ISSN 1984-9729 DOI: https://doi.org/10.26512/lstr.v15i2 EISSN 1984-8161
Volume 15 [2023] L.S.T.R. Issue 2

LAW, STATE and TELECOMMUNICATIONS REVIEW

Revista de Direito, Estado e Telecomunicações

October 2023

UNIVERSITY OF BRASILIA

Research Center on Communication Policy, Law, Economics, and Technology
School of Law Center on Law and Regulation

The University of Brasilia Law School Alumni donates paperback versions of this journal to Law School libraries abroad

Permanent Identifier for the Web
The Journal and each article individually at
LexML and DOI
http://lexml.gov.br/urn/urn:lex:br:rede.virtual.bibliotecas:revista:2009;000903260

Volume 1, Issue 1 (https://doi.org/10.26512/lstr.v1i1), May 2009 (8 double-blind peer-reviewed articles published)
Volume 2, Issue 1 (https://doi.org/10.26512/ls.t.r..v2i1), May 2010 (8 double-blind peer-reviewed articles published)
Volume 3, Issue 1 (https://doi.org/10.26512/ls.t.r..v3i1), May 2011 (9 double-blind peer-reviewed articles published)
Volume 4, Issue 1 (https://doi.org/10.26512/ls.t.r..v4i1), May 2012 (7 double-blind peer-reviewed articles published)
Volume 5, Issue 1 (https://doi.org/10.26512/ls.t.r..v5i1), May 2013 (8 double-blind peer-reviewed articles published)
Volume 6, Issue 1 (https://doi.org/10.26512/ls.t.r..v6i1), May 2014 (8 double-blind peer-reviewed articles published)
Volume 7, Issue 1 (https://doi.org/10.26512/ls.t.r..v7i1), May 2015 (7 double-blind peer-reviewed articles published)
Volume 8, Issue 1 (https://doi.org/10.26512/ls.t.r..v8i1), May 2016 (8 double-blind peer-reviewed articles published)
Volume 9, Issue 1 (https://doi.org/10.26512/ls.t.r..v9i1), May 2017 (8 double-blind peer-reviewed articles published)
Volume 10, Issues 1 (https://doi.org/10.26512/ls.t.r..v10i1) and 2 (https://doi.org/10.26512/ls.t.r..v10i2), May and October 2018 (14 double-blind peer-reviewed articles published)
Volume 11, Issues 1 (https://doi.org/10.26512/lstr.v11i1) and 2 (https://doi.org/10.26512/lstr.v11i2), May and October 2019 (23 double-blind peer-reviewed articles published)
Volume 12, Issues 1 (https://doi.org/10.26512/lstr.v12i1) and 2 (https://doi.org/10.26512/lstr.v12i2), May and October 2020 (21 double-blind peer-reviewed articles published)
Volume 13, Issues 1 (https://doi.org/10.26512/lstr.v13i1) and 2 (https://doi.org/10.26512/lstr.v13i2), May and October 2021 (18 double-blind peer-reviewed articles published)
Volume 14, Issues 1 (https://doi.org/10.26512/lstr.v14i1) and 2 (https://doi.org/10.26512/lstr.v14i2), May and October 2022 (15 double-blind peer-reviewed articles published)
Volume 15, Issues 1 (https://doi.org/10.26512/lstr.v15i1) and 2 (https://doi.org/10.26512/lstr.v15i2), May and October 2023 (24 double-blind peer-reviewed articles published)

R454 Law, State and Telecommunications Review = Revista de Direito, Estado e Telecomunicações / Grupo de Estudos em Direito das Telecomunicações = Research Group on Telecommunications Law. - v. 15, n. 2 - (2023) - Brasília: Universidade de Brasília, 2023.

ISSN 1984-9729
EISSN 1984-8161

1. Direito - Periódicos. 2. Telecomunicações. I. Grupo de Estudos em Direito das Telecomunicações. II. Título: Law, State and Telecommunications.

CDU: 347.83

ANVUR (Agenzia Nazionale di Valutazione del Sistema Universitario e dela Ricerca)
Area 12 - Scienze Giuridiche: Scientificità Riconosciuta.
Area 13 - Area Scienze Economiche e Statistiche : Scientificità Riconosciuta.
Area 14 - Scienze Politiche e Sociali: Scientificità Riconosciuta.

L.S.T.R Masthead

The Law, State and Telecommunications Review
ISSN 1984-9729– EISSN 1984-8161

University of Brasilia Center on Law and Regulation (School of Law)
Universidade de Brasília
Faculdade de Direito
Núcleo de Direito Setorial e Regulatório
Campus Universitário de Brasília
Brasília, DF, CEP 70919-970
Caixa Postal 04413, Brasil
Tel.: +55(61)3107-0713
getel@unb.br

Periodicity
The L.S.T.R publishes one annual issue released on May uninterrupted since May 2009 and two annual issues released on May and October uninterrupted since May 2018.

Mission/Scope/Focus/Areas of Expertise/Emphasis
The Law, State and Telecommunications Review mission is to publish legal and interdisciplinary analyses on telecommunications and communications focused on policy and regulation of communications services, telecommunications services, Internet-based services and rights, such as the right to communicate, to publish, to private exchange, to design communication platforms, and other related topics, such as privacy, intellectual property, universal access, convergence, satellite and spectrum regulation, telecommunication licensing and regulatory design, independent agencies, deregulation, e-commerce, big data, net neutrality, and so forth, with emphasis on national and foreign experiences through the lenses of legal and regulatory theories.

INFORMATION FOR AUTHORS AND READERS

Submission process and Criteria for the Double-Blind Peer Review Process
The journal hosts only original articles and the authors are requested to submit them through the website of the University of Brasilia Center on Law and Regulation (http://www.ndsr.org/SEER/index.php). The journal adopts the double-blind peer review process and each reviewer rates the article according to the article quality (10%), theoretical relevance (10%), originality (10%), adherence to the journal's topics of interest (10%), manuscript presentation (10%), reviewer's assessment (50%).

Languages
The journal accepts articles in Portuguese, English and Spanish.

Format for in-text Citations and References
The journal adopts the ABNT NBR (Brazilian Association of Technical Standards) citation and reference format.

Abstract and Keywords
The journal adopts structured abstracts with clear indication of purpose, methodology/approach/design, findings, practical implications, and originality/value of the papers. Keywords should depict the actual content of the article and be limited to five, according to the ABNT NBR 6028 standard.

Authorship of the paper
Authorship should be limited to those who have made a significant contribution to the conception, design, execution, or interpretation of the reported study. All those who have made significant contributions should be listed as co-authors and their specific contribution should be listed at the end of the article after the double-blind peer review process. Where there are others who have participated in certain substantive aspects of the research project, they should be acknowledged in a footnote or listed as contributors. All authors should be identified in a footnote after the review process with their academic status, institutional activities and email.

Disclosure and Conflicts of Interest
All authors should disclose in their manuscript any financial or other substantive conflict of interest that might be construed to influence the results or interpretation of their manuscript. All sources of financial support for the project should be disclosed.
Examples of potential conflicts of interest which should be disclosed include employment, consultancies, stock ownership, honoraria, paid expert testimony, patent applications/registrations, and grants or other funding. Potential conflicts of interest should be disclosed at the earliest stage possible.

Disclaimer and Liability
The editorial board accepts articles for educational and informational purposes only and should not be used to replace either official documents or professional advice. The information contained in this journal is not guaranteed to be up to date and does not provide legal advice. Any views expressed in the published articles are exclusively of their authors and should not be construed as an endorsement by the University of Brasilia or the editorial board of the article content or authors' views.

Expediente da RDET

Revista de Direito, Estado e Telecomunicações
ISSN 1984-9729– EISSN 1984-8161

Núcleo de Direito Setorial e Regulatório da Faculdade de Direito da Universidade de Brasília
Universidade de Brasília
Faculdade de Direito
Núcleo de Direito Setorial e Regulatório
Campus Universitário de Brasília
Brasília, DF, CEP 70919-970
Caixa Postal 04413, Brasil
Tel.: +55(61)3107-0713
getel@unb.br

Periodicidade
A RDET publica um número anual em maio de forma ininterrupta desde maio de 2009 e dois números anuais em maio e outubro de forma ininterrupta desde maio de 2018.

Missão/Escopo/Enfoque/Temática/Ênfase
A Revista de Direito, Estado e Telecomunicações da UnB tem por missão a publicação de artigos sobre telecomunicações e comunicações de qualquer espécie com enfoque em política pública e regulação dos serviços e direitos de comunicação, serviços e direitos de telecomunicações, serviços e direitos apoiados na internet, tais como o direito à comunicação, de publicar, de intercâmbio privado, de conceber plataformas de comunicação, e outros temas correlatos, como privacidade, propriedade intelectual, acesso universal, convergência, regulação de satélite, órbita e espectro de radiofrequências, outorga de telecomunicações, desenho regulatório, agências independentes, desregulação, comércio eletrônico, big data, neutralidade de rede e assim por diante, com ênfase em experiências nacionais e internacionais a partir de teorias jurídico-regulatórias.

INSTRUÇÕES AOS AUTORES E INFORMAÇÕES AOS LEITORES

Submissão de artigos e Critérios para Dupla Revisão Cega por Pares
A Revista de Direito, Estado e Telecomunicações somente aceita artigos originais, que devem ser submetidos exclusivamente no sítio eletrônico do Núcleo de Direito Setorial e Regulatório da Faculdade de Direito da Universidade de Brasília por intermédio do sistema eletrônico de submissões (http://www.ndsr.org/SEER/index.php), que adota o método de revisão duplo cego por pares, apoiados nos critérios de qualidade do conteúdo (10%), relevância teórica ou prática (10%), originalidade (10%), adequação à temática da Revista (10%), apresentação do trabalho (10%), recomendação geral do especialista revisor (50%).
Idiomas aceitos
A Revista de Direito, Estado e Telecomunicações aceita artigos escritos em português, inglês ou espanhol.
Normas Bibliográficas e de Citações
A Revista adota o formato ABNT NBR (Associação Brasileira de Normas Técnicas) para citações e referências bibliográficas.
Resumos e Palavras-Chave
A Revista adota o modelo de resumos estruturados, mediante clara indicação do propósito, metodologia/abordagem/design, resultados, implicações práticas e originalidade/relevância do artigo. As palavras-chave devem refletir o real conteúdo do artigo, limitadas a cinco descritores, e conforme norma ABNT NBR 6028.
Autoria
A autoria dos artigos submetidos à Revista de Direito, Estado e Telecomunicações deve estar limitada às pessoas que tenham contribuído significativamente à concepção, design, execução ou interpretação dos resultados. Todos que tiverem contribuído significativamente para o trabalho devem ser listados como coautores, inserindo-se, posteriormente ao processo de revisão cega por pares, ao final do artigo, a indicação da contribuição de cada autor. Quando alguém houver participado em momentos específicos e relevantes do projeto de pesquisa pertinente, a ele(a) deve-se atribuir a condição de auxílio à pesquisa e referidos em nota de rodapé de agradecimento. Os autores devem estar identificados, após processo de revisão cega por pares, com sua formação pregressa e vinculação institucional, inclusive email.
ireitos Autorais
A Revista de Direito, Estado e Telecomunicações é de acesso aberto, nos termos da licença *Creative Commons Attribution 4.0 International* (CC BY 4.0), que permite a reprodução e o compartilhamento do material licenciado, no todo ou em parte, a produção, reprodução e compartilhamento do material adaptado, condicionado a que o trabalho original não seja alterado ou transformado de qualquer modo e que o trabalho seja adequadamente citado.
Conflito de Interesse
Todos os autores devem divulgar em seus artigos qualquaer conflito de interesse, seja financeiro ou de outra natureza, que possa levar a influenciar os resultados ou a interpretação dos seus artigos. Todas as fontes de financiamento para o projeto de pesquisa pertinente devem ser divulgadas. Exemplos de conflitos de interesse potenciais que devem ser divulgados incluem vínculos empregatícios, consultorias, participação acionária, honrarias, perícia, registro de patentes, prêmios ou outro tipo de financiamento. Conflitos de interesse potenciais devem ser divulgados o quanto antes.
Indicação de Responsabilidade
A Comissão Editorial da Revista de Direito, Estado e Telecomunicações aceita artigos com a finalidade de divulgação científica, educacional ou meramente informativa. A Revista não deve ser utilizada como substitutivo a pesquisa de documentos oficiais ou à consulta profissional. Embora o Corpo Editorial da Revista preze pela qualidade e precisão de todos os artigos publicados, não há garantia de que a informação nela contida esteja atualizada, bem como ela não se destina a substituir a necessária consultoria advocatícia para quem dela necessite. Os dados e opiniões emitidas nos artigos publicados são de exclusiva responsabilidade dos autores correspondentes e não significam que a Universidade de Brasília, a Comissão Editorial ou qualquer membro do corpo editorial endossam seu conteúdo ou pontos de vista.

Dear Reader,

In this issue, the Law, State and Telecommunications Review (LSTR) publishes a number of original articles on topics relevant to digital rights and to information and communications technologies in different parts of the world from a myriad of interdisciplinary perspectives.

We are delighted to include articles on Kazakhstan's electronic money trends and the need legal reforms for its proper functioning and circulation; the evolution of regulatory debates on internet interoperability and network access through case studies from the United States and Europe; the right to be forgotten in digital law, with a focus on European Union Court of Justice and European Court of Human Rights decisions; the legal solutions for defining robots in civil relations and establishing effective regulations for robotics usage in Ukraine; the use of artificial intelligence in the Ukrainian Judicial System; the legal aspects of digital face identification technology in criminal proceeding in Ukraine, China's artificial intelligence-driven social credit system's impact on international human rights, particularly concerning privacy issue; the role of electronic money in modernizing Kazakhstan's monetary system; the development of a cyber-crime protection system in Indonesia, including cyber insurance regulations; the impact of digital transition and its intensification during crises like the COVID-19 Pandemic and the Ukraine War on the tourism industry in the European Union; the prevention of cyber sabotage in Ukraine and the control of its damages; and the standardization of cybersecurity threat terminology on a global scale.

We hope you will enjoy reading this issue, and we look forward to the next issue to be released in May 2024.

Sincerely,

Prof. Marcio Iorio Aranha
Editor, The Law, State and Telecommunications Review

Estimado Lector,

Este número de la Revista de Derecho, Estado y Telecomunicaciones (RDET) de la Universidad de Brasilia trae varios artículos originales sobre diversos temas relevantes para la teoría y práctica regulatoria en telecomunicaciones, cumpliendo con el propósito de servir como instrumento de investigación sectorial jurídica e interdisciplinaria.

En este número se insertaron artículos sobre las tendencias de dinero electrónico en Kazajistán y la necesidad de reformas legales para su correcto funcionamiento y circulación; la evolución de los debates regulatorios sobre la interoperabilidad de internet y el acceso a redes a través de estudios de casos de Estados Unidos y Europa; el derecho al olvido en la ley digital en las decisiones del Tribunal de Justicia de la Unión Europea y del Tribunal Europeo de Derechos Humanos; las soluciones legales para definir robots en relaciones civiles y establecer regulaciones efectivas para el uso de la robótica en Ucrania; el uso de inteligencia artificial en el sistema judicial ucraniano; los aspectos legales de la tecnología de identificación facial en procesos penales en Ucrania, el impacto del sistema de crédito social impulsado por inteligencia artificial en China en los derechos humanos internacionales, especialmente en lo que respecta a problemas de privacidad; el papel del dinero electrónico en la modernización del sistema monetario de Kazajistán; el desarrollo de un sistema de protección contra delitos cibernéticos en Indonesia, incluidas las regulaciones de seguros cibernéticos; el impacto de la transición digital en la industria turística de la Unión Europea y su intensificación durante crisis como la pandemia de COVID-19 y la guerra en Ucrania; la prevención del sabotaje informático en Ucrania y el control de sus daños; y la estandarización de la terminología de amenazas cibernéticas a nivel global.

Para los números que siguen, nos comprometemos a seguir publicando artículos sobre enfoques relevantes para la regulación de las (tele)comunicaciones desde una perspectiva estrictamente legal, así como interdisciplinaria.

Esperamos que haya disfrutado leyendo este número a la espera delsegundo número de lodecimotercer volumen de RDET que se publicará en Mayo de 2024.

Atentamente,

Prof. Marcio Iorio Aranha
Editor, The Law, State and Telecommunications Review

Prezado Leitor,

Este número da Revista de Direito, Estado e Telecomunicações (RDET) da Universidade de Brasília traz vários artigos originais sobre diversos temas relevantes para a teoria e a prática regulatória em telecomunicações e direitos digitais em vários países.

Neste número, foram inseridos artigos sobre as tendências de dinheiro eletrônico no Cazaquistão e a necessidade de reformas legais para seu funcionamento e sua circulação adequados; a evolução dos debates regulatórios sobre interoperabilidade da internet e acesso a redes por meio de estudos de casos dos Estados Unidos e da Europa; o direito ao esquecimento na lei digital, com foco nas decisões do Tribunal de Justiça da União Europeia e do Tribunal Europeu de Direitos Humanos; as soluções legais para definir robôs em relações civis e estabelecer regulamentos eficazes para o uso de robótica na Ucrânia; o uso de inteligência artificial no sistema judiciário ucraniano; os aspectos legais da tecnologia de identificação facial em processos criminais na Ucrânia, o impacto do sistema de crédito social impulsionado por inteligência artificial na China nos direitos humanos internacionais, especialmente em relação a questões de privacidade; o papel do dinheiro eletrônico na modernização do sistema monetário do Cazaquistão; o desenvolvimento de um sistema de proteção contra crimes cibernéticos na Indonésia, incluindo regulamentações de seguro cibernético; o impacto da transição digital na indústria de turismo na União Europeia e sua intensificação durante crises como a pandemia do COVID-19 e a guerra na Ucrânia; a prevenção de sabotagem cibernética na Ucrânia e o controle de seus danos; e a padronização da terminologia de ameaças cibernéticas em escala global.

Esperamos que tenha apreciado a leitura deste número no aguardo do próximo número a ser publicado em maio de 2024.

Atenciosamente,

Prof. Marcio Iorio Aranha
Editor, Revista de Direito, Estado e Telecomunicações

TABLE OF CONTENTS / SUMÁRIO

Legal Regulation of Electronic Money Turnover: Global Trends

Submitted: 1 July 2022
Reviewed: 14 July 2022
Revised: 2 August 2022
Accepted: 21 October 2022

Kamshat T. Raiymbergenova[*]
https://orcid.org/0000-0003-1251-7093
Gulnar T. Aigarinova[**]
https://orcid.org/0000-0001-6747-0953
Saltanat K. Atakhanova[***]
https://orcid.org/0000-0002-0198-5759
Bakhytzhan Zh. Saparov[****]
https://orcid.org/0000-0001-9151-1153
Makhabbat K. Nakisheva[*****]
https://orcid.org/0000-0002-8444-5212

Article submitted to blind peer review

DOI: https://doi.org/10.26512/lstr.v15i2.43920

Abstract

[Purpose] To analyse the existing trends in the turnover of electronic money, and their relationship with the conventional cash turnover on the territory of the Eurasian Economic Union (EEU), in particular, in the legal system of the Republic of Kazakhstan (RK).

[Methodology/Approach/Design] Deduction, content analysis, comparative analysis, and other general and special research methods were used.

[Findings] As a result, the existing problems in the functioning of the type of money considered in this study were analysed. The study includes recommended measures to introduce amendments to legislation aimed at removing barriers to the functioning and circulation of electronic money, which will benefit the economic system of the given state.

[Practical Implications] The information presented in this article can be useful material for representatives of public authorities in the implementation of reforms to modernise the economic system, for a wide range of readers interested in the development of digital

[*]Doctoral Student, Department of Customs, Financial and Environmental Law, Al-Farabi Kazakh National University, Almaty, Republic of Kazakhstan, e-mail: raiymbergenova@gmail.com.
[**]Associate Professor, Department of Customs, Financial and Environmental Law, Al-Farabi Kazakh National University, Almaty, Republic of Kazakhstan, e-mail: g.aigarinova@gmail.com.
[***]Associate Professor, Department of Civil Law and Civil Procedure, Labor Law, Al-Farabi Kazakh National University, Almaty, Republic of Kazakhstan, e-mail: atakhanova@aol.com.
[****]Director of the Administrative Department, Abai Kazakh National Pedagogical University, Almaty, Republic of Kazakhstan, e-mail: bak-saparov@yahoo.com.
[*****]Senior Lecturer, Department of Customs, Financial and Environmental Law, Al-Farabi Kazakh National University, Almaty, Republic of Kazakhstan, e-mail: nakisheva@gmail.com.

technologies and their impact on the commercial activities of subjects of the economic life of society.
Keywords: Currency. Payment System. Economy. Financial Organisation. Bank.

INTRODUCTION

Electronic money is a *de facto* prepaid payment product, which is positioned as a payment service with limited functions. Electronic money performs many functions, namely: this type of money acts as a starting financial product for people who previously had no access to financial services; electronic money is needed to increase the availability of financial services due to a lower entry threshold (that is, reduced requirements for customer identification and their level of financial literacy); it performs the role of infrastructure and is the basis for other innovative projects, which include, for example, the issuance of cards (banking or transport), and online lending (NEKHAICHUK et al., 2019; POIER et al., 2022).

Electronic money can be characterised as a relatively new phenomenon present in the financial market. The consequence of this is the fact that the supervision of their turnover is still in the process of development. The above can be evidenced, for example, by the fact that there is no single, generally accepted definition of the phenomenon considered in the article, namely electronic money. Nevertheless, in modern conditions, the role of this type of money is becoming increasingly important since it is one of the unique forms of money evolution in the digital economy (PANOVA, 2018; PATASHKOVA et al., 2021). Based on the results of examining the information scope from various studies, it can be stated that, in the scientific literature, the issue of electronic money has been considered sufficiently. Notably, the previous studies were aimed at considering the purely technical aspects of the functioning of electronic money, while the aspects of legislative, and legal regulation of electronic money were not fully covered. Furthermore, a more detailed consideration of the history of the development and legislative consolidation of the functioning of this type of money in the context of the Eurasian Economic Union (EAEU), in particular in the legal system of the Republic of Kazakhstan (RK) has not been conducted (AYUDYA and WIDOWO, 2018; VOZNIUK et al., 2020).

To address these shortcomings, within the framework of this study, the main emphasis is placed on the analysis of the role of electronic money in the EAEU member states, in particular, the history of the development, functioning, and legislative consolidation of electronic money in the Republic of Kazakhstan will be covered. The theoretical consideration of the studied phenomenon is also included, identifying the most important and key features of electronic money circulation, and correlating it with classical, cash circulation. In the course of

transferring the analysis to the state level, the regulatory framework of the Republic of Kazakhstan is considered in the framework of the study, in particular, specific laws regulating the sphere of functioning of electronic money systems are provided. Furthermore, the study identifies reasons for the insufficient distribution of this type of money in the Republic of Kazakhstan, based on which practical recommendations will be developed for the introduction of many adjustments to the current Kazakh legislation and the economic policy of the state to provide wider opportunities for the functioning of electronic payment systems. The above will increase the activity in the field of online commerce, resulting in the improvement of the economy and the creation of a more developed economic system (LASME and MAKOTO, 2020; SARSEMBAYEV, 2021; BLAHUTA et al., 2019).

The purpose of the article is to analyse the existing trends in the turnover of electronic money, and their relationship with the conventional cash turnover on the territory of the Eurasian Economic Union. Firstly, attention will be focused on the Republic of Kazakhstan.

MATERIALS AND METHODS

In reviewing the existing and functioning electronic money circulation system on the territory of the Eurasian Economic Union and the territory of the Republic of Kazakhstan, in the development of methodological recommendations for the modernisation of the legislative framework of the republic and its economic policy, many general and special research methods were applied. With the use of a set of methods in this study, it was possible to identify the key provisions that determine the scientific perception of electronic money, to discover the main characteristics of approaches to building regulatory mechanisms for this type of financial transaction, which is especially important when creating a scientific-theoretical, legal foundation on which, in the future, the actions of individual states will be based on, regarding the creation and implementation of national legislation or other mechanisms that will be aimed at preventing and countering crimes that have already been committed in the field of electronic money circulation by certain criminal entities. The development of electronic money in the legislative field was also disclosed, the ratio of classical, cash, and electronic money turnover was considered, the main areas of the development and functioning of the phenomenon considered in the framework of the study were identified, synthetic conclusions were formulated, together with the prospects of further research.

For example, upon using the deduction method, a description of existing, in particular in the legislative system of the Republic of Kazakhstan, adopted, and relevant regulations that introduce electronic payment systems into the legal field

was compiled, while the inductive method allowed structuring and generalising the publicly available scope of information directly related to electronic money. It should also be noted that other research methods were used in the course of the study. For example, the use of content analysis in the framework of this study allowed identifying key conclusions regarding the further recommended area of implementation of reforms. The use of comparative analysis allowed identifying the differences in the existing fundamental approaches to the definition of electronic money, considering how to fully fulfil one of the key advantages of the type of money under consideration, namely, very high competitiveness due to the expansion of the number of entities directly connected and interacting with electronic money.

The methodology generalisation used in the framework of this study allowed the creation of the most complete picture, which represents, firstly, modern and relevant features of the functioning of electronic money systems on the territory of the EAEU member states and the territory of the Republic of Kazakhstan, drawing conclusions regarding the prospects for the use of these technologies, formulating effective and usable methods of modernisation of the economic system and financial policy of this state. This study was conducted in three stages. In the first stage, guided by the scientific literature and the theoretical achievements formulated in it, the issues of the establishment and development of electronic payment systems on a global scale and the scale of the EAEU member states, the main approaches to scientific comprehension and perception of the phenomenon considered in the framework of the study were disclosed. In the second stage, a descriptive characteristic of the currently implemented economic and legal policy regarding electronic money circulation at the national level (in particular, in the Republic of Kazakhstan) is formed, and an analysis of current regulations in this area is also conducted. In the third stage, the recommended measures that, if implemented, can remove barriers to the full functioning of electronic money, which will have a very beneficial effect on the national economy of Kazakhstan are offered.

RESULTS

Money, acting as a payment instrument, determines the development of the economy at the international level and on the scale of a separate state, the society living on its territory. They provide for universal exchange between owners of a variety of goods and services to ensure the operation of the credit and financial systems of the state (WULANDARI et al., 2016). Regarding the history of the development of electronic payment systems at the modern level, the following should be noted. After computers began to gain popularity, the first area of application of new computing power was the conversion of calculations and

accounting into electronic format. Interbank settlements, which previously required direct physical transportation of banknotes, are now almost totally carried out electronically. Electronic payment instruments, which include card payments and electronic bank transfers, have gradually replaced cash and paper checks in retail payments, even though paper money is still in large circulation as, in some cases, a convenient means of paying for small-volume settlements and services. In the 1990s, there was a surge in the power of electronic computing machines (computers), moreover, new generations of computer technologies allowed investing in personal computers. The development of the Internet has also created a demand for the exchange of intangible goods and services in electronic form (KOVALENKO and SHERNIN, 2018; BLAHUTA et al., 2020). This trend has led to the emergence of a new payment instrument, namely electronic money.

Despite the relatively recent entry into the daily life of electronic money, the active and dynamic development of this area of economic activity can be observed. The "electronic money" in the framework of this study refers to a variety of payment instruments that are based on innovative technological and digital developments. Currently, it can be stated that there is no single, practically supported, and stable definition of this phenomenon. Regarding the currency, a number of its fundamental features and the duties that it must fulfil can be outlined. Thus, for example, they include the need to make payments (i.e., to facilitate the circulation of the money supply within the state and internationally), to serve as a recognised equivalent of value, and to be used as a unit of account for certain economic transactions (LESKOVA, 2017). It is possible to distinguish two main characteristics inherent directly in electronic money, the presence of which allows asserting that electronic payment systems belong to electronic money. In particular, electronic payment systems are capable of performing the function of money, serving as an alternative to conventional currency instruments, moreover, existing in electronic form, electronic money differs from conventional bank accounts and securities.

An important factor, which, depending on its state, hinders or stimulates the development of electronic money circulation in the state economy, is the technical subsystems and the level of informatisation of the state under consideration. As an opportunity for modernisation, in this case, attention should be paid to the prospects for the implementation of the functions of the international payment system operating on the territory of the EAEU member states (KHACATURYAN, 2016). Even though the functions of the international payment systems on the territory of different countries and the mechanisms of turnover of the countries of the Eurasian Economic Union are approximately the same, the volume of services provided by the international payment system will depend on the technical capabilities of each country. The lack of high-quality

Internet communication in all regions of the Eurasian Economic Union may pose a real threat to the mechanisms considered in the study. It seems that without proper development of electronic interaction channels, it is impossible to ensure acceptable interaction of financial and commercial organisations, their clients, and government agencies within national economic systems or a single integrated platform. Regarding the above, the Kyrgyz development of 2020 deserves consideration. A draft concept for the development of digital payment technologies in the period 2020-2022 has been formed in the Kyrgyz Republic (AMNAZHOLOVA, 2018).

As an opportunity to open prospects for the development of electronic payment system mechanisms, the possibility of using simplified customer identification mechanisms within the state economy should be considered. The absence of these platforms in the EAEU space may limit the number of commercial business enterprises that can be maintained through existing remote service channels. The National Bank, which is the main body and an important part of the national mechanism of circulation of electronic payment systems, is interested in promoting the development of electronic money circulation and payment methods. Considering the above, national regulatory authorities should be interested in stimulating the development of the national economy and, as a result, integrating the mechanisms of circulation of electronic payment systems. It seems that for the effective and safe development and functioning of the digital payment space, coordination measures are required at the level of all participants along with supervision corresponding to the modern technologies by national central banks, which are the main body of the electronic payment system turnover mechanism. On the one hand, it will maintain the stability of the payment system, and protect the rights and interests of consumers, on the other hand, it will contribute to the development and introduction of digital innovations.

DISCUSSION

The imperfect legal framework of the EAEU member states (especially the Central Asian states) in terms of using innovative digital payment technologies and products and the lag in the adoption of regulations for innovative payment technologies and products on the territory of the EAEU member states directly hinder the development of electronic payments (AFANASYEVA, 2020). Therewith, the introduction and improvement of measures aimed at coordinating the elements of the electronic payment system turnover mechanism provide the EAEU member states with additional opportunities for the development of these systems. The low level of use of digital channels by customers should be considered a threat when interacting with the participants of the payment system. This threat is caused by the lack of a high-quality Internet connection and a low

level of financial awareness of consumers of payment services. Thus, despite the presence of certain theoretical developments aimed at modernising the legislative framework in the field of functioning of the phenomenon under consideration, the level of development and use of this tool in such states as Belarus, Kyrgyzstan, Armenia, and Kazakhstan is still at a low level (ABRAMOVA et al., 2020).

In addition, the functioning of electronic payment systems should be considered to resolve the existing problem of creating a collective, single currency, which is relevant for the countries of the Eurasian space. All decisions of the financial authorities of these countries emphasise the need to use their national currencies for interaction between the countries of the Eurasian Economic Union. Even though the Eurasian Economic Union is currently working on the introduction of a single currency, the question of which currency should be introduced into the EAEU as a single currency has not yet been resolved. Among the available options, the possibility of using the Russian rouble as the strongest currency in the region is being considered (the alternative is to create a new currency). Thus, international experience shows that the development of electronic payments, especially electronic money, reduces the cost of cash turnover and, as a result, accelerates economic growth. Electronic money can also contribute to the development of new sectors of the economy and e-commerce. However, the development of the electronic money market largely depends on legal supervision (DOSTOV et al., 2020). If the relevant rules are not flexible enough, innovations in the field of electronic payments cannot be implemented at a high level.

With the adoption of the Law of the Republic of Kazakhstan No. 466-IV "On amendments and additions to certain legislative acts of the Republic of Kazakhstan on electronic money issues" (2011), electronic money was recognised at the legislative level as a legal instrument for payments and settlements. Furthermore, this concept was introduced into circulation from the Law of the Republic of Kazakhstan No. 11-VI "On payments and payment systems" (2016). The pioneer of issuing electronic currency in Kazakhstan is the joint-stock company "Eximbank Kazakhstan", which became the first issuer of electronic currency "e-kzt" in 2012, in its activities this bank relies on the Kazakhstan Interbank Settlement Centre of the National Bank of the Republic of Kazakhstan. The introduction of electronic money is aimed at developing alternative methods of non-cash payments. Electronic money, in its essence, is similar to paper money, yet payments are made in a non-cash form. This is how ordinary people perceive electronic money in everyday life. Nevertheless, this does not seem quite correct. Upon analysing the legislative framework, many differences in electronic money can be observed, the most important of which will be discussed below. The first considerable difference between electronic money and paper money is the form

of issue. According to Law of the Republic of Kazakhstan No. 11-VI "On payments and payment systems" (2016), the currency of Kazakhstan can exist in cash (in the form of paper money and coins) and in non-cash form (in the form of bank account records), therewith, the type of money in question can exist only in electronic form, not in the form of a bank account record (AYUDYA and WIBOWO, 2018).

Thus, the fundamental difference between electronic money and currency is in the form of existence. The form of non-cash currency is a type of bank account, its concept and exhaustive classification are determined by the legislation of Kazakhstan (DZHAKSYBEKOVA and NAMZHUDINOVA, 2020). Bank accounts cannot be a form of electronic money, that is, an unconditional and irrevocable monetary obligation of electronic money issuer, which is stored in electronic form and accepted by others as a means of payment in electronic money. This is due to many differences between electronic money and paper money, which are a condition for issuing money. For example, according to Law of the Republic of Kazakhstan No. 2155 "On the National Bank of the Republic of Kazakhstan" (1995), the issue of banknotes and coins, the organisation of their circulation, and withdrawal from circulation in the Republic of Kazakhstan is carried out only by the National Bank of the Republic of Kazakhstan. Following the provisions of the legislation of the Republic of Kazakhstan on payments, only second-tier banks can issue electronic money on the territory of the country. The following directly arises from the above-mentioned difference. For example, since the issuer of ordinary currency is the National Bank of the Republic of Kazakhstan, which is an affiliate of the country, the obligations on money issued by the National Bank of the Republic of Kazakhstan are guaranteed by the assets of the National Bank of the Republic of Kazakhstan (ZHIENDINOVA, 2016). Therefore, in any case, the person who owns paper money has the right to make claims to the state under the authority of the National Bank of the Republic of Kazakhstan in respect of this type of money, while the obligations on electronic money are secured solely by the issuer of specified electronic money.

Therefore, the owner of electronic money has the right to make requests only to the issuer of electronic money, including for the redemption of the above type of money. The exception is that if the issuer's functions in the electronic money system are performed by several secondary issuing banks, between which netting agreements have been concluded, then these issuers will be jointly and severally liable for the likely risks. Moreover, in this case, the rules related to the circulation of the corresponding electronic money system and the agreements signed between the issuer and the owner of electronic money should explicitly provide for the possibility of filing a claim against any issuer of the electronic money system. A considerable difference between electronic money and conventional money is in

the sphere of circulation, which is why their versatility and turnover possibilities also differ. An ordinary currency is a universal way of paying for certain economic services. Therefore, the owner of a regular currency can use it to pay for any goods or services in Kazakhstan, and the seller (or supplier) will be obliged to accept the specified currency unconditionally. Electronic money is not as universal as paper money since it can only be used to pay for goods and services presented in the electronic money system in circulation. The Law on Payments provides for the possibility of exchanging electronic money for other types of money, but this also does not violate their universality.

According to Law of the Republic of Kazakhstan No. 11-VI "On payments and payment systems" (2016), the possibility of exchanging electronic money for other electronic money is fixed. However, this does not endow this type of money with universality, since they can be exchanged for electronic money of another system, or they can be used solely to pay for goods and services that are available in a particular system of electronic money circulation. Thus, the electronic currency issued by secondary banks of Kazakhstan is the so-called non-fiduciary currency. According to publicly available information, fiduciary money became widely used after its introduction into scientific circulation at the beginning of the 18th century, in parallel with the Bank of England's issuance of banknotes that were not backed by an equivalent amount of gold. Currently, the term fiat money borrowed from American economists is more commonly used, the meaning of which is determined by the Latin word fiat (that is, decree, order). The literal translation of the word fiat is "let it be done". Currently, most of the national currency is legal tender, including tenge, rouble, United States dollar (USA), euro, and other currencies. In general, a fiduciary currency is a paper currency, and its solvency is determined by national legislation. When the economic and political power of the state falls, and trust in it decreases, the value of such money in this country will change. Its value depends on nominal value – the number indicated on the banknote, while the production price of paper money and coins is much lower than their nominal value (MAKHALINA and MAKHALIN, 2019).

