июля 2024 г.
Дата одобрения после рецензирования – 22 июля 2024 г.
Дата принятия к опубликованию – 13 декабря 2024 г.
Дата онлайн-размещения – 20 декабря 2024 г.

Research article
UDC 34:004:346.6:004.8
EDN: https://elibrary.ru/gnqswz
DOI: https://doi.org/10.21202/jdtl.2024.48

Legal Aspects of Personal Data Protection and the Issues of Competition in Digital Marketplaces

Kolawole Afuwape
O. P. Jindal Global University, Sonipat, India

Keywords

antitrust law,
competition law,
confidentiality,
consumer rights,
data abuse,
digital markets,
digital platforms,
digital technologies,
law,
personal data protection

Abstract

Objective: to develop approaches and proposals to improve the legal mechanisms for the personal data protection in the context of the evolving digital markets and the growing digital competition.

Methods: the article is prepared based on formal legal and comparative legal research methods.

Results: the unique features of digital markets are shown, which must be taken into account to achieve the goals of antimonopoly legislation. It is marked that the fundamental elements of the digital market include the big data concept and big data analytics, which, based on digital platforms, are capable of producing many direct and indirect network effects. The latter require understanding for an effective antitrust response and the application of appropriate legislation. The author proves that the growth of digital platforms as a business model and vital infrastructure of the digital economy should be viewed as a factor in improving legal regulation of relations in the sphere of data protection and confidentiality. The paper identifies the potential of digital platforms for assessing the current market power and the impact of competition on limiting this power. The data are considered as an integral component of the overall competitive market landscape. The current European Union regulation in the field of digital platforms and personal data protection is analyzed. The author identifies difficulties associated with the creation and application of effective regulations governing the activities of digital platforms. The article proves that antimonopoly authorities need to change approaches to analytics in order to take into account

© Kolawole A., 2024

This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (CC BY 4.0) (https://creativecommons.org/licenses/by/4.0), which permits unrestricted re-use, distribution and reproduction, provided the original article is properly cited.

the distinctive features of digital platforms. It is noted that such changes may require legislative reforms and revision of procedures to match the rapid development of these markets and ensure that any potentially anti-competitive behavior is thoroughly investigated.

Scientific novelty: the research contributes to the development of approaches to determining indicators of ensuring the personal data confidentiality under the digitalization of markets and to evaluating the effectiveness of antimonopoly legislation and its application in a new competitive environment.

Practical significance: the results obtained can be used as a basis for improving antimonopoly and personal data protection legislation, as well as legal regulation of digital platforms in general.

For citation

Kolawole, A. (2024). Legal Aspects of Personal Data Protection and the Issues of Competition in Digital Marketplaces. *Journal of Digital Technologies and Law, 2*(4), 1031–1053. https://doi.org/10.21202/jdtl.2024.48

Content

Introduction
1. Data as an integral component of the overall competitive market landscape
2. Digital transformation of the economy and the emergence of a “relevant market” in the digital environment
3. Conceptual foundations of market power and dominance
4. Evolution of the European antimonopoly legislation
5. Digital technology and data management: ethical and regulatory measures
   5.1. Digital Markets Act
   5.2. Digital Services Act
   5.3. Data Governance Act
6. Regulatory challenge in the digital market sphere
Conclusion
References

Introduction

Digitalization has significantly changed the competitive environment in the global economy, creating new markets and changing existing ones (Knudsen et al., 2021). Competition authorities face a difficult task as a result of this development. It is imperative that they address new forms of wrongdoing, investigate markets in which boundaries are ill-defined, and negotiate the uncertainty inherent in quickly changing

markets[1]. Concerns about behavior in digital marketplaces and signs of growing market strength have led to a simultaneous push for the creation of new competition regulation tools as well as a more proactive implementation of the ones that now exist (Budzinski & Stöhr, 2019).

Data management business practices have received increased attention from antitrust and data protection regulatory organizations (Lancieri, 2019). Data privacy is greatly impacted by the dynamics of digital marketplaces because many business models rely on the comprehensive acquisition of personal data (Bandara et al., 2021). Individual profiles, containing sensitive details about their personal life, can be generated using this data. The effectiveness and sufficiency of the legal frameworks controlling the processing of such personal data have thus been assessed by data protection authorities (Buckley et al., 2024).

After decades of rapid growth, scholars and regulators of competition policy are beginning to view the emergence of digital platforms as critical infrastructure and a key business model within the digital economy as a threat (Nuccio & Guerzoni, 2019). The once-dominant policy consensus to keep the digital economy unrestricted by traditional laws has given way, very quickly, to a new strategy marked by more intervention (Manne, 2020).

This paper contributes both theoretically and empirically to the search for better ways to quantify market power. It addresses a number of issues related to developing all-encompassing plans to safeguard and improve competition in digital marketplaces. The assessment of market power in modern digital contexts is a major area of interest for the research of effective antimonopoly response and using antimonopoly legislation in this sphere.

1. Data as an integral component of the overall competitive market landscape

Digital platforms possess the capacity to exploit data in ways that may be considered abusive; however, data also has the potential to influence a company's market dominance (Robertson, 2020). In contemporary platform business models, data has emerged as a crucial resource, and the proficiency in leveraging data to create novel and innovative services and products serves as a significant competitive advantage (Mariani & Wamba, 2020). The primary concern regarding data in the context of dominance evaluation lies in its application and the ambiguous nature of its value, which poses challenges for price-based tools used in assessing dominance (Sznajder, 2021). The value of data is not fixed. Conversely, the true potential lies in the insights that

[1] Popiel, P. (2020). Emergent Governance: The Politics of Competition in Digital Markets: Doctoral dissertation. University of Pennsylvania.

can be derived from the data set, and it is imperative for the company to harness this potential effectively. Merely accumulating or retaining data sets will not suffice over time, as they risk becoming obsolete. Continuous data collection and accessibility are essential, accompanied by algorithms capable of harnessing the information embedded within the data (Adadi, 2021). Consequently, platforms are motivated to retain users on their services. Given that substantial data collectors seldom engage in the trading of data sets, there exists a lack of genuine supply and demand for data that could be employed in market definition analysis. The increasing dependence on data within platform business models and the creation of platform services and products has resulted in a departure from conventional pricing strategies (Kretschmer et al., 2022). Consequently, data has emerged as an essential element that must be factored into the analysis of market dominance at multiple stages. Its influence on competition and market power can manifest in multiple ways, contingent upon its application; however, it must be considered as an integral component of the overall competitive landscape within a market.

The application of data significantly influences behavior within markets, as it enhances economic characteristics such as network effects, customer lock-in, and switching costs, particularly in platform markets (Cen & Li, 2020). For instance, once a social media platform achieves a substantial user base, it becomes appealing to prospective individual users seeking to engage with existing members (direct network effects) and to commercial entities (which generate revenue) that can advertise products and services through content or targeted ads on the platform (indirect network effects). Users may encounter challenges when switching between platforms, engaging with multiple social networks (multihoming), or facing a lack of interoperability among the services within the ecosystem, which can lead to lock-in effects (Pervin et al., 2019). Consequently, the inherent features of these markets can be leveraged to retain users on the platform, facilitating ongoing data collection. These economic variables have an impact on both the companies' ability to impose competitive limitations on one another and their respective market shares.