When issuing such money, the state solved two tasks – to minimise the costs of issuing currency symbol carriers, while protecting it from counterfeiting to the fullest degree. There is also non-fiduciary money, an example of which can be modern units of value, widely used in electronic payment systems on the Internet. Notably, states and their institutions are in no way responsible for the obligations of electronic money on the Internet. Another difference between conventional currency and electronic money is that the regulator has special restrictions on the owner of electronic currency, while there is no such function for owners of conventional currencies. Electronic currency can be used only by individuals for settlements, individual entrepreneurs and legal entities can accept it only as

payment for goods and services that they provide (in the case of services) or sell (in the case of goods). According to the established rules for the issuance, use, and return of electronic money, and the requirements of issuers of electronic money and electronic money systems in the Republic of Kazakhstan, holders of electronic money are divided into two types: identifiable and unidentifiable. Owners of electronic currencies set restrictions on transactions. Unidentified owners of electronic currencies cannot conduct transactions with electronic currencies, which, in terms of their volume, exceed a hundredfold size of the monthly calculation index set for a particular financial year according to the law of the republican budget (ASHIM and OMAROVA, 2017; GHARAIBEH et al., 2012).

In this case, the issuer is obliged to verify the identity of the specified person following the Law of the Republic of Kazakhstan No. 191-IV "On counteraction of legalisation (laundering) of incomes received by illegal means, and financing of terrorism" (2009). In addition, according to the policy of the regulatory body, in any case, regardless of how much the owner of electronic money owns, they must be of legal age. Therefore, a person under the age of 18 cannot become the owner of electronic money. To conclude, it should be noted that the legal approaches to control the turnover of electronic money are fundamentally different from the approaches to control regular, classical money circulation. In particular, electronic money is not a universal payment method, there are many restrictions for owners and issuers of electronic money, and legislators impose certain obligations on issuers of electronic money to ensure the safety of the electronic money system. It can be stated that the above factors do not contribute to the widespread use of electronic money in the Republic of Kazakhstan. Nevertheless, with the improvement of the legislative framework and the development of online payments, the use of the type of money considered in the framework of this study as a means of payment for goods and services provided will gradually be able to gain the trust of consumers, gain more popularity than now and have a beneficial effect on the economy of the Republic of Kazakhstan.

Above, there was a discussion of the expansion of the use of electronic money in an integral context, that is, as a means of uniting the economic systems of the EAEU member states based on a single currency. It was confirmed that the development of electronic money should be analysed as a factor that creates additional risks for individuals and the entire financial system of the country. The studies mentioned above have shown that the introduction of electronic money systems in economically highly developed countries took place amid two trends in the development of monetary circulation, namely, the reduction of cash turnover and its subsequent replacement with non-cash payments. Moreover, it is necessary to note the replacement of a cash paper loan with a non-cash loan, and

the varieties of the methods of state supervision over electronic money in different countries can be explained by the hope of the management to find the most acceptable solution to the "efficiency/risk" dilemma. Regarding the existing barriers to the full functioning of the turnover of electronic money, many problems can be observed, the elimination of which will entail active development. Notably, the phenomenon considered in the framework of this study should not be considered unique and peculiar to the Kazakh economy exclusively. Firstly, such problems include a low level of trust in electronic money on the part of private consumers and commercial enterprises. Secondly, it is possible to note the existing problems and imperfections of the electronic money systems themselves.

To increase consumer confidence in electronic money and expand its use in Kazakhstan, it is necessary to take a number of the following measures:

(1) It is necessary to supplement the composition of electronic currency issuers with financial organisations that have a license from the National Bank of the Republic of Kazakhstan to use the electronic currency for transactions, since this, undoubtedly, will stimulate competition between issuers and improve the quality of the system and services, which will be facilitated by the spread of electronic money.
(2) In addition to activities for the direct issuance of electronic money, it is necessary to formulate and legislate a list of those operations that can be performed by financial institutions-issuers of electronic money.
(3) It is necessary to carry out minimal, but clear and strict supervision of the issuing institution, which is based on tracking the activities of this type of organisation (namely banks and financial organisations).
(4) It is necessary to increase the transparency of the activities performed by issuers of electronic currencies, for example, to require them to provide a wide range of people with information about the financial condition of the issued electronic currency and the number of obligations assumed, which includes the repayment of electronic money.
(5) To solve the problems arising from the interaction of various electronic money systems, is required to create a single integrator that allows using and accepting electronic money in one system operating in parallel with other systems.

CONCLUSIONS

Electronic money can be characterised as a relatively new phenomenon present in the financial market. The consequence of this is the fact that the supervision of their turnover is still in the process of development. In particular, electronic money considered in the framework of this study is a very promising and actively developing field. Further forecasts regarding the popularisation of the use of this type of finance seem very optimistic, especially considering rapidly developing digital communication technologies and the much higher level of convenience of using electronic money. The consequence of these processes should be considered the growth of online commerce, which will contribute to the development of small and medium-sized businesses, whose activities will have a very favourable and improving effect on the economic system of a particular state, including the economy of the Republic of Kazakhstan considered in the study.

The material offered for review in this article may arouse the interest of specialists in the development of information technologies, for example, to introduce innovations and modern technologies into commercial processes. Furthermore, it will also be of interest to a variety of experts and consultants who, indirectly or personally, influence the decision-making of private or public structures in the field of informatisation of their activities. Notably, many problems were identified during the study. In particular, a very interesting area for further research is to study to what extent different interpretations and definitions of electronic money affect economic processes, and to what extent this factor can influence the growth of this sector in different states. In addition, researchers can focus their attention on further analysis of the generally accepted characteristics of electronic money, which have been considered in this article. In particular, the practical aspect of this issue should be analysed based on unbiased and real statistical information that could illustrate the level of development of the electronic money market in a particular country.

REFERENCES

Abramova, M. A; Dubova, S. Y; Krivoruchko, S. V. (2020). Factors of the development of electronic cash and payment turnover in the EAEU space. *Economics, Finance, and Production Management,* Vol. 3: 3-13.

Afanasyeva, M. A. (2020). Interstate cooperation of the EAEU countries in the digital economy. *Effective Governance: Scientific Almanac in Memory of Professor M. I. Panov,* Vol. 1: 29-41.

Amnazholova, B. A. (2018). Legal regulation of cryptocurrency in the world. *Education and Law***,** Vol. 5: 56-69.

Ashim, A. A; Omarova, A. A. (2017). Prospects for the development of the electronic money market: International experience and its use in Kazakhstan. *Problems of Science***,** Vol. 3: 16-32.

Ayudya, A. C.; Wibowo, A. (2018). The intention to use e-money using theory of planned behavior and locus of control. *Journal of Finance and Banking*, Vol. 22, Issue 2: 335-349.

Blahuta, R. I; Blikhar, V. S; Dufeniuk, O. M. (2020). Transfer of 3d scanning technologies into the practice of criminal proceedings. *Science and Innovation*, Vol. 16, Issue 3: 84-91.

Blahuta, R. I; Kovalchuk, Z. Ya; Bondarchuk, N; Kononova, O; Ilchenko, H. (2019). Financial resources and organizational culture as determinants for competitive strategy of enterprises. *International Journal of Economics and Business Administration*, Vol. 7, Issue 4: 471-482.

Dostov, V. L; Shust, P. M; Alekseev, G. V; Krivoruchko, S. V. (2020). Approaches to regulating the electronic money market in the EAEU: A comparative analysis. *Financial Journal*, Vol. 5: 89-119.

Dzhaksybekova, G. N; Namzhudinova, A. F. (2020). Main trends in the development of new banking products in the republic of Kazakhstan. *Eurasian Union of Scientists, Vol*. 4, Issue 73: 21-29.

Gharaibeh, B; Al-Refaie, A; Goussous, J; Shurrab, M. (2012). Effect of CCMS on customer satisfaction and loyalty in Jordanian banks. *Information (Japan)*, Vol. 15, Issue 12 C: 6227-6237.

Khacaturyan, M. V. (2016). On the problem of managing the risks of integration of the EAEU countries. *Bulletin of the Moscow University of the Ministry of Internal Affairs of Russia*, Vol. 1: 166-168.

Kovalenko, S. B; Shernin, P. G. (2018). Foreign exchange operations of Russian commercial banks: Current state, problems and ways of development. *Bulletin of the Saratov State Social and Economic University*, Vol. 2: 136-143.

Lasme, M; Makoto, K. (2020). Financial inclusion, mobile money, and individual welfare: The case of Burkina Faso. *Telecommunications Policy*, Vol. 44, Issue 3: 49-66.

Law of the Republic of Kazakhstan No. 11-VI. (2016). *"On payments and payment systems".* Available at: https://online.zakon.kz/Document/?doc_id=38213728#pos=3;-106.

Law of the Republic of Kazakhstan No. 191-IV. (2009). *"On counteraction of legitimization (laundering) of incomes received by illegal means, and financing of terrorism".* Available at: https://online.zakon.kz/Document/?doc_id=30466908.

Law of the Republic of Kazakhstan No. 2155. (1995). "*On the National bank of the Republic of Kazakhstan."* Available at: https://online.zakon.kz/Document/?doc_id=1003548.

Law of the Republic of Kazakhstan No. 466-IV. (2011). "*On amendments and additions to certain legislative acts of the Republic of Kazakhstan on electronic money issues."* Available at: https://adilet.zan.kz/rus/docs/Z1100000466.

Leskova, I. V. (2017). Electronic currency: Opportunities for use in the EAEU. *Archon,* Vol. 1: 18-35.

Makhalina, O; Makhalin, V. (2019). Digitalization of the cryptosphere of the EAEU countries: State and prospects. *Vestnik Universiteta,* Vol. 6: 143-149.

Nekhaichuk, D. V; Nekhaichuk, Yu. S; Budnik, S. A. (2019). On the issue of introducing electronic means of payment and electronic money as modern innovative banking technologies. *Bulletin of the Altai Academy of Economics and Law,* Vol. 3, Issue 2: 122-128.

Panova, G. S. (2018). Modern money: Cash and non-cash. *Scientific works of the Free Economic Society of Russia,* Vol. 213, Issue 5: 125-131.

Patashkova, Y; Niyazbekova, S; Kerimkhulle, S; Serikova, M; Troyanskaya, M. (2021). Dynamics of Bitcoin trading on the Binance cryptocurrency exchange. *Economic Annals-XXI,* Vol. 187, Issue 1-2: 177-188.

Poier, S; Nikodemska-Wołowik, A. M; Suchanek, M. (2022). How higher-order personal values affect the purchase of electricity storage—Evidence from the German photovoltaic market. *Journal of Consumer Behaviour,* Vol. 21, Issue 4: 909-926.

Sarsembayev, D. M. (2021). International legal currency regulation in the framework of Eurasian integration (on the issue of a single currency). *Bulletin of the Institute of Legislation and Legal Information of the Republic of Kazakhstan,* Vol. 1, Issue 64: 294-303.

Vozniuk, A. A; Savchenko, A. V; Tarasevych, T. (2020). Electronic money and payments as mean of committing crimes. *Academic Journal of Interdisciplinary Studies,* Vol. 9, Issue 4: 150-159.

Wulandari, D; Soseco, T; Narmaditya, B. S. (2016). Analysis of the use of electronic money in efforts to support the less cash society. *International Finance and Banking, Vol*. 3, Issue 1: 68-83.

Zhiendinova, S. B. (2016). Legal nature of electronic money in Kazakhstan: Comparison with the legal nature of money. *Questions of Modern Jurisprudence,* Vol. 2: 53-72.

The Law, State and Telecommunications Review / Revista de Direito, Estado e Telecomunicações

Contact:
Universidade de Brasília - Faculdade de Direito - Núcleo de Direito Setorial e Regulatório
Campus Universitário de Brasília
Brasília, DF, CEP 70919-970
Caixa Postal 04413

Phone: +55(61)3107-2683/2688

E-mail: getel@unb.br

Submissions are welcome at: https://periodicos.unb.br/index.php/RDET

Sobre Fronteiras, Cavalos e *Gatekeepers*: A Evolução do Debate sobre Interoperabilidade e Acesso às Redes no Direito Cibernético

About Borders, Horses and Gatekeepers: The Evolution of Interoperability and Networks Access Debate in Cyberlaw

Submitted: 7 October 2022
Reviewed: 2 November 2022
Revised: 6 November 2022
Accepted: 8 November 2022

Article submitted to blind peer review

Fábio Casotti*
https://orcid.org/0000-0003-2641-4570

DOI: https://doi.org/10.26512/lstr.v15i2.45341

Abstract

[Purpose] *To characterize the evolution of the regulatory debate on interoperability and network access in the evolutionary course of the Internet.*

[Methodology] *Based on bibliographical research on the academic publications of cyberlaw and study cases in the United States and Europe, the objectives and the role played by network access regulation are identified.*

[Findings] *From little or no regulatory concern in the early beginning of the Internet, interoperability converts itself into a relevant issue from the identification of the power asymmetries of the network participants, some of them being able even to limit or prevent the free flow of information, then the concept of gatekeeper arises. With the reorientation of the bargaining powers of the Internet supply chain, greater attention has been given to the content and application layer. Despite the challenges inherent to the sustainability of highly prescriptive regulatory designs, guarantees of interoperability are fundamental to the free flow of ideas, data and information, capable of preserving a free, plural and open to innovation Internet.*

Keywords*: Gatekeeper. Interoperability. Network Access. Cyberlaw. Internet Regulation.*

Resumo

[Propósito] O artigo busca caracterizar a evolução do debate regulatório de interoperabilidade e acesso às redes na trajetória evolutiva da Internet.

*Pós-graduado em Planejamento e Estratégias de Desenvolvimento (ENAP/2018), especializado em Regulação Econômica (INATEL/2011) e Engenheiro de Telecomunicações (UNI-BH/2006). Servidor público da Agência Nacional de Telecomunicações (ANATEL) desde 2005. E-mail: fcasotti@gmail.com.

[Metodologia] A partir de uma pesquisa bibliográfica sobre a produção acadêmica de direito cibernético e estudos de caso nos Estados Unidos e na Europa, são identificados os objetivos e o papel desempenhado pela regulação das condições de acesso às redes.
[Resultados] De pouca ou nenhuma preocupação regulatória no surgimento da Internet, a interoperabilidade se converte em uma questão relevante a partir da identificação da assimetria de poderes dos participantes das redes, alguns inclusive com capacidades para limitar ou impedir o fluxo de informações, surge então o conceito de *gatekeeper*. Com a reorientação de poderes de barganha da cadeia produtiva da Internet, maior atenção tem sido conferida à camada de conteúdos e aplicações. Apesar de desafios inerentes à sustentabilidade de desenhos regulatórios muito prescritivos, garantias de interoperabilidade se mostram fundamentais à livre circulação de ideias, dados e informações, capazes de preservar uma Internet livre, plural e aberta à inovação.

Palavras-Chave: *Gatekeeper*. Interoperabilidade. Acesso às Redes. Direito Cibernético. Regulação da Internet.

INTRODUÇÃO

Em meados do século XIX, a pacata cidade de Erie, no extremo noroeste do estado da Pensilvânia, foi palco de um marcante episódio na história da indústria ferroviária dos Estados Unidos, a chamada "*War of the Gauges*" ou, segundo tradução livre, a Guerra da Bitola dos Trilhos.

Conforme Kent (1948), o embate marcou disputa entre os estados da Pensilvânia e de Nova York quanto ao padrão construtivo escolhido para os trilhos ferroviários que se conectavam na região. Na ocasião, estavam em discussão três padrões de distância entre os trilhos da rede ferroviária em expansão na região (4'10", 6" e 4'8½").

Com a "quebra de padrões" ou descontinuidade existente entre os trilhos que se interconectavam na cidade de Erie, havia a necessidade inconveniente de migração de pessoas e cargas entre as diferentes composições dos trilhos, gerando atrasos, ineficiências e vários transtornos.

Ainda segundo Kent (1948), o conflito foi deflagrado com uma aparente quebra de promessa do estado Nova York quanto à bitola escolhida para os trilhos já em construção pela Pensilvânia. Os munícipes e empresários locais de Erie se insurgiram contra a construção impositiva de uma bitola distinta da avençada e o que começou com pequenas hostilidades aos funcionários da ferrovia, rapidamente escalou à destruição de ruas, ferrovias e pontes de ligação, redundando em agressões físicas e prisões. A Guerra da Bitola dos Trilhos chegou a interromper por duas semanas o tráfego ferroviário de Nova York com o Oeste norte-americano.

Na repercussão midiática, chegou-se a atribuir ao conflito a zombaria de revolta de vendedores de amendoim e tortas, irresignados com a iminente

padronização e a consequente frustração de vendas de produtos, que ocorria durante a troca de vagões. Na verdade, o tensionamento envolvia uma disputa comercial de eficiências e competitividade das rotas de transporte ferroviário, notadamente, o protagonismo e o domínio econômico sobre um modal estratégico de circulação de pessoas para o meio oeste, no eixo Ohio-Pensilvânia-Nova York.

Depois de aproximadamente dois anos, a Guerra da Bitola dos Trilhos de Erie foi objeto de acordo político-empresarial entre os governadores e as ferrovias. Além disso, toda a malha norte-americana passaria mais tarde por uma política pública de convergência em torno de um único padrão de bitola ferroviária, 4'8½" (quatro pés e oito polegadas e meia).

À primeira vista, este prosaico episódio pode parecer tão desconectado das discussões de direito cibernético quanto os padrões de bitola de trilhos de Erie. No entanto, para um olhar atento, este exemplo material e concreto, tão simples quanto a distância entre os trilhos concorrentes de uma ferrovia, ilustra como padrões de acesso e conexão são aspectos críticos para indústrias de redes.

Para essa dinâmica de indústrias, aspectos de interoperabilidade são estratégicos para as dinâmicas de desenvolvimento e poderes de barganha envolvidos, podendo inclusive esconder sob o manto de narrativas técnicas e assépticas, alavancas de poder de mercado, que distanciam o mercado de condições de competição sustentadas apenas no mérito dos agentes participantes da indústria.

Conforme se pretende desenvolver a seguir, essa questão se revela particularmente crítica em um contexto de erosão de fronteiras jurisdicionais de aplicação do direito, inquietações sobre a necessidade de um regime jurídico próprio e diante de poder acumulado por gigantes controladores do fluxo informacional (*gatekeepers*) no novo paradigma da economia digital.

Com esse objetivo, o presente estudo busca identificar e sistematizar a evolução do debate do acesso a redes e interoperabilidade do direito cibernético (*cyberlaw*), a partir da literatura e estudos de caso nos Estados Unidos e Europa.

Dessa forma, o texto segue organizado da seguinte forma, buscando sempre que possível a delimitação cronológica dos grandes períodos de desenvolvimento da Internet. Inicialmente é feito um resgate dos primeiros tensionamentos jurídicos de acesso às redes que marcaram o surgimento comercial da Internet. Em seguida, se evolui para o entendimento das relações de poder no ambiente cibernético e a importância das condições de conexão. A terceira parte do artigo se dedica ao desenvolvimento sobre a reorientação do poder de *gatekeeper* e as primeiras respostas regulatórias já observadas. Por fim, são apresentadas na seção final as considerações finais do estudo.

DO VELHO OESTE DIGITAL AO CIBERPATERNALISMO

Nas origens, ainda enquanto um experimento recém-saído de laboratórios de centros de pesquisa e campi universitários, a Internet apresentava um ideário de abertura, liberdade, colaboração e ausência de qualquer controle ou moderação na circulação de informações.

Conforme Zittrain (2008, p. 8, 27, 30), o desenvolvimento da rede não estava orientado à oferta de serviços e aplicações específicas (quiçá negócios), mas sim, ao simples objetivo de conectar pessoas a quaisquer outros indivíduos. E teria sido justamente essa despretensiosa visão de seus fundadores a razão crítica para o sucesso da rede. Isto é, onde ninguém era particularmente dono e estariam todos interessados em acessar e se interligar, a Internet nasceu e se organizou à margem do conhecimento daqueles com poderes e capacidades para restringir seu desenvolvimento.

Esse espírito aberto e libertário vigorou dos anos 1980 até a primeira metade dos anos 1990, encerrando a chamada era do "velho oeste da Internet".

Mas com os primeiros ensaios da fase comercial da Internet, têm início então os primeiros tensionamentos e discussões acadêmicas quanto à ilegitimidade ou inabilidade de governos do "mundo real" disciplinarem a conduta de seus cidadãos no espaço cibernético (MURRAY, 2011, p. 197,198).

Com a experimentação de várias aplicações de comunicação e compartilhamento de arquivos, acompanhada de um processo acelerado de ampliação da rede e do número de seus participantes, ficaram evidentes as dificuldades de respostas jurídicas adequadas e suficientes para lidar com dilemas de privacidade, problemas de difusão de conteúdos impróprios ou mesmo violações sistemáticas de direitos de propriedade e autoria intelectual.

Com efeito, esses tópicos ainda seguem desafiando acadêmicos e operadores do direito a sua correta compreensão e tratamento, inclusive com novos desdobramentos que só se agravaram (em volume ou complexidade). Para citar alguns rápidos exemplos contemporâneos, a divulgação massiva de notícias falsas, o grau de coleta e processamento de dados pessoais, o poder econômico das plataformas digitais, com repercussões nada triviais sobre a tutela de direitos à privacidade, à dignidade, o bem-estar econômico, a saúde das democracias e, no limite, a organização social contemporânea.

Mas ainda na segunda metade dos anos 1990, a capacidade prospectiva de autores referenciais como Joel Reidenberg e Lawrence Lessig já indicava que o modelo de "uma terra sem lei" na Internet seria um ambiente fértil à prática de atividades nocivas e ilícitas das mais variadas. Esses autores integraram o movimento que Murray (2011, p. 199) denominou paternalismo cibernético.

Em trabalho pioneiro sobre os desafios de gestão das redes e regulação no ciberespaço, Reidenberg (1996, p. 913-915) estruturou o reconhecimento da desintegração dos paradigmas tradicionais de direito, os quais foram historicamente lastreados na presença física e em territórios geográficos muito bem delimitados. Defendeu que a fluidez transnacional de informações seria capaz de comprometer as soberanias estatais e suas capacidades de regulação e fiscalização de comportamentos de seus cidadãos.

Sustentou ainda que, em substituição às fronteiras físicas, surgiam no ciberespaço novas jurisdições, não demarcadas por geografias físicas, mas pela arquitetura de rede dos provedores de serviços participantes da Internet, que passariam a ditar a dinâmica de acesso e o grau de interoperabilidade, a partir dos contratos privados (REIDENBERG, 1996, p. 917).

Em destaque, os controladores das redes assumem características políticas de entidades autogovernadas, com poderes para impor a seus participantes suas regras de acesso, comportamento e "cidadania" (REIDENGER, 1996, p. 919).

Na continuidade de seus estudos, Reidenberg (1998) identificou um espaço de normatividade inerente às escolhas técnicas e ao desenvolvimento da arquitetura Internet, ao que denominou *Lex Informatica.* No tocante à compatibilidade entre redes e sistemas, defendeu a aplicação do *soft law* da *Lex Informatica* como mais adequada para lidar com questões de interoperabilidade da Internet, quando comparada à abordagem rígida e estanque do regime jurídico tradicional (REIDENGER, 1998, p. 587).

Mas o movimento paternalista digital dos anos 1990 não foi livre de críticas. Talvez a mais ácida e icônica tenha sido a proferida pelo juiz norte-americano Frank H. Easterbrook.

O Direito do Cavalo

Em conferência sobre o direito cibernético realizado na Universidade de Chicago e posteriormente publicado na forma de artigo no fórum universitário, assim se pronunciou Easterbrook (1996):

> "Quando ele era diretor desta Faculdade de Direito, Gerhard Casper era orgulhoso do fato de que a Universidade de Chicago não oferecia um curso de 'Direito do Cavalo'. [...] Em vez de oferecer cursos adequados a diletantes, a Universidade de Chicago oferecia cursos de Direito e Economia, Direito e Literatura, ministrados por pessoas que poderiam ser nomeadas para os principais departamentos de economia e literatura do mundo [...]
>
> Corremos o risco do diletantismo multidisciplinar, ou [...] da esterilização cruzada de ideias. Junte dois campos sobre os quais você sabe pouco e obtenha o pior dos dois mundos. [...] As crenças que os advogados têm sobre computadores e as previsões que eles fazem sobre novas tecnologias são

> altamente prováveis de serem falsas. Isso deve nos fazer hesitar em prescrever adaptações legais para o ciberespaço.
>
> [...] a melhor maneira de aprender a lei aplicável a empreendimentos especializados é estudar as regras gerais. Muitos casos tratam da venda de cavalos; outros lidam com pessoas que tomaram coices de cavalos; ainda lidam com o licenciamento e corridas de cavalos, ou com os cuidados veterinários com os cavalos, ou com prêmios em exposições de cavalos. Qualquer esforço para reunir esses fios em um curso sobre 'A Lei do Cavalo' está fadado a ser superficial e a perder princípios unificadores.
>
> [..] Não sei muito sobre ciberespaço; o que eu sei estará desatualizado em cinco anos (senão em cinco meses!); e minhas previsões sobre a direção da mudança são inúteis, tornando fútil qualquer esforço para adaptar a lei ao assunto. [...]
>
> Um rápido resumo: Errar na legislação é comum, e especialmente quando a tecnologia avança a galope. [...] Então deixemos o mundo do ciberespaço evoluir como quiser e aproveitemos os benefícios." (tradução livre)

Na construção de seu argumento, o juiz Easterbrook evoca esse icônico animal, símbolo de velocidade e vigor físico, parceiro da humanidade na evolução e na domesticação do ambiente ao seu redor. Com efeito, desde as sociedades primitivas, os cavalos eram empregados na agricultura, no transporte, na conquista de territórios, nas guerras e, posteriormente, serviu de principal força motriz do maquinário e dos meios de transporte do século XIX.

Apesar de não ter merecido uma disciplina jurídica específica na Universidade de Chicago, esse nobre equino já esteve envolvido em um par de questões regulatórias curiosas ao longo da história humana. Para citar alguns exemplos rápidos, recorre-se inicialmente a um drama urbanístico vivido por grandes cidades como Londres e Nova York ao final do século XIX e que motivou intensos debates regulatórios sobre o futuro do desenvolvimento dessas metrópoles. Com o emprego majoritário de tração animal no transporte de cargas e pessoas no período, havia um grande desafio logístico e sanitário para a grande quantidade de dejetos animais gerados pela superpopulação equina, ainda que empregando novamente o transporte animal no manejo ambiental necessário[1]. Essa questão específica só foi superada com a mudança do paradigma dos meios de transporte para motores a vapor, o que reposicionou o desafio ambiental para questões regulatórias de emissão de outros poluentes, inicialmente, a queima do carvão e, posteriormente, de combustíveis fósseis.

E justamente nesse período de substituição massiva da tração animal pelos motores a vapor, quando da primeira revolução industrial, o *horse-power* (HP) foi empregado como padrão de comparabilidade de potência e, mesmo hoje, segue

[1] The Great Horse Manure Crisis of 1894 by Ben Johnson. Historic UK.

sendo um padrão *de facto* para a aferição de potência de motores a combustão ou elétricos. Para trazer uma última situação mais atual, novamente a cidade de Nova York apresenta hoje para o transporte turístico de carruagens a cavalo uma regulação bastante prescritiva sobre jornadas de trabalho máximas permitidas, padrões de equipamentos e cuidados sanitários, com fito em assegurar a segurança do transporte para condutores e turistas, a saúde e o bem-estar dos animais[2].

Partindo da iconografia do argumento de Easterbrook, essas ilustrações não seriam exemplos aplicados de diferentes leis (ou direito) do cavalo?

Com a devida vênia por essa breve digressão equina, para além do título, este artigo não se pretende à justa homenagem a esse utilitário e valoroso animal. Neste exato ponto, o propósito consiste em um alerta quanto à armadilha argumentativa oferecida por diagnósticos tão absolutos e, por vezes, simplificados por analogias incompletas ou imperfeitas.

Costumeiramente, a defesa de princípios de não intervenção regulatória se faz acompanhar de uma crença quase dogmática no longo prazo. Contudo, para algumas conjunturas específicas, essa espera pode ser revelar excessivamente danosa, citando a célebre frase atribuída ao economista britânico John Maynard Keynes, "no longo prazo estaremos todos mortos".

Retomando ao paradigma do direito cibernético, as indústrias da informação não podem ser adequadamente compreendidas a partir da mera comparação com outras indústrias tradicionais, que lidam com quaisquer tipos de mercadoria (WU, 2012, p. 427). Trata-se da tecnologia de mais rápida difusão e adesão entre todas as outras formas de comunicação da história (CASTELLS, 2017, p. 36).

Há inclusive provisões mais arrojadas de que o novo paradigma da revolução industrial das Tecnologias da Informação e Comunicação - TICs seja capaz de reconfigurar o paradigma econômico capitalista dominante (RIFKIN, 2014).

Dessa forma, tem sido exigido cada vez mais dos juristas um entendimento acurado e multidisciplinar para as questões do direito cibernético, a fim de lidar com a velocidade de transformações sociais ocorridas e os desafios jurídicos apresentados por essa nova conformação.

Em resposta específica à contribuição de Easterbrook, Lessig (1999) defende exatamente a conexão entre o direito e o espaço cibernético, em particular, os benefícios do emprego integrado de ferramentas do direito tradicional com outras ferramentas também capazes de constranger comportamentos (normas sociais, mercados e a arquitetura ou código).

[2] Caring for Horses Working in NYC. Rules of the City of New York. Title 24 - Department of Health and Mental Hygiene. Chapter 4 - Health, Safety And Well-Being Of Rental Horses.

No desenvolvimento e na complexificação dessa teoria, Lessig (2006) desenvolve então o *CODE*. Nessa publicação, o autor busca descontruir o pensamento anárquico inicial do ciberespaço, oferecendo em substituição uma perspectiva orientada à arquitetura da Internet, que fosse capaz de aperfeiçoar o controle de comportamentos por meio da "mão invisível do ciberespaço". Na visão de Lessig, "*code is law*", isto é, o algoritmo (ou o código) seria a lei suficiente e necessária ao constrangimento de condutas.

Neste primeiro recorte temporal, restou demonstrado como os integrantes da Internet são capazes de constituir novos ambientes digitais "quase soberanos" e com poderes para fixar suas próprias regras de entrada e convivência. Sobre interoperabilidade, não se identificaram grandes questões, pois a necessidade de ligação entre redes prevalecia como um dos valores fundacionais da própria Internet e a aderente à dinâmica de incentivos prevalecente.

As principais discussões então se pautaram pelo reconhecimento desse novo paradigma técnico-econômico e a necessidade ou dispensa de um novo regime jurídico para lidar com as questões comportamentais nascentes. Os principais tensionamentos orbitaram dilemas informacionais e violações a direitos de propriedade e autoria, a partir de características intrínsecas à Internet, como a fácil reprodutibilidade e acelerada difusão de conteúdos eletrônicos, o que habilitou e reduziu substancialmente os custos dessa natureza de ilícito.

Contudo, na tentativa de fornecer soluções de constrangimento de comportamentos desviantes no ciberespaço, o ciberpaternalismo ainda teria se mantido demasiadamente concentrado no aspecto geográfico e talvez até em virtude de algum otimismo da visão de Lessig, teria deixado escapar o mapeamento preciso do poder de influência não uniforme dos integrantes da rede, em especial, a capacidade de controlar ou influenciar fluxo da informação, os *gatekeepers* (MURRAY, 2011, p. 213).

Conforme desenvolvimento a seguir, essas discussões ganham contornos mais sutis e interessantes a partir do mapeamento das condições não uniformes de poder, interesses e influência de cada agente participante da Internet. Pois conforme a lição de Castells (2017, p. 36), os processos de desenvolvimento e adesão a novas tecnologias não são livres e autônomos, mas sim, objeto de modificação e adequação aos desejos e necessidades das pessoas, além de influências culturais, da organização social e o ambiente institucional onde estão inseridos.

A INTERNET DA CHAPEUZINHO VERMELHO E OS "LOBOS MAUS" DO MUNDO CORPORATIVO

Inspirado em modelos de Governança Nodal, Murray (2011, p. 204) propõe uma visão regulatória responsiva às dinâmicas comunicativas entre os integrantes da rede, reconhecendo o poder de influência desses agentes.

O autor confere especial destaque ao poder do discurso, do diálogo e dos fluxos de comunicação no ambiente cibernético em seu processo regulatório. Se cada integrante é individualmente capaz de partilhar ideias, crenças, ideais e formar opiniões, eles podem se associar em comunidades com interesses convergentes, com habilidades para legitimar ou esvaziar diferentes ações regulatórias. Ignorar essa dinâmica é contribuir com a frustração e a perda de efetividade de quaisquer tentativas de regulação (MURRAY, 2011, p. 205-207).

Prossegue Murray (2011, p. 212) argumentando como os pontos de convergência entre várias comunidades e grupos de interesse são capazes de controlar o fluxo informacional da Internet, sistematizando uma proposta conceitual de *gatekeepers*.

Em alusão ao trabalho de Laidlaw (2010, p.2), tem-se o gênero agregado de *gatekeepers* (guardiões dos portões) como entidades capazes de decidir o que deve ou não passar por um determinado portão de controle. Em destaque, a percepção da autora de que para aquela natureza de preocupações o *gatekeeper* não estaria em condições de se locupletar com más condutas, mas estaria sim em posição de evitar que elas ocorressem. Daí o acionamento de *gatekeepers* por autoridades regulatórias como mecanismo indireto de constrangimento ao desvio de conduta de terceiros.

No processo de governança cibernética, a dificuldade ou mesmo a inviabilidade de governos constrangerem diretamente as condutas de indivíduos tem levado as autoridades regulatórias a confiar progressivamente em *gatekeepers* como entes delegados de controle de atividades nas redes (MURRAY, 2011, p. 213).

No ambiente cibernético, os *gatekeepers* da Internet controlam o fluxo informacional da rede, podendo inclusive no processo de controle apresentar repercussões culturais e democráticas (LAIDLAW, 2010, p.2).

Mas superando a inocência do ciberpaternalismo, que presume a distribuição equitativa de poderes dos participantes da rede, Murray (2011, p. 220) reconhece o poder assimétrico dos *gatekeepers*, com capacidades únicas de controle de acesso a determinados espaços, comunidades ou conteúdos.

Interessa notar como a proposição diagnóstica de Murray (2011) tangencia conceitos próprios da economia industrial e instrumentais importantes da defesa

e promoção da concorrência, como as externalidades de redes[3] e o poder de mercado[4].

De fato, com a maturação e o desenvolvimento acelerado da fase comercial da Internet, essa perspectiva econômica-empresarial vai se tornando cada vez mais relevante, sobretudo após o estouro da bolha especulativa das empresas ponto com e a primeira década dos anos 2000.

Conforme o provocador enunciado de Manuel Castells (2017, p. 167), trata-se do encontro da Internet da Chapeuzinho Vermelho com os "lobos maus" do mundo corporativo. Isto é, o processo de desenvolvimento das Tecnologias da Informação e Comunicação - TICs é dependente de decisões políticas, resultados de debates e conflitos entre grupos de interesses comerciais, sociais e políticos (p. 153).

De fato, com o advento da convergência tecnológica entre diferentes plataformas de redes, habilitou-se um processo acelerado de massificação do acesso à Internet por meio da utilização das redes de operadoras de cabos e de telefonia e, posteriormente, de redes móveis sem fio.

Diferentemente de um despretensioso empreendimento científico e experimental de suas origens, a Internet passava agora a integrar um intrincado "ecossistema" de Tecnologias da Informação – TICs. Conforme a visão esquemática oferecida por Fransman (2010), os agentes do "ecossistema de TICs" compreendem então quatro grandes as camadas de relações simbióticas, a saber, os fabricantes de equipamentos de redes, operadores de redes, provedores de conteúdo e aplicações e os consumidores finais.

Figura 1 – Relações entre as Camadas de Fransman (2010).