2. Digital transformation of the economy and the emergence of a "relevant market" in the digital environment

The objective of delineating a market as stipulated in Article 102 TFEU, along with the subsequent examination of market power, is to ascertain and establish the limits of competition among firms (Andriychuk, 2023a). This entails determining if the potentially dominant entity has genuine competitors that can limit market conduct, ensuring that the entity cannot operate without facing significant competitive pressure, which could adversely affect consumers. Within the framework of EU competition law, the concept of the relevant market is utilized to assess market share thresholds and market power, thereby establishing the economic context for specific cases and guiding the theoretical understanding of competitive harm. The definition of a market relies on substitutability assessments that are instrumental in identifying a pertinent antitrust product market (Parker et al., 2020).

These assessments were developed within the context of static markets. While market definition constitutes merely one phase in the analysis of dominance, it plays a crucial role in assessing market power by delineating the breadth of the market. This delineation subsequently influences the ease or difficulty of achieving dominance within that market. The fundamental purpose of defining the market is to facilitate inferences regarding the extent of market power.

However, the evolving nature of digital markets complicates the process of delineating the relevant market significantly. Digital markets exhibit several distinct characteristics that set them apart from conventional static markets. These unique features must be considered when defining relevant product markets for the purposes of competition law. Key characteristics include the rapid evolution of digital markets, the presence of zero-price markets or market segments, the 'winner-takes-all' dynamics observed in certain digital sectors, the tendency of digital platform markets to experience tipping due to network effects, which can lead to user lock-in, and the competition for the market itself, which is a notable aspect of competition within digital environments.

The concepts of big data and big analytics serve as fundamental elements within the data-driven digital marketplace, making it essential to comprehend their intricacies (Perera & Iqbal, 2021). Further, the emergence of platforms, often referred to as multi-sided markets, has established a prevalent business model that warrants thorough understanding, particularly regarding the direct and indirect network effects that underpin such platforms (Dunne, 2021). In conjunction with platforms, digital ecosystems are evolving, which may result in consumer lock-in and diminished competition (Jenny, 2021). This phenomenon is closely associated with the growing trend of conglomerate corporate structures. The digital transformation of the economy has resulted in markets where identical or comparable products can be purchased through both offline and online channels, such as printed books from a physical store or e-books from an online platform (Ratchford et al., 2022). This situation prompts an inquiry into whether online and offline markets are merging or if they should be regarded as distinct relevant markets. In scenarios where one side of the market acquires services in return for data instead of a direct monetary transaction, conventional economic methodologies for defining markets are not readily applicable. It must be emphasized that digital platforms are prevalent within the digital landscape. These platforms function as intermediaries, facilitating interactions among multiple market participants, thus characterizing them as 'multi-sided markets.' An alternative perspective is to consider each side of the market as a distinct relevant antitrust market. However, economists argue that evaluating a platform's market sides in isolation fails to capture the comprehensive dynamics of digital platforms. This limited viewpoint overlooks critical insights essential for effective antitrust analysis. Conversely, defining a relevant market that includes the entire platform may be excessively broad for conventional antitrust evaluations, potentially incorporating markets that are not substitutable (Bietti, 2024). This approach would necessitate substantial modifications in the application of competition law concerning market definition.

3. Conceptual foundations of market power and dominance

Significant fluctuations in market capitalization serve as evidence of the substantial potential inherent in ecosystem companies. The major technology companies known as GAFAM – Apple, Alphabet (Google), Microsoft, Amazon, and Facebook[2]—have strategically leveraged platforms and ecosystems to assert their dominance in the market, as evidenced by their substantial market capitalizations (Lianos & McLean, 2021). It is noteworthy that these entities have not only supplanted the conventional leaders – such as major oil companies, industrial conglomerates, and financial institutions – but have also solidified their standings and experienced significant growth in both absolute and relative measures. Their market capitalizations, bolstered by the impacts of the coronavirus disease (COVID)-19, now exceed $1 trillion for all involved (Liang & Whalen, 2022).

The generosity of capital markets has had significant implications, particularly in eroding a crucial advantage of established firms during times of swift transformation: inertia. Historically, the cash reserves and capital possessed by incumbents have restricted the growth potential of disruptive entities. The situation has changed significantly, as stock markets have emerged as the predominant mechanism for capital allocation. This shift has been largely influenced by the low-interest-rate environment of the early 21st century, a consequence of unconventional monetary policies and the repercussions of the global financial crisis. Consequently, an abundance of capital has been in search of investment opportunities, allowing any venture with growth potential to secure funding rapidly. Consequently, investments directed towards emerging platforms and ecosystems such as the digital economy garnered significant financial resources. By being sought after by the very incumbents they aimed to displace, these new enterprises managed to reverse the traditional power dynamics within the established industrial framework.

Given that capital markets prioritize growth, these companies focus on expansion over immediate profitability, thereby disrupting the conventional dynamics of their respective sectors. The evolving landscape of production economics is characterized by distinctive features, particularly as software gains prominence. A notable aspect is the disproportionately high ratio of fixed to variable costs. The process of coding constitutes a significant portion of innovation, and once developed, the cost of replication is minimal. These dynamic fosters competitive environments where a single entity can dominate the market. The interplay between globalization and digitalization has significantly broadened the concept of the «relevant market,» thereby underscoring the importance of these phenomena. This expansion is further augmented by economies of scope and learning, as consumer data can be leveraged across various contexts rather than being confined to a single application.

[2] The social network belongs to Meta, which is recognized as an extremist organization, its functioning is prohibited in the territory of the Russian Federation.

Concept of a social market economy and the possibility of regulatory intervention

Market power serves as a crucial criterion for regulatory intervention within the framework of the European social market economy. To fully understand the significance of market power in this context, it is essential first to define the concept of a social market economy. A primary objective of the European Union is to create an internal market that operates under the principles of a highly competitive social market economy, as articulated in Article 3(3) of the Treaty on the Functioning of the European Union (TFEU) (Gerstenberg, 2020).

The concept of a social market economy can be understood as the integration of free market economic principles within a framework that prioritizes social welfare. In a free market environment, a profit-maximizing firm would typically seek to set prices at the highest feasible level (Mascarenhas et al., 2024). Nevertheless, the presence of competitive forces would limit firms from imposing prices that exceed those of their rivals, as consumers are likely to prefer purchasing from businesses that provide lower prices. Consequently, firms would either maintain their prices at a competitive threshold or strive to enhance the quality of their products and services in comparison to their competitors. In a free market economy, it is considered unnecessary for regulatory bodies to intervene in trade, as the inherent dynamics of the free market foster effective competition. This competition functions as a natural self-regulating mechanism that maintains market equilibrium (Texocotitla et al., 2017).

The critique of the free-market economy has given rise to the concept of the social market economy. Fundamentally, the social market economy acknowledges the core tenets of the free market system. Nevertheless, it is my view that it also emphasizes the necessity of regulatory intervention to maintain social equilibrium. This can be achieved, for example, by ensuring the availability of essential services or by regulating anti-competitive behaviors of firms that may operate autonomously from both competitors and consumers. In this context, regulatory intervention within a social market economy serves as a protective mechanism, ensuring that the market operates with the anticipated efficiency.

It is also essential to delineate the appropriate level of intervention by public authorities. Excessive regulatory involvement may hinder individual autonomy within society and potentially disrupt market competition. Conversely, insufficient regulatory measures could facilitate anticompetitive behaviors and lead to an inequitable distribution of essential services, as previously discussed. Consequently, identifying the appropriate level of regulatory intervention is crucial for the effective operation of the market. In this regard, public authorities establish specific measures when deliberating on the necessity of economic intervention, including the protection of services deemed to be of general economic interest, the safeguarding of intellectual property rights, and the maintenance of a competitive environment that prevents enterprises from abusing their market power.

Market power exists along a continuum that ranges from perfect competition, characterized by the absence of market power, to monopoly power, where the critical point for dominance is defined as «significant market power.» This dominance implies that the entity can operate with a considerable degree of independence from its competitors, customers, and ultimately, the consumers. Although multisided digital platforms may encounter genuine competition, the dynamics of the market can often be significantly limited by the threat of potential competition. The possession and capability to gather extensive data sets can enhance market power by creating entry barriers for competitors who lack access to or the ability to collect comparable data. Additionally, these platforms may gain advantages from associated economic elements such as network effects and switching costs.

4. Evolution of the European antimonopoly legislation

The international regulation governing digital platform markets exhibit common themes, particularly regarding issues related to content, data, and the concentration of market power (Cammaerts & Mansell, 2020). This alignment is largely influenced by the global reach of major platform companies and the ongoing collaborative discussions among regulatory bodies across different nations. Every entity engaged in economic activity is subject to competition legislation. The principal aim of this legislative framework is to maintain and promote competitive processes, which will enable the most efficient distribution of resources and protect the economic freedoms of various market participants. The enforcement methods, which vary by jurisdiction, are intended to guard against economic harm, which could show up as negative impacts on elements like pricing, quality, customer choice, or innovation, and to guarantee that companies compete on the basis of their natural advantages.

The primary objective of competition policy is to guarantee that the actions of companies—whether they are independent, collaborative, or the outcome of a merger — do not obstruct any economic dimension of consumer welfare or the overall economic welfare, as well as the competitive landscape. Consequently, competition policy serves to safeguard a «public interest» within competitive markets, addressing individual rights in an indirect manner, in contrast to data privacy policy.

Numerous nations globally have suggested or enacted legislative modifications designed to tackle challenges associated with digital competition. These modifications involve the introduction of new ex ante regulations intended to enhance ex post enforcement measures within digital markets. In conjunction with proposals aimed at refining existing competition policy frameworks, several recommendations have been put forth to create new ex ante legislative and regulatory bodies.

Reinforced by a thorough regulatory framework, the European Union has become a leader in the regulation of digital platforms. There are a number of significant reforms that will be closely examined in terms of their implementation and effects. These include

the upcoming Digital Services Act (DSA), which seeks to improve online safety and address illegal content, and the Digital Markets Act (DMA), which attempts to encourage competition within concentrated platform markets. The attempts to regulate internet platforms are multifaceted and political. The normative and ideological tenets that underpin the regulatory frameworks that oversee the platform economy are primarily embodied by them. Moreover, conflicting political interests, notably those of the major platform firms, often lead to these activities. As a result, this dynamic leads to tensions and compromises that are inherent in the regulation of digital markets. In the United States, several legislative initiatives are being introduced to enhance data privacy and foster competition. Notable among these are the American Innovation and Choice Online Act (AICOA), the Open App Markets Act, and the American Data Privacy and Protection Act (ADPPA). The United Kingdom is pursuing an independent agenda following Brexit, implementing new legislation and initiating inquiries related to online safety, consumer protection, and competition. The Competition and Markets Authority (CMA), the Information Commissioner's Office (ICO), along with various other significant regulatory bodies, are collaborating to lead this initiative.

Grasping the nuances and practical consequences of these evolving legal frameworks will increasingly be essential. The escalation of regulatory measures creates the possibility of overlapping and conflicting enforcement actions. It is expected that litigation will increase as both corporations and regulatory bodies work to adapt to these new requirements.

5. Digital technology and data management: ethical and regulatory measures

The discussion regarding the management of the digital domain is vast, encompassing many facets that remain to be understood and theorized. A key observation emerges: the governance, ethical considerations, and regulatory measures pertaining to digital environments constitute separate normative frameworks. These frameworks possess a complementary relationship and should not be confused with one another; instead, it is essential to distinctly separate them.

Digital governance encompasses the organized formulation and implementation of policies, procedures, and standards designed to facilitate the efficient development, use, and management of the information environment. This practice encompasses established conventions and effective coordination, functioning within a realm that resists straightforward classification as either moral or immoral, as well as legal or illegal. Digital governance refers to a framework of principles and suggestions that may overlap with digital regulation; however, the two concepts are not identical. This concept can be interpreted as a discussion regarding relevant legal frameworks, which are composed of a set of laws established and implemented by social or governmental bodies to regulate the behavior

of pertinent entities within the infosphere. It is essential to recognize that not every aspect of digital regulation is encompassed by digital governance, and conversely, not all elements of digital governance are related to digital regulation. A relevant example of this differentiation is the General Data Protection Regulation. The relationship of compliance serves as a fundamental mechanism through which digital regulation influences digital governance.

Digital ethics encompasses the field of ethics that examines and assesses moral dilemmas associated with data and information—covering aspects such as generation, recording, curation, processing, dissemination, sharing, and utilization. It also includes the study of algorithms, which involves artificial intelligence, artificial agents, machine learning, and robotics, as well as the relevant practices and infrastructures, such as responsible innovation, programming, hacking, and professional codes and standards. The aim is to develop and advocate for solutions that are morally sound. Digital ethics influences the frameworks of digital regulation and governance by assessing the moral standards that determine what is deemed socially acceptable or desirable. The primary challenge in contemporary society lies in the governance of digital technologies. This encompasses not only the frameworks of digital governance but also the principles of digital ethics and the mechanisms of digital regulation, thereby addressing the entire spectrum of normative considerations.

Digital regulation delineates the boundaries of permissible and impermissible actions within the digital landscape; however, it does not provide guidance on the optimal or most beneficial actions that can be taken within the legal framework to achieve societal advancement. This responsibility falls to digital ethics, which focuses on moral values and preferences, as well as to effective digital governance, which emphasizes management practices. This rationale underpins the establishment of the Ethics Advisory Group by the European Data Protection Supervisor (EDPS), the independent data protection authority of the EU, in 2015. The group's purpose is to examine the emerging ethical challenges arising from digital advancements and existing legal frameworks, particularly concerning the GDPR.

Legislative measures related to data protection offer a constrained approach to addressing the challenges associated with the misuse of user privacy and data. This constraint stems from its neglect to account for the possible long-term effects on users of digital platforms, the considerable power held by specific platforms, and the distinct obligations that come with such authority. In this regard, data protection laws may benefit from the addition of notions of exploitation and exclusion found in competition law.

A platform may intentionally diminish the intensity of positive network effects or compromise the quality of the services it provides to users on at least one side. This behavior can be interpreted as a sign of market power. In the absence of such market power, a platform tends to achieve greater success when network effects are robust, and service quality is elevated. In abusive situations, the purported wrongdoing—more especially,

the search or matching algorithm manipulation—may function as a barometer of market dominance. This idea supports the basic idea of market power that was previously covered, i.e., it suggests that certain market behaviors may indicate the existence of market power or even market dominance. It may initially seem unexpected to commence this discourse with the concept of consent rather than adequacy; however, this methodology has proven to be a seemingly appealing option for international genomics initiatives thus far. Primarily, researchers are typically required to secure participant consent for biomedical research, making it relatively effortless to extend this consent to encompass the international transfer of participants' data. Additionally, broad consent for research purposes is acknowledged within European legislation and is reinforced by the General Data Protection Regulation (GDPR) (Recital 33). Lastly, consent appears to offer a consistent framework that mitigates the inconsistencies associated with measures like adequacy decisions, which are unlikely to encompass all research projects within a consortium as it expands to include initiatives in countries lacking an adequate data protection framework.