[3] Quando o valor da associação de um usuário a uma rede é afetado positivamente quando outro usuário se associa e amplia essa rede, diz-se que esses mercados exibem "efeitos de rede" ou "externalidades de rede" (KATZ e SHAPIRO, 1994).

[4] O poder de mercado refere-se à habilidade de uma firma elevar preços de maneira lucrativa acima de algum nível competitivo, o nível de referência, sendo usualmente definido como a diferença entre os preços cobrados pela empresa e seus custos marginais de produção (MOTTA, 2004).

Contudo, o registro histórico da indústria de comunicações nos Estados Unidos oferece justificativas de sobra às preocupações com os ricos de apropriação corporativa e influências restritivas ao desenvolvimento da Internet. No *lócus* de convergência das redes Internet com as redes de cabo e telefonia, os estudiosos do direito cibernéticos apontavam para o iminente choque entre os valores intrínsecos à Internet e a cultura corporativa das indústrias da telefonia e do cabo nos Estados Unidos. Em especial, a trajetória do conglomerado Bell no século XX.

Os Guardiões dos Circuitos contra Dispositivos Estranhos

Nesse contexto, tem-se o curioso caso da *Hush-A-Phone Corporation*, que lançou nos idos do século XX um intrigante acessório telefônico plástico com a promessa de conferir maior privacidade às chamadas telefônicas. Desenvolvido na forma de uma concha e acoplável ao bocal de telefones fixos, o dispositivo apresentava de fato propriedades acústicas capazes de oferecer maior ressonância à voz de seu utilizador (WU, 2012, p. 145).

Curiosamente, apesar do questionável potencial de dano do inocente acessório, os seus desenvolvedores enfrentaram uma virulenta resposta do poderoso conglomerado norte-americano Bell, materializada em sucessivas demandas administrativas e judiciais, sob a alegação de inefetividade do dispositivo, riscos à operação da rede e até mesmo à higiene sanitária dos utilizadores. Funcionários da AT&T chegaram a notificar os consumidores de telefonia de que o uso do produto *Hush-A-Phone* seria passível de violação da legislação federal, com riscos de suspensão da prestação do serviço de telefonia (WU, 2012, p. 145).

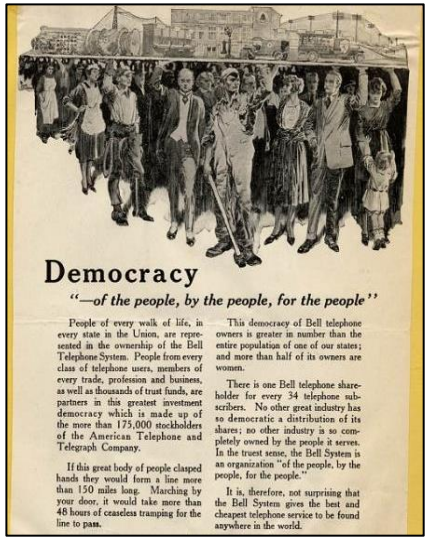
Além de uma agressiva abordagem de fusões e aquisições, cabe destacar que parcela relevante do sucesso empresarial alcançado pela AT&T no século XX se deveu a uma estratégica de marketing e comunicação escorada em narrativas de centralização, unificação e universalização da rede de telefonia, o que fica refletido em seu próprio lema corporativo do período: "Uma política, um sistema, serviço universal, e todos direcionados para o Melhor Serviço." (tradução livre) (WIRED, 2011, p. 10).

Tem-se o interessante registro da audiência pública promovida pelo regulador de comunicações norte-americano, a FCC (*Federal Communications Commission*) com o objetivo de debater os supostos danos causados pela utilização do *Hush-A-Phone*. Na ocasião, o então vice-presidente da AT&T, sustentando um veto à utilização de "acessórios telefônicos estranhos", evocou a necessidade de tutela do consumidor contra o risco de "parafernálias inúteis" e ainda argumentou, com uma dose de presunção corporativa, que caso houvesse

alguma utilidade efetiva para o *Hush-A-Phone*, a própria AT&T já o teria inventado e disponibilizado ao mercado (WU, 2012, p. 154).

A questão fundamental de uma abordagem de inovação centralizada é que ela está fadada a admitir a invenções incrementais e abandonar ideias disruptivas, especialmente aquelas com o mínimo potencial de dano, ameaça ou revolução dos negócios estabelecidos (WU, 2012, p. 154).

De modo a ilustrar esse ideal corporativo, seguem trechos de peças publicitárias do período que refletem exatamente uma narrativa de controle centralizado, de uma estrutura industrial monopolística tutelada pelo governo norte-americano e fechada a inovações externas.



Democracy

"—of the people, by the people, for the people"

People of every walk of life, in every state in the Union, are represented in the ownership of the Bell Telephone System. People from every class of telephone users, members of every trade, profession and business, as well as thousands of trust funds, are partners in this greatest investment democracy which is made up of the more than 175,000 stockholders of the American Telephone and Telegraph Company.

If this great body of people clasped hands they would form a line more than 150 miles long. Marching by your door, it would take more than 48 hours of ceaseless tramping for the line to pass.

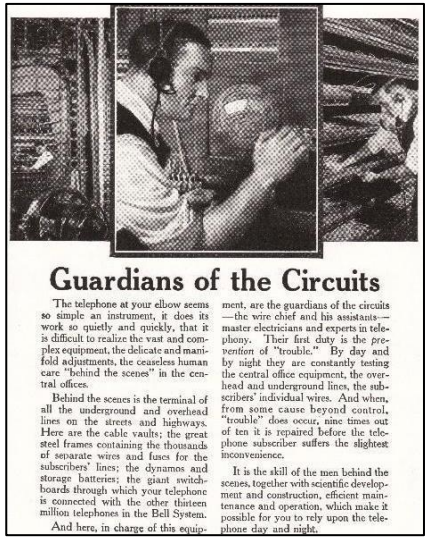
This democracy of Bell telephone owners is greater in number than the entire population of one of our states; and more than half of its owners are women.

There is one Bell telephone shareholder for every 34 telephone subscribers. No other great industry has so democratic a distribution of its shares; no other industry is so completely owned by the people it serves. In the truest sense, the Bell System is an organization "of the people, by the people, for the people."

It is, therefore, not surprising that the Bell System gives the best and cheapest telephone service to be found anywhere in the world.

"Pessoas de todas as esferas da vida, em todos os estados da União, estão representadas na propriedade do Sistema Telefônico Bell. [...] são sócios desta democracia de maior investimento que é formada pelos mais de 175 mil acionistas da *American Telephone and Telegraph Company*." (tradução livre)

Figura 2 – A Democracia do Sistema Bell (1921).



Guardians of the Circuits

The telephone at your elbow seems so simple an instrument, it does its work so quietly and quickly, that it is difficult to realize the vast and complex equipment, the delicate and manifold adjustments, the ceaseless human care "behind the scenes" in the central offices.

Behind the scenes is the terminal of all the underground and overhead lines on the streets and highways. Here are the cable vaults; the great steel frames containing the thousands of separate wires and fuses for the subscribers' lines; the dynamos and storage batteries; the giant switchboards through which your telephone is connected with the other thirteen million telephones in the Bell System.

And here, in charge of this equipment, are the guardians of the circuits —the wire chief and his assistants—master electricians and experts in telephony. Their first duty is the *prevention* of "trouble." By day and by night they are constantly testing the central office equipment, the overhead and underground lines, the subscribers' individual wires. And when, from some cause beyond control, "trouble" does occur, nine times out of ten it is repaired before the telephone subscriber suffers the slightest inconvenience.

It is the skill of the men behind the scenes, together with scientific development and construction, efficient maintenance and operation, which make it possible for you to rely upon the telephone day and night.

"O telefone ao seu lado parece um instrumento tão simples, faz seu trabalho de forma tão silenciosa e rápida, que é difícil perceber o equipamento vasto e complexo, os ajustes delicados e múltiplos, o incansável cuidado humano "nos bastidores" dentro das centrais telefônicas. [...] É a habilidade dos homens nos bastidores, juntamente com o desenvolvimento e construção científica, manutenção e operação eficientes, que permitem que você conte com o telefone dia e noite." (tradução livre)

Figura 3 – Os Guardiões dos Circuitos (1922).

Oito anos depois da primeira demanda administrativa apresentada à FCC, a *Hush-A-Phone Corporation* prevaleceu perante a AT&T no Tribunal de Apelação Federal. Obviamente, essa batalha administrativa-jurídica foi muito mais penosa para o inventor do *Hush-A-Phone* do que para o conglomerado Bell.

E esse teria sido apenas o primeiro de vários enfrentamentos contra o uso de outros acessórios e condições de acesso às redes, evidenciando a disposição em litigar administrativa e judicialmente do sistema Bell (*Bellheads*) em face daqueles que viriam posteriormente a suportar um modelo de desenvolvimento aberto da Internet, capaz de oferecer soluções mais inovadoras (*Netheads*) (WU, 2012, p. 156, 162).

Anos mais tarde, de 1974 a 1982, em face do poder acumulado pelo sistema Bell, o conglomerado passou por processo de desmembramento estrutural, um caso paradigmático para a história do antitruste nos Estados Unidos.

Mas este episódio do *Hush-A-Phone* denota o quão antigas são as tentativas de discriminação ou restrição das regras de conexão e acesso. E para indústrias de redes, tanto infraestruturas duras e tradicionais (*utilities*) como ferrovias, rodovias, cabotagem e aeroportos, quanto para as infovias de telefonia e comunicação, as condições de acesso e os padrões de interoperabilidade são críticos à saúde e ao bom desenvolvimento de mercados.

Não por acidente, no contexto da globalização e abertura dos mercados nos anos 1990, as reformas legislativas de vários países trouxeram além da previsão da participação da iniciativa privada na indústria de telecomunicações, fortes

compromissos comerciais e regulatórios de um regime compulsório de interconexão e abertura das redes incumbentes (LAFFONT e TIROLE, 1996).

Nesse ponto da história, com o advento da convergência tecnológica, as culturas das indústrias de redes de telefonia, de cabo e da Internet (agora comercial) se chocaram e produziram um grande embate sobre quem teria o efetivo poder de *gatekeeper*, isto é, a condição de controlar ou restringir o livre fluxo de informações.

A seguir, um dos mais aquecidos debates político-regulatórios e de governança cibernética, a discussão sobre neutralidade de redes (VAN SCHEWICK, 2010, p. 1).

Ser Neutro ou Não Ser, Eis a Questão

Atribui-se a Tim Wu (2003) o protagonismo pela sistematização de preocupações concorrenciais sobre condutas discriminatórias de conteúdos e aplicações no ambiente cibernético, o que viria a se cristalizar no conceito regulatório de neutralidade de rede.

Wu (2003, p. 141-143) argumentou sobre o tensionamento instalado entre os operadores de redes provedores de acesso à Internet e os provedores de conteúdos e aplicações. Alegou haver evidências de condições contratuais ou escolhas de arquitetura de rede limitadoras de certas classes de aplicações, ameaças de banimento de tecnologias emergentes, riscos de distorcer os mercados e, no limite, comprometer o desenvolvimento e a essência inovadora da Internet.

De fato, a exemplo do ceticismo já instalado com posturas oportunistas da indústria de telefonia norte-americana desde o século XX, a primeira década do século XXI foi marcada por atritos envolvendo a oferta de serviços de telefonia pela Internet na forma de pacotes (VoIP – *voice over Internet Protocol*), a tecnologia considerada aplicação matadora para o período (*killer application*).

Conforme Lessig (2005), o "primeiro tiro" da mais importante guerra da Internet teria sido disparado pela FCC em março daquele ano, ao determinar que uma operadora regional suspendesse o bloqueio de seus consumidores que utilizaram serviços de VoIP. Na provocação de Lessig, isso teria convertido o dirigente máximo da FCC da época em um "herói improvável" na defesa dos direitos de liberdade na rede, de acesso a conteúdos e aplicações inovadoras na Internet.

Realmente, as preocupações de que ofensas à interoperabilidade prejudicassem o ambiente de competição e inovação no mercado de conteúdo e aplicativos da Internet trouxeram reflexões sobre a necessidade de disciplinar previamente as condutas (YOO, 2005, p. 3).

O discurso sobre a manutenção do livre acesso às redes e de efetiva interoperabilidade se conectou ao discurso de plataformas e abordagens de inovação abertas e o fomento a tecnologias consideradas disruptivas.

No dizer de Tim Wu (2003, p. 146, 149):

> "Uma rede de comunicações como a Internet pode ser vista como uma plataforma para uma competição entre desenvolvedores de aplicativos. [...] Portanto, é importante que a plataforma seja neutra para garantir que a concorrência continue meritocrática.
>
> [...] a operadora é, em última análise, a guardiã da qualidade de serviço para um determinado usuário, porque somente a operadora de banda larga está em condições de oferecer garantias de serviço que se estendem ao computador (ou rede) do usuário final."

A proposição inicial de Wu (2003, p. 165) foi um "princípio de antidiscriminação (uma regra, apenas se necessário)" e a defesa do equilíbrio entre, de um lado, banir restrições danosas e, do outro, preservar a liberdade geral dos operadores realizarem a gestão de tráfego em seus domínios de rede, ao passo que "indícios de restrições baseadas na interconexão entre redes devem ser vistas com suspeição".

A despeito dessa visão mais funcional e principiológica apresentada inicialmente por Wu, o que se sucedeu foi uma difusão de marcos legais (alguns bastante prescritivos) catalisada por algum ativismo legítimo de direitos digitais e liberdade na Internet.

Importante também reconhecer o apoio conferido pela conformação de grandes interesses privados da camada de conteúdos e aplicações, por exemplo, os conflitos pela remuneração de rede e responsabilidade pela entrega de conteúdo audiovisual entre os operadores de rede nos Estados Unidos e o Netflix (KASTRENAKES, 2017).

Na cena acadêmica, o grau de intervenção regulatório necessário a preservar o acesso e a interoperabilidade de redes não foi consensual. Apesar de reconhecer a importância da interoperabilidade e a sua criticidade econômica para empresas com modelos de negócios centrados na Internet, Christopher Yoo (2005) ponderou o princípio da cautela. Questionou se a conduta desviante de um operador de rede seria suficiente para justificar respostas legislativas tão prescritiva de governos, fez então uma defesa de uma abordagem equilibrada e ajustada ao dinamismo tecnológico e às circunstâncias particulares de cada mercado.

Contudo, a visão acadêmica majoritária aparentemente convergiu a uma visão mais prescritiva e detalhada do que seriam condutas concorrencialmente

danosas dos operadores de rede. Nesse sentido, a perspectiva defendida por Barbara van Schewick (2010, p. 2) sobre os critérios que deveriam ser preenchidos por uma boa regulação de não discriminação e neutralidade de rede:

> "Deve proteger os fatores que estimularam a inovação de aplicativos no passado para garantir que a Internet possa continuar a servir como um motor de inovação e crescimento econômico no futuro.
>
> Deve proteger os fatores que permitiram à Internet melhorar o discurso democrático e proporcionar um ambiente descentralizado de interação social e cultural em que qualquer pessoa possa participar.
>
> Não deve restringir a evolução da rede mais do que o necessário para atingir os objetivos da regulação da neutralidade da rede.
>
> Deve facilitar a determinação de qual comportamento é ou não permitido para fornecer a tão necessária certeza para os participantes do setor.
>
> Deve manter os custos de regulação baixos."

A autora ainda sustentou que essa abordagem seria a solução para assegurar a concorrência na camada das aplicações, com incentivos à concorrência meritória, prestigiando a preferência do consumidor (VAN SCHEWICK, 2010, p. 8).

No Brasil, essas visões reconhecidamente influenciaram a concepção de regras de não discriminação constantes do Marco Civil da Internet - Lei nº 12.965, de 23 de abril de 2014.

Mas é válido perceber que qualquer escolha regulatória não é livre de vieses ou efeitos, ainda que não previstos no diagnóstico motivador daquela intervenção. Nesse sentido, uma ponderação do próprio Tim Wu (2012, p. 377) sobre o dinamismo tecnológico e a reconfiguração industrial das TICs, visto que a resultante regulatória da Internet teria abençoado algumas empresas e amaldiçoado outras, visto que a mesma neutralidade de rede que catapultaria os negócios de Google e Amazon, destruiria valor de empresas como a AOL-Time Warner.

E esse tensionamento segue ativo nos Estados Unidos, com avanços e retrocessos, ou erros e reparações, a depender do viés do leitor. Mas o que resta claro é entrincheiramento de grandes interesses econômicos e, a julgar pelos últimos passos, a questão regulatória sobre o regime de acesso às redes e interoperabilidade parece ainda longe de uma pacificação.

Dois pra Lá, Dois pra Cá

Durante as administrações Bush e Obama, a FCC passou anos buscando estabelecer regras e aplicar medidas protetivas de neutralidade de rede.

Além do já mencionado episódio de voz sobre IP, outro grande enfrentamento se deu em 2008, quando a FCC determinou à Comcast que se abstivesse de degradar conexões de usuários que utilizavam o aplicativo de compartilhamento de arquivos entre usuários (*peer-to-peer*) BitTorrent. A Comcast recorreu ao poder judiciário e obteve decisão favorável da Corte de Apelações do Distrito de Columbia, que apontou ausência de competência para aplicar regras de neutralidade (IDG, 2010).

Em 2010, o regulador norte-americano empreendeu nova tentativa, dessa vez com a aprovação uma regulação específica mais detalhada, a *Open Internet Order*, com princípios de transparência, não bloqueio e não discriminação.

Mas a regra foi também questionada no judiciário, desta vez pela Verizon. Em 2014, a mesmo Corte de Apelações do Distrito de Columbia decidiu que a Agência não tinha autoridade para aplicar a regulação de neutralidade aos operadores não enquadrados como *common carriers* do Título II do *Communications Act* (FINLEY, 2020).

Em nova tentativa empreendia em 2015, a FCC buscou reclassificar os operadores de banda larga sob Título II do *Communications Act*, embora com menos obrigações se comparados com as operadoras de telefonia fixa. Nessa oportunidade, as tentativas de enfrentamento judicial não prosperaram (FINLEY, 2020).

No entanto, a mudança de cenário não viria agora do poder judiciário, mas sim, da reorientação política. Com a eleição de Donald Trump à presidência dos Estados Unidos, um dos primeiros pronunciamentos da nova gestão Republicana da FCC dava a tônica do novo direcionamento (FCC, 2017):

> "Nos dias finais do último governo, os birôs e os escritórios da *Federal Communications Commission* emitiram uma série de ordens e relatórios controversos. Em alguns casos, os Comissionados [Diretores] não foram avisados com antecedência sobre esses regulamentos da meia-noite... Essas ações de última hora, que não tiveram o apoio da maioria dos Comissionados quando foram tomadas, não devem nos obrigar a seguir em frente. Assim, estão sendo revogados." (tradução livre)

Em abril de 2017, a FCC anunciou então um plano de "reestabelecer a liberdade da Internet" e eliminar "a mão pesada de regulação da Internet". Em dezembro daquele ano foi então aprovada a nova regulação, ela essencialmente revogou as disposições de 2015, preservando apenas as condições de

transparência. Restou à *Federal Trade Commission* a tutela administrativa das relações de consumo, além de eventuais regulações individuais dos estados ou mesmo o poder judiciário para o enfrentamento de casos concretos (FINLEY, 2020).

Por fim, com a eleição de Joe Biden à presidência dos EUA, o tema da neutralidade de rede voltou à cena de discussões políticas e regulatórias, com especulações sobre o posicionamento da nova gestão (SHIELDS, 2022).

Mas essas aparentes idas e vindas, não são exclusividades da realidade norte-americana. A Europa também estabeleceu marcos regulatórios de neutralidade e agora tem também tem estado às voltas com inseguranças sobre a aplicação da regulação no continente, sob a faceta da prática comercial denominada *zero rating*. Isto é, quando operadores, principalmente móveis, adotam um tarifário diferenciado para certa aplicação ou classe de aplicativos de modo a não computar o consumo na franquia de dados contratada.

Apesar de ser prática corriqueira e muito difundida, o Tribunal Superior da Europa decidiu em dois casos paradigmáticos que a prática de *zero rating* atenta contra a regulação de tratamento igualitário de tráfego (LOMAS, 2021).

Em face dessas deliberações, o corpo de reguladores europeus (BEREC – *Body of European Regulators for Electronic Communications*) se viu obrigado a atualizar suas diretrizes de neutralidade de rede que reconheciam certas condições de *zero rating* como regulares, para agora orientar todas as Autoridades Reguladoras Nacionais do continente a banir esse tipo de prática (BRODKIN, 2022).

E a controvérsia não se encerra com a prática do *zero rating*. A quinta geração das comunicações móveis (5G) é uma concepção de rede orientada a aplicações desde seu desenho e concepção, particularmente voltada aos requisitos e exigências de comunicação das máquinas e a Internet das Coisas (IoT – *Internet of Things*).

Nesse sentido, o 5G inova com a possibilidade tecnológica de diferenciação dos níveis de serviço experimentados dentro de uma mesma rede. Isto é, o chamado fatiamento de rede (*network slicing*) irá permitir a gestão eficiente de recursos de redes e a coexistência de aplicações críticas e sensíveis a atraso, por exemplo, o tráfego de cirurgias remotas (telemedicina) ou de veículos autônomos, com alocação prioritária de recursos sobre o consumo de conteúdos audiovisuais de redes sociais.

Diante das primeiras inquietações sobre a conformidade do 5G com o princípio da neutralidade de rede, o BEREC já se apressou em firmar uma resposta formal e um tanto protocolar, com algumas reservas de incerteza no horizonte de aplicações:

> "De acordo com o atual entendimento e análise do BEREC, a Regulamentação parece deixar bastante espaço para a implementação de tecnologias 5G, como o fatiamento de rede, 5QI [Identificadores de Qualidade de Serviço do 5G] e a computação de borda móvel. Até a presente data, o BEREC não tem conhecimento de nenhum exemplo concreto oferecido pelas partes interessadas em que a implementação da tecnologia 5G como tal seria impedida pela Regulamentação. Assim como acontece com todas as outras tecnologias, a utilização específica das tecnologias 5G deve ser avaliada caso a caso à luz da Regulamentação. O BEREC convida as partes interessadas a se engajarem em um diálogo informal com as Autoridade de Regulação Nacional se as partes interessadas tiverem dúvidas sobre se uma utilização específica de uma tecnologia 5G está em conformidade com a Regulamentação." (tradução livre)

Até aqui se exploraram as dinâmicas de análise do poder de barganha e capacidade daqueles qualificados como *gatekeepers* ao longo da história evolutiva das TICs.

Na era de maturidade comercial da Internet, o debate sobre o regime de neutralidade de rede dominou a cena regulatória, com idas e vindas sobre a compreensão do poder detido pelos operadores de rede em face da circulação de conteúdo na rede.

Contudo, a dinâmica evolutiva das redes e do ecossistema das redes tem demonstrado mais recentemente uma reorientação industrial das dinâmicas de poder de barganha envolvidos. E apesar de questões ainda por resolver na aplicação de marcos regulatórios de neutralidade, outros guardiões dos portões têm se revelado no horizonte.

O GATEKEEPER AGORA É OUTRO

Reconhecidamente, o desenvolvimento alcançado pelas TICs impactou de forma definitiva a organização produtiva mundial, gerando um paradigma de oferta de produtos e serviços digitais com escala global e custos marginais tendentes a zero (RIFKIN, 2014).

O debate sobre a nova conformação de poderes na chamada economia digital constitui um desafio de fronteira global, que tem ganhado atenção crescente da academia e nas disciplinas específicas do direito. No palco central deste debate se encontram as grandes plataformas digitais, cujo poder acumulado tem suscitado reflexões quanto ao papel do Estado e sua eventual resposta (CADE, 2020).

Enquanto opções únicas reais de intermediação do acesso aos usuários, essas plataformas têm se qualificado como *gatekeepers*, com poderes de alavancagem a outros mercados relacionados, riscos de extração e exploração de

dados, ameaças de definição de agendas temáticas, manipulação e influência de pessoas (FRAZÃO, 2021).

As formulações hipotéticas iniciais têm considerado a aplicação de medidas de portabilidade de dados e interoperabilidade como mecanismo mitigador do poder concentrado pelas plataformas (OECD, 2021). No entanto, subsistem várias questões de desenho, eficácia e implementação dessa abordagem, por exemplo, a existência de efetivos rivais potenciais, os efeitos reflexos em mercados correlacionados, efeitos concorrenciais indesejados, riscos à privacidade, elevação não intencional de custos de entrantes, repercussões sobre a eficiência dinâmica e incentivos à inovação.

Assim, de forma aderente aos propósitos deste estudo, são explorados a seguir os principais desenvolvimentos regulatórios-jurídicos da Europa e nos Estados Unidos para lidar com as novas dinâmicas de poder de *gatekeeper* nas camadas de aplicações e conteúdo no ecossistema de TICs.

Os Portões de Acesso ao Velho Continente

Com o objetivo manifesto de assegurar mercados justos e efetivamente contestáveis na economia digital, o Parlamento Europeu e o Conselho aprovaram o Regulamento dos Mercados Digitais ou, em língua inglesa, o *Digital Markets Act* (UNIÃO EUROPEIA, 2022).

Nas considerações a decidir do documento, há explícito reconhecimento de características singulares de mercados digitais e como as plataformas têm desempenhado um papel de crescente relevância na economia contemporânea.

Adicionalmente, os serviços de plataforma considerados essenciais apresentam enormes economias de escala, fortes efeitos de rede, a capacidade de atuação em múltiplos mercados, efeitos de enclausuramento (*lock-in*), ausência de migração efetiva entre serviços similares (*multi-homing*), integração vertical e alavancagem baseadas em dados.

Reconhece então a União Europeia como a combinação destas características, em conjunto com práticas concorrencialmente injustas de alguns agentes, podem reduzir a contestabilidade dos serviços essenciais de plataforma, conferindo a eles a condição de *gatekeeper* (UNIÃO EUROPEIA, 2022, p. 3-5).

Com o propósito de mitigar esses efeitos danosos à concorrência, o Regulamento apresenta a interoperabilidade como uma medida promissora, capaz de promover efetiva contestabilidade e permitir a entrada de concorrentes. O atributo da interoperabilidade foi definido como:

> "a capacidade de trocar informações e de utilizar mutuamente as informações trocadas através de interfaces ou outras soluções, de modo a que todos os elementos de *hardware* ou software funcionem com outro *hardware* ou software e com os utilizadores de todas as

> formas as quais foram concebidas para operar" (UNIÃO EUROPEIA, 2022, p. 111) (tradução livre)

Além disso, os *gatekeepers* designados deverão cumprir, para cada dos serviços essenciais de plataforma, as seguintes obrigações de interoperabilidade:

(1) Permitir e tornar tecnicamente possível a instalação e a utilização efetiva de aplicações de *software* ou lojas de aplicativos de terceiros que se utilizem ou interoperem com o seu sistema operacional e permitir o acesso a esses serviços por outros meios além dos serviços essenciais de plataforma desse *gatekeeper*, além de não induzir na escolha de aplicações dos usuários (art. 6º n. 4);
(2) Permitir aos prestadores de serviços e aos fornecedores de *hardware*, a título gratuito, a interoperabilidade efetiva e o acesso para efeitos de interoperabilidade com as mesmas funcionalidades de *hardware* e *software* ofertados pelo *gatekeeper* (art. 6º n. 7);
(3) Para serviços de comunicação interpessoal, assegurar que as funcionalidades básicas dos seus serviços sejam interoperáveis com os serviços de comunicação interpessoal de outro prestador, mediante pedido e a título gratuito, fornecendo as interfaces técnicas necessárias ou soluções que facilitem a interoperabilidade, em um horizonte de até quatro anos prevendo a troca de mensagens, arquivos de áudio, imagens, vídeos entre indivíduos ou grupos (art. 7º n. 1);
(4) Publicar oferta de referência com as especificações técnicas, segurança, criptografia, os termos e as condições gerais da interoperabilidade com os seus serviços de comunicação e, a partir da publicidade das ofertas, atender em até três meses os pedidos de interoperabilidade recebidos (art. 7º n. 4-5).

Fica evidente como a Europa apostou fortemente em condições compulsórias de acesso e interoperabilidade para viabilizar a desconcentração de mercado e mitigar o poder detido pelos *gatekeepers*. Contudo, há um longo esforço de implementação pela frente, com incertezas sobre eventuais dificuldades operacionais que possam surgir no caminho.

Do outro lado do Atlântico, a realidade dos Estados Unidos é substancialmente distinta da observada no continente europeu, em termos de maturação regulatória dos debates, com novas possibilidades a partir da gestão Democrata na *Federal Trade Commission* – FTC.

Na via judicial norte-americana, já há um interessante precedente sobre o reconhecimento da importância do acesso e da interoperabilidade, além de uma

primeira proposta legislativa afeta às condições de concorrência das grandes plataformas, o *American Innovation and Choice Online Act*.

I Want You to Interoperate

Nos anos 1990, a Sun Microsystems desenvolveu a linguagem Java como um ambiente de programação aberta e interoperável, onde os programadores podiam "escrever uma vez, executar em qualquer lugar", disponibilizando a maioria de suas implementações gratuitamente, permitindo ao Java se tornar um padrão *de facto* (LEMLEY; SAMUELSON, 2021, p. 27).

Em 2009, a Sun Microsystems foi adquirida pela Oracle Corporation e, em 2010, a Oracle acionou juridicamente por suposta infração de patentes e direitos autorais envolvendo as interfaces de programação de aplicativos (APIs - *application programming interfaces*) da linguagem Java.

As APIs estabelecem as regras e procedimentos pelos quais os programas podem se comunicar, ou seja, trocar informações seguindo um padrão de interoperabilidade entre *softwares*, eventualmente *hardware*. Essas definições governam como os serviços de um programa específico podem ser chamados, incluindo quais tipos de entrada o programa deve receber e que tipo de saída será retornada. Ao realizar a interface entre aplicações, as APIs ainda têm a importância de isolar os programas, permitindo alterar a maneira como um determinado aplicativo realiza uma tarefa, sem interromper outros programas que usam o serviço (LEMLEY; SAMUELSON, 2021, p. 5).

A questão jurídica principal remete à proteção autoral de interface de software (API) e se o seu uso na construção de novo software constituiria uma condição de uso justo (*fair use*).

A disputa foi recentemente decidida pela Suprema Corte norte-americana, que reconheceu a utilização do Google das APIs Java como um uso justo (*fair use*), ou seja, afastando a violação de direitos para interfaces e a sua utilização para garantir a compatibilidade. Houve o reconhecimento da essencialidade de padrões de interoperabilidade para permitir a entrada de novos competidores. O caso foi considerado uma grande vitória para a comunidade dos desenvolvedores de software e os defensores de uma Internet aberta (LEMLEY; SAMUELSON, 2021, p. 2, 41, 54).

Além do acionamento do poder judiciário, as condições de acesso às redes e interoperabilidade têm surgido também no debate legislativo.

Trata-se do projeto de lei *American Innovation and Choice Online Act*, de iniciativa bipartidária no Comitê Judiciário do Senado dos Estados Unidos.

A ideia central da legislação é impedir que grandes plataformas digitais se engajem em ações de favorecimento de seus próprios produtos e serviços (*self-*

preference), tipificando essa conduta, capaz de estrangular as chances reais de competição de suas concorrentes (EDELMAN, 2022).

Com efeito, em análise da proposta ainda em tramitação são identificadas vedações específicas e muito claras contra comportamentos impeditivos ou restritivos da interoperabilidade ou do acesso a dados gerados em plataformas.

CONCLUSÕES

Buscou-se explorar aqui a evolução do discurso de acesso às redes e de interoperabilidade no direito cibernético ao longo da trajetória evolutiva da Internet, desde a sua primeira infância até os desafios vividos na atualidade.

Inicialmente, no período anárquico e libertário da Internet, o acesso às redes e a interoperabilidade não foram objeto de grandes questões jurídicas. Nos primórdios, as garantias de efetiva conexão entre as redes se confundiam com as próprias razões fundantes da Internet e os interesses majoritários de seus participantes.

Nesse sentido, os primeiros tensionamentos e dilemas vieram da reprodutibilidade de conteúdos e do livre e não moderado fluxo de informações, demando reflexões sobre o constrangimento necessário ao desvio de conduta dos indivíduos. As condições de acesso às redes surgem nesse período como figuras de portais de acesso às fronteiras digitais, em substituição ao paradigma jurídico tradicional sustentado em limites territoriais geograficamente definidos.

Com a evolução do debate de governança, principalmente na primeira década dos anos 2000, tem início uma compreensão sobre o papel não uniforme dos vários integrantes da rede, ou seja, os diferentes níveis de influência sobre os rumos de desenvolvimento da Internet. Começa a se estruturar então o conceito de *gatekeeper*, em sua capacidade de restringir ou mesmo impedir o fluxo informação, no limite, comprometer a interoperabilidade da rede com diversos conteúdos e aplicações. O direito cibernético se faz então acompanhar de conceitos de economia industrial e do direito da concorrência.

As primeiras respostas regulatórias a esse mapeamento de *gatekeepers* trouxeram limitações à gestão de tráfego pelos operadores de rede com o intuito de preservar o desenvolvimento aberto e interoperável em sua plenitude da Internet, sob o manto da regulação da neutralidade de rede. Essa regulação vem sofrendo testes de sustentabilidade, não apenas por grupos de interesse e resistência, mas também em face do dinamismo tecnológico das TICs.

Com a reorientação do poder de barganha e do maior valor gerado agora nas camadas de conteúdos e aplicações da Internet, as atenções quanto ao poder de restringir os fluxos informacionais com fins comerciais estão se voltando para as plataformas digitais, com algumas intervenções judiciais e regulatórias em

curso na Europa e nos Estados Unidos, inclusive para assegurar a interoperabilidade das plataformas.

Em suma, entende-se que o valor da interoperabilidade sempre foi valor muito caro ao desenvolvimento da Internet, embora tenha assumido diferentes formatos ao longo da história, ora como um incentivo natural, ora como uma garantia assegurada em face de um agente com poder de *gatekeeper*.

A interoperabilidade é condição fundamental à livre circulação de ideias, dados e informações para se manter a Internet um mercado digital plural e aberto à inovação, evitando a formação de "jardins murados". No entanto, a exemplo da experiência adquirida com as incertezas e oscilações na implementação de marcos regulatórios de neutralidade de rede, há que se ter cautela com desenhos regulatórios estáticos e excessivamente prescritivos que não se sustentem perante o "vento perene da destruição criadora" de Schumpeter (1984), muito presente nas Tecnologias da Informação e Comunicação.

REFERÊNCIAS BIBLIOGRÁFICAS

Brodkin, J. (2022). Europe cracks down on data cap exemptions in update to net neutrality rules. *ArsTechnica*.

Castells, M. (2017). *O poder da comunicação*. 2 ed. Rio de Janeiro: Paz e Terra.

Conselho Administrativo de Defesa Econômica. (2020). *Concorrência em mercados digitais*: uma revisão dos relatórios especializados. Brasília: CADE.

Easterbrook, F. H. (1996). Cyberspace and the Law of the Horse. *University of Chicago Legal Forum*, v. 207.

Edelman, G. (2022). The Senate Bill That Has Big Tech Scared. *Wired*.

Federal Communications Commission. (2017). *Chairman Pai Statement On Revoking Midnight Regulations*. Washington: FCC.

Finley, K. (2020). The WIRED Guide to Net Neutrality. *Wired*.

Fransman, M. (2010). *The new ICT ecosystem*: implications for policy and regulation. New York: Cambridge.

Frazão, A. de O. (2021). *Big Data e aspectos concorrenciais no tratamento de dados pessoais*. In: DONEDA, Danilo et al (Org.). Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, p. 535-552.

IDG News Service. (2010). Court rules against FCC's Comcast net neutrality decision. *Reuters*.

Kastrenakes, J. (2017). A timeline of Netflix's conflicting stances on net neutrality. *The Verge*.

Katz, M. L.; Shapiro, C. (1994). Systems Competition and Network Effects. *Journal of Economic Perspectives*, vol. 8, n. 2, p. 93–115.

Kent, D. H. (1948). The Erie War of the Gauges. *Pennsylvania History*, vol. XV, n. 4.

Laffont, J; Tirole, J. (1996). Creating competition through interconnection: theory and practice. *Journal of Regulatory Economics*, p. 227-256.

Laidlaw, E. (2010). A framework for identifying Internet Information Gatekeepers. *International Review of Law, Computers & Technology*, v. 24, n. 3, p. 1-16.