The justifications for transfer outlined in Article 49(1), specifically those pertaining to public interest and legitimate interest, are significantly more limited compared to the justifications for lawful processing found in Article 6(1). For instance, Article 49(1)(d) explicitly states that the transfer must be necessary for important reasons of public interest. The concept of adequacy has served as a fundamental justification for the transfer of data within the framework of EU data protection since the implementation of the Data Protection Directive in 1995. While an adequacy decision is often regarded as the most favorable and reassuring foundation for such transfers, it is important to recognize three significant limitations associated with this approach. Firstly, not all nations have received approval[3]. Secondly, even in jurisdictions with an approved mechanism, the adequacy determinations applicable to countries such as Canada and the United States are limited to specific entities governed by those mechanisms. Lastly, following the pivotal Schrems ruling, which annulled a prior adequacy decision, and in light of the GDPR's requirement for regular reassessment of these decisions, stakeholders who depend on adequacy can no longer assume that an approved adequacy decision will remain valid indefinitely. In this context, Austrian student Max Schrems initiated his legal challenge against the European Commission's prior determination that the U.S./EU Safe Harbour Framework offered sufficient data protection. The European Court of Justice explicitly referenced indiscriminate surveillance as a significant rationale for its annulment of the previous adequacy decision in the case of Schrems[4].

[3] European Commission 2018. https://clck.ru/3FDEBs

[4] European Court of Justice 2015. https://clck.ru/3FDEML

An additional method for adhering to the GDPR's regulations regarding data transfers involves the integration of standard «model clauses» that have received prior approval from the EU Commission into legally binding agreements between the data sender and the recipient (GDPR Article 45(2)(c)–(d)). Following the annulment of the adequacy decision for the U.S./EU Safe Harbour framework by the European Court of Justice in the 2016 Schrems ruling, these clauses emerged as a prominent alternative mechanism for data transfer, as noted by various stakeholders (Galehr, 2023). Binding Corporate Rules (BCRs), while acknowledged as a preferred justification for data transfer under the General Data Protection Regulation (GDPR), are seldom advantageous in the context of genomics research (Phillips, 2018). These rules are primarily intended for large multinational entities or groups that require the transfer of personal data across borders while remaining within their internal organizational structures (Article 47 GDPR). To utilize BCRs, an organization must develop a set of rules that align with the stipulations of Article 47 of the GDPR, which must then receive external validation from the relevant data protection authority. This approach necessitates considerable initial investments that are often characterized by complexity, time demands, and high costs. Additionally, it may not represent the most suitable mechanism for data transfer, particularly in the framework of international genomic research projects, especially those involving partnerships or consortia with distinct, nationally based member initiatives.

The General Data Protection Regulation (GDPR) stipulates that an organization's compliance with a sector-specific code of conduct, which has received approval from the European Commission in accordance with the procedures outlined in the GDPR (Schütz, 2022), can serve as a valid basis for the transfer of personal data to that organization, provided that there are binding and enforceable commitments to implement the necessary safeguards. However, a significant limitation of this framework is the absence of any currently established code of conduct that meets these criteria.

5.1. Digital Markets Act

The main legal documents pertaining to the Digital Markets Act (DMA) consist of Regulation (EU) 2022/1925, enacted by the European Parliament and the Council on 14 September 2022, which addresses the establishment of contestable and equitable markets within the digital domain, along with the Procedural Implementing Regulation.

The Digital Markets Act (DMA) represents a pivotal advancement in the development of European Union competition law (Petit, 2021). It draws upon the extensive experience gained by the European Commission and the Court of Justice of the European Union (CJEU), while simultaneously establishing a departure from previous methodologies. This legislation signifies a novel regulatory approach to digital markets that is both precise and centered on compliance. A significant aspect of this evolution is the critical relationship and interaction between the European Commission and the Court of Justice of the European Union (CJEU). The Commission is responsible for making decisions, which

are subsequently subjected to scrutiny by the CJEU, thereby shaping the competition framework and illustrating the concept of path dependency. At times, these developments occur in a fragmented manner, disrupting established practices, while at other times, they may encompass both continuity and change. The Act should not be classified as a competition law initiative. It was enacted solely under Article 114 TFEU, with the objective of enhancing the effective operation of the internal market. This enhancement is to be achieved through regulations that promote contestability and fairness within digital markets, particularly concerning core platforms operated by gatekeepers as defined by the Act. Consequently, the Act possesses a regulatory character, aiming to influence the conduct of core platforms to foster fairness and contestability, thus serving as a complement to various other regulatory frameworks, including the Digital Services Act.

A fundamental principle of the Digital Markets Act (DMA) is the establishment of particular responsibilities for gatekeeper platforms. These responsibilities aim to promote equitable competition and establish a balanced environment within the digital marketplace. For example, gatekeepers must permit business users on their platforms to advertise their products and conduct transactions with customers beyond the limitations of the gatekeeper's platform. Additionally, the DMA forbids gatekeepers from favoring their own services and products over those offered by third parties on their platforms, thereby ensuring a more unbiased ranking system.

In order to guarantee compliance with the DMA, comprehensive enforcement strategies have been implemented. Digital companies that fail to meet the specified obligations may face significant repercussions. Financial penalties can reach as high as 10 % of a company's total global annual revenue, with the potential for this figure to double to 20 % in instances of repeated violations, thereby acting as a strong deterrent. Furthermore, authorities may impose periodic fines amounting to 5% of the average daily revenue. In situations where persistent violations are detected following market investigations, the DMA grants regulatory bodies the authority to enforce additional corrective actions. The DMA serves as a crucial regulatory instrument designed to oversee the influence wielded by major digital companies. This legislation seeks to foster a more fair, transparent, and competitive landscape within digital markets by establishing and implementing specific standards and limitations for identified gatekeepers. The DMA should be understood as a supplementary framework that does not alter existing competition laws within the European Union. Instead, it is intended to tackle the unique challenges posed by digital marketplaces.

5.2. Digital Services Act

The Digital Services Act (DSA), which came into effect on 19 October 2022, outlines a phased approach to its implementation. Extensive online platforms that fall under the direct supervision of the Commission must report their user statistics within a timeframe of three months. Following their designation, these platforms are granted a period of four

months to comply with the regulations set forth by the DSA. Starting on 17 February 2024, the DSA regulations will extend to include smaller platforms, with Member States empowered to ensure adherence to these regulations.

The DSA signifies a substantial shift in regulatory frameworks, heralding the onset of a new era in digital governance throughout the European Union. The intricacies of the DSA are underscored by its core legislative framework, specifically Regulation (EU) 2022/2065, which was adopted by the European Parliament and the Council on 19 October 2022. The DSA seeks to modernize and improve the existing E-Commerce Directive, which has been operational for two decades. It creates a comprehensive set of uniform regulations, primarily emphasizing the obligations of due diligence and the conditional exemptions from liability for online intermediary services.

The DSA strengthens user autonomy by facilitating the reporting of illegal content and allowing users to challenge the content moderation decisions implemented by platforms. It presents transparency measures that mandate online platforms to disclose information about their algorithms, service agreements, and advertising practices. Further, it establishes particular obligations for extremely large platforms, which are required to implement risk-based strategies and undergo independent assessments of their risk management systems.