Lasar, M. (2018). How AT&T conquered the 20th century. *Wired*, Business.

Lemley, M. A.; Samuelson, P. (2021). Interfaces and Interoperability After Google v. Oracle. *Stanford Law and Economics Olin Working Paper*, n. 562.

Lessig, L. (1999). The law of the horse: What cyberlaw might teach. *Harvard Law Review*, v. 113, n. 2, p. 501-549.

Lessig, L. (2005). Voice-Over-IP's unlikely hero. *Wired*.

Lessig, L. (2006). *Code*: version 2.0. New York: Basic Books.

Lomas, Natasha. (2021). Europe's top court slaps down 'zero rating' again. *TechCrunch*.

Motta, M. (2004). *Competition policy*: theory and practice. Cambridge: Cambridge Press.

Murray, A. D. (2011). Nodes and Gravity in Virtual Space. *Legisprudence*, v. 5, n. 2, p. 195-221.

Organisation for Economic Co-Operation and Development. (2021). *Data portability, interoperability and digital platform competition*. Paris: OECD.

Parlamento Europeu e Conselho. (2022). Relativo à disputabilidade e equidade dos mercados no setor digital e que altera as Diretivas (UE) 2019/1937 e (UE) 2020/1828 (Regulamento dos Mercados Digitais). Bruxelas: União Europeia.

Reidenberg, J. R. (1996). Governing networks and rule-making in cyberspace. *Emory Law Journal*, v. 45, p. 911-930.

Reidenberg, J. R. (1998). Lex informatica: The formulation of information policy rules through technology. *Texas Law Review*, v. 76, p. 553-593.

Rifkin, J. (2014). *The zero marginal cost society*: the internet of things, the collaborative commons, and the eclipse of capitalism. New York: Macmillan.

Schumpeter, J. A. (1984). *Capitalismo, socialismo e democracia*. Rio de Janeiro: Jorge Zahar.

Senate of the United States. (2022). S.2992 - 117th Congress (2021-2022). Washington: US Senate.

Shields, T. (2022). Biden's FCC is having trouble getting started. *Bloomberg*, Businessweek, Tehcnology.

Van Schewick, B. (2010). Network Neutrality: what a non-discrimination rule should look like. *Stanford Public Law Working Paper*, n. 402.

Wu, T. (2003). Network neutrality, broadband discrimination. *J. On Telecomm. & High Tech. L.*, vol. 2, p. 141-175.

Wu, T. (2012). *Impérios da comunicação*: do telefone à internet, da AT&T ao Google. Rio de Janeiro: Zahar.

Yoo, C. (2005). S. Beyond Network Neutrality. *Harvard Journal of Law & Technology*, v. 19, n. 1, p. 1-77.

Zittrain, J. L. (2008). *The future of the Internet*: and how to stop it. Harrisonburg: Yale University Press.

The Law, State and Telecommunications Review / Revista de Direito, Estado e Telecomunicações

Contact:
Universidade de Brasília - Faculdade de Direito - Núcleo de Direito Setorial e Regulatório
Campus Universitário de Brasília
Brasília, DF, CEP 70919-970
Caixa Postal 04413

Phone: +55(61)3107-2683/2688

E-mail: getel@unb.br

Submissions are welcome at: https://periodicos.unb.br/index.php/RDET

The Right to be Forgotten as a Special Digital Right

Submitted: 17 August 2022
Reviewed: 6 October 2022
Revised: 8 November 2022
Accepted: 9 November 2022

Tereziia Popovych*
https://orcid.org/0000-0002-2498-5874

Mariia Blikhar**
https://orcid.org/0000-0002-2741-5308

Svitlana Hretsa***
https://orcid.org/0000-0003-2037-0263

Vasyl Kopcha****
https://orcid.org/0000-0002-8086-5527

Bohdana Shandra*****
https://orcid.org/0000-0002-1669-5017

Article submitted to blind peer review

DOI: https://doi.org/10.26512/lstr.v15i2.44692

Abstract

[Purpose] The purpose of this study is to investigate aspects of digital law in Ukraine and other countries of the world in the context of the right to be forgotten.

[Methodology/Approach/Design] To achieve the objective, induction, deduction, and comparative analysis were used, both the proximate topics and aspects of the legal framework of different countries together with the legal information provided by online services were considered.

[Findings] The study identified the main features of the right to be forgotten in different countries, the impact of the European Union Court of Justice and European Court of Human Rights on it and the little-studied intricacies of the legal aspect of this mechanism.

[Practical Implications] This paper can be of interest both as introductory material and as a basis for further study because there is a growing human need to be able to control personal data in the face of the expanding phenomenon of globalization and digitalization.

* PhD in Law, Associate Professor at the Department of Theory and History of State and Law, Uzhhorod National University, Uzhhorod, Ukraine, E-mail: t.popovych93@yahoo.com.

** Full Doctor in Law, Professor at the Department of Administrative and Informational Law, Lviv Polytechnic National University, Lviv, Ukraine, E-mail: m.blikhar@gmail.com.

*** Full Doctor in Law, Associate Professor at the Department of Constitutional Law and Comparative Jurisprudence, Uzhhorod National University, Uzhhorod, Ukraine, E-mail: Svitlana-hretsa@gmail.com.

**** Full Doctor in Law, Associate Professor at the Department of Criminal Law and Process, Uzhhorod National University, Uzhhorod, Ukraine, E-mail: v-kopcha@gmail.com.

***** PhD in Law, Associate Professor at the Department of Philosophy, Uzhhorod National University, Uzhhorod, Ukraine, E-mail: b.shandra@yahoo.com.

Keywords: Law. Digital Law. Search Engines. Internet Law. Information.

INTRODUCTION

The right to be forgotten implies the right of a person in certain specific situations to demand the deletion of data about their personal or family members. The establishment of the right to be forgotten is caused by the ability to find information about individuals in search engines at any time, regardless of the time frame for its placement. In its current form, it means the right to demand the exclusion from search engines of URLs (uniform resource locator) that were legally posted on the network, including by a person independently, due to their obsolescence or changing circumstances (DOVGAN, 2018). According to E.A. Voynikanis (2016), the attention of the European community to the right to be forgotten takes place in connection with the existing belief that the Internet, as a technology that allows storing a potentially unlimited amount of information, is a threat to privacy. In the context of this problem, the right to be forgotten is perceived as a certain additional means of controlling the personal data subject over the processing of their personal information in an online environment. At the same time, the researcher notes that the information stored on the network is not just indestructible, capable of infinite replication, but also closed in the eternal present, because due to its technical characteristics, the Internet is an environment within which it is impossible to disappear and within which a "digital dossier" for each user is actually stored (FILATOVA, 2020; SPASIBO-FATEEVA, 2019).

According to Yu.S. Razmetaeva (2018), the right to be forgotten is not fully covered by the right to privacy. The latter protects information about a person that they do not want to make publicly known, while the right to forget – involves erasing information that has been publicly known for a certain time and preventing access to it for others. The right to be forgotten refers to truthful or once-true information that interferes or negatively affects a person's life or destroys their reputation in society. Researchers of the right to be forgotten generally believe that the "locomotive" for the further legal regulation of this right was the decision of the European Union (EU) Court of Justice in the case "Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" (2014). In its decision, the court ordered Google to remove information about Spanish citizen Mario Costech Gonzalez regarding the forced sale of real estate, which took place in connection with his social security debt ten years ago. The court also concluded that the right to be forgotten can be granted to an individual only when there is no interest of the Internet community

in information about a particular person, and when the person does not play a particularly significant public role.

The main question before the Court of Justice in the Mario Costeja Gonzalez case was whether it was possible to consider search engines as data controllers, and hence whether they should provide users with tools to make changes or delete false personal data. The conclusions reached by the court were as follows:

(1) Firstly, search engines should be considered data controllers, because they process personal data;
(2) Secondly, search engines, as data controllers, are required to remove from the list results that are displayed after a search performed based on links to a person's name on web pages published by third parties, and that contain information about this person, even if the latter is legitimate;
(3) Thirdly, when analysing the request of the personal data subject for the removal of links to search results, the authorities must balance the interests of the subject under the Convention for the Protection of Human Rights and Fundamental Freedoms, the economic interests of the service provider, and the role of the personal data subject in public life and the public interest in accessing information (GUADAMUZ, 2017; PETRYSHYN and HYLIAKA, 2021).

The right to be forgotten in the system of digital human rights today is a very promising area of legal research, because it follows from the need to ensure the privacy of a person on the Internet, and is also the latest addition to the right to privacy and the right to protect personal data. In Ukraine, research on the right to be forgotten remains insignificant. Among the researchers who have investigated certain aspects of this phenomenon, the following can be noted: O.M. Kalitenko (2019), Yu.S. Razmetaeva (2018), A.A. Antopolsky (2019), N.V. Varlamova (2019), E.A. Voynikanis (2016). But above all, the right to be forgotten is the object of interest and analysis in international legal doctrine, as evidenced by the works of such researchers as A. Guadamuz (2017). The study reviewed and compared the results of court cases on the exercise of the right to be forgotten between Google divisions and various individuals or states. In the course of the study, a comparative analysis was carried out, and conclusions were developed using deductive and inductive approaches, considering the specifics of each of the situations, the importance of the case in the eyes of the court and the public, and a retrospective aspect in the context of the specifics of the state structure, information control, and the legal system of different states.

INTERNATIONAL PRACTICE OF APPLYING THE RIGHT TO BE FORGOTTEN

The consequences of the decision taken by the Court of Justice of the European Union are of interest. Thus, to minimise possible lawsuits, Google has created a special online application form, through which a person can apply to the company to delete certain personal information. As of 2018, according to Google, it received more than 860 thousand requests to delete information from the search engine, as a result of which more than 3.4 million links were deleted. Based on the analysis of completed requests to delete information from the Google search engine, O.M. Kalitenko (2019) determines the following grounds for deleting information: the statute of limitations of circumstances that are the content of information (on the example of the case of Spanish citizen Mario Costech Gonzalez, which refers to ten years); unreliability or irrelevance of information about a person; public interest in information about a person. The last of these aspects is the most difficult because it shows the confrontation between the interests of an individual and the interests of society regarding information about a particular person. Therefore, the main focus here is directly on the subject of the request to delete information. This includes several types of such subjects: subjects that do not play a significant role in public life; subjects that play a significant role in public life (political or public figures, religious leaders, "stars" of show business, sports; subjects that play a limited role in public life (civil servants, individual officials) (LUKIANOV et al., 2021; UVAROVA, 2020). At the same time, as it becomes clear, the main criterion for the possibility of removing information about a person from a search engine is the public significance of the relevant information. Accordingly, information about the first category of persons may be deleted, about the second – not, about the third – deleted depending on its content and significance for society.

In the case of M.L. and W.W. v Germany. (2018), the European Court of Human Rights dismissed a complaint lodged by the applicants (who had been convicted of murder) concerning the commission by anonymous of several materials in the Internet archive given: the public interest and the wide visibility of the case; the objective and reliable nature of the publications; the lack of intent to damage the applicants' reputation. N.V. Varlamova (2019) points out that the EU Court of Justice imposes on search engine operators the obligation to remove links to web pages published by third parties and containing information about a person from the list of search results made based on the name of the interested person, if such information has lost its relevance, but causes harm to it. The right to delete such information, according to the EU Court of Justice, must prevail over

the economic interests of the search engine operator and the public interest in obtaining access to the relevant information about a person, except in cases of the special situation and role of the personal data subject in public life, which make the interference with their rights justified.

The right to be forgotten, as defined by A.M. Boyko (2018), is a human right that allows a person to demand, under certain conditions, the removal of their personal data from public access through search engines, that is, links to those data that, in their opinion, can harm the person. This refers to outdated, inappropriate, incomplete, inaccurate, or redundant data or information, the legal grounds for storing which have disappeared over time. Therefore, it is important to note that it is not information about a person that is deleted but only links to this information on the Internet since the Internet is by its very nature a space where it is impossible to completely delete information. It remains on the servers of one resource or another. Therefore, the exercise of this right means that links to certain information about a person are removed from the search results so that the relevant information becomes inaccessible to public access users for their search queries. The URL must be removed from the search engine index, after which it becomes invisible to the user when executing a search query, but the source data remains available in the original source (VARLAMOVA, 2019).

Thus, the applicants M.L. and W.W. were found guilty of committing a crime against a famous actor in 1993 and sentenced to life in prison. However, in August 2007 and January 2008, they were released on probation from serving their sentences. However, in 2007 the applicants first brought a claim against the Deutschlandradio radio station in the Hamburg court to make anonymous personal data in the documentation about them, which was posted on the radio station's website. The Hamburg court and subsequently the court of appeals upheld the claim of applicants M.L. and W.W. However, the Federal Court overturned the decision of the appeal in the case, arguing that the radio station has the right to freedom of expression, as well as the public's interest in awareness.

In its conclusions, the European Court of Human Rights drew attention, first of all, to the importance of striking a balance between the applicants' right to respect for private life, the radio station's right to freedom of expression, and the public's right to be informed (BARABASH and BERCHENKO, 2019). In addition, the court pointed out that the indication in media reports, for example, of the name of a certain person (as was the case with M.L. and W.W.) there is an important aspect of the work of the press, especially when covering information about criminal proceedings that have attracted considerable public attention. Attention was focused on the increased public interest in the applicants in view of the public outcry that they had committed the murder of a famous actor. As it

turned out, during their conviction, the applicants themselves repeatedly turned to the media to cover their case before the public. This factor further reinforced the court's reasoning as to the rejection of claims by M.L. and W.W. The German Federal Court of Justice and the European Court of Human Rights also noted that the veracity of the information about the applicants publicly posted online was not disputed, and the media did not intend to offend M.L. and W.W. or damage their reputation. Dissemination of information about the latter was limited because it was carried out through a paid subscription. In addition, the applicants did not provide information that they applied to search engine operators to restrict the tracking of information about them. Ultimately, the European Court of Human Rights concluded that there had been no violation of Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms (1950) in relation to the applicants M.L. and W.W. (JUDGMENT M.L. and W.W. V. GERMANY, 2018).

Therefore, as the above-mentioned decision shows, the court in the case of finding the truth must find a fair balance between the right of a person to privacy (through which the right to be forgotten is implemented) and freedom of expression and the right of the public to be informed. At the same time, as the case of M.L. and W.W. v Germany. (2018), the search for such a balance of interests is not an easy case, because at different levels of judicial instances, there were different interpretations of the courts of the essence of the dispute, and, accordingly, different decisions from each other. According to O.M. Kalitenko (2019), the debatable and problematic nature of the right to be forgotten lies in the fact that it is on the verge of two personal non-property rights of a person – the right to information (open access, lack of censorship) and the right to privacy (respect for private and family life, protection of personal data).

Resolution of the European Parliament and the Council No. 2016/679 "On the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)" (2016) provides for the right of the personal data subject to correct and erase (the "right to be forgotten") their personal data by their controller. In the sense of erasure, personal data may be deleted by the control at the request of the subject, if: they are not necessary from the standpoint of the purposes for which they were collected or processed; consent to their processing is revoked or objected to processing; they were processed illegally, etc. At the same time, there are exceptions – cases where the rule on erasure of personal data cannot be applied: for the purpose of exercising the right to freedom of expression and information; considering the public interest in public health; for achieving the

goals of public interest, scientific, historical research, statistics; for the purpose of forming, implementing, or protecting legal claims.

In Argentina, the case of a 30-year-old model, singer, and actress Virginia Da Kunha v. Yahoo and Google, where the key question was raised about the responsibility of search engine operators for information that is provided to users in the search result. Thus, according to the plot of the case, Da Kunha, who published various kinds of photos on her website and social networks, including herself in short shorts, swimsuits, T-shirts, etc., filed a lawsuit against Yahoo and Google, because photos with her in search results appeared on websites of a sexual, pornographic nature, as well as related to sex trafficking. The applicant submitted that such information had damaged her career as a singer and actress. In addition, her appearance on this type of website does not correspond to her personal beliefs and professional activities. She demanded compensation for property and moral damage in the amount of 200 thousand Argentine pesos. The court granted Da Kunha's claim, ordering Yahoo and Google to filter out all links to pornography and sexual services from search results. The key issue for the court's resolution was the conflict between freedom of expression and a person's right to control the use of their image (the right to privacy). This refers to the need to obtain permission to use images of a person in public space. In turn, the federal civil appeals court, at the request of representatives of Yahoo and Google, overturned the decision of the court of the first instance, releasing the applicants from certain obligations for them. The court's arguments were based on the fact that search engine operators cannot be held responsible for the damage caused to Da Kunha by Internet users through the placement of her photos on pornographic and sexual websites. The fact that Yahoo and Google catalogued relevant sites and provided links to websites is not sufficient to determine the causal relationship of Da Kunha's harm (CARTER, 2013).

A similar aspect of the liability of search engine operators (information intermediaries) was the subject of Google India Pvt. Ltd. v. Vinay Rai & Anr when an appeal was filed by the aggrieved party before the Delhi High Court over a breach of privacy caused by a third party seeking to hold even Google liable. However, the court dismissed the complaint on the grounds that for the Resolution of the Parliament of India No. 21 “On digital technologies” (2000), the intermediary (search engine operator) is not responsible for the content of information to which users are granted access. Exceptions here may be cases where: the transfer of information was initiated by an intermediary; the information was selected or modified by the intermediary; the intermediary colluded, facilitated, or encouraged the transfer of information; the intermediary cannot promptly delete or prohibit access to information after receiving actual

knowledge or notification to the government that the data or communication line that takes place in a resource controlled by the intermediary is used to commit an illegal act (CHAKRABORTY, 2019). Thus, the issue of liability of search engine operators remains controversial in judicial practice, requiring proof of the positions of the parties. The latter, at the request of interested parties, can remove the demonstration of certain information about a person from the search results, but they should not be responsible for the content of certain personal data about a person posted on the Internet.

PRACTICE OF THE EUROPEAN COURT OF HUMAN RIGHTS IN THE CONTEXT OF THE RIGHT TO BE FORGOTTEN

From the standpoint of the practice of the European Court of Human Rights, the solution of problematic aspects of the implementation of the right to be forgotten is carried out by establishing by the court the presence or absence of a violation of Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms (1950), which protects the right to respect for a person's private and family life.

For example, in one of the European Court of Human Rights cases, Khelili v. Switzerland (2011), the right to respect Sabrina Khelili's private life was upheld. According to the plot of the case, during a police check in Geneva in 1993, the applicant was found to have business cards that read: “A pretty, beautiful woman in her 30s, would like to meet a man to have a drink together or go outside from time to time. Phone number ...”. The police wrote her name on their records as a “prostitute”, despite Khelili's insistence that she was never one. In turn, the police referred to the cantonal law on personal data, which allegedly allowed them to keep records of personal data to the extent necessary for the performance of official duties. On this basis, in November 1993, the Federal Office of Foreigners issued a two-year ban on Khelili's residence in Switzerland. In 2001 two criminal complaints were lodged against the applicant for threatening and abusive behaviour. In 2003, from a letter from the Geneva police, she learned that the word “prostitute” in relation to her name still appears in police cases. Subsequently, in 2005, the Geneva police chief told Khelili that the word for her profession had been replaced by “tailor”. However, after learning from a telephone conversation that in 2006 the word “prostitute” still appeared in the police's computer files, Khelili asked to delete the relevant information again and asked the Geneva police to delete data on criminal complaints filed against her, among which the word “prostitute” was included. However, in this request, the applicant was refused on the grounds that such information should be kept as a preventive measure, given her past offences.

In its conclusions, the European Court of Human Rights determined that the word “prostitute”, which is kept in the police records, can damage the reputation of Khelili and make her daily life more problematic because this data can be passed on to the authorities. The problem situation is compounded by the fact that such data is subject to automatic processing, which facilitates access to it and its distribution. The court also drew attention to the vagueness of Khelili's allegations of unlawful prostitution and to the insufficient proximity of the link between the retention of the word "prostitute" and the applicant's conviction for threatening and abusive behaviour. Thus, the court concluded that the retention of false data in the police records violated Khelili's right to respect for her private life, and in particular the word “prostitute” – neither justified nor necessary (KHELILI V. SWITZERLAND, 2011).

It is important to note that the right to be forgotten in its implementation must have its limits. This, in particular, is confirmed by the decision of the EU Court of Justice in Google v. France in September 2019 in its decision, the Court indicated that the right in question applies only to the version of the search engine in the EU, but not outside it. The essence of the dispute between Google and France was that the National Commission for Informatics and Freedom of France asked Google to completely remove information that was granted the right to be forgotten from search results. The company did not comply with the National Commission for Informatics and Freedom of France request but only used geo-blocking. In other words, the information was displayed in the search results, but not in the EU. The National Commission for Informatics and Freedom of France imposed a fine of 100 thousand euros on Google. Therefore, the company appealed to the French Council of State to cancel this decision. The latter sent the dispute to the EU Court of Justice. Despite the arguments of France that geo-blocking does not give proper results, because the search results can be circumvented via a virtual private network (VPN), the EU Court of Justice did not take them into account. At the same time, the court took into account Google's position that if states were given the opportunity by law to perform actions similar to those required of the search engine by the National Commission for Informatics and Freedom of France, in the future this would allow censoring the Internet network (ANDROSCHUK, 2021).

A frequent area of implementation of the right to be forgotten is associated with the removal of information about a person's past experience in criminal activities from search engines. Thus, this refers to protecting the right of a person to rehabilitation. Thus, for example, in September 2014, the Kyoto District Court (Japan) rejected a person's claim against Google Japan, which asked to remove information about their arrest in the past from search results. At the same time,

the court determined that such actions should be performed by the parent company, not the subsidiary. Consequently, in October 2014, the Tokyo District Court ordered Google to remove headlines and snippets on websites that reveal the name of a person who claimed that their privacy rights were violated due to articles hinting at past criminal activity. In addition, in June 2015, the Saitama District Court in Japan ordered Google to remove from search results details of an arrest that took place three years ago for violating child prostitution laws, saying that the crime was relatively minor and had no historical or social significance (VOSS and CASTETS-RENARD, 2016).

CONCLUSIONS

Thus, the exercise of the right to be forgotten is one of the modern forms of protection of privacy and personal data on the Internet, which has gained its significance due to the practice of the EU Court of Justice and the European Court of Human Rights. At the heart of this right is the freedom of a person to handle personal information about them, which a person, in particular, wishes to remove from public access. At the same time, it is not about deleting information directly, but about links to it contained in search engines. The study found that there is a contradiction in the exercise of the right to be forgotten, namely in maintaining a balance between ensuring private and public interests (in terms of access to information).

In addition, it is worth noting that in the light of the exercise of the right to be forgotten, it is necessary to discuss two main legal obligations: the first – established – concerns search engine operators who must remove links to information about a person on their request, which is outdated, inaccurate, unreliable, etc.; the second – concerns the obligation to obtain the consent of a person to place information about them on the network. Given the specific nature of the Internet, obtaining such consent is necessary, because in the future it would allow avoiding situations in which a person will contact search engine operators to delete information about them placed without their consent. An exception here may be information about public or socially significant persons, or certain personal data of civil servants and individual officials.

REFERENCES

Androschuk, G. (2021). *EU Court: Google has won the dispute over the right to forget.* Available at: https://cutt.ly/cZmrs10.

Antopolsky, A. A. (2019). Human rights and the Internet: the case law of the European Court of Human Rights. *Proceedings of the Institute of State and Law of the Russian Academy of Sciences,* 14(2), 171-172.

Barabash, Y. & Berchenko, H. (2019). Freedom of Speech under Militant Democracy: The History of Struggle against Separatism and Communism in Ukraine. *Baltic Journal of European Studies*, 9(3), 3-24.

Boyko, A. M. (2018). The right to forget: some aspects of theory and practice. *Journal of Eastern European Law*, 48, 124-131.

Carter, E. L. (2013). Argentina's right to be forgotten. *Emory International Law Review*, 27, 25-31.

Chakraborty, S. (2019). Right to be forgotten – the most recent dispute in data protection. *International Journal for Legal Developments & Allied Issues,* 1, 86-87.

Convention for the Protection of Human Rights and Fundamental Freedoms. (1950). Available at: https://zakon.rada.gov.ua/laws/show/995_004#Text.

Dovgan, E. F. (2018). Human rights in the age of information technology. *Journal of the O.E. Kutafin* University, 5, 109-125.

Filatova, N. (2020). Smart contracts from the contract law perspective: Outlining new regulative strategies. *International Journal of Law and Information Technology*, 28(3), 217-242.

Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González. (2014). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131.

Guadamuz, A. (2017). Developing a right to be forgotten. *EU Internet Law:* Regulation and Enforcement, 59-76. Cham: Springer.

Judgment M. L. and W.W. v. Germany (2018). Available at: https://cutt.ly/xZn4Rpz.

Kalitenko, O. M. (2019). The right to be forgotten: a European or a global achievement? *Journal of Civilization*, 35, 60-64.

Khelili v. Switzerland. (2011). Available at: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22002-345%22]}.

Lukianov, D. V., Hoffmann, T. & Shumilo, I. A. (2021). Prospects for recodification of private international law in Ukraine: Do conflict-of-laws rules require a new haven? *Journal of the National Academy of Legal Sciences of Ukraine*, 28(2), 198-210.

Petryshyn, O. V. & Hyliaka, O. S. (2021). Human rights in the digital age: Challenges, threats and prospects. *Journal of the National Academy of Legal Sciences of Ukraine*, 28(1), 15-23.

Razmetaeva, Y. S. (2018). *Formation of new human rights under the influence of IT.* IT law: problems and prospects of development in Ukraine. Lviv: Ivan Franko National University of Lviv.

Resolution of the European Parliament and the Council No. 2016/679**.** *"On the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)".* (2016). Available at: https://zakon.rada.gov.ua/laws/show/984_008-16#Text.

Resolution of the Parliament of India No. 2. *"On digital technologies".* (2000). Available at: https://uk.upwiki.one/wiki/Information_Technology_Act,_2000.

Spasibo-Fateeva, I. (2019). Implementation and Protection of the Right to Freedom of Expression in Ukrainian Civil Law: Modern Problems. *Baltic Journal of European Studies*, 9(3), 205-223.

Uvarova, O. (2020). Business and human rights in times of global emergencies: A comparative perspective. *Comparative Law Review*, 26, 199-224.

Varlamova, N. V. (2019). Digital rights – a new generation of human rights? *Proceedings of the Institute of State and Law of the Russian Academy of Sciences,* 14(5), 9-46.

Voss, W. G. & Castets-Renard, C. (2016). *Proposal for an international taxonomy on the various forms of the "right to be forgotten": a study on the convergence of norms.* Available at: https://cutt.ly/SZmthCh.

Voynikanis, E. A. (2016). The right to be forgotten: legal regulation and its theoretical understanding. *Jurisprudence*, 3, 70-89.

The Law, State and Telecommunications Review / Revista de Direito, Estado e Telecomunicações

Contact:
Universidade de Brasília - Faculdade de Direito - Núcleo de Direito Setorial e Regulatório
Campus Universitário de Brasília
Brasília, DF, CEP 70919-970
Caixa Postal 04413

Phone: +55(61)3107-2683/2688

E-mail: getel@unb.br

Submissions are welcome at: https://periodicos.unb.br/index.php/RDET

Autonomous Robots and Their Legal Regime in the Context of Recodification of Civil Legislation of Ukraine

Submitted: 5 September 2022
Reviewed: 12 October 2022
Revised: 9 November 2022
Accepted: 19 November 2022

Yurii Khodyko*
https://orcid.org/0000-0002-7768-4135

Article submitted to blind peer review

DOI: https://doi.org/10.26512/lstr.v15i2.44893

Abstract

[Purpose] The issues of understanding what a robot is as an object of civil legal relations and the civil law regime that must be applied to ensure effective legal regulation of relations related to the use of robotics require legal solutions. Special attention should be paid to the study of liability for damage caused by robotics to a person or their property.

[Methodology/Approach/Design] The main methods on which this work was based are the method of systematization and the method of analysis. The article summed up various basic materials related to robots as objects of civil legal relations, as well as the impact of their existence on the current development of the world.

[Findings] Considering the purpose of robotics in the modern world, it is proposed to carry out legal regulation of robotics relations using an approach of the extension of civil law regulation applied to things. This does not exclude the introduction of special rules that will apply exclusively to robots as objects.

Keywords: Object of Civil Legal Relations. Autonomous Robot. Legal Regime. Concept Of Robot. Liability For Damage Caused by Robot.

INTRODUCTION

The development of technology and the desire of society to automate production processes has led to the emergence of robotic systems (robots). A fairly long process of technology development in the area of robotics and artificial intelligence, which is considered for more than a decade, has provided the "technological evolution" of robots from laboratory prototypes to the mass use of robots in the industrial sector and the first significant steps in the use of robotics in consumer services, medicine, military and space spheres. Every year,

*Yurii Khodyko is a PhD in Law, Associate Professor at the Department of Civil Law No. 1, Yaroslav Mudryi National Law University, Kharkiv, Ukraine. Address: Yaroslav Mudryi National Law University 61024, 77 Pushkinska Str., Kharkiv, Ukraine. E-mail: khodykoyurii@gmail.com.

KHODYKO, Y. *Autonomous Robots and Their Legal Regime in the Context of Recodification of Civil Legislation of Ukraine*. **The Law, State and Telecommunications Review**, v. 15, no. 2, p. 54-65, October 2023.

robots are given an increasing number of functions, they begin to be used in various fields, and robots become more autonomous when used (DANCHUK et al., 2021). All this is the path that humanity is quite successful in the field of robotics, the pinnacle of which is the creation of a universal intelligent anthropomorphic robot. The emergence of robots was predominantly conditioned upon the aim to simplify human life in the field of production, displace human labour in areas that are complex and dangerous, as well as to accelerate the pace of production at the expense of robots, making it more technologically advanced, accurate, and high-quality. Robotisation of production processes has led to changes in the labour market around the world, the emergence of new professions, which are usually associated with the management, control of technological processes, etc. (GINTERS et al., 2010).

Even though humanity has managed to replace humans with robots in many areas of production and life support, robots will never be on a par with humans in their status, regardless of what level technological advance has reached in the field of creating robots, in particular an intelligent anthropomorphic robot. For humanity, robots should remain only a means of a better way of life – helpers. As noted by N. Richards and W. Smart (2013), the idea of possible equality between a robot and a human in terms of its status should be unequivocally rejected. As the world is filled with robotic and artificial technologies, lives and relationships of social, political, and economic power are also changing, creating new and unexpected problems for law (LARSON, 2010; BALKIN, 2015). Solving problems of legal regulation of relations arising in the field of robotics use, their legal nature is a natural process, as with the emergence of any new objects of civil legal relations (KHARYTONOV et al., 2021).

To date, there is no civil law regulation, as well as in general legislative regulation of relations regarding robots as such in Ukraine. This cannot be stated about the European Union, which Ukraine seeks to join and has committed itself, in particular in the legislative sphere, to harmonise legislation with the latter. The European Parliament adopted a resolution "Report with recommendations to the Commission on Civil law Rules on Robotics" (2017), which defined the key issues and ways to form civil law regulation of relations in the European Union regarding the use of robots. Notably, legislation in the field of robotics in the form of a special law was adopted in 2008 (with subsequent changes) in South Korea "Intelligent Robots Development and Distribution Promotion Act" (2008). However, this law does not contain conceptual provisions of civil law regulation of relations regarding the use of robots but is only aimed at developing a national policy for the development of robotics in the state. The key issues to be resolved include determining what

should be understood by robots in general, from the standpoint of legal regulation, the civil law turnover of such robots, as well as liability for damage caused to a person or property during the robot's work (activity). The solution of these issues will ensure the development of the fundamental principles of the civil law concept of legal regulation of relations in the field of human use of robotics in Ukraine.

HISTORICAL ASPECTS OF ROBOTISATION

The idea of ordinary people about robots, as a rule, is based on films and literature of the science fiction genre, and the robot is associated with the "Iron Man". Such a view, today, is not devoid of real content, but it is rather distorted and narrow. Thus, indeed, humanity is striving to create an anthropomorphic intelligent robot and there are real first steps in this direction. However, excessive "humanisation" of robots is to a certain extent a trend of modern realities (KHAN et al., 2012). Although a robot may once be considered a human, this situation is unlikely to happen in the near future (ASARO, 2007). Most of the robots that currently exist do not have a uniform similarity but are designed for practical application in a particular field, and in the first place is not its appearance, habits, abilities similar to human ones, but its autonomy and functionality according to the needs of the field of application. The word "robot" was first proposed in a science fiction play by Czech writer Karel Capek (2021) R.U.R. (Rossumovi univerzální roboti (Czech.), "Rossumi Universal Robots"), which the world saw in 1920. In the play, robots are considered as humanoid mechanisms used as slave labour in a factory. Later, in the collection of science fiction stories by Isaac Asimov "I, Robot" (2018), the "Three Laws of robotics" were formed for the first time, which are still relevant today and form the basis for developing the rules of ethics for robots around the world. These two literary works of the science fiction genre marked the beginning of robotics, the idea of which was picked up by the fields of engineering and programming to bring fantastic ideas to life.

Today, much attention is paid to defining the understanding of the robot for the purposes of legal regulation both in the legal scientific literature, and there are also the first steps to consolidate the legal understanding of the robot as an object of civil legal relations in regulations. R. Calo (2016) refers to a robot as an artificially created object or system that can receive and process information, as well as act according to their surrounding world. N. Richards and W. Smart (2013) define a robot as a developed system that demonstrates both physical and intelligent activity but is not alive in the biological sense. Evidently, in the definition of a robot, scientists emphasise that it is not a biological object, but an artificially created one. Even though the current

legislation of Ukraine does not govern the issue of robots, the Appendix to the Procedure for state control of international transfers of military goods provides a legal definition of a robot. The specified Appendix determines that robot is a manipulative mechanism that can move continuously or from point to point, can use sensitive elements (sensors) and has all the following characteristics:

(1) Multi-functionality;
(2) Ability to set or orient material, parts, tools, or special devices using variable movements in three-dimensional space;
(3) Equipped with three or more closed-loop or open-loop servomechanisms, which can include stepper motors;
(4) Ability "to be programmed by the user" using the teach/repeat method or using an electronic computer, which can be programmed by a logic controller, i.e., without mechanical intervention (RESOLUTION, 2002).

The legislator based this understanding of the robot on the fact that the robot is a manipulative mechanism that can perform tasks independently in space according to the programmed functionality of the robot.

MAIN CHARACTERISTICS OF ROBOTS

The Law of South Korea "Intelligent Robots Development and Distribution Promotion Act" (2008) indicates one of the main characteristics of a robot as its mechanical nature upon defining the concept of a robot, namely as a mechanical device that perceives the external environment for itself, distinguishes between circumstances and moves voluntarily (Article 2.1 of the Law). At the same time, clause 1 of the European Parliament resolution "Report with recommendations to the Commission on Civil law Rules on Robotics" (2017) emphasises that the following characteristics are necessary to qualify a certain device as a smart robot:

(1) Ability to become autonomous using sensors and/or exchange data with the environment, the ability to exchange this data and analyse it;
(2) Ability to self-learn based on experience gained and interaction (optional criterion);
(3) Presence of at least minimal physical support;
(4) Ability to adapt actions and behaviour according to environmental conditions;
(5) Absence of life from a biological standpoint.

Considering the above-mentioned scientific opinions and legislative provisions in terms of understanding the robot as an object of civil legal relations, the robot has 4 main components (features): materiality, intelligence, functionality, and autonomy.

Materiality. A robot is an object of the material world, a device created by human intelligent/manual labour, and not by nature. The materiality of the robot on the one hand allows considering it as a thing, on the other hand, the absence of life in the robot from a biological standpoint excludes the possibility of qualifying it as a person – an individual (subject of civil legal relations), and as an animal – an object of civil legal relations.

Intelligence. The intelligent component of the robot ensures that the latter performs all actions according to its functionality. The intelligent attribute of the robot is software, artificial intelligence, which in their unity form the "digital (electronic) brain" of the robot. It is the intelligent component of a robot that transforms it from a simple thing – an object of the material world – into a robot as an independent object in the system of objects of civil legal relations. The basic abilities of a robot are laid down (programmed) by a person according to its functionality. Thanks to artificial intelligence, which can be a component of the robot's "digital (electronic) brain", it can be programmed for self-study, considering the principles of ethics for robotics, which can ensure its functional self-improvement (BAPIYEV et al., 2021). In terms of artificial intelligence as a component of the "digital (electronic) brain" of the robot, artificial intelligence is an independent object of civil legal relations, and as a result of intellectual (creative) human activity, it is an object of intellectual property rights. From the standpoint of material features, "the difference between a robot and artificial intelligence is that artificial intelligence does not require physical form, and robots can be represented in forms of distinctive designs" (LARSON, 2010; BUIL et al., 2015).

Functionality. The functionality of a robot should be understood as a set of features that the robot can perform. The developer determines the functionality of the robot according to the needs of the scope of application of the corresponding robot. The robot can be equipped with one function or several (a combination of them). In a robot, functionality can be "physical" and/or "intelligent". Physical functionality lies in performing physically active actions in space – moving (walking, running, jumping, flying, etc.), transporting, or performing other actions with objects according to the established task. At the same time, intelligent functionality can include speaking, counting, learning, analysing, decision-making, etc.

Autonomy. The autonomy of a robot should be considered as the ability of a robot to perform its functional component independently, without external

interference. The robot's autonomy depends on two factors. First, the level of autonomy of the robot depends on the level of its intelligence component, since it activates the functionality component of the robot and thereby ensures its independent performance of certain actions. The second factor of robot autonomy depends on the level of human intervention in the robot's activity when the robot performs certain actions that make up its functional component. The level of human intervention that makes up the second factor of robot autonomy is majestic relative and is directly dependent and proportional to the first factor. Since engineers, programmers, and other specialists involved in the development of robotics face a considerable number of extremely complex problems that need to be solved for maximum autonomous operation of a robot that worked efficiently and would ensure the achievement of the goal in a particular field of robotics use. Thus, the robot is an object of the material world (device), which, depending on the level of autonomy and intelligence components, can perform the functions laid down by the developer according to the scope of application.

CIVIL LAW REGIME OF ROBOTS IN MODERN LEGAL REGULATION

Considering the civil law regime of robots in modern legal regulation, it can be compared with the legal status of slaves in the Roman state. Modern robots that are used in production, in human life support and other spheres of public life have a similar purpose as a slave in Rome. The main principle underlying the legal status of a slave was servi res sunt (slave – thing) (NOVITSKII, 2008). The slave was a thing that could speak. The only difference between a slave and an ox or mule was that they were an "instrument that speaks" (instrumentum vocale) (CHERNILOVSKIY, 1991). Robots are objects of the material world, i.e., de facto – things, but the combination of the above features that describe a robot as an object of civil legal relations gives grounds, de jure, to consider the robot along with things and other objects-goods as an independent object in the system of objects of civil legal relations. At the same time, the current level of development of robotics does not indicate the need to create an entirely new, special civil law regulatory regime for them as objects. The set of legal tools already formed in the legislation, which form the civil law regime of things, can be extended to robots, which is more than sufficient to ensure their effective civil law turnover for the next several decades (ELENEY et al., 2022; NASS et al., 2021). However, this does not exclude the addition of certain special provisions to the current civil legislation in the legal regulation of robotics (e.g., in the field of liability for damage caused by a robot to a person or their property).

A separate aspect of the civil law regime of robots that requires attention is the issue of liability for damage caused by the robot to a person or their property. Being an object of civil legal relations, a robot cannot be held liable for damage caused to a person or property, since the responsibility is borne by the subject of civil legal relations, and not by the object. Accordingly, it can be assumed that the subject of liability for damage caused by the robot may be the owner of the robot or its manufacturer (developer), etc. In this case, the resolution of the European Parliament "Report with recommendations to the Commission on Civil law Rules on Robotics" (2017) identifies two approaches to liability for damage caused by a robot:

(1) Objective liability, wherein it is necessary to prove the damage caused and the causal relationship between the functioning of the robot and the damage caused;
(2) Risk management, when responsibility is assigned to the person who should have minimised risks and consider negative consequences.

Considering that the robot is essentially a mobile thing and guided by the provisions of the Civil Code of Ukraine (2003), on compensation for damage caused by defects in goods, works and the Law of Ukraine No. 3390-VI "On liability for damage caused by product defects" (2011), it can be stated that in Ukraine, as a general rule, the first approach is laid down – the objective responsibility of the manufacturer (developer). And today, if harm is caused by a robot in Ukraine, the manufacturer (developer) will be held responsible. However, since the robot is not just an object of the material world, the choice of the approach of liability for damage caused by the robot is not sufficiently unambiguous towards the responsibility of the manufacturer (developer).

Quite striking in this regard will be the example of the use of robotics in the field of medicine. At the end of January 2022, Johns Hopkins University published information that for the first time in the world, the STAR (Smart Tissue Autonomous Robot) performed laparoscopic surgery without human assistance (GRAHAM, 2022). The STAR robot performed the procedure on animals, which requires the surgeon to apply stitches with high accuracy and consistency. A unique feature of the STAR is that it is the first robotic system that plans, adapts, and performs a surgical plan in human soft tissues. In this case, an autonomous robot in surgical intervention acted as a high-precision tool that substituted the hands of a human surgeon in terms of applying high-precision and consistent sutures to soft tissues (DE PAGTER, 2021).

Without detracting from advances in technology and artificial intelligence, carrying out such an operation would not be without human

participation, namely making a diagnosis, preparing for surgery, administering anaesthesia, monitoring vital signs during the operation, and most importantly quality control of the work performed by the robot on suturing soft tissues and stating the success of the surgical intervention by the human doctor. Ultimately, the surgeon who performed the operation using an autonomous robot is responsible for the quality of the operation as a whole and is obliged to assess all risks when performing such a surgical intervention using an autonomous robot as an instrument. If a patient dies during such an intervention using an autonomous robot, then when determining who should bear responsibility (manufacturer (developer) of the robot or a surgeon) the degree of autonomy of the robot, the quality of the work performed by it (considering its technological capabilities in this situation) and the actions of the doctor, who was generally responsible for such a surgical intervention, regarding its taking all sufficient, in this situation, measures according to medical instructions. Only after evaluating these two circumstances can one determine the degree of guilt of the manufacturer (developer) of the robot and the surgeon, and accordingly the amount of responsibility or lack thereof.

Another illustrative example that indicates that a risk management liability approach to robot harm should be considered when using robotics occurred in the United States. With the widespread advent of autopiloted cars, accidents involving such vehicles have become more frequent in the United States. The very first high-profile case was in December 2019 with 27-year-old driver Kevin George Aziz Riad in the Los Angeles suburb of Gardena. He was driving at high speed in a Tesla Model S car using autopilot, left the freeway, ran a red light, and crashed into a Honda Civic at the intersection. Two people who were in the Civic died at the scene. Riad was charged with manslaughter, although he denied his guilt, since the car was not driven by him, but by autopilot. Tesla, in this case, stated that autopilot and the more complex “full self-driving” system cannot control the car independently, and that drivers must be careful and ready to respond at any time, as indicated in the instructions (KRISHER and DAZIO, 2022). In this case, as with the robot surgeon, autopilot is a tool (assistant) for more comfortable and safe driving, and not a full-fledged driver. The absence of the driver's fault, in this case, could only be said if there were defects in the autopilot, which clearly could have caused the accident, and the driver, with all caution, could not prevent it (O'SULLIVAN et al., 2019).

Therefore, when it comes to liability for damage caused by a robot, it is considered that the approach of risk management is more correct than objective liability. When considering the issue of liability for damage caused by a robot, one cannot fail to pay attention to the conditionally third alternative approach of liability, according to which the robot is given the status of a subject – a legal or

electronic entity. Giving the robot the status of a subject suggests its tort status, and accordingly the ability of the robot to independently bear responsibility for the damage caused (LI et al., 2022). This, in turn, will eliminate such a problem as the difficulty of determining the presence of guilt and its degree in relation to the manufacturer (developer) and the owner of the robot. This approach is most beneficial for the manufacturer (developer) of robots, since it factually exempts them from liability for damage caused by the robot. One of the key issues of civil liability of the robot as a subject is the availability of property, at the expense of which compensation for the damage caused will be carried out. Evidently, the robot itself does not possess property as such.

Appropriate legal structures are required to ensure that the robot has such a property component. There are several solutions in this aspect: robot's civil liability insurance; creation of a financial fund, into which a certain percentage of the amount will be deducted when purchasing a robot (e.g., according to the principle of how value-added tax is paid when buying goods), which can later serve as a source of compensation for damages. However, despite some positive aspects of this approach for certain participants in civil legal relations, this approach is currently at least premature and impractical. Since the introduction of robots into the status of a subject will complicate their civil law turnover, the question arises whether a subject can be an object of turnover.

CONCLUSIONS

This scientific study suggests that an autonomous robot is an independent object of civil legal relations in the system of objects and is described by four key features: materiality, intelligence, functionality, and autonomy. Considering the legal nature of the robot as an object of civil legal relations, first of all its materiality, it allows introducing a regime of things regarding the legal regulation of robotics relations. This does not exclude the existence of special legislation exclusively for autonomous robots, which will determine the specific features of certain aspects of legal regulation. Furthermore, the available legal structures of civil liability in civil law are quite competitive in the approach of liability of the robot as a subject, formed doctrinally and worked out in law enforcement.

Liability for damage caused by the robot to a person or their property should be assigned to the manufacturer (developer) or owner of the robot. An analysis of the two approaches of objective responsibility and risk management suggests that the approach of responsibility of risk management is fairer. At the same time, giving the robot the status of a subject of law and assigning responsibility to the robot is not relevant, since the available well-established structures are quite effective and worked out in practice. Despite everything,

regardless of what difficulties legal science currently faces in legal regulation of robotics relations, the introduction of effective legal regulatory mechanisms is an inevitable process, since this is required by the present, and all the shortcomings and gaps of legal structures that will sometimes be identified in practice can be eliminated in the future.

REFERENCES

Asaro, P. M. (2007). *Robots and responsibility from a legal perspective.* Available at: https://peterasaro.org/writing/ASARO%20Legal%20Perspective.pdf.

Asimov, I. (2018). *I, Robot.* London: Harper Voyager.

Balkin, J.B. (2015). The Path of Robotics Law. *California Law Review,* 6, 45-60.

Bapiyev, I., Kamalova, G., Yermukhambetova, F., Khairullina, A. & Kassymova, A. (2021). Neural network model of countering network cyber attacks using expert knowledge. *Journal of Theoretical and Applied Information Technology,* 99(13), 3179-3190.

Buil, R., Piera, M. A., Gusev, M., Ginters, E. & Aizstrauts, A. (2015). Mas simulation for decision making in urban policy design: Bicycle infrastructure. *Proceedings of the International Conference on Harbour, Maritime and Multimodal Logistics Modelling and Simulation, 95-102)*. Bergeggi: I3M Conference.

Calo, R. (2016). Robots in American law**.** *University of Washington School of Law Research Paper,* 4, 1-45.

Capek, K. (2021). *R.U.R.* Kyiv: Komora.

Chernilovskiy, Z. M. (1991). *Lectures on Roman Private Law.* Moscow: Yuridicheskaya Literatura.

Danchuk, V., Bakulich, O., Taraban, S. & Bieliatynskyi, A. (2021). Simulation of traffic flows optimization in road networks using electrical analogue model. **Advances in Intelligent Systems and Computing**, 1258 AISC, 238-254.

De Pagter, J. (2021). Speculating about robot moral standing: On the constitution of social robots as objects of governance. *Frontiers in Robotics and AI*, 8.

Eleney, C.M., Bradley, M., Alves, S. & Crudden, D. M. (2022). Development of a low-cost semi-automated robotic orthophosphate system for batch analysis. *Analytical Methods*, 14(35), 3444-3450.

European Parliament. (2017). *Report with recommendations to the commission on civil law rules on robotics.* Available at:

https://www.europarl.europa.eu/doceo/document/A-8-2017-0005_EN.html.

Ginters, E., Barkane, Z. & Vincent, H. (2010). System dynamics use for technologies assessment. *22th European Modeling and Simulation Symposium*, EMSS 2010, 357-361.

Graham, C. (2022). *Robot performs first laparoscopic surgery without human help.* Available at: https://hub.jhu.edu/2022/01/26/star-robot-performs-intestinal-surgery/.

Khan, P.H.; Kanda, T.; Ishiguro, H.; Gill, B.T. & Ruckert, J.H. (2012). Do people hold a humanoid robot morally accountable for the harm is causes? *Proceedings of the Seventh Annual ACM.IEEE International Conference on Human-Robot Interaction, 1-8.* Boston: Attitudes and Responses to Social Robots.

Kharytonov, E., Kharytonova, O., Kostruba, A., Tkalych, M. & Tolmachevska, Y. (2021). To the peculiarities of legal and non-legal regulation of social relations in the field of sport. *Retos*, 41, 131-137.

Krisher, T. & Dazio, S. (2022). *Felony charges are 1st in a fatal crash involving Autopilot*. Available at: https://cutt.ly/qLmMI1h.

Larson, D. (2010). Artificial intelligence: robots, avatars, and the demise of the human mediator. *The Ohio State Journal on Dispute Resolution*, *25*(1), 105-164.

Li, Y., Guo, S. & Gan, Z. (2022). Empirical prior based probabilistic inference neural network for policy learning. *Information Sciences*, 615, 678-699.

Nass, O., Kamalova, G., Shotkin, R. & Rabcan, J. (2021). Analysis of Methods for Planning Data Processing Tasks in Distributed Systems for the Remote Access to Information Resources : Topic: Communication and control systems and networks. *International Conference on Information and Digital Technologies 2021*, IDT 2021, 273-276.

Novitskii, I. B. (2008). *Roman Private Law***.** Moscow: Jurisprudence.

O'sullivan, S., Nevejans, N., Allen, C., Blyth, A., Leonard, S., Pagallo, U. & Ashrafian, H. (2019). Legal, regulatory, and ethical frameworks for development of standards in artificial intelligence (AI) and autonomous robotic surgery. *International Journal of Medical Robotics and Computer Assisted Surgery*, 15(1).

Republic Of Korea. (2008***). Intelligent Robots Development and Distribution Promotion Act.*** Available at: https://cutt.ly/5LmKVi6.

Richards, N. & Smart, W. (2013). How should the law think about robots? *SSRN Electronic Journal***,** 5, 1-25.

Ukraine. (2003). *Resolution of the Cabinet of Ministers of Ukraine No. 1807* "On approval of the Procedure for state control of international transfers of military goods". Available at: https://cutt.ly/bLmByvP.

Ukraine. (2011). *Law of Ukraine No. 3390-VI* "On liability for damage caused by product defects". Available at: https://zakon.rada.gov.ua/laws/show/3390-17#Text.

Ukraine. *Civil Code of Ukraine.* (2003). Available at: https://zakon.rada.gov.ua/laws/show/435-15#Text.

The Law, State and Telecommunications Review / Revista de Direito, Estado e Telecomunicações

Contact:
Universidade de Brasília - Faculdade de Direito - Núcleo de Direito Setorial e Regulatório
Campus Universitário de Brasília
Brasília, DF, CEP 70919-970
Caixa Postal 04413

Phone: +55(61)3107-2683/2688

E-mail: getel@unb.br

Submissions are welcome at: https://periodicos.unb.br/index.php/RDET

The Concept of Artificial Intelligence in Justice

Submitted: 6 September 2022
Reviewed: 20 October 2022
Revised: 18 June 2023
Accepted: 5 July 2023

Article submitted to blind peer review

Oleksandra Karmaza[*]
https://orcid.org/0000-0002-1536-0776
Sergii Koroied[**]
https://orcid.org/0000-0003-4769-2262
Vitalii Makhinchuk[***]
https://orcid.org/0000-0001-7313-7911
Valentyna Strilko[****]
https://orcid.org/0000-0002-9620-0458
Solomiia Iosypenko[*****]
https://orcid.org/0000-0002-2250-8601

DOI: https://doi.org/10.26512/lstr.v15i2.44906

Abstract

[Purpose] The aim of the article is to cover the main definitions of the concept of artificial intelligence, its origins, characteristics, grounds for application, as well as direct interaction and influence on the implementation of the main tasks of justice through the use and development of artificial intelligence in the judicial procedure.

[Methodology/Approach/Design] To solve the tasks set, the study employed the appropriate methods and materials of scientific research, namely dialectical, historical, statistical, sociological, and other methods of cognition of processes and phenomena, including specialised methods of grammatical consideration and interpretation of legal norms. Furthermore, an entire block of logical methods was used, including classification (upon creating a complete classification and structuring of scientific hypotheses and assumptions), extrapolation, induction and deduction, analogy, abstraction, comparison.

[Findings] This paper investigates the emergence and transformation of artificial intelligence in modern technological and information relations, its gradual introduction in various spheres of life, namely the ways of implementation and the possibility of

[*] Full Doctor in Law, Professor at the Department of Jurisdiction Forms of Legal Protection of Subjects of Private Law, Academician F.H. Burchak Scientific Research Institute of Private Law and Entrepreneurship of the National Academy of Legal Sciences of Ukraine, Kyiv, Ukraine, e-mail: o.o.karmaza@outlook.com.

[**] Full Doctor in Law, Professor at the Department of the Civil Law and Procedure, King Danylo University, Ivano-Frankivsk, Ukraine, e-mail: s.o_koroied@gmail.com.

[***] Full Doctor in Law, Senior Research at the Department of Jurisdiction Forms of Legal Protection of Subjects of Private Law, Academician F.H. Burchak Scientific Research Institute of Private Law and Entrepreneurship of the National Academy of Legal Sciences of Ukraine, Kyiv, Ukraine, e-mail: vit_m_makhinchuk@gmail.com.

[****] PhD in Law, Senior Specialist at the Division for Translation Organization of the Main Department for International Legal Cooperation and Asset Recovery, Prosecutor General's Office, Kyiv, Ukraine, e-mail: v-yu-strilko@outlook.co.

[*****] PhD in Law, Senior Lecturer at the Department of International, Civil and Commercial Law, Kyiv National University of Trade and Economics, Kyiv, Ukraine, e-mail: iosypenko-s@outlook.com.

application in justice. Furthermore, the study analyses possible ways and legal consequences of introducing artificial intelligence into the e-justice system in Ukraine and proposes the stages of reformation.

[Practical Implications] The materials of this study are of practical value in the implementation of the goals set for the active use of artificial intelligence tools and their gradual improvement, including the development of methodological guidelines, legislative acts covering the judicial procedure and reference books and recommendations for the interpretation of regulations that have already been adopted in the process of introducing electronic justice in the country.

Keywords: Legal Proceedings. Artificial Intelligence. Electronic Justice. Corporate Disputes.

INTRODUCTION

The development of information systems that help a person make decisions began with the emergence of expert systems in the 1950s, which describe the algorithm of actions for choosing a solution depending on particular conditions. Expert systems have been replaced by machine learning, thanks to which information systems independently form rules and find solutions based on dependency analysis, using initial data sets (without first drawing up a list of possible solutions by a person), resulting in the emergence of artificial intelligence. Technological solutions developed using machine learning methods are an example of artificial intelligence that can only solve highly specialised problems (weak artificial intelligence) (PONKIN and REDKINA, 2018). The creation of a universal (strong) artificial intelligence, capable, like that person, to solve various problems, think, interact, and adapt to changing conditions, is a complex scientific and technological issue, the solution of which is at the intersection of various areas of scientific knowledge – natural science, technical, and socio-humanitarian (ARTIFICIAL INTELLIGENCE…, 2017; APPLICATION OF ARTIFICIAL INTELLIGENCE…, 2021). Solving this problem can lead not only to positive changes in key areas of life, but also to negative consequences caused by social and technological changes that accompany the development of artificial intelligence technologies (LARINA and OVCHINSKY, 2020; YAROSHENKO et al., 2020).

In recent years, the expert community has increasingly discussed whether it is possible to automate the entire procedure of delivering justice using artificial intelligence, as well as replacing a judge with a system of universal (strong) artificial intelligence capable of analysing the factual circumstances of a case, giving them a legal assessment and making an appropriate decision (ALETRAS et al., 2018; CHERNIAVSKYI et al., 2019). In China, the United States, Great Britain, France, and some other countries, such computer programmes are already

finding their application, but currently serve merely as an auxiliary tool for analysing documents and do not replace a judge. In December 2018, the first International Act specifically dedicated to the use of artificial intelligence in justice appeared – the European Ethical Charter on the use of artificial intelligence in judicial systems, approved by the European Commission for the Efficiency of Justice of the Council of Europe (EUROPEAN COMMISSION, 2020). The Charter sets out five principles for the use of artificial intelligence: the principle of respect for human rights, by virtue of which the use of a computer programme should not detract from the adversarial nature of the procedure and the right to a fair trial; principle of prohibition of discrimination; the principle of quality and safety, which makes provision for the use of certified software, which is evaluated by both technical specialists and lawyers; the principle of transparency, by virtue of which all technologies used must be brought to the public attention in an understandable form (COUNCIL OF EUROPE, 2018).

Thus, more than three decades of improvements in information and communication technologies (ICT) are breaking into the activities of courts and prosecutors, promising transparency, efficiency, and radical changes in working practices, such as paperless courts. Even if such promises have not yet been fulfilled in most jurisdictions, programmes and algorithms are already performing increasingly more judicial procedures. The impact of such technologies on the functioning of justice and the values established by international principles of judicial conduct are mostly positive. The latest technological wave in the foreign experience of well-known countries is based on artificial intelligence (AI) and promises to change the way court decisions are made (LOMAKIN and SAMORODOVA, 2017). This purpose is mainly pursued through a specific technology called “machine learning”, which makes predictions by evaluating case materials, both procedural documents and related court decisions. This data set, known as “training data,” is analysed to build statistical correlations between cases and related court decisions.

The more data the algorithm processes, the more accurately it predicts decisions in new cases (LOMAKIN and SAMORODOVA, 2017). For this reason, such systems “learn” (even if only in terms of improved statistical accuracy) to reproduce the results that judges have already achieved in such cases. Unlike the already available technological tools that digitise the exchange of data and documents, this technology of "predictable justice" (as it is usually labelled) is intended to influence judicial decision-making (APPLICATION OF ARTIFICIAL..., 2021). However, it is not yet clear whether this trend leads to better solutions or undermines the proper performance of the system. That is precisely why, to solve this and other related issues, the scientific literature contains many studies on this matter, conducted by Ukrainian and foreign

researchers such as R. F. Zakirov (2017), S. O. Furashev (2018), I. V. Pokin and A. I. Redkina (2018), V. A. Shemshuchenko (2018), M. G. Matveev, A. S. Sviridov, N. A. Aleinikova (2008), K. Pittman (2016), J. Nesbitt (2017).

The present paper aims to cover the main definitions of the concept of artificial intelligence, its origins, characteristics, grounds for application, as well as direct interaction and influence on the implementation of the main tasks of justice through the use and development of artificial intelligence in the judicial procedure.

MATERIAL AND METHODS

Using dialectical and historical methods, the authors of this study considered the ways of establishment and development of artificial intelligence in the scientific field, its main functions and tasks, signs and conditions of application. The Aristotelian and sociological method allowed determining the main stages of the development of artificial intelligence, as well as the analysis of scientific research of Ukrainian and legislative researchers, and their significance in its further development. Comparison is one of the key methods in this paper, since the subject of the analysis covers not only the legal scope of its application, but also the experience of the existence of artificial intelligence in various spheres of human and state life. Methods of grammatical analysis and interpretation of legal provisions helped identify the available regulations governing the existence of artificial intelligence in the process of regulating public relations in the state. Monitoring and making suggestions for its improvement. The methods of scientific cognition used in this study are most often general scientific methods. Within the framework of general scientific methods, the authors analyse the available opinions of foreign authors on this controversial issue.

The authors of this study describe and compare legal opinions on the regulation of the activities of artificial intelligence abroad. The paper proposes the classification of approaches to the legal understanding of artificial intelligence proposed in the scientific literature. Apart from the aforementioned methods, the study employed the comparative legal method. Firstly, to investigate the success of legal regulation of the issues under study in other countries and the possibility of implementing the corresponding legal constructions in Ukrainian legislation. Secondly, the method of legal modelling allowed formulating the alleged positive aspects and disadvantages of certain legal structures for regulating the legal status of artificial intelligence. Based on Ukrainian and foreign legislation, as well as judicial practice, the study identifies the most viable options for resolving controversial legal issues that correspond to the legal nature of artificial intelligence.

Notably, the hermeneutical method was used in this paper to interpret the essence and content of the main definitions that describe artificial intelligence in the legal plane. The provisions and conclusions of this study are also based on articles on philosophy, economic theory, general theory of state and law, financial law, theory of administrative law, other branch legal sciences, studies of individual foreign researchers. Current legislation, scientific publications, statements, assumptions, and other regulations that establish and regulate the procedure for resolving socio-legal conflicts constitute the main legal basis for scientific research. Using the sociological method, the authors clarified the positions and opinions of lawyers, prosecutors, and judges on the practical application of artificial intelligence in the justice system proceeding from judicial practice. The statistical method is used to generalise and analyse the conclusions of Ukrainian and foreign researchers and investigate the problems under study. The empirical and informational structure of this study also comprises generalisations of practical activities of subjects of jurisprudence, statistical materials, reference publications, political and legal journalism, and other legal achievements.

RESULTS

Trends in the development of modern public relations indicate a desire to use artificial intelligence in the field of electronic justice. The developed ideas about the technological aspects of artificial intelligence do not fully fit into the legal consciousness of both Ukrainian and foreign researchers of law. The legislator's unwillingness to determine the legal mode of operation of artificial intelligence is conditioned upon the lack of any experience in its use. The introduction of artificial intelligence in the life of society will show its advantages and disadvantages only after a long time. Under these circumstances and modern forecasting of mechanisms of legal regulation of machine intelligence is rather conditional and imperfect. That is why this study investigates the possible ways and legal consequences of introducing artificial intelligence into the e-justice system in Ukraine (SHEMSHUCHENKO, 2018).

Upon considering court cases, artificial intelligence will allow the court to quickly and reliably establish the essential circumstances of the case, verify the arguments of the participants in the process and, as a result, considerably reduce the time for making an objective decision. In such disputes, it is often necessary to evaluate the integrity of the behaviour of participants in public relations, regardless of the emotional and psychological factors that affect, in particular, the work of a human judge. Understanding artificial intelligence as a digital programme based on the mathematical algorithms laid down by its developers, which produces “new” solutions (machine thinking), requires studying the

algorithms of its work in court, including from the standpoint of optimising the judicial procedure and the purpose of establishing the truth in the case. This article reveals the problems of two areas of application of artificial intelligence in court when considering legal disputes: office management and general issues of litigation; assessment of evidence and establishment of legally significant circumstances in a public or private legal dispute (PONKIN and REDKINA, 2018).

Thus, in the specialised literature, artificial intelligence is understood either as a device capable of "acting, determining its actions and evaluating their consequences without full human control based on the results of processing information coming from the external environment", or as a computer programme that simulates the human brain, which has a learning mechanism built in (GOLDFARB and TREFLER, 2018). In Europe, artificial intelligence (AI) is a cyberphysical (non-biological) autonomous, but physically (energy) dependent support system that can exchange data with its environment and analyse it, self-learn based on acquired experience and interaction, and adapt its actions and behaviour in accordance with environmental conditions. According to the philosophical encyclopaedia, artificial intelligence is a digital system that simulates human intellectual and sensory abilities using computing devices (a neural network). The fact that artificial intelligence will be neutral in relation to humans is a myth. It was dispelled in modern times, when it became clear that technology has its autonomy and independence from humans. The humankind has become a hostage to the technology it created, it cannot free itself from its reverse influence on themselves It is obvious that artificial intelligence created by humans contains not only unlimited possibilities, but also unlimited dangers.

At the present time, the artificial intelligence system is spontaneously improving, influencing a person and subjugating them; it can grow into a dangerous world for humans, which is partly what is happening today and becomes an inevitable threat. Artificial intelligence has its own laws and language, the lack of a deep understanding of which in humans makes decisions unpredictable (SHEMSHUCHENKO, 2018). For example, procedural legislation requires a judge to be guided by his internal belief when evaluating evidence, which is a much more complex category than software algorithms. Depending on the particular circumstances, the same evidence may be rejected in one case and, on the contrary, accepted as a basis in another case. Admittedly, the artificial intelligence system will never be capable of penetrating the depth of the human psyche. Artificial intelligence can assess the circumstances of a case only from the standpoint of formal logic, and that is why it will never be capable of fully understanding the plot of the case, since in many cases, for example, family, and especially criminal, there is a lot of irrationals, as opposed to formal-logical.

Furthermore, upon making a decision, the court is guided by numerous evaluation and value criteria stipulated by the law. For example, the principles of justice and humanism in the imposition of punishment, the requirements of reasonableness and good faith in civil law. Understanding of such general categories is formed in a person in the process of socialisation, upbringing, and personality development – all this cannot be reproduced in a software algorithm.

In the context of dynamic updating of legislation caused, among other things, by the technological advance, it is not uncommon for courts to apply the analogy of statute and the analogy of law, which is understood as dispute resolution based on the general principles and content of legislation. The meaning of legislation, that is, its spirit, can only be revealed by a person with a high level of legal culture, and not by a computer. With particular clarity, the impossibility of replacing a judge with artificial intelligence is established in cassation proceedings. After all, the basis for cancelling a court decision in cassation is not any formal violation, but only a substantial violation of legal norms that affected the results of consideration of the case and without the elimination of which it is impossible to restore and protect violated rights, freedoms, and legitimate interests. These criteria derive from the principle of legal certainty, by virtue of which the quashing of a judicial decision on formal grounds is inadmissible. Only a professional judge can evaluate whether the violation committed meets the materiality criterion and whether it can affect the outcome of the case (COUNCIL OF EUROPE, 2018).

In turn, the computer algorithm will record any violation and come to the conclusion that the judicial act is subject to cancellation, even if the formal cancellation leads to the same outcome of the case. Therefore, it is at least premature, but most likely impossible, to contemplate replacing the judge with artificial intelligence. Therewith, the use of artificial intelligence in the consideration of the already mentioned indisputable requirements is not excluded, primarily in writ proceedings, since such work is not related to the analysis of legal relations between the parties and is more technical in nature. In some developed countries, such systems are already being implemented (PONKIN and REDKINA, 2018).

Admittedly, the constant expansion and change of the regulatory framework, judicial practice, increasing the burden on the judicial system, which leads to a large number of investigative and judicial errors, actualises the use of artificial intelligence in the Ukrainian judicial system as it is disinterested, incorruptible, objective, and capable of finding almost infallible legal solutions, ways, and methods of effective justice. The authors of the present study cannot but agree that such systems will not only be of great service in the work of courts, prosecutors, officials of investigative bodies, and advocates, but will also enable

an objective external control over their activities. Unfortunately, to date, no official document of the legislative framework of Ukraine contains a regulatory definition of the term "artificial intelligence", although the term itself is actively used in many countries. This situation is conditioned upon the lack of a single legal approach to establishing its common characteristics in different countries. In particular, the creators of the European civil legislation on robotics point out that it is impossible to give an accurate definition of artificial intelligence, which is associated with the real presence of various robots. In this regard, in their opinion, the study of the latter should be approached casuistically, considering each work individually, as a separate unique case.

DISCUSSION

Thus, the term "artificial intelligence" is used to refer to a large scope of scientific and applied research. This name, which is attached to this subject area, most people are more likely to associate with smart robots or thinking computers, numerous images of which were created in science fiction works. That is why many concerns about artificial intelligence are circulating in modern society, and such alarm signals continue to arrive with increasing force. Artificial intelligence is not only associated with the display of human qualities in machines, it also helps drive vehicles, can become an ideal tool for stealing confidential data, increase company productivity, or create ideal opportunities for corporate spies. Artificial intelligence is not yesterday's invention. The history of its creation is full of memorable moments and names of reputable scientists, ups and downs, extravagant promises and loud disappointments. Artificial intelligence is finally starting to bring real benefits to the state, business, citizens, and the humankind in general.

The power of computers has dramatically increased, there are more algorithms for solving tasks, and, most importantly, the world produces a huge amount of fuel that feeds artificial intelligence – billions of gigabytes every day. Notably, despite the active development of AI technologies, the level of their implementation remains low, which complicates the assessment of the true potential of such technologies. McKinsey Institute experts conducted detailed case studies on five sectors of government activity. The obtained results allow assuming a hypothetical transformation of some types of activities, which, in turn, will disrupt the work of other sectors by a chain reaction (ARTIFICIAL INTELLIGENCE…, 2018). Artificial intelligence has broad prospects for many stakeholders, including multinational corporations, start-ups, governments, and social institutions (WORLD BANK GROUP, 2016). There is no doubt that artificial intelligence has a huge potential for fundamental change in society. However, at this stage, it is difficult to predict the direction that the development

of this technology will take. Corporations, governments, and employees themselves are guided by the principle of time intervals. However, there is already a need for urgent and clear measures to respond to risks, which are also evident in every existing state (PONKIN and REDKINA, 2018).

The development of digital technologies in the era of the information society and the processes of globalisation, the speed of data transmission, confirmed the prospect of introducing artificial intelligence in the courts. It became evident that artificial intelligence is our present, and not the future, which the humankind has long begun to study and only recently approved and began to apply it in most countries of the world. Therewith, the current state of the research on artificial intelligence in the world indicates a long workflow of software engineers together with neuroscientists to build an artificial cognitive system close to human physiology and the reproductive abilities of the human brain, which are still not studied by science (PONKIN and REDKINA, 2018; BABAK et al., 2021). In legal proceedings, human activity is limited by certain formal rules, which is why it is permissible to use only specialised intelligent systems that can work, although independently, but under full human control (EUROPEAN COMMISSION, 2020). Artificial intelligence should be recognised as a source of increased danger; therefore, in this case, it is necessary to assign responsibility for the damage caused by its activities to its creators in accordance with the law. Responsibility for damage caused as a result of the use of artificial intelligence in legal proceedings should be borne by the state. After all, only the state should act as the sole creator of intelligent systems, if they are used in state bodies, to perform the obligations assigned to them. Therefore, the creation and use of "smart" robots for criminal purposes, as well as illegal interference in the activities of artificial intelligence systems, which will lead to causing socially dangerous harm, should impose criminal liability (SHEMSHUCHENKO, 2018; TACIJ et al., 2014).

For example, in the United States, scientists have long begun to think about the use of artificial intelligence in court proceedings. The country annually considers a huge number of cases of deprivation of parental rights. Considering the fact that there is a case law in the USA, that is, the possibility of copying a decision from another case that is suitable in terms of parameters, the idea is not so strange. It is enough to find a similar case in the database and see what decision was made then. And if there is a large amount of information, evidence base in the case, then the task is completely reduced to analysing statistics and actions according to the template. Thus, such algorithms are created by people, which means that they somehow reflect the picture of the world of their creators. Neural networks used in artificial intelligence technologies are based on decisions made by humans. Therewith, as data accumulates, it is possible to identify patterns that

have nothing to do with decision-making (BUOCZ, 2018). But the neural network is designed in such a way that it will certainly take the detected pattern for the necessary material. For example, if men were convicted more often than women in any type of criminal case, then for artificial intelligence, the defendant's gender may eventually turn into a significant factor and would influence decision-making.

In December 2018, the European Commission for the Efficiency of Justice of the Council of Europe approved the European Ethical Charter, which contains the principles of the use of artificial intelligence in judicial and law enforcement systems (ARTIFICIAL INTELLIGENCE…, 2020). This is the first international act regulating such a sensitive and unknown area. The Charter deals with the need for user control: a judge has the right to disagree with a decision proposed by artificial intelligence, and any participant in a dispute has the right to appeal against such a decision and demand that the court consider their case without using artificial intelligence in court. There is, however, another aspect that cannot be ignored. In the present-day world, “advanced" technologies are used not only by lawyers, but also by representatives of criminal structures, organised crime, etc. If their actions are not countered by the same modern technology, the criminals will find themselves in a deliberately advantageous position. The same reasoning allows contemplating the importance of maintaining equality before the law or the court: if modern technologies are used, then ideally, they should be accessible to everyone. Thus, the question of whether or not artificial intelligence will penetrate the field of law should not be considered critically. It is only important to understand where it belongs, and which areas of activity of the state and citizens in it will forever or at least for a long time remain with a person (SHEMSHUCHENKO, 2018).