The DSA is fundamentally supported by robust enforcement mechanisms. It establishes a framework that includes financial penalties, recurring fines, and corrective actions for entities that fail to comply (Eifert et al., 2021). The governance framework requires EU member states to designate a Digital Services Coordinator, who operates in conjunction with the European Board for Digital Services. Additionally, the Commission directly oversees very large platforms, possessing enforcement authority similar to that found in anti-trust regulations.

5.3. Data Governance Act

The DGA establishes a unique legal structure for Data Intermediation Services (DISs). While the Regulation specifies the definition of a “data intermediation service”, it does not provide a definition for the data intermediary that offers these services (Carovano & Finck, 2023). DISs are designed to facilitate the creation of commercial partnerships that enable data sharing among an unspecified number of data subjects and data holders, as well as data users. This is achieved through various technical, legal, or alternative methods, including the promotion of data subjects’ rights concerning their personal data.

Article 2(11) of the Data Governance Act delineates four criteria that must be met for a service to be classified as a data intermediation service: (i) the primary objective of the service must be data sharing; (ii) the sharing process should either establish

or seek to establish a commercial relationship; (iii) the data sharing must involve an unspecified number of data holders or subjects in conjunction with data users. Additionally, this provision encompasses a wide-ranging material scope by stating that (iv) intermediation may be facilitated through technical, legal, or alternative methods. The DGA pertains to actors who create or seek to create commercial partnerships for the purpose of data sharing. Data sharing is characterized as the act of a data subject or data holder supplying data to a data user for either collective or individual utilization of that data. This process is governed by voluntary agreements or applicable Union or national legislation, and may occur directly or via an intermediary, such as through open or commercial licenses that may involve a fee or be provided at no cost.

The DGA delineates its material scope by excluding services that facilitate the intermediation of copyright-protected content, as well as consolidated tape providers and account information service providers. These entities do not solely engage in data sharing; rather, they pursue supplementary objectives. Additionally, data brokers, consultancies, and providers of products that derive added value from the data are also excluded from the DGA's purview.

Article 2(11), on the other hand, covers data intermediation activities that occur "for the purpose of exercising the rights of data subjects concerning personal data". Here, personal information management services (PIMS) are specifically mentioned, as they are classified as a "distinct category" of data intermediation services.

6. Regulatory challenge in the digital market sphere

Optimists contend that the dominance displayed by some ecosystem firms could reflect their exceptional dynamic capacities. Pragmatists, on the other hand, take a more grounded viewpoint (Andriychuk, 2023b). The troubling actions of these recently powerful corporations have been brought to light by several writers, as has the regulatory authorities' inability to enact laws and other measures that might effectively curb unethical activity (Richter et al., 2021). The consumer welfare standard posits that the absence of demonstrable harm to consumers from elevated prices negates the existence of an antitrust issue, suggesting that a monopoly may simply stem from superior innovation (Newman, 2021). This perspective, however, overlooks the challenges faced by suppliers, employees, and, particularly in the context of platforms and ecosystems, complementary businesses. Regulatory bodies often lack sufficient personnel and resources to effectively address these challenges, leading to potential oversights in enforcement. However, societal expectations continue to rise. In some cases, the severity of the situation suggests that technology companies could gain from proactively and credibly limiting their own practices through self-regulation. Failing to do

so may provoke scrutiny regarding their legitimacy to operate within society, potentially resulting in more stringent external regulations.

The concentration of power among a limited number of companies is often regarded as a significant issue that may jeopardize not only economic operations but also the very foundations of democracy and governance, particularly through the erosion of conventional press and the increasing influence of social media platforms (Davola & Malgieri, 2023). The complete overhaul of the regulatory framework was essential. This was accompanied by substantial regulatory measures, such as the lawsuits initiated by the United States against Google and other major technology firms, as well as the European Union's implementation of the Digital Services Act and the Digital Markets Act (Jacobides, 2020). Despite the fact that many regulatory bodies continue to struggle with insufficient expertise, resources, and concentration to adequately respond to the worldwide call for reform, countries such as the United Kingdom and India are proactively advancing the establishment of a new Digital Competition Unit (Moreno Belloso & Petit, 2023). There is a pressing necessity for the development of novel regulatory instruments aimed at enhancing competition, both among platforms and within them. Additionally, it is essential to revise existing frameworks, theoretical constructs, and overall methodologies as we address the contemporary regulatory challenges, especially those posed by platforms and ecosystems.

Conclusion

This article examines the formulation and execution of solutions within digital markets. The emergence of digital platforms, coupled with growing apprehensions regarding their effects on both markets and society, is rapidly transforming the regulatory environment. This shift is expanding the potential for interaction between competition and regulatory frameworks. To effectively address these challenges, our theoretical perspectives on these dynamics must also adapt and progress.

Selecting an appropriate remedy is a task that is susceptible to mistakes, which may result in expensive over-enforcement or under-enforcement. Generally, authorities ought to be prepared to implement more rigorous remedies as their confidence in the detrimental effects of specific conduct grows. This also necessitates a careful approach when exploring new theories of harm. Most importantly, any intricate remedy should be regarded as a dynamic process that is periodically evaluated and modified as additional information regarding its effects on actual behavior becomes available.

The constant exploration and adaptation process requires different authorities to leverage their institutional advantages. The effective coordination of the various enforcement actions carried out by National Competition Authorities (NCAs) and National

Regulatory Authorities (NRAs) can be made more flexible by outlining the three crucial but distinct activities of (i) identifying behaviors or particular market structures that negatively impact welfare, (ii) formulating appropriate remedies, and (iii) supervising and adjusting implementation over time.

It is imperative to develop a more comprehensive academic examination of remedies, particularly in relation to their implementation within the digital domain. Remedies ought to extend beyond mere conclusions in infringement rulings and necessitate a well-defined and substantial framework. Given the intricate nature of the issues associated with remedies, there is a need for more advanced designs and adaptable institutional structures than those presently available globally.

References

Adadi, A. (2021). A survey on data-efficient algorithms in big data era. *Journal of Big Data*, *8*(1), 24. https://doi.org/10.1186/s40537-021-00419-9

Andriychuk, O. (Ed.) (2023a). *Antitrust and the Bounds of Power: 25 Years On*. Bloomsbury Publishing.

Andriychuk, O. (2023b). EU Digital Competition Law: The Socio-legal Foundations. *Cambridge Yearbook of European Legal Studies*, *25*, 81–104. https://doi.org/10.1017/cel.2023.12

Bandara, R., Fernando, M., & Akter, S. (2021). Managing consumer privacy concerns and defensive behaviours in the digital marketplace. *European Journal of Marketing*, *55*(1), 219–246. https://doi.org/10.1108/ejm-06-2019-0515

Bietti, E. (2024). Structuring Digital Platform Markets: Antitrust and Utilities' Convergence. *University of Illinois Law Review*, *2024*(4).

Buckley, G., Caulfield, T., & Becker, I. (2024). GDPR and the indefinable effectiveness of privacy regulators: Can performance assessment be improved? *Journal of Cybersecurity*, *10*(1), tyae017. https://doi.org/10.1093/cybsec/tyae017

Budzinski, O., & Stöhr, A. (2019). Competition policy reform in Europe and Germany – institutional change in the light of digitization. *European Competition Journal*, *15*(1), 15–54. https://doi.org/10.1080/17441056.2018.1555942

Cammaerts, B., & Mansell, R. (2020). Digital platform policy and regulation: Toward a radical democratic turn. *International Journal of Communication*, *14*, 135–154.