Undoubtedly, for more than three decades, advances in information and communication technologies (ICT) have been penetrating the work of courts and prosecutors, promising transparency, efficiency, and radical changes in the procedure and methods of activity, such as the transition to paperless proceedings (GETMAN et al., 2019). Although these promises have not yet been fulfilled in most countries, computer programmes and algorithms are carrying out a growing number of judicial procedures. These technologies have a predominantly positive impact on the operation of judicial systems and the values stipulated by international principles of judicial conduct. The latest wave of technologies is based on artificial intelligence and promises to transform the way court decisions are made. This goal is achieved mainly through a special technology called "machine learning", which makes forecasts by analysing case materials – both procedural documents and corresponding court decisions (SHEMSHUCHENKO, 2018). Based on the analysis of this set of data (“training data”), statistical

comparisons are established between cases and corresponding court decisions. The more data the algorithm processes, the more accurate its predictions for new cases will be. Consequently, these systems "learn" to reproduce decisions that judges would make on similar ones. Unlike the already used technologies for digital data and document exchange, this technology of "predictable justice" (as it is often incorrectly called) is designed to influence court decisions. At present, it remains unknown whether it will improve the quality of solutions or interfere with the proper operation of the system (LARINA and OVCHINSKY, 2020).

The potential impact of such technology on the administration of justice can be assessed by examining the problems posed by already used information technologies, such as record-keeping and electronic filing systems. In England and Wales, a simple arithmetic error in the official form of the document used in divorce cases led to an incorrect calculation of alimony in 3,600 cases in 19 months. The problem is not the error itself, but the reasons why the Ministry of Justice and those who used this form did not notice it for so long. Users usually pay attention to the interface and the tools that enable them to use technological systems, rather than their internal operation (MATVEEV et al., 2008). Judicial technologies provide access to an array of court case data to increase transparency, but the way systems assess this data internally is difficult to evaluate and control. Therefore, the main question is whether it is possible to create effective mechanisms to control the internal operation of ICT and data processing algorithms. Another question is how to guarantee due oversight of technologies and their accountability, namely using the example of artificial intelligence (or rather machine learning).

Some countries, including the United States, use technology that makes recommendations for making decisions about pre-trial detention. Such programmes use algorithms calculating the probability of relapse and "estimate" the probability that the accused will commit a crime if they are not taken into custody. Technologies, whether office management systems, simple online forms, or more complex programmes that use artificial intelligence in their activities, should only be used in litigation if there are appropriate human-side control mechanisms (BUOCZ, 2018; SHULZHENKO and ROMASHKIN, 2021). After all, today, the problem of control is even more acute when it comes to artificial intelligence systems based on machine learning. In this case, the forecasts are based on algorithms that change over time. In machine learning, algorithms "learn" (change) based on their experience. When algorithms change, one no longer knows how they work or why they behave in a certain way. How can the humans ensure their accountability if they do not possess effective monitoring mechanisms? This question remains open. And until technical and institutional solutions are found, the principle of caution should be guided. The reservations

and precautionary principle mentioned are part of the Ethical Charter on the use of artificial intelligence in the judicial systems of the Council of Europe. This specifically refers to the principles of compliance with fundamental rights and user control of artificial intelligence (SHEMSHUCHENKO, 2018). However, the way these principles are to be implemented remains unclear. This task is certainly not for lawyers, parties to the case, or judges. It can only be carried out with the involvement of specialists from various fields, monitoring the operation of systems and evaluating artificial intelligence for compliance with key values stipulated by international principles of judicial conduct and regulations available in national legislation in each state practicing artificial intelligence.

CONCLUSIONS

Considering the arguments brought up in the present study, broad discussions at international conferences and scientific discussions, the issue of developing common approaches to understanding the place of artificial intelligence in the modern system of knowledge and international relations is topical. However, the scientific literature contains enough reasons to doubt the use and implementation of artificial intelligence. In this regard, it would be correct to suggest the following questions that are to be resolved, namely:

(1) development of approaches to the future strategy or concept of legal regulation of artificial intelligence;
(2) determination of the scope of its legal personality and probability of liability;
(3) suggestions of areas for development in both national and international law;
(4) investigation of legally significant problems relating to links with new developments in artificial intelligence, as well as relating to the application of the available types of autonomous intelligent systems, in various transport, communication, security, legal systems, etc.;
(5) determination of the prospects for creating doctrines and legal provisions concerning the developers, control and improvement of autonomous intellectual systems, legal regimes, variables for the use of such systems, as well as the development of links between new mechanisms of legal support for artificial intelligence;
(6) permissibility and limits of application of modern legal norms concerning liability (administrative, civil, criminal) against developers of artificial intelligence systems, their operators, and other persons.

An analysis of those arguments suggests that litigation and the work of artificial intelligence are impossible in isolation from a human judge. The available artificial intelligence technologies do not allow making "machine decisions" (judicial acts) independently and completely. Questions of law and legal qualification cannot be transmitted to artificial intelligence without their evaluation by a human judge. It is necessary to use artificial intelligence in matters that require processing a large amount of information and documents in electronic form. Thus, artificial intelligence will ensure procedural savings and terms of consideration of a legal dispute on the merits by means of speed and error-free calculation and processing of a large number of incoming and outgoing correspondence, procedural documents in the case, evidentiary material, including decisions made in the given proceedings. The use of artificial intelligence ensures the development of technological legal science in Ukraine in terms of objective establishment of legal facts. Public disclosure of digital algorithms for the operation of judicial artificial intelligence will bring greater digital publicity to Ukrainian litigation and ensure transparency of the entire judicial system in the state.

REFERENCES

Aletras, N., Tsarapatsanis, D., Preoţiuc-Pietro, D. & Lampos, V. (2018). Predicting judicial decisions of the European Court of Human Rights: A Natural Language Processing Perspective. *PeerJ Computer Science, 2*, e93.

Application of Artificial Intelligence on the Basis of the Court of First Instance: VRP Initiates the Launch of a Pilot Project. (2021). Available at: https://jurliga.ligazakon.net/news/201578_zastosuvannya-shtuchnogo-ntelektu-na-baz-sudu-persho-nstants-vrp-ntsyu-zapusk-plotnogo-proektu.

Artificial Intelligence: The Next Digital Frontier? (2017). Available at: https://www.mckinsey.com/~/media/mckinsey/industries/advanced%20electronics/our%20insights/how%20artificial%20intelligence%20can%20deliver%20real%20value%20to%20companies/mgi-artificial-intelligence-discussion-paper.ashx

Babak, V. P., Babak, S.V., Eremenko, V.S., Kuts, Y.V., Myslovych M.V., Scherbak, L.M. & Zaporozhets, A.O. (2021). Models of Measuring Signals and Fields. *Studies in Systems, Decision and Control, 360*, 33-59.

Buocz, T. J. (2018). Artificial intelligence in court: Legitimacy problems of AI assistance in the judiciary. *Retskraft — Copenhagen Journal of Legal Studies, 2*(1), 41-59.

Cherniavskyi, S. S., Holovkin, B. M., Chornous, Y. M., Bodnar, V. Y. & Zhuk, I. V. (2019). International cooperation in the field of fighting crime: Directions, levels and forms of realization. *Journal of Legal, Ethical and Regulatory Issues, 22*(3), 1-11.

Council of Europe. (2018). *European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and Their Environment.* Available at: https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c.

European Commission. (2020). *On Artificial Intelligence – A European approach to excellence and trust.* Available at: https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf.

Furashev, S. O. (2018). *Internet of things:* Problems of legal regulation and implementation. Kyiv: Polytechnic Publishing House.

Getman, A., Karasiuk, V., Hetman, Y. & Shynkarov, O. (2019). Ontological representation of legal information and an idea of crowdsourcing for its filling. *Advances in Intelligent Systems and Computing, 836*, 179-188.

Goldfarb, A. & Trefler, D. (2018*). AI and International Trade.* Cambridge: National Bureai of Economic Research.

Larina, O. S. & Ovchinsky, V. S. (2020). *Artificial intelligence. Ethics and law.* Moscow: Knizhnyĭ mir.

Lomakin, N. I. & Samorodova, I. A. (2017). *Digital economy with artificial intelligence,* 254-257. Advances in Science and Technology: Collection of articles based on the results of the IX International Scientific and Practical Conference. Moscow: Research and Publishing Center "Aktualnost.RF".

Matveev, M. G., Sviridov, A. S. & Aleinikova, N. A. (2008). *Artificial intelligence models and Methods.* Application in economics. Moscow: Publishing House "Finansy i Statistika".

Nesbitt, J. (2017). *Ways artificial intelligence is transforming trade.* Available at: https://www.tradeready.ca/2017/topics/import-export-trade-management/4-ways-artificial-intelligence-transforming-trade/

Pittman, K. (2016). *Infographic*: A brief history of collaborative robots. Available at: https://www.engineering.com/story/infographic-a-brief-history-of-collaborative-robots.

Ponkin, I. V. & Redkina, A. I. (2018). Artificial intelligence from the point of view of law. *Bulletin of the Peoples' Friendship University of Russia. Series: Legal Sciences, 22*(1), 91-109.

Shemshuchenko, V. (2021). *Artificial intelligence in justice***.** Available at: https://cedem.org.ua/analytics/shtuchnyj-intelekt-pravosuddia/.

Shulzhenko, N. & Romashkin, S. (2021). Types of individual criminal responsibility according to article 25 (3) of Rome Statute. *Juridical Tribune, 11*(1), 72-80.

Tacij, V. J., Tjutjugin, V. I. & Grodeckij, J. V. (2014). Conceptual model establish responsibility for offense in the legislation of Ukraine. *Criminology Journal of Baikal National University of Economics and Law, 2014*(3), 166-183.

World Bank Group. (2016). *Harnessing the Power of Big Data for Trade and Competitiveness Policy*. Available at: https://openknowledge.worldbank.org/bitstream/handle/10986/26266/113275-WP-PUBLIC-P152206-8-3-2017-17-28-0-BigDataTCEdited.pdf?sequence=5&isAllowed=y.

Yaroshenko, O. M., Vapnyarchuk, N. M., Burnyagina, Y. M., Kozachok-Trush, N. V. & Mohilevskyi, L. V. (2020). Professional development of employees as the way to innovative country integration. *Journal of Advanced Research in Law and Economics, 11*(2), 683-695.

ZAKIROV, R.F. (2018). The use of modern IT-technologies as a means to achieve the main objectives of the judiciary. *Bulletin of the Civil Process*, *2*(1), 211-219.

The Law, State and Telecommunications Review / Revista de Direito, Estado e Telecomunicações

Contact:
Universidade de Brasília - Faculdade de Direito - Núcleo de Direito Setorial e Regulatório
Campus Universitário de Brasília
Brasília, DF, CEP 70919-970
Caixa Postal 04413

Phone: +55(61)3107-2683/2688

E-mail: getel@unb.br

Submissions are welcome at: https://periodicos.unb.br/index.php/RDET

Image-Based Digital Face Identification Technologies: Criminal Law Aspect

Submitted: 23 August 2022
Reviewed: 18 October 2022
Revised: 26 October 2022
Accepted: 22 November 2022

Article submitted to blind peer review

Sofiia Ya. Lykhova[*]
https://orcid.org/0000-0003-2861-519X
Andrii V. Svintsytskyi[**]
https://orcid.org/0000-0002-0956-0341
Andrii M. Padalka[***]
https://orcid.org/0000-0003-3713-1007
Yuriy Yu. Nizovtsev[****]
https://orcid.org/0000-0002-7641-6403
Andrii Lyseiuk[*****]
https://orcid.org/0000-0002-9026-1188

DOI: https://doi.org/10.26512/lstr.v15i2.44744

Abstract

[Purpose] The purpose of this article is to analyze the theoretical and practical aspects of digital face identification technology in Ukraine and suggest the necessary corrections to the optimal legal regime for the use of such technology in criminal proceedings.

[Methodology/Approach/Design] The leading research method is the inductive method of the legal analysis that involves the problem formulation, analysis of the legal provisions regulating this question, practical study of the law enforcement, and formulation of conclusions.

[*]Sofiia Ya. Lykhova is Doctor of Law, Professor, Head of the Department of Criminal Law and Procedure of the he National Aviation University. Address: 03058, 1 Lubomyr Husar Ave., Kyiv, Ukraine. E-mail: lykhova8094@edu-knu.com.

[**]Andrii V. Svintsytskyi is PhD in Law, Professor at the Department of Criminal Procedure and Criminalistics of the Educational and Scientific Institute of Humanities of the National Academy of the Security Service of Ukraine. E-mail: svintsytskyi8143@acu-edu.cc.

[***]Andrii M. Padalka is Doctor of Law, Deputy Director of the Ukrainian Scientific and Research Institute of Special Equipment and Forensic Expertise of the Security Service of Ukraine. Dr. Padalka is also Associate Professor at the Department of Financial Investigations of the University of the State Fiscal Service of Ukraine. E-mail: padalka8143@neu.com.de.

[****]Yuriy Yu. Nizovtsev is PhD in Law, Leading Researcher of the Research Laboratory of the Center for Forensic and Special Expertise of the Ukrainian Scientific and Research Institute of Special Equipment and Forensic Expertise of the Security Service of Ukraine. E-mail: nizovtsev8218@sci-univ.com.

[*****]Andrii Lyseiuk is PhD in Law, Associate Professor at the Department of Investigative Activities of the National University of the State Fiscal Service of Ukraine. E-mail: lyseiuk8143@sci-univ.com.

[Findings] In this article, the authors present a complex analysis of the Ukrainian legislation, define the particularity of criminal responsibility for the violation of privacy under the Ukrainian law in the context of the use of digital face identification technology, and suggest a list of reasonable amendments to the legislation to improve the level of such protection.
[Practical Implications] The materials of this article have practical value for investigating crimes and protecting individuals against illegal use of their images by using digital face identification technology in the context of Ukrainian law.
[Originality/Value] The topicality of the study is due to the fact that over the past decade face recognition has become one of the most powerful biometric technologies capable of identifying and verifying people involved in crimes based on digital images or video frames, but the legal regime of said identification had not yet been sufficiently explored in Ukraine.

Keywords: Digital Identification. Biometric Technologies. Portrait Expertise. Privacy. Face Identification.

INTRODUCTION

A person's face is the central feature by which one can be identified. It changes relatively little over time and is a typical identification object. Somehow, the person's identification by his or her face has been used by investigators since very ancient times. Even before the invention of photography, law enforcement agencies employed artists to draw portraits of criminals based on the victim's description. The invention of photography made it possible to photograph criminals, create card indexes, and identify a person by photos and not only directly as it was. It has expanded the opportunities of investigators in detecting crimes. The next step of the person identification by appearance was the creation of a facial composite, which was a tool that allowed to make an approximate portrait of a suspect provided by an eye witness without the involvement of a forensic artist. However, only the invention of the technology that allows identifying a person by a photo or video directly, without human intervention, has been a real revolutionary development in this field. Moreover, modern identification technologies often determine who is in the photo more precisely than traditional direct recognition by photos in the criminal proceeding (Inshyn et al., 2021).

C. Poirson states face recognition has become one of the most powerful biometric technologies over the last decade, capable of identifying and verifying people based on a digital image or video frame (Poirson, 2021). The modern investigative practice makes the research of this subject especially relevant. In particular, the recent case of Victoria Kotlenets caused a great resonance in the Ukrainian mass media. According to investigators, she resembled a woman who

escorted the Ukrainian military prisoners in Donetsk in August 2014. As for the woman, the investigators applied the facial recognition approach at the Forensic Center of the Ministry of Internal Affairs using her photos from social networks. At the same time, the defense provided alternative data for comparing photos using a modern batch data identification system. The court has now sided with the defense and released Victoria Kotlenets from custody (Shramovich, 2021). This example is illustrative but not unique. In particular, in 2017, a victim reported it to the US police service on the following issue. After a date at a bowling club, she found herself missing $400 and asked the manager to view the security footage that showed her companion stealing the money from her bag. Despite the clear evidence, the search for the woman's companion was difficult: she only knew his name, and he deleted his profile from the dating site where they had met. His number, then disconnected, was tied to a hard-to-track phone. The security video spotted his car in the parking lot, but the number plate was not visible. After some time, the investigator provided a photo from the victim's mobile phone for digital face identification. It helped to identify the man, his personal data, and the address (Merchlinsky, 2019).

Antoaneta Roussi points out that there are a lot of claims in the USA right now that are aimed at forbidding (at least temporary) the use of face identification technologies by the police (Roussi, 2020). To date, a lot of cities in the USA forbid, at least temporarily, the use of face identification technology by government agencies to enact legislation that would make the procedure of face identification more transparent. Europe and the USA are now considering suggestions on how to regulate this technology. However, Thakur and other scientists say it is important to remember that the digital identification system has been recently directed on a person’s identification, approvals of payments, identification of criminals, etc. So, the identification of criminals is not the main way to utilize such systems (Thakur et al., 2020).

Given the above, the purpose of this article is to analyze the theoretical and practical aspects of the use of digital face identification technology in Ukraine and to propose an optimal legal regime for the use of such technology in criminal proceedings based on the study.

METHODOLOGICAL FRAMEWORK

At this stage of the development of legal science, most legal scholars do not pay enough attention to the methodology of legal research. Legal research involves the interpretation of the law through various methods, such as interpreting the content of the text itself, analyzing case law, using the history of the law to determine the intentions of the legislator and studying the views of other legal scholars or experts. Scientific and legal research involving the use of

primarily inductive methods by the researcher (analytical research) differ from the positivist research paradigms both in form and essence. In general, in science, the researcher must indicate methods, procedures, statistics, and information about the boundaries of a study for it to be reproducible. However, analytical legal research cannot be considered strictly reproducible in this case since the materials, taken for generalization (for example, the most famous cases), cannot be often selected at random like samples in biology or respondents in sociology. Examples from practice, the scientists' approaches for analysis are selected on the principle of reputation and authority. Choosing just random cases from the practice of different courts at different times will not demonstrate the appropriate scientific effect.

N. Semchuk points out that legal science is currently actively seeking new solutions to methodology issues (Semchuk et al., 2019). Sunstein notes that when applying the method of legal analogy in the analysis of specific issues, the following components should be taken into account: causation, focus on details, avoidance of purely theoretical statements, and principles operating at low and medium levels of abstraction (Sunstein, 1993). T.R. Tyler points out that the classical method of legal research is a normative analysis of law (doctrinal analysis) that involves an attempt to understand the optimal balance of rights and responsibilities within the framework defined by law (Tyler, 2017). Claire Nolasco claims that the most common method of classical legal research in Europe is the IRAC acronym, which means a method of legal analysis that consists of a problem statement, analysis of legal provisions governing this issue, study of law enforcement practice, and formulation of conclusions (Nolasco et al., 2010).

Given the above, this study has an analytical nature, aims to study the current state of legal regulation on the issue of theoretical and practical aspects of the use of digital face identification technology in Ukraine, and applies the primarily inductive scientific method. In this scientific work, the inductive method of legal analysis is used as the main one, which involves a problem statement, analysis of the provisions, rights governing this issue, the study of the law enforcement, and formulation of conclusions.

RESULTS

As Bah points out, from the technical point of view, face identification is a computer program that is able to find, track, identify, and check a person's face by a photo or video that is made with a digital camera (Bah e Ming, 2020). There are a number of factors that influence the program: different light conditions, noise in the pictures, scale, pose, etc. Variations of the Local Binary Pattern (LBP) are usually used as an algorithm. It is a type of a visual descriptor used to classify

in computer vision as a special case of the texture spectrum model proposed in 1990. OpenCV (Open-Source Computer Vision Library) is also an often-used method. It is a library of functions and algorithms of the computer vision, image processing and numerical algorithms of a general-purpose type with open source.

Thakur described advantages of the OpenCV – the library that was created by Intel in 1999. It is mainly built to work in real-time image processing systems that include state-of-the-art computer vision algorithms (Thakur et al., 2020). Ramnya stated that a face is the most important part of a human body that unambiguously confirms the identity. Using facial features as biometric, you can implement a face recognition system (Ramya et al., 2020). There was a project used in practice to check attendance of students. The project was grounded on the face identification technology system that is based on OpenCV and showed a good result. Herewith Intorna and Nissenbaum paid attention to the fact that it is important to have an extensive photo base to compare the images for the right functioning of the digital algorithms (Introna e Nissenbaum, 2020). J. Detsing also paid attention to the technical advantages and the high accuracy of the method, sometimes even more than 90% (Detsing e Ketcham, 2017).

It is also important to mention that now, the most popular programs for face recognition are Clarifai, DeepFace, DeepVision, FaceFirst, Face++, OpenFaceTracker, Paravision, Rohos Face Logon, Trueface etc. At the same time, Google (Google lance) and Facebook have powerful face recognition capabilities as well. That is, today, face recognition systems are a software product owned by its developers, private companies, and distributed primarily on a commercial basis. For instance, in criminal procedure, an attorney may possess a high-quality and functional face recognition system that he bought. Meanwhile, investigators may have no face recognition system, because the state has not purchased such a system for the police yet.

The next important aspect of the face recognition system is the fact that for its successful functioning there is a need for an extensive library of humans' images that will be taken for comparison. One of the top-priority questions for the legal science is processing the digital photos of an individual, unbeknownst to him or her, with the purpose to identify a person. As C. Poirson pointed, the technology of the face recognition system is not only being used during investigations but also in a lot of other fields (Poirson, 2021). At the same time, scientists are seriously concerned about the limits of the use of the technology, because face recognition can indeed have a very serious and irreversible impact on fundamental human rights and civil liberties. Meanwhile, it is worth noting that from the criminal point of view, such human identification based on the physical characteristics, on one hand, may be classified as the subspecies of forensic portrait examination, because it also has an aim to clench the matter whether one

or different people are depicted in the presented photographs or other objective images of the person's appearance. On the other hand, given the possibility of conducting such a study using simple software in real time (i.e., ease of use), it can be compared with the use of the police databases or forensic records.

From a legal point of view, there are reasons to consider the results of digital visual identification of an individual as operational measures (for preliminary identification and construction of versions that will be supported by other evidence or refuted by them during the investigation in the future) as well as appropriate evidence in the form of expertise that will be provided to the court (Britchenko & Saienko, 2017). In this case, despite the almost identical technical procedure of identification, from a legal point of view, there will be some differences. From the point of view of criminal law, in this context, there are such problematic aspects as the legal regime of photographs imported into the face recognition databases and photographs used for comparison with those available in databases, as well as the limits of such technology in Ukraine in terms of privacy in criminal law.

Firstly, let us look at the way of dealing with the said problem abroad. C. Poirson pointed on the main features of legal regulation of the face identification technology in different countries. He also stated that the Chinese Cybersecurity Law from November 7th, 2016 gave to the Chinese government a big range of authority to regulate and control Internet services. Article 24, of this law, obliges Internet providers to identify the user before entering into the agreement or delivering them any services. Under the pretext of protection of users' rights, providers, social networks, and websites of China require users to make their photos available for further digital identification. Such an approach that is not democratic nonetheless makes China a world leader in the development of digital face identification technology. In contrast to China, Japan provides high standards of personal data protection according to the 2003 Act on the Protection of Personal Information. The Act provides for the consent of the data subject, except in exceptional cases. In exceptional cases, the use of such technologies without the consent of the subject may be possible only if the Ministry of Justice gives a special permit (Poirson, 2021).

In Europe, the processing of photographs is generally not considered to be the processing of biometric data unless such data are processed by a technical system for the purpose of unambiguous identification or authentication of an individual. However, the General Data Protection Order No. 2016/679 of 27 April 2016 prohibits the processing of images for identification purposes without the consent of the data subject (Poirson, 2021). Claire Merchlinsky notes that in the United States, face recognition is usually decided at the state level. Many states, including Massachusetts, California, and others, are currently considering

banning such use because of the high risk of human rights abuses. The rest of the states treat this technology with caution (Merchlinsky, 2019).

The legislation of Ukraine regulates the legal regime of photographs in a rather outdated way, without taking into account the development of technology. The Civil Code of Ukraine (2003) in Art. 303 still classifies photographs of an individual as personal papers and considers them as personal property of the person. The Law of Ukraine "On Information" (1992) contains a definition of the term “document”. In this case, the document is a material medium that contains information, the main functions of which are its storage and transmission in time and space. At the same time, the information is any information and / or data that can be stored on physical media or displayed electronically. As it can be seen, different laws in virtually the same sense operate with the concepts of personal "papers" and "documents". In this regard, it would be important for the legislator to unify the terminology by amending the Civil Code of Ukraine by clarifying, for example, "personal papers (documents)". Nevertheless, it should be noted that the Law correctly states that the main function of documents is to store information.

On the other hand, in accordance with Art. 307 of the Civil Code of Ukraine, an individual may be photographed, filmed, televised or videotaped only with his or her consent. A person's consent to be photographed, filmed, televised, or videotaped is presumed if the filming is carried out openly on the street, at meetings, conferences, rallies and other public events. In this case, an individual who has agreed to be photographed, filmed, televised or videotaped may demand the cessation of his or her public showing in the part that concerns their personal life. Expenses related to the dismantling of the image or record are reimbursed by this individual. The norm formulated in Art. 308 of the Civil Code of Ukraine indicates that a photograph, other works of art depicting an individual may be publicly shown, reproduced, distributed only with the consent of this person, and in case of death - with the consent of their heirs (except for the cases of posing for a fee) (Lytvyn et al., 2022).

The above gives grounds to conclude that such legal regulation was quite justified in pre-digital times, when the photograph had no direct identification value and could be used only as part of a paper file. In the digital age, the direct provision that an individual may be photographed or videotaped without his or her consent in any public place (without specifying whether such an image may then be stored, distributed, or included in an appropriate identification database) may be considered as excessive interference in their personal life. By contrast, a total ban on filming in public places will make it impossible for, for example, car video recorders, traffic cameras, etc. to work. Therefore, at this stage, the structure available in the Civil Code of Ukraine calls for rethinking in terms of the balance of public interests and private life.

The Law of Ukraine "On Personal Data Protection" (2010) indicates that consent of the personal data subject is a voluntary expression of the individual's will (on the condition that the person was informed) to give a permission for the processing of their personal data according to the aim of such processing that was expressed in written form or in any other form that provides an opportunity to confirm that there was such permission. In the field of e-commerce, the consent of the personal data subject may be given during registration in the information and telecommunication system of the e-commerce subject by marking the permission to process their personal data in accordance with the stated purpose of their processing, provided that such system does not create opportunities for personal data processing up to the moment of marking.

Article 264 of the Criminal Procedure Code of Ukraine (2013) points out that the search, detection and recording of the information contained in the electronic information system or its parts, access to the electronic information system or its part, as well as obtaining such information without the knowledge of its owner, possessor or holder may be carried out by decision of the investigating judge, if there is any data on the availability of the information in the electronic information system or its part that is important for a certain pre-trial investigation. It does not require the permission of the investigating judge to obtain information from electronic information systems or parts thereof, access to which is not restricted by its owner, possessor or holder or is not related to overcoming the logical protection principles.

Herewith, the compression of Art. 245 and Art. 160 of the Criminal Procedure Code of Ukraine involves receiving of samples for examination in the form of things and documents by the decision of the investigating judge in the order of temporary access to things and documents. Art. 182 of the Criminal Code of Ukraine (2011) sets responsibility for illegal collection, storage, using, destruction, sharing of confidential information about an individual or illegal alteration of such information, except cases provided by other articles of the Criminal Code of Ukraine. At the same time, the Criminal Code of Ukraine has an explanatory norm, according to which public, including through the media, journalists, public associations, trade unions, notification about a criminal or other offenses committed in compliance with the law, are not actions provided for in this article, and does not entail criminal liability.

However, the question arises: has the face recognition system ever been used illegally in the world? For example, the Data Protection Authority in Sweden fined the local authority 200,000 SEK ($20,700) last year as it used face recognition technology to monitor student attendance at school. Data Protection Authority in France said such a technology violates the EU General Data Protection Regulation. Local authorities in Skelleftea have illegally processed

sensitive biometric data and did not perform a proper impact assessment provided for consulting with the regulatory body and obtaining prior approval. Although the school provided parental consent to monitor students, the regulatory body did not consider this an adequate legal reason for collecting such personal data.

The regulatory body notes that some parts of the school can be called public spaces. However, students shall have the right to privacy when they are in the classroom. The decision stated that it would have been possible to record attendance without surveillance cameras since other ways existed. Apart from this case, Big Brother Watch researched that face recognition technology has been secretly used in shopping malls, museums, and conference venues in Britain (Levchenko et al., 2021).

The research described a situation where a 14-year-old child, wearing a school uniform, was misidentified by the facial recognition system and subsequently surrounded by four plainclothes police officers. They dragged her out to a side street, held her hands, interrogated and asked for her phone number, and even took her fingerprints. When the officers realized that the "system" was wrong, they released the child within ten minutes. However, the child remained scared and said that she felt as if the police were following her.

As for the situation in Ukraine, there is little experience in regulating face fixation and recognition systems. So, the Constitution of Ukraine stipulates that the collection, storage, use, and dissemination of confidential information about a person without his consent shall not be permitted except for the cases determined by the law and only in the interests of national security, economic welfare, and human rights. The local authority is known to use surveillance cameras. For example, there are more than 6,200 CCTV cameras with a face recognition system in Kyiv, but the grounds of local authorities to use them still are unclear. Unfortunately, no law provides for the powers of local authorities to use a surveillance camera.

At the same time, the police can use the information received from video surveillance systems set up within the territory of someone else's possession. Article 25 of the Law of Ukraine "On the National Police" contains provisions that allow the police to use the databases of the Ministry of Internal Affairs and other public authorities. As known, local self-government bodies and utilities do not belong to public authorities. There is a need to fill in such gaps and develop documents regulating access to video surveillance systems and processing of personal data.

Let us analyze all this contradictory set of normative legal acts from the point of view of criminal law. Firstly, let us note that photos from the bases and photos of a person that are used for the identification have a status of documents (although due to defects in legal technique it is called "personal paper"). Herewith,

it is important to mention that the law points correctly that the main function of the document is to store information. That is, these photos are confidential information and belong to the object of the crime, the set of facts of which is provided in the Art. 182 of the Criminal Code of Ukraine. From an objective point of view, the actions that are provided in the Art. 182 of the Criminal Code of Ukraine, may be divided into two categories: the first is collection, storage, using, detention and sharing of confidential information about a person. The second is illegal alteration of such information.

From the practical side, illegal actions against the photos that are used during digital identification, usually fall into the first category: illegal collecting of someone's digital photos, preservation of such photos (including digital data base) and detention of such photos (including identification purposes) and destruction of such photos which is also possible. However, talking about the second category, illegal changes of such information, committing violation of this nature is more unlikely. Criminal offense, the set of facts of which is provided in Art. 182 of the Criminal Code of Ukraine, does not provide any specific consequences. That is why establishing a corresponding causal correlation does not seem appropriate.

The subject of criminal offense is an individual of sound mind who have attained the age of 16. In this regard, according to this legal norm, it means that even an unscrupulous investigator may be liable for breaking the image processing rules, as well as the owner of the paid database if some photos were included in there in an illegal way, and also users of such databases if there were violations that occurred during the processing. An interesting question, therefore, is what the form of the guilt is in this case - intent or imprudent. On one hand, there is a possibility of performing such acts intentionally (with direct or oblique intention). However, given the complicated procedure of obtaining consent for the photo processing, especially digital images, to perform such acts due to imprudence or negligence is theoretically possible, because a person may not consider his or her actions as illegal regarding someone's digital photos due to the difficult processing procedure from the legal point of view. Also, it is important to note that the majority of such face identification systems work online within several jurisdictions. In this case, according to Art. 6 of the Criminal Code of Ukraine, a crime that was started, continuing, and finished or stopped on the territory of Ukraine is considered as the one that was committed in Ukraine.

Theoretically, any digital face identification databases used by at least one individual or legal person on the territory of Ukraine in breach of law fall under the criminal jurisdiction of Ukraine. This means both the opportunity of investigating and convicting the perpetrators on the territory of Ukraine and blocking the relevant content on the territory of Ukraine in case it violates the law.

At the same time, many photo comparisons programs where it is possible to identify a person by a photo online (Google lance, etc.) artificially partially block such an opportunity in order to protect the privacy of individuals.

As mentioned above, there are some grounds to consider results of digital visual identification of an individual as operational measures (for preliminary identification and construction of versions that will be supported by other evidence or refuted by them during the investigation in the future) as well as independent evidence of expertise that will be submitted to the court. Herewith, there is again a question of the legal status of the photos that are used for the identification. During uploading the photos to the Internet on your own or while taking photos in the public places, the permission of the subject is necessary. In fact, uploading a photo to the Internet in its current form on your own may be interpreted by the owner of the facial recognition database in their favor - as consent to comprehensive processing of personal data, including the import of the photos to the facial recognition database and the use of these photos for identification purposes in the future. On the other hand, there is always the possibility of challenging such a presumption as well as the constant possibility of withdrawing consent, making the processing of such information still legally risky for the owners of such image identification programs.

When conducting a pre-trial investigation, first of all, it is difficult to obtain digital photos without the consent of the suspect or accused. There are two options possible – to freely receive photos from the electronic information systems or parts thereof, access to which is not limited to its owner, possessor or holder and not related to overcoming the logical protection principles (for example, excluding the official website of the employer, a personal page in social networks and etc.). The second option is to receive temporary access to things and documents with the subsequent appointment of the relevant examination. It should be noted that, in general, the legislation of Ukraine on the protection of the rights of the subject to his or her own image is developing alongside the European tradition. In particular, cases of the image use without the consent of the subject are extremely limited. That being said, the protection of personal data in Ukraine is at a fairly high level. By contrast, the legislation in this field is quite imperfect all over the world, so the Ukrainian example, taking into account the clarifications proposed by the authors of this article, can be a model for other countries.

DISCUSSION

As it can be seen from what was stated above, the use of digital face identification technologies based on the image provides opportunities for the qualified investigation of crimes. Some of the foreign scientists such as C. Poirson (2021), L. Introna and H. Nissenbaum (2020), J. Detsing and M. Ketcham (2017);

Ramya (Ramya et al., 2020), etc. noted a number of technical advantages of this method. We fully agree with named scientist on the effectiveness of such approach. Herewith other scientist, for example Antoaneta Roussi, paid attention to the necessity to take into account human rights while using the technology; to limit the fields where the technology can be implemented at the legislative level, and also to set strict rules of using such technology by investigators.

There is currently a direct contradiction between the continuity of technological progress in the field of digital technologies and the need to protect human rights. In this case, the almost total ban which is supported by a number of countries is as detrimental as the extremely broad powers granted by the state to companies and law enforcement agencies in this field. It should be noted that the procedure for obtaining the consent of the subject of identification and the processing of images without such consent in different countries has significant national characteristics. However, there are also common trends. On one hand, the example of China, where companies are actually obliged to process images of users, is illustrative. On the other hand, it is the example of the European Union, where cases of such processing without the consent of the identification subject are extremely limited.

In comparison with foreign legislation, Ukraine has a fairly broad and reasonable regulation of the protection of human rights by law (including criminal) in terms of digital identification. At the same time, the legislation provides sufficient opportunities for law enforcement officials to use modern technology to identify criminals. The study of foreign experience is sufficient because theoretically any digital face identification database used by at least one individual or legal person in Ukraine in breach of law falls under the criminal jurisdiction of Ukraine. This means both the opportunity of investigating and convicting the perpetrators on the territory of Ukraine and blocking the relevant content on the territory of Ukraine in case it violates the law.

Facial recognition can indeed have a very serious and irreversible impact on fundamental human rights and freedoms. At the same time, maximizing benefits and mitigating risks depends on sound regulation of this issue at the legislative level. After conducting the study, we can agree on that. It is important to protect the rights of an individual who was photographed in a public place without his or her direct consent and a person who uploaded their own images to the Internet, given the recent developments of the digital age. In the modern context, the direct provision that an individual may be photographed without his or her consent in any public place (without an indication of whether such an image may then be stored, distributed, or included in an appropriate identification database) may be considered excessive interference with individual's privacy. By contrast, a total ban on filming in public places will make it impossible for, for

example, car video recorders, traffic cameras, etc. to work. Moreover, peculiarities of the use of digital face identification technology in Ukraine, taking into account the Ukrainian legislation, were analyzed for the first time. Especially since this method is already being used in practice. The obtained results can be considered the latest, as previously this issue has not been actively explored due to the innovative nature of digital face identification technology.