Carovano, G., & Finck, M. (2023). Regulating data intermediaries: The impact of the Data Governance Act on the EU's data economy. *Computer Law & Security Review*, *50*, 105830. https://doi.org/10.1016/j.clsr.2023.105830

Cen, Y., & Li, L. (2020). Effects of network externalities on user loyalty to online B2B platforms: an empirical study. *Journal of Enterprise Information Management*, *33*(2), 309–334. https://doi.org/10.1108/jeim-02-2019-0050

Davola, A., & Malgieri, G. (2023). Data, Power, and Competition Law: The (Im) possible Mission of the DMA? In *The Economics and Regulation of Digital Markets* (pp. 53–74). Emerald Publishing Limited. https://doi.org/10.1108/s0193-589520240000031003

Dunne, N. (2021). Platforms as regulators. *Journal of Antitrust Enforcement*, *9*(2), 244–269. https://doi.org/10.1093/jaenfo/jnaa052

Eifert, M., Metzger, A., Schweitzer, H., & Wagner, G. (2021). Taming the giants: The DMA/DSA package. *Common Market Law Review*, *58*(4). https://doi.org/10.54648/cola2021065

Galehr, S. (2023). *Transatlantic Data Transfers under the GDPR*. EIZ Publishing. https://doi.org/10.36862/eiz-ng001

Gerstenberg, O. (2020). Fundamental rights and democratic sovereignty in the EU: the role of the Charter of Fundamental Rights of the EU (CFREU) in regulating the European Social Market Economy. *Yearbook of European Law*, *39*, 199–227. https://doi.org/10.1093/yel/yeaa008

Jacobides, M. G. (2020). *Regulating Big Tech in Europe: why, so what, and how understanding their business models and ecosystems can make a difference*. https://doi.org/10.2139/ssrn.3765324

Jenny, F. (2021). *Competition law enforcement and regulation for digital platforms and ecosystems: understanding the issues, facing the challenges and moving forward*. https://doi.org/10.2139/ssrn.3857507

Knudsen, E. S., Lien, L. B., Timmermans, B., Belik, I., & Pandey, S. (2021). Stability in turbulent times? The effect of digitalization on the sustainability of competitive advantage. *Journal of Business Research, 128*, 360–369. https://doi.org/10.1016/j.jbusres.2021.02.008

Kretschmer, T., Leiponen, A., Schilling, M., & Vasudeva, G. (2022). Platform ecosystems as meta-organizations: Implications for platform strategies. *Strategic Management Journal*, *43*(3), 405–424. https://doi.org/10.1002/smj.3250

Lancieri, F. M. (2019). Digital protectionism? Antitrust, data protection, and the EU/US transatlantic rift. *Journal of Antitrust Enforcement*, *7*(1), 27–53. https://doi.org/10.1093/jaenfo/jny012

Liang, Y., & Whalen, C. J. (2022). Money manager capitalism and the coronavirus pandemic. In *A Modern Guide to Post-Keynesian Institutional Economics* (pp. 89–120). Edward Elgar Publishing. https://doi.org/10.4337/9781800885752.00012

Lianos, I., & McLean, A. (2021). *Competition law, big tech and financialisation: The dark side of the moon*. https://doi.org/10.2139/ssrn.3930565

Manne, G. A. (2020). Error Costs in Digital Markets. *The Global Antitrust Institute Report on the Digital Economy*, *3*. https://doi.org/10.2139/ssrn.3733662

Mariani, M. M., & Wamba, S. F. (2020). Exploring how consumer goods companies innovate in the digital age: The role of big data analytics companies. *Journal of Business Research*, *121*, 338–352. https://doi.org/10.1016/j.jbusres.2020.09.012

Mascarenhas, O. A., Thakur, M., & Kumar, P. (2024). Critical Thinking Applied to Profit Maximization and Its Presumptive Capitalist Models. In *A Primer on Critical Thinking and Business Ethics* (pp. 31–64). Emerald Publishing Limited. https://doi.org/10.1108/978-1-83753-312-120231002

Moreno Belloso, N., & Petit, N. (2023). *The EU digital markets act (DMA): a competition hand in a regulatory glove*. https://doi.org/10.2139/ssrn.4358589

Newman, J. M. (2021). The Output-Welfare Fallacy: A Modern Antitrust Paradox. *Iowa L. Rev.*, *107*, 563. https://doi.org/10.2139/ssrn.3866725

Nuccio, M., & Guerzoni, M. (2019). Big data: Hell or heaven? Digital platforms and market power in the data-driven economy. *Competition & Change*, *23*(3), 312–328. https://doi.org/10.1177/1024529418816525

Parker, G., Petropoulos, G., & Van Alstyne, M. W. (2020). *Digital platforms and antitrust*. https://doi.org/10.2139/ssrn.3608397

Perera, A., & Iqbal, K. (2021). Big data and emerging markets: Transforming economies through data-driven innovation and market dynamics. *Journal of Computational Social Dynamics*, *6*(3), 1–18.

Pervin, N., Ramasubbu, N., & Dutta, K. (2019). Habitat traps in mobile platform ecosystems. *Production and Operations Management*, *28*(10), 2594–2608. https://doi.org/10.1111/poms.13072

Petit, N. (2021). The proposed digital markets act (DMA): a legal and policy review. *Journal of European Competition Law & Practice*, *12*(7), 529–541. https://doi.org/10.1093/jeclap/lpab062

Phillips, M. (2018). International data-sharing norms: from the OECD to the General Data Protection Regulation (GDPR). *Human genetics*, *137*, 575–582. https://doi.org/10.1007/s00439-018-1919-7

Ratchford, B., Soysal, G., Zentner, A., & Gauri, D. K. (2022). Online and offline retailing: What we know and directions for future research. *Journal of Retailing*, *98*(1), 152–177. https://doi.org/10.1016/j.jretai.2022.02.007

Richter, H., Straub, M., Tuchtfeld, E., Buri, I., van Hoboken, J., De Gregorio, G., Pollicino, O., Peukert, A., Appelman, N., Quintais, J. P., Fahy, R., Zech, H., Goanta, C., Ruschemeier, H., Leerssen, P., Janal, R., Rodríguez, H. B. T., Graef, I., Franck, J.-U. ... & Vergnolle, D. S. (2021). To Break Up or Regulate Big Tech? Avenues to Constrain Private Power in the DSA/DMA Package. *Max Planck Institute for Innovation & Competition Research Paper*, 21–25. https://doi.org/10.2139/ssrn.3932809

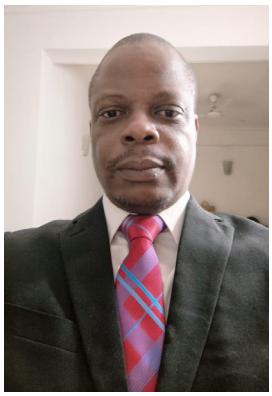
Robertson, V. H. (2020). Excessive data collection: Privacy considerations and abuse of dominance in the era of big data. *Common Market Law Review*, *57*(1). https://doi.org/10.54648/cola2020006

Schütz, P. (2022). Data protection authorities under the EU General Data Protection Regulation-a new global benchmark. In *Handbook of Regulatory Authorities* (pp. 128–145). Edward Elgar Publishing. https://doi.org/10.4337/9781839108990.00018

Sznajder, M. (2021). No Strings Attached? Zero-Price Practices on Social Media Markets under EU Abuse of Dominance Assessment. *Yearbook of Antitrust and Regulatory Studies (YARS)*, *14*(24), 33–62.