It is forbidden to identify a person's face who is in a public place. The EU temporarily bans face recognition technology to use in public places for three to five years. The EU considers this as the only way to prevent the risks associated with the rapid and uncontrolled distribution of face recognition software. In the media space, reliable news has repeatedly spread about effective ways to mislead the algorithms of the recognition technology. In the media space, reliable news has repeatedly spread about effective ways to mislead the algorithms of the recognition technology.

The draft regulation refers to the right of EU citizens under the General Data Protection Regulation – "not to be subject to a decision based solely on automated processing, including profiling" (Article 22 of the General Data Protection Regulation). Under the document, a new regulatory framework for artificial intelligence is introduced, which may include a time-limited ban on face recognition technology used in public places. The use of face recognition technology in public places by public or private entities is prohibited under the document for a certain period (up to 5 years). This period is needed to develop a reliable methodology for impact assessment of face identification technology and possible measures for risk management. Not everyone shares the precautionary measures Brussels takes. Law enforcement officials in Great Britain are testing face recognition software as an "innovative" way to identify people suspected of a crime. Even though Great Britain has left the EU, the draft regulation on AI (artificial intelligence) also matters there. The common European rules will apply here at least until the end of 2020. However, everything can change in the future. Negotiations on the future relationship will determine how the rules of Great Britain comply with EU requirements, including data processing and collection.

The EU sees perspectives in face recognition technology, but it takes time to introduce it gradually. European politicians give a message that the identification of a person is prohibited and indicate, at the same time, that this is an exclusively temporary measure. The goal is to get enough time to develop and implement an adequate legal regulation. The German government plans to introduce face recognition technology at 134 train stations and 14 airports following a successful test in Berlin. France is set to become the first country in the EU, which allows its citizens to access secure government websites using face

recognition software. The French Parliament is preparing a new regulatory framework that will allow using technology in the future.

At the same time, non-governmental organizations are concerned that face recognition technology is being introduced so fast. The Information Commissioner's Office in the UK has been urged to be cautious with face recognition technology. Brussels currently considers several solutions to ethical and legal issues caused by using "artificial intelligence" and software with corresponding algorithms. The Commission plans to implement minimum standards for government departments and use legally binding instruments if the use of "artificial intelligence" is of high risk in such areas as transportation, healthcare, law enforcement, and justice.

A Commission spokesperson said: "To multiply the benefits and address the challenges in using artificial intelligence, Europe must act as a whole and define its own path. Technology should serve purpose and people. So, the EU strategy will focus on the trust, guarantees, and security of citizens." The benefits of using "artificial intelligence" and associated software algorithms are well understood. The prospect of using facial identification technology seems like a winning strategy in many areas. However, the potentially negative consequences and possible violations of the rights enshrined in the General Data Protection Regulation call for balanced and gradual steps.

CONCLUSIONS

From a forensic perspective, the identification of a person by his or her physical characteristics, on the one hand, can be considered a subspecies of portrait examination, because it also aims to identify one or different individuals depicted in photographs or other objective images of human appearance. On the other hand, given the opportunity of conducting such a study using simple real-time software (i.e., ease of use), it can be compared with the use of police databases or forensic records. Today, facial recognition systems are software products owned by its developer, private companies, and distributed primarily on a commercial basis, which limits the use of such systems during the investigation.

An important aspect of the facial recognition system is the fact that their successful functioning requires the largest possible library of images that are taken for comparison. Therefore, one of the priority issues to be addressed by legal science is the processing of personal digital photos without the knowledge of that person in order to establish the identity. These photos are confidential information and relate to the subject of the crime, the set of facts of which is provided in the disposition of Art. 182 of the Criminal Code of Ukraine. From an objective point of view, the actions provided for in Art. 182 of the Criminal Code of Ukraine can be divided into two categories. First - collection, storage, using, destruction,

dissemination of confidential personal information. Second - illegal alteration of such information. From a practical point of view, illegal actions against photographs used in the process of digital identification are most likely to fall into the first category: illegal collection of other people's digital photos, storage of such photos (including in digital databases), use of such photos including for identification purposes) and even the destruction of such photos is also possible. However, the second category, illegal alteration of such information, the commission of such an encroachment in digitally identifying photos, seems unlikely. The subject of a criminal offense is an individual of sound mind who has attained the age of 16.

In this regard, according to this legal norm, it means that even an unscrupulous investigator may be liable for breaking the image processing rules, as well as the owner of the paid database if some photos were included in there in an illegal way, and also users of such databases if there were violations that occurred during the processing. An interesting question, therefore, is what the form of the guilt is in this case - intent or imprudent. On one hand, of course there is a probability of performing such acts intentionally (with direct or oblique intention). However, given the complicated procedure of obtaining consent for photo processing, especially digital images, to perform such acts due to imprudence or negligence is theoretically possible, because a person may not consider their actions as illegal regarding someone's digital photos due to the difficult processing procedure from the legal point of view. Also it is important to note that the majority of such face identification systems work online within several jurisdictions via the Internet.

Theoretically, any digital face identification databases used by at least one individual or legal person on the territory of Ukraine in breach of law fall under the criminal jurisdiction of Ukraine. This means both the opportunity of investigating and convicting the perpetrators on the territory of Ukraine and blocking the relevant content on the territory of Ukraine in case it violates the law. At the same time, many photo comparisons programs where it is possible to identify a person by a photo online (Google lance, etc.) artificially partially block such a possibility in order to protect the privacy of individuals.

During the pre-trial investigation, first of all, it is difficult to receive digital photos without the consent of the suspect or accused. There are two options possible – to freely receive photos from the electronic information systems or parts thereof, access to which is not limited to its owner, possessor, or holder and not related to overcoming the logical protection system (for example, excluding the official website of the employer, a personal page in social networks and etc.). The second option is to receive temporary access to things and documents with the subsequent appointment of the relevant examination.

Thus, one must abide by the law when processing biometric data, including face recognition, and the latest documents of the EU have only confirmed this. The GDPR generally prohibits such processing. Similar to the provision of the Law of Ukraine "On the Protection of Personal Data," these data can be processed only in particular cases (a person provides clear consent in order to protect his life or the case is of significant public interest) and when appropriate guarantees, adapted to these risks, are provided. Under the Data Protection Directive, law enforcement activity follows the same logic, allowing such data to be processed only when unconditionally necessary. On June 20, 2018, ther4e were amendments to the French Data Protection Act to comply with European documents. Consequently, if there is no consent, the owner, public or private, can process biometric data only when its first permission by law.

RECOMMENDATIONS

At present, a number of amendments to the basic legislation that regulates issues related to the legal regime of digital face identification are necessary. Based on the analysis, we propose to make certain changes in the legislation of Ukraine. One of the proposed changes is the unification of terminology through amendments to Art. 303 of the Civil Code of Ukraine by specifying, for example, "personal papers (documents)".

It is also necessary to radically change the wording of Art. 307 of the Civil Code of Ukraine that requires the consent of the subject to be photographed, filmed, televised or videotaped. Such consent is presumed if the filming is carried out openly on the street, at meetings, conferences, rallies and other public events. At the time this article was adopted, it was only possible to visually identify a person in a photo by his or her personal acquaintances, and not to accurately identify a person based on a photo only. Therefore, the provision that an individual who has agreed to be photographed, filmed, televised, or videotaped may require the cessation of a public screening in the part relating to his or her personal life that needs to be clarified insofar as it has become relevant not only to ban on a person showing his or her photo in terms of personal life, but also a ban on such use for digital identification purposes.

REFERENCES

Bah, S. M. & Ming, F. (2020). An improved face recognition algorithm and its application in attendance management system. *Array, 5*.

Britchenko, I. & Saienko, V. (2017). The perception movement economy of Ukraine to business. *Ikonomicheski Izsledvania*, *26*(4), 163-181.

Civil Code of Ukraine. (2003). Available at: https://zakon.rada.gov.ua/laws/show/435-15.

Criminal Code. (2011). Available at: https://zakon.rada.gov.ua/laws/show/2341-14#Text.

Criminal Procedure Code. (2013). Available at: https://zakon.rada.gov.ua/laws/show/4651-17#Text.

Detsing, J. & Ketcham, M. (2017). Detection and facial recognition for investigation. *2017 International Conference on Digital Arts, Media and Technology (ICDAMT), 407-411*. (Chiang Mai, 1-4 March 2017) Chiang Mai: IEEE.

Inshyn, M., Vakhonieva, T., Korotkikh, A., Denysenko, A. & Dzhura, K. (2021). Transformation of labor legislation in the digital economy. *InterEULawEast, 8*(1), 39-56.

Introna, L. & Nissenbaum, H. (2020). *Facial recognition technology a survey of policy and implementation issues*. New York: Center for Catastrophe Preparedness & Response.

Law of Ukraine "On Information". (1992). Available at: https://zakon.rada.gov.ua/laws/show/2657-12#Text.

Law of Ukraine "On Personal Data Protection". (2010). Available at: https://zakon.rada.gov.ua/laws/show/2297-17#Text.

Levchenko, I., Dmytriieva, O., Shevchenko, I., Britchenko, I., Kruhlov, V., Avanesova, N., Kudriavtseva, O., & Solodovnik, O. (2021). Development of a method for selected financing of scientific and educational institutions through targeted capital investment in the development of innovative technologies. *Eastern-European Journal of Enterprise Technologies, 3*, 55-62.

Lytvyn, N. A., Berlach, A. I., Kovalko, N. M., Melnyk, A. A. & Berlach, H. V. (2022). Legal regulation of the state financial guarantees of medical services for the population: Domestic and international experience. *International Journal of Health Governance*, Article in Press.

Merchlinsky, C. (2019). How facial recognition became a routine policing tool in America. Available at: https://www.nbcnews.com/news/us-news/how-facial-recognition-became-routine-policing-tool-america-n1004251.

Nolasco, C., Vaughn, M.S. & del Carmen, R.V. (2010). Toward a new methodology for legal research in criminal justice. *Journal of Criminal Justice Education, 21*(1), 1–23. DOI:10.1080/10511250903518944.

Poirson, C. (2021). The legal regulation of facial recognition. *The Fourth Industrial Revolution and Its Impact on Ethics. Sustainable Finance*, 283-302. Cham: Springer.

Ramya, N., Manasa, D., Ramya Sri, N. & Naveed, Sk. (2020). Testing of modules for facial recognition. *EPRA International Journal of Research and Development (IJRD), 5*(11), 132-136.

Roussi, A. (2020). Resisting the rise of facial recognition. *Nature, 587*, 350-353.

Semchuk, N., Lykhova, S. & Demianenko, U. (2019). Using English as a foreign language when teaching subject of the criminal law cycle. *The Asian International Journal of Life Science. Supplement, 21*(2), 517–534.

Shramovich, V. (2021). She or she is not: a veteran of the Right Sector is suspected of escorting Ukrainian prisoners in Donetsk. Available at: https://www.bbc.com/ukrainian/news-55752337.

Sunstein, C. (1993). On analogical reasoning. *Harvard Law Review, 106*, 741–791.

Thakur, A., Prakash, A., Mishra, A.K., Goldar, A., & Sonkar, A. (2020). Facial recognition with Open Cv. *Computational Vision and Bio-Inspired Computing*. *Advances in Intelligent Systems and Computing, 1108*, 213-218. Cham: Springer.

Tyler, T.R. (2017). Methodology in legal research. *Utrecht Law Review, 13*(3), 130–141.

The Law, State and Telecommunications Review / Revista de Direito, Estado e Telecomunicações

Contact:
Universidade de Brasília - Faculdade de Direito - Núcleo de Direito Setorial e Regulatório
Campus Universitário de Brasília
Brasília, DF, CEP 70919-970
Caixa Postal 04413

Phone: +55(61)3107-2683/2688

E-mail: getel@unb.br

Submissions are welcome at: https://periodicos.unb.br/index.php/RDET

China's Social Credit System: A Challenge to Human Rights*

Submitted: 29 September 2022
Reviewed: 6 October 2022
Revised: 23 November 2022
Accepted: 24 November 2022

Article submitted to blind peer review

Quan Van Nguyen**
https://orcid.org/0000-0002-2094-5584
Sébastien Lafrance***
https://orcid.org/0000-0003-0588-8662
Cu Thanh Vu****
https://orcid.org/0000-0002-1685-4807

DOI: https://doi.org/10.26512/lstr.v15i2.44770

Abstract

[Purpose] To examine the origin and evolution of China's social credit system.
[Methodology/Approach/Design] A doctrinal approach is employed with secondary sources.
[Findings] China's social credit system has some adverse effects on the fundamental principles of international human rights law.

Keywords: Artificial Intelligence. Public Governance. Social Credit System. Human Rights. Limitation of Rights.

INTRODUCTION

The Chinese government introduced the Social Credit System (SCS) to improve the socialist market economy system, to reform social governance, to create a positive living environment, to enhance the nation's competitiveness, to promote social development, and, which is a broad statement to say the least, to

*This work was prepared separately from Sébastien Lafrance's employment responsibilities at the Public Prosecution Service of Canada. The views, opinions and conclusions expressed herein are personal to this author. They should not be construed as those of the Public Prosecution Service of Canada or the Canadian federal Crown.

**Quan Van Nguyen (PhD, University Toulouse 1 Capitole) is a lecturer-researcher at University of Law, Vietnam National University. He started his academic career in Vietnam since 2014. His research interest focuses on public law. Address: University of Law, Vietnam National University, E1 Building, 144 Xuan Thuy, Cau Giay, Hanoi, Vietnam. E-mail: nvquan@vnu.edu.vn.

***Sébastien Lafrance (LLM, Laval University) is an Adjunct Professor at Universitas Airlangga, Indonesia and an Adjunct Lecturer at Ho Chi Minh City University of Law, Vietnam. He also is a Prosecutor (Crown Counsel) at the Public Prosecution Service of Canada. E-mail: seblafrance1975@gmail.com.

****Cu Thanh Vu is a senior student at University of Law, Vietnam National University. E-mail: cu.vuthanh@gmail.com.

improve civilization (LIANG e colab., 2018). The SCS is theoretically defined as both an essential part of the socialist market economy system and of social governance (ZHANG, 2020). Two essential elements are included in the foundation of SCS: (i) an infrastructure to score members' credit and (ii) a complete network system containing credit records for all members of the Chinese society. More precisely, the system sets a mechanism of reward and punishment to encourage creditworthiness and to limit non-creditworthiness to improve the degree of compliance with it (KOTSKA, 2019).

According to Beijing, establishing such a system is deemed to be essential in developing a "more civilized" and "more harmonious" society. Because the degree of "trust" among economic entities in the Chinese society is deemed to be too low by the government, the latter wishes to rebuild that trust (SHEN, 2018). It is part of a strategy devised by the General Secretary and President Xi Jinping to bring back stronger Confucian ethical traditions into Chinese society (See LAMS, 2018).

Xi Jinping continued his commitment to promoting China's cultural and philosophical history as a valuable resource for strengthening the Chinese Communist Party (CCP)'s performance since his election as party leader (See NEEDHAM, 1960). Xi has drawn on analogies from the ancient philosophy of Chinese political practice to propose cadre management and anti-corruption measures. Despite the CCP's prior anti-traditionalist policies from early 1950s until Xi Jinping taking paramount power in 2008[1], Xi today portrays the CCP as the natural inheritor and beneficiary of China's cultural heritage (KUBAT, 2018).

"Social Credit System" was officially referred to for the first time as a legal document in the planning outline for constructing a Social Credit System from 2014 to 2020 issued by the State Council of China on June 14th, 2014 (STATE COUNCIL OF THE PEOPLE'S REPUBLIC OF CHINA, 2014). However, in 2002, Jiang Zemin, the General Secretary of the CCP, was the first to use the term "social credit system" in his speech at the 16th Congress of the Chinese Communist Party (JIANG, 2002). The Chinese SCS resembles credit systems in liberal democracies in specific ways (GRIFFITHS, 2019; WONG and DOBSON, 2019). This point can be explained by the fact that SCS "derives from its Western counterpart" and that "Chinese law may, in many respects, not be fundamentally different from its Western counterpart" (SÍTHIGH and SIEMS, 2019). However, the Chinese and Western credit systems have some profound differences

[1] The CCP seized power in 1949, absorbing and reproducing long-standing statecraft and power norms in order to project power and increase legitimacy in a modernist fashion (TATLOW, 2018). Deng Xiaoping then implemented the Cultural Revolution from 1966 to 1976, which is heavily criticized by Xi Jinping—"The destruction in the Cultural Revolution was particularly severe. Everything was condemned, the good things from our ancestors were also tossed out." (BUCKLEY, 2014)

(NGUYEN, LAFRANCE, HO, NGUYEN, 2020). The SCS "is apparently not equipped to centralise and share the raw information that each department holds about citizens" (ARSÈNE, 2019). On the other hand, the SCS "is not based on the subjective ratings by other citizens" (SÍTHIGH and SIEMS, 2019). Furthermore, the SCS is operated by the Chinese government, rather than private actors like in the Western world (NGUYEN e colab., 2020).

In China, a planning outline of the CCP can be understood as a normative legal document – it is a unique feature of socialist countries (BUI, 2017). More specifically, it contains legal norms for other institutions in the state apparatus to implement. In the planning outline, the CCP analyzed the development situation of the SCS in "the decisive phase of economic structural transformation and the refining of the socialist-oriented market economy system begun." The Party also stated that to move the construction of a social credit system forward comprehensively, China must continue to follow Deng Xiaoping's Theory[2], the important "Three Represents" thought[3], and the scientific development view as guides, acting by the spirit of the 18th Party Congress, the 3rd Plenum of the 18th Party Congress, and the "12th Five-Year Plan."[4]

In fact, in 2007, the State Council of China released a Notice of Inter-ministerial Conference System to build a social credit system including 15 state offices in commerce, tax, and banking (STATE COUNCIL OF CHINA, 2007). The number of state offices involved in the construction of SCS by 2012 increased to 35, including the financial sector and other areas such as health, education, and agriculture (STATE COUNCIL OF CHINA, 2012). In addition, several studies report that the SCS has been piloted at a local unit in northern Shanghai since 2010 (MURRELL, 2018). However, aside from the general and entirely theoretical content mentioned in the planning outline for constructing a Social Credit System from 2014 to 2020, there has been almost no official statement detailing how to collect information, data sources, or the entire SCS works since then.

According to the annual report of China's National Public Credit Information Center (NPCIC) (KUO, 2019), would-be travelers are banned from buying airline and train tickets 17.5 million times and 5.5 million times,

[2] Deng Xiaoping adopted a theory so-called "socialism with Chinese characteristics" merging capitalism into central planning to boost productivity, enhance Chinese culture, and enhance populist interests. Deng distinguishes socialism and capitalism based on the state intervention for economic outcomes (MOAK and LEE, 2015). Socialist countries always attempt to forge their identity through neologism by creating socialist version of Western theories, such as rule of law and market economy (BUI, 2014; GILLESPIE, 2006).
[3] The idea of the "Three Represents" holds that the CCP represents the most developed forces of production, the most developed culture, and the most fundamental interests of the vast majority of people (FEWSMITH, 2003).
[4] See (AHO e DUFFIELD, 2020; CREEMERS, 2018; LEE, Michelle, 2019).

respectively. In order to accomplish this plan, China installed a vast network of 200 million CCTV cameras across the country (CARNEY, 2018). It is meant to monitor each person every single minute, at every step, for every action taken and it also implies that every item purchased can be tracked and evaluated to score an individual's credit in real-time.

Currently, China accomplished the goal of establishing a legal system with fundamental standards and regulations on a social credit system; a system of credit investigation and assessment for the entire community based on information sharing; a credit monitoring and management system; to have created a relatively complete credit service market system, and a fully promoted mechanism of credit score encouragement and sanctions (See CHEN, Yu-Jie e colab., 2018; ROBERTS e colab., 2021).

Western reporting has only covered the 2014–2020 period thus far, and the most of it has taken the form of criticism of the evaluation criteria (e.g., political loyalty, a highly problematic principle in the West) (WOESLER e colab., 2019). It has depicted and condemned a system of almost complete surveillance, a lack of the rule of law, a disdain for data protection and privacy, and has primarily concentrated on dramatic individual outcomes (as in the event of system failures or draconian punishments) (WOESLER e colab., 2019)[5]. It primarily refers to decreasing credit scores and the punishments meted out to those deemed to have low credit scores by the Chinese government.

Specific examples are given as follows. At the end of 2013, the Chinese Supreme Court published the names and information of more than 31,000 people supposed to fail or delay their repayment obligations in civil transactions on its official website. Along with disclosing personal information, defaulters placed on that blacklist were prevented from booking a room at 3-star or more hotels, air tickets, high-speed train tickets, or charged a higher fee for car booking (CHAN, 2017). As of April 21, 2020, anyone who visited the Chinese Supreme Court's website[6] can access the blacklist of 13 million citizens with their names placed on it.

In 2015, the People's Bank of China granted licenses to eight significant companies to test the construction and operation of the credit system (CENTRAL BANK OF CHINA, 2015). Sesame Credit of Alibaba Group and Tencent with the WeChat application is notable names listed. The credit assessment of the individuals involved is based on data from at least 400 million customers of Alibaba's online shopping and payment platforms and 850 million WeChat users.

[5] The legal instrumentalism in China has long been criticized by the West, especially concerning human rights (See POTTER, 2011; WANG, Juan e TRUONG, 2021). Since China adopted the SCS, the literature focused on the privacy protection under the mass surveillance (See RAGHUNATH, 2020).

[6] http://zxgk.court.gov.cn

Accordingly, the system collects user purchasing and payment information, then develops a unique credit score system and commercial benefits depending on user credit ratings, such as priority for hotel reservations.

Thus, it can be understood that the SCS planned by the Chinese government encompasses many different interdependent social credit rating systems (LIU, 2019; THE GENERAL OFFICE OF THE CENTRAL COMMITTEE OF THE COMMUNIST PARTY OF CHINA, 2016). It is believed that in the future, China will establish a unified social credit rating system under the state management as stated in the planning outline on the SCS from 2014 to 2020. In detail, some credit system scoring citizens are named as follows: Supreme Court Blacklist; Central Bank's credit rating; Alibaba Group's Sesame Credit; Tourism blacklist of the Ministry of Culture and Tourism and the National Development and Reform Commission's Blacklist (LI and ZHAO, 2019).

Algorithmic Ambiguity

In terms of punishment, no one knows how many penalties the Chinese government will apply to citizens with low credit scores in the future (BACH, 2020). While there are some guidelines for blacklists (e.g., evidence of non-compliance), one may readily conceive an extensive range of regional variances. Blacklists have spread to the point where breaches of administrative rules (not only court orders) constitute grounds for placing someone on a blacklist, and any institution can institute blacklists (CREEMERS, 2018).

This does not appear to have impacted the system's apparent high levels of popular support, particularly among those who stand to benefit the most from the rewards (e.g., well-off, educated, urban males), but also more broadly among those who see the system as a reasonable faith effort to improve people's quality of life (KOSTKA, 2019; RUENGRANGSKUL and WENZE, 2019). However, there is no way of knowing how all of one's offenses will sum up. While people should always be told before being placed on a blacklist and given the opportunity to appeal or remove themselves by compliance, this does not always appear to happen. Furthermore, even though public data often has a 5-year sunset clause, there is little control over how third parties may harvest or re-use released data, let alone hostile operators who may break into the system (CHEN, Yongxi e CHEUNG, 2017).

However, in 2016, CCP Central Committee General Office, State Council General Office published the full text of "Opinions concerning Accelerating the Construction of Credit Supervision, Warning and Punishment Mechanisms for Persons Subject to Enforcement for Trust-Breaking" (CREEMERS, 2016). Accordingly, a person can suffer sanctions in the following main groups: (i) restrictions of engaging in particular sectors or affairs; (ii) restrictions on

government support or subsidy; (iii) restrictions on qualifications to hold positions; (iv) restrictions on access qualifications; (v) restrictions in terms of honour and credit awarding; (vi) restrictions on special market transactions; (vii) restrictions on conspicuous consumption and related consumption (CREEMERS, 2016).

The nature of the SCS can be paradoxical. Suppose the social credit system was completely opaque, and no one knew why they were on a black or red list (AHMED, 2019). The system's stated goal of encouraging responsible behavior would be impossible to achieve, as learning from it would be impossible. Meanwhile, the other end of the spectrum is also problematic: if the system is entirely transparent, it will be open to large-scale gaming, and norm compliance will resemble market transactions, contradicting the system's declared goal of reconciling morality and the market. Englemann et al. conclude that keeping the system semi-transparent helps it to guard against the "transformation of moral activity into market transactions," a risk that appears as an unwelcome but seemingly inevitable by-product of a scoring system that adapts market-based governance procedures (ENGLEMANN and colab., 2019, 10).

To sum up, China's Social Credit System (SCS) is, in essence, a system established to gather all information on all aspects, including but not limited to living activities, traveling, shopping, payment, entertainment, making friends, individual's expression on a social network which are all used to evaluate and score every behavior of each individual, and then to encourage behaviors that are considered good, and to punish those who are inadequate according to the standards set by this system. In other words, SCS is an "always-on" system that continuously collects data from a broad and expanding array of behavioral traces and feeds it into algorithmic systems that generate the rewards or punishments intended to change the social environment.

Role of Artificial Intelligence in SCS

On July 8, 2017, China's State Council released the New Generation Artificial Intelligence Development Plan by 2030 (THE STATE COUNCIL OF CHINA, 2017). In particular, artificial intelligence (AI) technology has been identified as a tool to significantly improve the capacity and degree of national and social governance in China[7]. Indeed, with the ambition to build a system capable of information gathering and management and behavior assessment of 1.3 billion people, SCS is undeniably driven to be built upon the achievements of artificial intelligence (AI) technology.

Roles and tasks of AI in SCS include:

[7] The use of AI probably poses some threats to privacy (See LAFRANCE, 2020).

Face Recognition: the most basic and vital technology in SCS in which, based on images collected from CCTV cameras, AI is tasked to compare with the database of 1.3 billion people and calculate to know who is being followed, distinguish each person in the crowd, and immediately link to the database relating to this person. It is noted as a job that no one or a mechanism based on human capability can do. When blacklisted people, for example, go through certain intersections in Beijing, AI instantly recognizes faces to spot the person in the crowd and immediately releases an alert with their photos and ID numbers on the big screen (CAMPBELL, 2019).

Behavior Tracking and Analysis: identified individuals, cameras, microphones, or any other means are controlled to track and detect behaviors by AI. It could be buying an item from a supermarket in which AI, thanks to the development of technology, can tell what it is from the image. In addition, internet behaviors can be evaluated and collected by AI. For instance, consuming too much alcohol or junk food and playing too many video games are some of the actions the Chinese government considers that they are "bad behaviors", which warrant punishment (KOTSKA, 2019). However, the government can get a taste of its own medicine because this policy fosters ingrained corruption instead of promoting the expected better citizenry (LILLY, 2018). It is worth mentioning that China's SenseTime, the world's most valuable AI startup, is now providing Chinese governments surveillance solutions in which AI can screen out online videos, read and recognize languages to remove videos that contain pornographic or text containing messages deemed sensitive by the Chinese authorities (JING, 2018).

Citizen Grading: Based on all data collected by the system, compared to all behaviors identified as good or bad, AI, in the context of the Social Credit System, is coded to assess and grade every behavior of every citizen. It seems impossible to know how the Chinese government currently uses algorithms to score citizens. However, with the immense data volume of 1.3 billion citizens attached to a diverse system of human behaviors, it should be noted that the application of artificial intelligence is inevitable due to the size of this data.

Thus, from the practice of SCS implementation in China, it can be said that AI is a vital prerequisite for a system to track and score citizens like the SCS.

SCS' IMPACT ON FUNDAMENTAL HUMAN RIGHTS

The SCS under the State Perspective

Rogier Creemers argues that the introduction of the SCS first derived from the ineffectiveness of the legal system: difficult situations in the enforcement of civil judgments, inadequate protection of intellectual property rights, environmental protection, and food safety remain prominent (CREEMERS,

2018). The Chinese leadership has recognized the situation, identifying the improvement of implementation and compliance mechanisms as a critical component of the legal reform agenda outlined at the 4th Plenum of 2014 (CCP CENTRAL COMMITTEE, 2014).

In addition, many indications show that the rapid development of China's economy is not accompanied by the improvement of people's behavior, self-awareness, and respect for cultural values in the citizen's social life. Behaviors indicating poor awareness of Chinese tourists are recorded worldwide, or socially insensitive behaviors are reported that even the Chinese feel unacceptable (VOLODZKO, 2016; ZUO, 2013).

It is found that, in this context, the vigorous technological development lacking the practical mechanisms of human rights protection has provided Chinese leadership with the idea of a comprehensive citizen tracking and controlling system to improve the legal compliance of China's citizens. In other words, the genesis of the SCS can be seen as the solution to an ineffective legal system and an education system that fails to achieve the goal of nourishing civilized generations in a society where human rights are less respected, and its protection mechanism remains blank. Rogier Creemers states that the SCS is basically framed as a set of mechanisms providing rewards or punishments as feedback to individual actions that are based not just on the lawfulness but also on the morality of their actions, which includes economic, social, and political conduct (CCP CENTRAL COMMITTEE, 2014; CREEMERS, 2018).

Three fundamental issues arise as to how the SCS works:

(1) Is the government provided with the right to track and record all activities of the people?
(2) Is the government provided with the right to assess the morality aspect of all people's economic, social, and political actions under its ruling standards?
(3) Is the government provided with the right to punish people in forms not currently regulated by law? (See AHO e DUFFIELD, 2020; BANNISTER e CONNOLLY, 2011; DAWES, 2010; HOU, 2017; LIANG e colab., 2018; QIANG, 2019)

"No" is the answer that should be given to all these three questions so that a State may still be considered as a genuine democracy. Provided within its Constitution, China upholds "the uniformity and dignity of the socialist legal system" as one of its basic fundamental principles. All acts of State organs must abide by the Constitution, and the law and accountability must be enforced for all acts that violate the Constitution or laws (Constitution of the People's Republic

of China 1982, Article 5). The Chinese socialist legal system has a top-down institutional design and it seems impossible to establish judicial review in such a system without judicial independence (CUI e colab., 2019; HUNG, 2004; ZHANG, Qianfan, 2018)[8].

To the extent of each individual, the operation of the SCS, especially the imposition of penalties covering, among other things, the right to travel, study, or publish personal information anywhere, is seen to harshly infringe all the fundamental rights of citizens, which constitutionally remains a minority, including freedom of politics (Article 35), personal freedom (Article 37), personal dignity (Article 38), and the inviolable right to the home of citizens (Article 39).

It is found that SCS has switched the position of the people from empowering the state to manage society and protect its citizenship to being tracked, monitored, and controlled in every aspect. A more severe threat is shown since fundamental human rights such as travel, education, and political freedom supposed to be undertaken by the state are planned as rewards for those the state considers with a high credit score or physical deprivation of those the state scores low credit one.

A new social institution would be formed since the SCS operation is no longer a natural state in common sense. It also unavoidably raises questions related to transparency of the State in its dealings with its citizens. While using AI or any other means to score people since accepting such a social institution could exist. Yoshua Bengio, the father of AI, comments on the application of AI in SCS in an interview: "Technology, as it gets more powerful, outside of other influences, just leads to more concentration of power and wealth… That is bad for democracy. That is bad for social justice and the general well-being of most people" (KAHN, 2019).

In brief, the operation of SCS results entirely against the nature, role, and function of the state and thereby seriously violates citizens' fundamental human rights values. Hence, any excuse or reason given to justify the existence and operation of a system like SCS in human society remains questionable.

SCS under Personal Rights Infringements Perspective

How China applied AI to collect and analyze personal information would have raised concerns about data credibility, data protection and invasion of privacy in China due to weak regulations and law enforcement (LEE, 2020). However, we are witnessing the internationalization of such an infringement of human rights. For example, China has exported AI tracking technology worldwide, including face recognition technology to Bolivia, Ecuador, and Peru (ROLLET, 2018); 110,000 tracking cameras with face recognition were exported

[8] Vietnam, a socialist neighbor, is in the same boat as China (See BUI, 2018).

to Singapore (JOPLIN, 2018); a total of 54 countries worldwide imported this technology (FELDSTEIN, 2019).

Governments use AI to track their citizens. Nowadays many top-tier technology companies today, namely Google, Facebook, Apple, and Twitter, consider it essential to gather and analyze user information used and exchanged as a profitable commodity. Facebook is even said to collect all information of non-Facebook users (WAGNER, 2018).

The threat imposed on privacy in these countries led to the event that United Nations General Assembly provided Resolution 68/176 in December 2013 on "The right to privacy in the digital age" (UN GENERAL ASSEMBLY, 2014). The resolution states that

> "Noting that the rapid pace of technological development enables individuals all over the world to use new information and communication technologies and at the same time enhances the capacity of governments, companies, and individuals to undertake surveillance, interception, and data collection, which may violate or abuse human rights, in particular the right to privacy."

The right to privacy is to ensure: "no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, and the right to the protection of the law against such interference and recognizing that the exercise of the right to privacy is important for the realization of the right to freedom of expression and to hold opinions without interference and is one of the foundations of a democratic society." Following that, the right to privacy in the technological era has been viewed as a report of the United Nations High Commissioner for Human Rights as well as plenary discussions at the United Nations.

Privacy in the technological age has become an important and demanding content for implementing human rights on a global scale. In its conclusion, however, the annual report of the United Nations High Commissioner for Human Rights No. 27/37, dated 30 June 2014 (UNITED NATIONS HIGH COMMISSIONER FOR HUMAN RIGHTS, 2014) states: "practices in many States have, however, revealed a lack of adequate national legislation and/or enforcement, weak procedural safeguards, and ineffective oversight, all of which have contributed to a lack of accountability for arbitrary or unlawful interference in the right to privacy" (UNITED NATIONS HIGH COMMISSIONER FOR HUMAN RIGHTS, 2014).

Expressly, the right to privacy in the technological age includes the following aspects (CRAIG and LUDLOFF, 2011, p. 14–15):

(1) The right to privacy in communication activities, including the right to privacy in the way of using email, phone, and social media content.
(2) The right to privacy in living activities, including all acts of living, trading, traveling, and information seeking.
(3) Personal privacy, including photos, personal information, and information related to friends and relatives.

Provided with the definition of privacy stipulated by the United Nations and concretizing the aspects mentioned above, it is clear that SCS, as well as the citizen tracking systems around the world, or the user information collection systems of technology companies and social media platforms, for whatever purpose, is a blatant infringement of the privacy of individuals. A living environment where freedom of speech and other grounds of a democratic society is not guaranteed inevitably results from violating the right to privacy.

SCS and the Principles of Rights Limitation

In a democratic society, freedom is based on the idea that no right is considered absolute. The demands from social life and especially the requirements from public order leading to restrictions on the exercise of fundamental rights are believed necessary to protect the public order, which is guaranteed for these rights. Scholar Pierre Bon argues that public order "assumes a specific function of restricting freedoms only when compulsory and limiting the rights in a way commensurate with what the protection of other rights required." (BON, 1975, p. 226)

Limitations of rights provide the state the power to infringe human rights to further commonly accepted legitimate goals—including domestic legality and compliance with international responsibilities. Article 29.2 of the UDHR states that the limitations of rights have to be determined by law solely to secure due recognition and respect for the rights and freedoms of others and to meet the just requirements of morality, public order, and the general welfare in a democratic society.[9] As stated in the UDHR, there is a high presumption in favor of human rights, and Article 29.2 places the burden of evidence on those who seek to restrict such rights (BROWN, 2016).

Under international and domestic human rights laws, any limitations or restrictions of human rights must be explained and justified.[10] It is based on

[9] The notion of "law" in international human rights treaties usually has a broader—encompassing customary law and judge-made law in common law tradition because they are general norms and perceptible for individuals (SCHABAS, 2015, p. 336; TRIANTAFYLLOU, 2002, p. 60).
[10] An international human right does not legally exist outside the limits drawn whether they are expressive or inherent (CHASKALSON, 2002; JOSEPH e CAPSTAN, 2013).

democratic principles, such as the idea that the law represents the will of the people and the rule of law, which provides the ability to know in advance any restrictions that the State may impose on the exercise of rights (TOMUSCHAT, 2013).