Texocotitla, M. A., Hernandez, M. D. A., & Hernandez, S. A. (2017). *The Doctrine of Free Markets: Origin, Nature and Implications*.

Author information



Kolawole Afuwape – LLM, Assistant Lecturer, Jindal Global Law School, O.P. Jindal Global University
Address: Sonipat Narela Road, Near Jagdishpur Village, Sonipat, Haryana 131001, NCR of Delhi, India
E-mail: kolawole.afuwape@jgu.edu.in
ORCID ID: https://orcid.org/0009-0001-5686-230X
WoS Researcher ID: https://www.webofscience.com/wos/author/record/LPP-5259-2024
Google Scholar ID: https://scholar.google.com/citations?user=2tZOhdcAAAAJ

Conflict of interests

The author declare no conflict of interests.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law
PASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – October 4, 2024
Date of approval – October 20, 2024
Date of acceptance – December 13, 2024
Date of online placement – December 20, 2024

Научная статья
УДК 34:004:346.6:004.8
EDN: https://elibrary.ru/gnqswz
DOI: https://doi.org/10.21202/jdtl.2024.48

Правовые аспекты защиты персональных данных и проблемы конкуренции на цифровых рынках

Колаволе Афувапе

Глобальный университет имени О. П. Джиндала, Сонипат, Индия

Ключевые слова

антимонопольное законодательство,
защита персональных данных,
злоупотребление данными,
конкурентное право,
конфиденциальность,
права потребителей,
право,
цифровые платформы,
цифровые рынки,
цифровые технологии

Аннотация

Цель: разработка подходов и предложений по совершенствованию правовых механизмов защиты персональных данных в условиях развивающегося характера цифровых рынков и роста цифровой конкуренции.

Методы: статья подготовлена на основе формально-юридического и сравнительно-правового методов исследования.

Результаты: показаны уникальные особенности цифровых рынков, которые необходимо учитывать для достижения целей антимонопольного законодательства. Отмечается, что основополагающими элементами цифрового рынка являются концепция больших данных и аналитики больших данных, которые на основе цифровых платформ способны производить многие прямые и косвенные сетевые эффекты, требующие понимания для эффективного антимонопольного реагирования и применения соответствующего законодательства. Рост цифровых платформ как бизнес-модели и жизненно важной инфраструктуры цифровой экономики рассмотрен как фактор совершенствования мер правового регулирования отношений, связанных с защитой данных и конфиденциальностью. Определен потенциал в сфере цифровых платформ показателей оценки сложившейся рыночной силы и влияния потенциальной конкуренции на ограничение этой силы. Данные рассмотрены как неотъемлемый компонент общего конкурентного ландшафта на рынке. Анализу подвергнуто действующее в Европейском союзе правовое регулирование в сфере функционирования цифровых платформ и защиты персональных данных. Выявлены трудности, связанные с созданием и применением эффективных нормативных актов, регулирующих деятельность цифровых платформ. Обоснована необходимость изменения антимонопольными органами подходов к аналитике с тем, чтобы учесть отличительные особенности цифровых

© Колаволе, А., 2024

Статья находится в открытом доступе и распространяется в соответствии с лицензией Creative Commons «Attribution» («Атрибуция») 4.0 Всемирная (CC BY 4.0) (https://creativecommons.org/licenses/by/4.0/deed.ru), позволяющей неограниченно использовать, распространять и воспроизводить материал при условии, что оригинальная работа упомянута с соблюдением правил цитирования.

платформ. Отмечено, что такие изменения могут потребовать законодательных реформ и пересмотра процедур, чтобы соответствовать быстрому развитию этих рынков и обеспечить тщательное изучение любого потенциально антиконкурентного поведения.

Научная новизна: проведенное исследование вносит вклад в разработку подходов к определению показателей обеспечения конфиденциальности персональных данных в условиях цифровизации рынков и оценке эффективности антимонопольного законодательства и практики его применения в новой конкурентной среде.

Практическая значимость: полученные результаты могут быть положены в основу совершенствования антимонопольного законодательства и законодательства в сфере защиты персональных данных, а также правового регулирования деятельности цифровых платформ в целом.

Для цитирования

Колаволе, А. (2024). Правовые аспекты защиты персональных данных и проблемы конкуренции на цифровых рынках. *Journal of Digital Technologies and Law*, *2*(4), 1031–1053. https://doi.org/10.21202/jdtl.2024.48

Список литературы

Adadi, A. (2021). A survey on data-efficient algorithms in big data era. *Journal of Big Data*, *8*(1), 24. https://doi.org/10.1186/s40537-021-00419-9

Andriychuk, O. (Ed.) (2023a). *Antitrust and the Bounds of Power: 25 Years On*. Bloomsbury Publishing.

Andriychuk, O. (2023b). EU Digital Competition Law: The Socio-legal Foundations. *Cambridge Yearbook of European Legal Studies*, *25*, 81–104. https://doi.org/10.1017/cel.2023.12

Bandara, R., Fernando, M., & Akter, S. (2021). Managing consumer privacy concerns and defensive behaviours in the digital marketplace. *European Journal of Marketing*, *55*(1), 219–246. https://doi.org/10.1108/ejm-06-2019-0515

Bietti, E. (2024). Structuring Digital Platform Markets: Antitrust and Utilities' Convergence. *University of Illinois Law Review*, *2024*(4).

Buckley, G., Caulfield, T., & Becker, I. (2024). GDPR and the indefinable effectiveness of privacy regulators: Can performance assessment be improved? *Journal of Cybersecurity*, *10*(1), tyae017. https://doi.org/10.1093/cybsec/tyae017

Budzinski, O., & Stöhr, A. (2019). Competition policy reform in Europe and Germany – institutional change in the light of digitization. *European Competition Journal*, *15*(1), 15–54. https://doi.org/10.1080/17441056.2018.1555942

Cammaerts, B., & Mansell, R. (2020). Digital platform policy and regulation: Toward a radical democratic turn. *International Journal of Communication*, *14*, 135–154.

Carovano, G., & Finck, M. (2023). Regulating data intermediaries: The impact of the Data Governance Act on the EU's data economy. *Computer Law & Security Review*, *50*, 105830. https://doi.org/10.1016/j.clsr.2023.105830

Cen, Y., & Li, L. (2020). Effects of network externalities on user loyalty to online B2B platforms: an empirical study. *Journal of Enterprise Information Management*, *33*(2), 309–334. https://doi.org/10.1108/jeim-02-2019-0050

Davola, A., & Malgieri, G. (2023). Data, Power, and Competition Law: The (Im) possible Mission of the DMA? In *The Economics and Regulation of Digital Markets* (pp. 53–74). Emerald Publishing Limited. https://doi.org/10.1108/s0193-589520240000031003

Dunne, N. (2021). Platforms as regulators. *Journal of Antitrust Enforcement*, *9*(2), 244–269. https://doi.org/10.1093/jaenfo/jnaa052

Eifert, M., Metzger, A., Schweitzer, H., & Wagner, G. (2021). Taming the giants: The DMA/DSA package. *Common Market Law Review*, *58*(4). https://doi.org/10.54648/cola2021065

Galehr, S. (2023). *Transatlantic Data Transfers under the GDPR*. EIZ Publishing. https://doi.org/10.36862/eiz-ng001

Gerstenberg, O. (2020). Fundamental rights and democratic sovereignty in the EU: the role of the Charter of Fundamental Rights of the EU (CFREU) in regulating the European Social Market Economy. *Yearbook of European Law*, *39*, 199–227. https://doi.org/10.1093/yel/yeaa008

Jacobides, M. G. (2020). *Regulating Big Tech in Europe: why, so what, and how understanding their business models and ecosystems can make a difference*. https://doi.org/10.2139/ssrn.3765324

Jenny, F. (2021). *Competition law enforcement and regulation for digital platforms and ecosystems: understanding the issues, facing the challenges and moving forward*. https://doi.org/10.2139/ssrn.3857507

Knudsen, E. S., Lien, L. B., Timmermans, B., Belik, I., & Pandey, S. (2021). Stability in turbulent times? The effect of digitalization on the sustainability of competitive advantage. *Journal of Business Research, 128*, 360–369. https://doi.org/10.1016/j.jbusres.2021.02.008

Kretschmer, T., Leiponen, A., Schilling, M., & Vasudeva, G. (2022). Platform ecosystems as meta-organizations: Implications for platform strategies. *Strategic Management Journal*, *43*(3), 405–424. https://doi.org/10.1002/smj.3250

Lancieri, F. M. (2019). Digital protectionism? Antitrust, data protection, and the EU/US transatlantic rift. *Journal of Antitrust Enforcement*, *7*(1), 27–53. https://doi.org/10.1093/jaenfo/jny012

Liang, Y., & Whalen, C. J. (2022). Money manager capitalism and the coronavirus pandemic. In *A Modern Guide to Post-Keynesian Institutional Economics* (pp. 89–120). Edward Elgar Publishing. https://doi.org/10.4337/9781800885752.00012

Lianos, I., & McLean, A. (2021). *Competition law, big tech and financialisation: The dark side of the moon*. https://doi.org/10.2139/ssrn.3930565

Manne, G. A. (2020). Error Costs in Digital Markets. *The Global Antitrust Institute Report on the Digital Economy*, *3*. https://doi.org/10.2139/ssrn.3733662

Mariani, M. M., & Wamba, S. F. (2020). Exploring how consumer goods companies innovate in the digital age: The role of big data analytics companies. *Journal of Business Research*, *121*, 338–352. https://doi.org/10.1016/j.jbusres.2020.09.012

Mascarenhas, O. A., Thakur, M., & Kumar, P. (2024). Critical Thinking Applied to Profit Maximization and Its Presumptive Capitalist Models. In *A Primer on Critical Thinking and Business Ethics* (pp. 31–64). Emerald Publishing Limited. https://doi.org/10.1108/978-1-83753-312-120231002

Moreno Belloso, N., & Petit, N. (2023). *The EU digital markets act (DMA): a competition hand in a regulatory glove*. https://doi.org/10.2139/ssrn.4358589

Newman, J. M. (2021). The Output-Welfare Fallacy: A Modern Antitrust Paradox. *Iowa L. Rev.*, *107*, 563. https://doi.org/10.2139/ssrn.3866725

Nuccio, M., & Guerzoni, M. (2019). Big data: Hell or heaven? Digital platforms and market power in the data-driven economy. *Competition & Change*, *23*(3), 312–328. https://doi.org/10.1177/1024529418816525

Parker, G., Petropoulos, G., & Van Alstyne, M. W. (2020). *Digital platforms and antitrust*. https://doi.org/10.2139/ssrn.3608397

Perera, A., & Iqbal, K. (2021). Big data and emerging markets: Transforming economies through data-driven innovation and market dynamics. *Journal of Computational Social Dynamics*, *6*(3), 1–18.

Pervin, N., Ramasubbu, N., & Dutta, K. (2019). Habitat traps in mobile platform ecosystems. *Production and Operations Management*, *28*(10), 2594–2608. https://doi.org/10.1111/poms.13072

Petit, N. (2021). The proposed digital markets act (DMA): a legal and policy review. *Journal of European Competition Law & Practice*, *12*(7), 529–541. https://doi.org/10.1093/jeclap/lpab062

Phillips, M. (2018). International data-sharing norms: from the OECD to the General Data Protection Regulation (GDPR). *Human genetics*, *137*, 575–582. https://doi.org/10.1007/s00439-018-1919-7

Ratchford, B., Soysal, G., Zentner, A., & Gauri, D. K. (2022). Online and offline retailing: What we know and directions for future research. *Journal of Retailing*, *98*(1), 152–177. https://doi.org/10.1016/j.jretai.2022.02.007

Richter, H., Straub, M., Tuchtfeld, E., Buri, I., van Hoboken, J., De Gregorio, G., Pollicino, O., Peukert, A., Appelman, N., Quintais, J. P., Fahy, R., Zech, H., Goanta, C., Ruschemeier, H., Leerssen, P., Janal, R., Rodríguez, H. B. T., Graef, I., Franck, J.-U. ... & Vergnolle, D. S. (2021). To Break Up or Regulate Big Tech? Avenues to Constrain Private Power in the DSA/DMA Package. *Max Planck Institute for Innovation & Competition Research Paper*, 21–25. https://doi.org/10.2139/ssrn.3932809

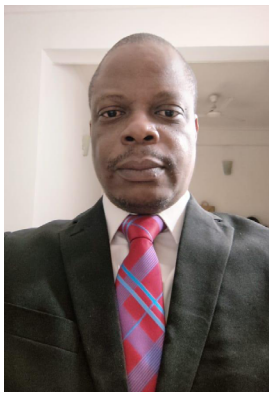
Robertson, V. H. (2020). Excessive data collection: Privacy considerations and abuse of dominance in the era of big data. *Common Market Law Review*, *57*(1). https://doi.org/10.54648/cola2020006

Schütz, P. (2022). Data protection authorities under the EU General Data Protection Regulation-a new global benchmark. In *Handbook of Regulatory Authorities* (pp. 128–145). Edward Elgar Publishing. https://doi.org/10.4337/9781839108990.00018

Sznajder, M. (2021). No Strings Attached? Zero-Price Practices on Social Media Markets under EU Abuse of Dominance Assessment. *Yearbook of Antitrust and Regulatory Studies (YARS)*, *14*(24), 33–62.

Texocotitla, M. A., Hernandez, M. D. A., & Hernandez, S. A. (2017). *The Doctrine of Free Markets: Origin, Nature and Implications*.

Сведения об авторе



Колаволе Афувапе – магистр права, ассистент преподавателя, Школа права, Глобальный университет имени О. П. Джиндала
Адрес: 131001 Нарьяна, Индия, г. Сонипат, Нир Ягдишпур Виледж, Сонипат Нарела Роуд
E-mail: kolawole.afuwape@jgu.edu.in
ORCID ID: https://orcid.org/0009-0001-5686-230X
WoS Researcher ID: https://www.webofscience.com/wos/author/record/LPP-5259-2024
Google Scholar ID: https://scholar.google.com/citations?user=2tZOhdcAAAAJ

Конфликт интересов

Автор сообщает об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.19.31 / Право на информацию
Специальность ВАК: 5.1.3 / Частно-правовые (цивилистические) науки

История статьи

Дата поступления – 4 октября 2024 г.
Дата одобрения после рецензирования – 20 октября 2024 г.
Дата принятия к опубликованию – 13 декабря 2024 г.
Дата онлайн-размещения – 20 декабря 2024 г.