Mentioning rights and exceptions is considering the interactions between right holders and duty bearers—citizens and states because "the constitutional right and its limitations are flip sides of the same constitutional concept" (BARAK, 2010, p. 6). There is widespread misuse of state authority as the primary responsibility bearers worldwide, including in China. (GEARTY, 2017; PAUL and colab., 2017). States' dual roles as primary guarantors of human rights and frequent abusers of those rights create an ongoing conundrum that international monitoring institutions work to resolve or at least lessen.

Specifically, "the notion of arbitrariness is not to be equated with "against the law," but must be interpreted more broadly to include elements of appropriateness, injustice, lack of predictability and due process of law, as well as elements of reasonableness, necessity, and proportionality" (UN HUMAN RIGHTS COMMITTEE (HRC), 2014 para 12).

CONCLUSIONS

Artificial intelligence is a significant scientific and technological breakthrough (LAFRANCE, 2020). Nonetheless, various governments, technological companies, and social media platforms that use it to acquire personal data may infringe individual's privacy (WANG, Zhong e YU, 2015). At the same time, the achievements of AI present the risk of a social paradigm where human rights may not be considered as important, and then they may not be respected.

REFERENCES

Ahmed, S. (2019). The Messy Truth About Social Credit. *Logic*, 7. Available at: https://logicmag.io/china/the-messy-truth-about-social-credit/.

Aho, B. & Duffield, R. (2020). Beyond surveillance capitalism: Privacy, regulation and big data in Europe and China. *Economy and Society*, 49, 2,187–212.

Arai-Takahashi, Y. (2013). Proportionality. Shelton, D. (Org.). *The Oxford Handbook of International Human Rights Law*. Oxford Handbooks. Oxford: Oxford University Press, 2013, 446–468. Available at: https://academic.oup.com/edited-volume/42626/chapter/358048027.

Arsène, S. (2019). China's Social Credit System: A Chimera with Real Claws. Asie. IFRI. *Visions*, 110.

Bach, J. (2020). The red and the black: China's social credit experiment as a total

test environment. *The British Journal of Sociology*, 71, 3, 489-502.

Bannister, F. & Connolly, R. (2011). The trouble with transparency: a critical review of openness in e-government. *Policy & Internet*, 3, 1, 1-30.

Barak, A. (2010). Proportionality and Principled Balancing. *Law & Ethics of Human Rights*, 4, 1, 1-16.

Bon, P. (1975). *La police municipale.* Thèse Dactylographiée. Bordeaux: Bordeaux I.

Brown, G. (Org.). (2016). *Limitations and Derogations.* The Universal Declaration of Human Rights in the 21st Century: A Living Document in a Changing World. Open Book Publishers, 57-62.

Buckley, C. (2014). Xi Touts Communist Party as Defender of Confucius's Virtue. *New York Times*, 13 Fev 2014. Available at: https://archive.nytimes.com/sinosphere.blogs.nytimes.com/2014/02/13/xi-touts-communist-party-as-defender-of-confuciuss-virtues/.

Bui, N. S. (2017). The Law of China and Vietnam in Comparative Law. *Fordham International Law Journal*, 41, 1, 135.

Bui, N. S. (2018). Why Do Countries Decide Not to Adopt Constitutional Review? The Case of Vietnam. Chen, H. & Harding, A. (Org.). *Constitutional courts in Asia:* a comparative perspective. Comparative constitutional law and policy. Cambridge University Press, 335-364.

Bui, T. H. (2014). Deconstructing the "Socialist" Rule of Law in Vietnam: The Changing Discourse on Human Rights in Vietnam's Constitutional Reform Process. *Contemporary Southeast Asia*, 36, 1, 77.

Campbell, C. *How China Is Using Big Data to Create a Social Credit Score.* Available at: https://time.com/collection/davos-2019/5502592/china-social-credit-score/.

Carney, M. (2018). *She's a model citizen, but she can't hide in China's "social credit" system.* Available at: https://www.abc.net.au/news/2018-09-18/china-social-credit-a-model-citizen-in-a-digital-dictatorship/10200278.

CCP Central Committee. *Guanyu quanmian tuijin yifa zhiguo ruogan zhongda wenti de jueding* [Decision concerning Some Major Questions in Comprehensively Moving Governing the Country According to the Law Forward]. Available at: https://chinacopyrightandmedia.wordpress.com/2014/10/28/ccp-central-committee-decisionconcerning-some-major-questions-in-comprehensively-moving-governing-the-country-according-tothe-law-forward/.

Central Bank of China. (2015). *Notice on the personal credit information system.* Available at: http://www.gov.cn/xinwen/2015-01/05/content_2800381.htm.

Chan, T. F. (2017). *Debtors in China are placed on a blacklist that prohibits them from flying, buying train tickets, and staying at luxury hotels.* Available at: https://www.businessinsider.com/chinas-tax-blacklist-shames-

debtors-2017-12.

Chaskalson, A. (2002). Human Dignity as a Constitutional Value. KRETZMER, D. & KLEIN, E. (Org.). *The concept of human dignity in human rights discourse.* Kluwer Law International, 133-144.

Chen, Y. & Cheung, A. S. Y. (2017). The Transparent Self Under Big Data Profiling: Privacy and Chinese Legislation on the Social Credit System. *SSRN Electronic Journal*. Available at: https://www.ssrn.com/abstract=2992537.

Chen, Y.; Lin, C. & Liu, H. (2018). Rule of trust: The power and perils of china's social credit megaproject. *Colum. J. Asian L*., 32, 1.

Craig, T. & Ludloff, M. E. (2011). *Privacy and big data*. Sebastopol, CA: O'Reilly.

Creemers, R. (2018). China's Social Credit System: An Evolving Practice of Control. *SSRN Electronic Journal*. Available at: https://www.ssrn.com/abstract=3175792.

Creemers, R. (Trad.). (2016). *Opinions concerning Accelerating the Construction of Credit Supervision, Warning and Punishment Mechanisms for Persons Subject to Enforcement for Trust-Breaking.* Available at: https://chinacopyrightandmedia.wordpress.com/2016/09/25/opinions-concerning-accelerating-the-construction-of-credit-supervision-warning-and-punishment-mechanisms-for-persons-subject-to-enforcement-for-trust-breaking/.

Cui, W., Cheng, J. & Wiesner, D. (2019). Judicial Review of Government Actions in China. *China Perspectives*, 2019, 1, 35-44.

Dawes, S. S. (2010). Stewardship and usefulness: Policy principles for information-based transparency. *Government Information Quarterly*, 27, 4, 377-383.

Englemann, S. (2019). Clear sanctions, vague rewards: How China's social credit system currently defines "good" and "bad" behavior. *Conference on Fairness, Accountability, and Transparency*, 31/1.

Feldstein, S. (2019). *How artificial intelligence systems could threaten democracy.* Available at: http://theconversation.com/how-artificial-intelligence-systems-could-threaten-democracy-109698.

Fewsmith, J. (2003). Studying the Three Represents. *China Leadership Monitor*, 8. Stanford: Hoover Institution.

Gearty, C. (2017). Is the human rights era drawing to a close? *European Human Rights Law Review*, 22.

Gillespie, J. (2006). *Transplanting commercial law reform:* developing a "rule of law" in Vietnam. Aldershot, England: Ashgate Pub. Company.

Griffiths, J. T. (2019). *The great firewall of China:* how to build and control an alternative version of the internet. London: Zed Books.

Hou, R. (2017). Neoliberal governance or digitalized autocracy? The rising market for online opinion surveillance in China. *Surveillance & Society*, 15, 3/4, 418-424.

Hung, V. M. (2004). China's WTO Commitment on Independent Judicial Review: Impact on Legal and Political Reform. *The American Journal of Comparative Law*, 52, 1, 77-132.

Jiang, Z. *Full Text of Jiang Zemin's Report at the 16th Party Congress.* Available at: http://www.china.org.cn/english/2002/Nov/49107.htm#.

Jing, M. *The world's most valuable AI start-up just moved into online censorship.* Available at: https://www.scmp.com/tech/start-ups/article/2143324/worlds-most-valuable-ai-start-sensetime-eyes-move-online-censorship.

Joplin, T. *China's Newest Global Export? Policing Dissidents.* Available at: https://www.albawaba.com/news/china%E2%80%99s-newest-global-export-policing-dissidents-1139230.

Joseph, S. & Capstan, M. (Org.). (2013). *The International Covenant on Civil and Political Rights: Cases, Materials, and Commentary*. Oxford: Oxford University Press. Available at: http://opil.ouplaw.com/view/10.1093/law/9780199641949.001.0001/law-9780199641949.

Kahn, J. *Deep Learning 'Godfather' Bengio Worries About China's Use of AI.* Available at: https://www.bloomberg.com/news/articles/2019-02-02/deep-learning-godfather-bengio-worries-about-china-s-use-of-ai.

Kostka, G. (2019). China's social credit systems and public opinion: Explaining high levels of approval. *New Media & Society*, 21, 7, 1565-1593.

Kubat, Aleksandra. (2018). Morality as Legitimacy under Xi Jinping: The Political Functionality of Traditional Culture for the Chinese Communist Party. *Journal of Current Chinese Affairs*, 47, 3, 47-86.

Kuo, L. *China bans 23m from buying travel tickets as part of "social credit" system.* Available at: http://www.theguardian.com/world/2019/mar/01/china-bans-23m-discredited-citizens-from-buying-travel-tickets-social-credit-system.

Lafrance, S. (2020). The Impact of Artificial Intelligence on the Formation and the Development of the Law. *Vietnamese Journal of Legal Sciences*, 2, 1, 1-15.

Lams, L. (2018). Examining strategic narratives in Chinese official discourse under Xi Jinping. *Journal of Chinese Political Science*, 23, 3, 387-411.

Lee, A. *What is China's social credit system and why is it controversial?* Available at: https://www.scmp.com/economy/china-economy/article/3096090/what-chinas-social-credit-system-and-why-it-controversial.

Lee, M. (2019). *Beyond Big Brother:* Implications of China's Social Credit System for Global Credit and Governance. Columbia University.

Li, D. & Zhao, Y. *This Is How Chinese Citizens Are Watched and Rated.* Available at: https://www.bloomberg.com/news/articles/2019-04-09/the-list-of-ways-china-keeps-tabs-on-citizens-is-getting-longer.

Liang, F. (2018). Constructing a data-driven society: China's social credit system

as a state surveillance infrastructure. *Policy & Internet*, 10, 4, 415-453.

Lilly, S. (2018). *15 "Bad Behaviors" China Is Targeting with Its Social Credit System (And Why It Won't Work).* Available at: https://fee.org/articles/china-s-social-credit-scheme-will-create-more-corruption-not-a-better-citizenry/.

Liu, C. (2019). *Multiple Social Credit Systems in China.* (In Press). SocArXiv. Available at: https://osf.io/v9frs.

Moak, K. & Lee, M. W. N. (2015). Deng Xiaoping Theory. Moak, K. & Lee, M. W. N. (Org.) *China's Economic Rise and Its Global Impact.* New York: Palgrave Macmillan US, 91-115.

Murrell, A. (2018). *Pushing the Ethical Boundaries of Big Data:* A Look At China's Social Credit Scoring System. Available at: https://www.forbes.com/sites/audreymurrell/2018/07/31/pushing-the-ethical-boundaries-of-big-data-a-look-at-chinas-social-credit-scoring-system/.

Needham, J. (1960). The past in China's present: a cultural, social, and philosophical background for contemporary China. *The Centennial Review of Arts & Science,* 4, 2, 145-178.

Nguyen, V. Q., Lafrance, S., Ho, N. H. & Nguyen, H. A. (2020). Legal and Social Challenges Posed by the Social Credit System in China. *International Journal of Innovation, Creativity and Change,* 14, 5, 413-428.

Paul, N. W. (2017). Human rights violations in organ procurement practice in China. *BMC Medical Ethics*, 18, 1, 11.

Potter, P. B. (2011). 4 June and Charter 08: Approaches to remonstrance. *China Information,* 25, 2, 121-138.

Qiang, X. (2019). The road to digital unfreedom: President Xi's surveillance state. *Journal of Democracy*, 30, 1, 53-67.

Raghunath, N. (2020). A Sociological Review of China's Social Credit Systems and Guanxi Opportunities for Social Mobility. *Sociology Compass,* 14, 5. Available at: https://onlinelibrary.wiley.com/doi/10.1111/soc4.12783.

Roberts, H. (2021). The Chinese approach to artificial intelligence: an analysis of policy, ethics, and regulation. *AI & Society,* 36, 1, 59-77.

Rollet, C. (2018). *Ecuador's All-Seeing Eye Is Made in China.* Foreign Policy. Available at: https://foreignpolicy.com/2018/08/09/ecuadors-all-seeing-eye-is-made-in-china/.

Ruengrangskul, N. & Wenze, M. F. (2019). China's social credit system as a stimulant of donation behavior: Assessment of student opinions. *International Journal of Organizational Innovation*, 11, 4, 165-178.

Schabas, W. (2015). *The European convention on human rights: a commentary.* Oxford, United Kingdom: Oxford University Press. (Oxford Commentaries on International Law).

Shen, C. F. (2018). *Social credit system in China.* Digital Asia, 21-31.

Síthigh, D. D. & Siems, M. *The Chinese social credit system: A model for other countries?* Working Paper. European University Institute, 2019.

State Council of China. (2012). *Agreement to adjust the construction of the social credit system - Responsibilities of inter-ministerial joint meetings and approval of member units.* Available at: http://www.gov.cn/zwgk/2012-07/25/content_2191732.htm.

State Council of China. (2007) *Notice of Inter-ministerial Conference System for Building a Social Credit System.* Available at: http://www.gov.cn/gongbao/content/2007/content_632090.htm.

State Council of the People's Republic of China. (2014). *Notice concerning Issuance of the Planning Outline for the Construction of a Social Credit System (2014–2020).* Available at: http://www.gov.cn/zhengce/content/2014-06/27/content_8913.htm.

Tatlow, D. K. (2018). *China's Cosmological Communism:* A Challenge to Liberal Democracies. Available at: https://www.merics.org/en/report/chinas-cosmological-communism-challenge-liberal-democracies.

The General Office of the Central Committee of the Communist Party of China. (2017). *Opinions on accelerating the construction of credit supervision, warning and punishment mechanisms for persons with low creditworthiness.* Available at: http://www.xinhuanet.com/politics/2016-09/25/c_1119620719.htm.

The State Council of China. (2017). *Notice on the New Generation Artificial Intelligence Development Plan by 2030.* Available at: http://www.gov.cn/zhengce/content/2017-07/20/content_5211996.htm.

Tomuschat, C. (2013). Democracy and the Rule of Law. SHELTON, D. (Org.). *The Oxford Handbook of International Human Rights Law.* Oxford: Oxford University Press, 2013. p. 469–496. Available at: https://academic.oup.com/edited-volume/42626/chapter/358048032.

Triantafyllou, D. (2002). The European Charter of Fundamental Rights and the Rule of Law: Restricting Fundamental Rights by Reference. *Common Market Law Review*, 39, 1, 53-64.

United Nations General Assembly. (2014). *The right to privacy in the digital age.* Resolution, A/RES/68/167. Available at: https://digitallibrary.un.org/record/764407/?ln=en.

United Nations Human Rights Committee (HRC). (2014). *General Comment No. 35, Article 9 (Liberty and security of person).* UN Doc, CCPR/C/GC/35.

United Nations High Commissioner for Human Rights. (2014). *The right to privacy in the digital age.* Annual Report, A/HRC/27/37.

Volodzko, D. (2016). *Why Are Chinese Tourists So Badly Behaved?* Available at: https://thediplomat.com/2016/10/why-are-chinese-tourists-so-badly-behaved/.

Wagner, K. (2018). *This is how Facebook collects data on you even if you don't have an account.* Available at: https://www.vox.com/2018/4/20/17254312/facebook-shadow-profiles-data-collection-non-users-mark-zuckerberg.

Wang, J. & Truong, N. (2012). Law for What? Ideas and Social Control in China

and Vietnam. *Problems of Post-Communism*, 68, 3, 202-215.

Wang, Z & Yu Q. (2015). Privacy trust crisis of personal data in China in the era of Big Data: The survey and countermeasures. *Computer Law & Security Review*, 31, 6, 782-792.

Woesler, M. (2019). The Chinese Social Credit System. *European Journal Of Chinese Studies*, 2, 7-35.

Wong, K. L. X. & Dobson, A. S. (2019). We're just data: Exploring China's social credit system in relation to digital platform ratings cultures in Westernised democracies. *Global Media and China*, 4, 2, 220-232.

Zhang, C. (2020). Governing (through) trustworthiness: technologies of power and subjectification in China's social credit system. *Critical Asian Studies*, 52, 4, 565-588.

Zhang, Q. (2018). Establishing Judicial Review in China: Impediments and Prospects. Chen, A. H. Y. & Harding, A. (Org.). *Constitutional Courts in Asia*. Cambridge University Press, 311–334.

Zuo, M. (2013). *Chinese tourists carving out a bad reputation abroad.* Available at: https://www.scmp.com/news/china/article/1261692/chinese-tourists-carving-out-bad-reputation-abroad.

The Law, State and Telecommunications Review / Revista de Direito, Estado e Telecomunicações

Contact:
Universidade de Brasília - Faculdade de Direito - Núcleo de Direito Setorial e Regulatório
Campus Universitário de Brasília
Brasília, DF, CEP 70919-970
Caixa Postal 04413

Phone: +55(61)3107-2683/2688

E-mail: getel@unb.br

Submissions are welcome at: https://periodicos.unb.br/index.php/RDET

The Essence and Role of Electronic Money: Specifics of Legal Regulation

Submitted: 5 July 2022
Reviewed: 28 July 2022
Revised: 29 November 2022
Accepted: 1 December 2022

Article submitted to blind peer review

Kamshat Raiymbergenova*
https://orcid.org/0000-0002-7671-6932
Aizhan Zhatkanbayeva**
https://orcid.org/0000-0002-6358-8521
Aizhan Satbayeva***
https://orcid.org/0000-0002-2364-6387
Alisher Gaitov****
https://orcid.org/0000-0003-4036-3810
Botakoz Shansharbayeva*****
https://orcid.org/0000-0003-0610-3759

DOI: https://doi.org/10.26512/lstr.v15i2.43948

Abstract

[Purpose] The purpose of the study is to conduct legal analysis on the legal regulation problems concerning the concept of "electronic money" and the development of the modern monetary system of Kazakhstan based on the digitalisation of certain processes in the modern state.

[Methodology/approach/design] Based on the legal and general scientific research methods, an analysis of the existing legal framework and other documents in the studied area was carried out. Also, a comparative-structural analysis of individual norms of legal acts of the Commonwealth of Independent States countries was made.

[Findings] The issues of legal regulation and the incorporation of various concepts related to electronic money circulation into the laws of individual countries were examined based on the focus of the study. The idea of introducing a single digital electronic currency into Kazakhstan's national payment system, which would be backed by government finances and the obligations of the country's National Bank, was also substantiated. The arguments

*Kamshat Raiymbergenova is a Doctoral Student at the Department of Customs, Financial and Environmental Law, Al-Farabi Kazakh National University, Almaty, Republic of Kazakhstan. E-mail: kamshat.raiymbergenova@outlook.com.

**Aizhan Zhatkanbayeva is a Full Doctor in Law, Professor at the Department of Customs, Financial and Environmental Law, Al-Farabi Kazakh National University, Almaty, Republic of Kazakhstan. E-mail: zhatkanbayevaaizhan@yahoo.com.

***Aizhan Satbayeva is a PhD in Law, Associate Professor at the Department of Law, Kazakh National Agrarian Research University, Almaty, Republic of Kazakhstan. E-mail: satbayevaaizhan098@gmail.com.

****Alisher Gaitov is a PhD in Law, Associate Professor at the Department of Law, Kazakh National Agrarian Research University, Almaty, Republic of Kazakhstan. E-mail: alishergaitov8@gmail.com.

*****Botakoz Shansharbayeva is a PhD, Senior Lecturer at the Department of Law, Eurasian Technological University, Almaty, Republic of Kazakhstan. E-mail: bshansharbayeva@yahoo.com.

in support of this initiative by Kazakhstan's "main" bank and the country's government to launch a pilot process for the introduction of the digital tenge were formulated. This process will operate in circulation along with other cash and non-cash fiat currencies. In this regard, the chosen subject of the study is certainly promising for further scientific and theoretical deepening. This includes a further study of the prospects of digitalisation of the country's monetary system. Furthermore, a legal approach to the issue has revealed particular shortcomings in the enshrining of certain terms in Kazakhstan's legislation.

Keywords: Electronic Means of Payment. Cryptocurrency. Blockchain. Electronic Payment Systems. Electronic Money.

INTRODUCTION

The subject of the study is relevant from a theoretical point of view. There is a lack of a comprehensive scientific concept for the development of electronic money and electronic payment systems in the world and individual countries and regions. Originally, the formation of a certain number of electronic money systems was often initiated by privately owned financial institutions with little support and interest from public financial authorities and institutions. As a result, the whole monetary system of the state was imbalanced: the introduction of electronic payment systems was ahead of the development of legislation and methodological apparatus regulating economic, social and legal relations of subjects in the field of electronic payments and settlements from a practical point of view (BLAHUTA et al., 2019; HRYNKO et al., 2021; TRUSOVA et al., 2020).

The subject of the study is also relevant in practical terms, as electronic money turnover causes the emergence of risks at the macro and micro levels. This requires the creation of an adequate and effective system of electronic money turnover regulation and the monitoring and oversight mechanism in the state. Hence the importance of and need for the study of the problems associated with electronic money and the cryptocurrency phenomenon.

There is a fairly large number of studies and dissertations by various specialists and scholars related to the regulation and use of electronic money. They focus on the legal basis and the nature of this legal and financial phenomenon. In particular, some experts consider e-money as an element of the distribution of financial and legal power in society. It is also seen as an instrument of a decentralised governance structure that transforms civil and credit-banking sector legislation within a country, and modernises international relations (AJEVSKIS and VITOLA, 2010; CRITTENDEN, 2020). Furthermore, scholars address the legal regulation of the digital payment system in the legislation of the European Union (REULE and HÄRDLE, 2021; PETUKHINA et al., 2021). M. Fourcade and J. Gordon (2020) study the development of the state's digital sphere and the legal regulation of new payment systems in the world. The issue of the

need for regulation of private electronic network platforms is also frequently raised (XU, 2020).

The practical and scientific relevance of the study lies in the raised role of electronic money issues and in the use of relevant regulatory sources to identify law enforcement problems in the field of electronic money circulation. The originality of the study is determined by the involvement of legal documents of recent years, the works of scholars 2019-2021 on the spread of cryptocurrency in the world, the importance of using blockchain in modern global and national monetary systems, the creation and development of electronic means of payment as "new" types of money.

The purpose of the study is to investigate the normative characteristics, legal nature, and organisational and functional role of electronic money, cryptocurrency and blockchains in the modern financial processes of Kazakhstan. The tasks of this study that need to be solved include: giving a comparative legal characteristic of the legal concept of "electronic money" based on the study of its legislative consolidation in various countries; investigating the drawbacks of legal regulation of e-money turnover in Kazakhstan; to explore the issues of introduction in the country of a new digital currency – digital tenge as an important tool of the virtual state payment system.

MATERIALS AND METHODS

The theoretical-scientific study of the subject matter was carried out in several logical, task- and goal-oriented stages. Firstly, the first stage of the study was to identify and highlight relevant issues and questions required to elaborate on the use of various terms and concepts in the legislation of Belarus, Armenia, Kyrgyzstan, Kazakhstan and other countries relating to electronic (virtual) money processes in the circulation of national and other currencies. Furthermore, the issue of studying the specifics of promoting electronic money as a country's payment system instrument was raised. The methodological tools of the study were also formulated and defined. They were used to analyse and summarise the findings of the study concerning the internal content of certain documents. For example, the Report of the National Bank of the Republic of Kazakhstan for public discussions "Digital tenge" (2021); Resolution of the Board of the National Bank of the Republic of Kazakhstan No. 133 "On approval of the Program for the development of the national payment system in the Republic of Kazakhstan until 2025" (2020).

The second stage of the theoretical and methodological study involved content analysis of the findings. It also included a study of summarised data from scientific sources, normative literature and the results of terminology analysis concerning legal concepts related to electronic money circulation, digital payment

systems and virtual money (cryptocurrency and bitcoins). Some aspects related to the regulation of the concept of "e-money" in the legislation of different countries, including Belarus, Armenia and Kyrgyzstan, were also described in detail. The scope of the study did not allow for involving all sources of legislation in Europe, Asia, America, etc. However, even a superficial examination of the regulations of the European Union, United States of America (USA), United Kingdom, Singapore and other countries led to the conclusion that there is a lack of common understanding in terminology. Diversity in the interpretation of "electronic money" by legislators and enforcers was also noted either in its expansion (i.e., recognising all electronic means of payment as such) or its unjustified narrowing towards certain types of fiat money.

General logical and generally scientific methods of cognition of legal and political processes and phenomena were widely used in this study. This included the analysis of scientific works and other information (to identify specific problems of a legal definition of "electronic money"), synthesis of various findings, and generalisation of the research results. The tools for the concretisation of legal categories and processes enabled the identification of specific features concerning the legal regulation and consolidation of the fundamentals of electronic money circulation and digital payment systems in the modern national legislation of Kazakhstan. The formal-legal method was used to study the specific legal processes, and the acts of legislation in the country regulating the relations in the examined area. The method of comparative political science and comparative law was necessary to highlight the principal provisions of legislative acts and other governing documents of different Commonwealth of Independent States (CIS) and other countries when analysing the introduction of digital national currency.

Content analysis as a specific research method involved examining the internal content of individual regulatory documents. The final stage involved summarising the findings of the study to formulate an original position regarding the identified problematic elements. The methodological toolkit used in this study has produced results of a scientific and problematic nature that have unquestionable legal value.

To achieve the purpose and tasks of this study, the specifics of the regulation of electronic money circulation in Kazakhstan and other countries were investigated. In addition, certain features of digital means of payment were considered to illustrate the role of electronic money in the monetary policy of the state. This explains the increased interest of the legislator in establishing the legal foundations of this sphere.

RESULTS

The organisational and legal specifics and problems of regulating the circulation of electronic means of payment are linked directly to the definition of the nature and content of the legal concept of "electronic money". The terms related to electronic money and the role of electronic payment systems in the functioning of the banking and monetary structures of national states and institutions of the international community are also highlighted. The concepts of "electronic means of payment", "electronic money", "blockchain", "cryptocurrency", "digital currency", "information and communication technology", etc. differ in their legislative and other official wording in different national systems. However, they still essentially share common characteristics and attributes.

For example, the legislation of Belarus provides terminology for electronic money circulation and digital payments in two main acts – Law of the Republic of Belarus No. 455-Z "On Information, Informatization and Information Protection" (2008) and Resolution of the Board of the National Bank of the Republic of Belarus No. 201 "On approval of the Rules for conducting operations with electronic money" (2003). These acts clarify certain legal concepts and provide the wording in the field of electronic payments: "electronic wallet", defined by the legislator as a special plastic card, other technical or information technology device, or computer software that provides access to monetary information and contains electronic money; "pre-paid card" as a type of electronic wallet for conducting special cashless transactions in info kiosks, bank and other self-service payment terminals; "e-money exchange", defined by the legislator as a special virtual operation of an intangible digital nature for the exchange of electronic money (PROSKURNINA et al., 2021). At the same time, the concept of electronic money itself is not enshrined in the legislation of this country or the draft law "On Payment Systems and Payment Services". It can be found in the Banking Republican Code of Belarus, which defines electronic money as special digital monetary units of value put into circulation in exchange for cash or non-cash financial instruments, and monetary obligations between different entities (IDRYSHEVA, 2021).

This legal concept of electronic money suggested by the Belarusian legislator seems to be excessively voluminous and not quite correct or accurate, as it includes all types of electronic means of payment. Other CIS countries have also enshrined the concept and content of the legal term "electronic money" in their national legislation. In particular, the Law of the Republic of Armenia No. ZR-150 "On Payment and Settlement Systems and Payment and Settlement Organizations" (2004) clause "x" of Article 3 contains the definition of

"electronic money" through a detailed description of its features and functional purpose. It is understood as monetary value, expressing a monetary relation in the form of a claim to the issuer, which has digital content, stored on special information technology devices (MIETHLICH et al., 2021). Also, it refers to various types of electronic payments through information and highly technical means of communication. Article 2 of the Law of the Kyrgyz Republic No. 21 "On the Payment System of the Kyrgyz Republic" (2015) defines the basic legal concepts and categories. Its regulations include a definition of the concept of "electronic money", which means money, or rather its value is accepted as a means of payment in various areas and stored on special software and hardware devices in digital form. They also provide the definition of the concepts of electronic money issuer and electronic payment documents. The concept of international electronic money and payments is also enshrined in a meaningful way.

At the same time, the issuers of electronic money in the form of e-money are recognized only by banking structures. This is in contrast to the normative consolidation of the concept of issuers in Kazakhstan, where they, according to the Law of the Republic of Kazakhstan No. 11-VI "On Payments and Payment systems" (2016), can be various legal entities issuing e-money, also have the right to redeem digital money. In other words, according to paragraph 2 of Article 42 of the above-mentioned regulatory document, these are the National Bank of the country, second-tier banks, and the national postal operator. The advantage of the content of terminology in Law of the Republic of Kazakhstan No. 11-VI "On Payments and Payment systems" (2016) is the fact that it clearly defines the concepts of an electronic money system, the operator of this system, and functional concepts of use, redemption, issue of the specified digital money. However, the notion of electronic money as certain obligations or property rights is not entirely correct. This is also emphasised by S.K. Idrysheva (2021), a scholar-practitioner, in her insightful and comprehensive comparative legal study of the laws and civil legislation in the CIS countries. According to this scholar, electronic money is a special object of civil rights and represents a special property that has some of the characteristics of things and only some of those liability rights.

Moreover, the disadvantages of the legislative framework concerning electronic money as a financial asset include the provision of paragraph 3 of Article 25 of Law of the Republic of Kazakhstan No. 11-VI "On Payments and Payment Systems" (2016). It specifies separately by enumeration "transmission of electronic money" and the use of "means of electronic payment". It seems more appropriate to merge these notions by amending this provision and stating it in the following form: "the use of electronic means of payment, including the

transmission of electronic money". When considering the role of electronic money in modern Kazakhstan, it is necessary to highlight the following directions for improving its organisational and legal basis of functioning. First, as numerous academics and experts have pointed out, there is the problem of tax evasion, concealment of illegal income, and financing of terrorism through the use of cryptocurrency and other electronic means of payment, which are more difficult to identify and trace in today's information world. There is a need to better regulate the process of tracing illegal transactions on the global network and to set regulatory limits on the size of transactions. This is necessary to prevent the use of anonymous digital money to conceal proceeds, launder illicit funds, finance illegal activities, etc. The availability of a variety of electronic money and electronic payment systems (27 such systems were registered by the main bank of Kazakhstan as of 11 May 2020) creates a certain instability in the digital circulation of monetary means of payment. Some of them are listed below (Table 1).

System of Electronic Means of Payment (Money)	**Issuers of Digital Monetary Liabilities**	**Operators of the Digital Payment System**
"Wooppay", "Qiwi Wallet", "Halyk", "Homebank Wallet", "PAYBOX.money", "ASIAPAY", "Bloomzed.kz".	"Halyk Bank of Kazakhstan".	Limited Liability Partnerships (LLP): "QIWI Kazakhstan", "WOOPPAY", "PAYBOX.money"; and directly "Halyk Bank of Kazakhstan".
"Qiwi Wallet", "Paypoint", "AllPay", "Wallet One", "MyBonus", "RPS", "Indigo24", "Senim", "AlmaPay", "Onay Pay", "About Click", "Innopay", "WebMoney Kazakhstan".	Joint-stock company (JSC) "AsiaCredit Bank", which uses multiple electronic payment systems in its operations.	LLP: "Hermes Garant Group", "Innoforce systems", "MAER Soft", "RPS Asia".
"Wooppay", "Aitu – Payment Solutions".	JSC "Eurasian Bank".	LLP: "Aitu – Payment Solutions", "Wooppay".
"Wooppay", "Qiwi Wallet", "Kassa24", "Wallet One", "RPS", "Innopay", "WebMoney Kazakhstan", "Silkpay", "Interpay".	JSC "Alfa-Bank".	LLP: "QIWI Kazakhstan", "WOOPPAY", "Interpay", "Aitu – Payment Solutions".

"Wooppay".	JSC "Capital Bank Kazakhstan".	LLP "WOOPPAY".
"Kassa24".	"First Heartland Jusan Bank".	LLP "Kassa24".
"Wooppay", "Homepay".	"Home Credit Bank".	LLP "WOOPPAY", "Internet Payment Center".
"ONE", "KAZEUROMOBILE".	JSC "ForteBank".	LLP "ONE Technologies", "KAZEUROMOBILE".
"Kazpost", "Kaspi Bank".	JSC: "Kazpost", "Kaspi Bank", and others issuing their own electronic funds.	JSC: "Kazpost", "Kaspi Bank".

Table 1 – Modern structure of electronic money and virtual payment systems in Kazakhstan (as of 1 January 2022).

Therefore, the study supports the global trend and initiatives of the National Bank of the Republic to introduce a fiat currency in the form of the digital tenge. It would be an official national currency, along with existing cash and non-cash currency, secured by state guarantees and therefore would require additional normative consolidation and regulation in practice. This initiative was supported by a study of a collective analytical paper by European scientists and experts on the implementation of national and interstate digital currencies in the world. Moreover, it was supported by the achievements of individual countries in this regard (AUER et al., 2020) and a Report of the National Bank of the Republic of Kazakhstan for public discussions on "Digital tenge" (2021) on the justification of the effectiveness and need for a new national currency – the "digital tenge". Furthermore, paragraph 6.7. Resolution of the Board of the National Bank of the Republic of Kazakhstan No. 133 "On approval of the Program for the development of the national payment system in the Republic of Kazakhstan until 2025" (2020) also includes a provision to develop and promote an initiative to create and introduce electronic national currency, the digital tenge.

At the same time, according to the Report of the National Bank of the Republic of Kazakhstan for public discussions "Digital tenge" (2021), the introduction of a new electronic currency "will ensure further development of the National Payment System and reduce dependence on cash payments". This type of money has significant advantages and unique technological characteristics: interoperability, i.e., ease of circulation and ability to fully interact with other means of payment; confidentiality and security; the scale of movement and

immediacy of transfers; exchange rate flexibility. The term will also need to be legally defined in the future. According to a report by the National Bank, there is "still no universally accepted definition of the term". Moreover, there is a significant advantage of digital tenge over such financial instruments and phenomena of the modern information age as "cryptocurrency" and "stablecoin". The national electronic currency is fully capable of sustaining all monetary functions. In other words, it can be used by all entities in Kazakhstan to pay for any goods and services. Besides, it can be a full-fledged measure of value and a universal nationwide means of circulation, just like cash national currency (AJEVSKIS, 2011).

Many countries around the world are already testing digital official money or considering introducing a national digital currency. In particular, Russia, represented by the Central Bank, unveiled the concept of the digital ruble in 2020 and it is being actively discussed; China is in the active stage of developing and testing a Digital Currency Electronic Payment (DC/EP) platform, and the digital yuan has already been tested in 2020 in four metropolises; the Monetary Authority of Singapore is already in the final stages of testing and implementing a new digital currency. There are cross-border projects on wholesale digital currencies between the following countries: Hong Kong-Thailand, Singapore-Canada, Europe-Japan, and United Arab Emirates-Saudi Arabia (REPORT OF THE…, 2021). Consequently, the prospects for the development of Kazakhstan's monetary and financial system based on the digitalisation of national currency circulation seem quite positive for the following reasons: improving the system of mutual payments among various entities, increasing the availability of financial services, and developing cross-border payment systems.

DISCUSSION

Electronic payment systems, virtual currencies, electronic "wallets" and other high-tech financial information tools and resources have become the subject of study by various experts and scholars in terms of their security as a means of payment, legal and other government regulation and oversight, legitimacy of their use in practice, problems and prospects for the international circulation market. There is a considerable number of studies by foreign experts and scholars related to the regulation and use of electronic money. Such studies are aimed at examining the legal basis and nature of this legal and financial phenomenon.

The publication by C. Crittenden (2020) (chairman of the study group) contains the most comprehensive information on the activities of the working group. It studied the specifics of electronic means of payment in California and other regions of the USA and the specifics of regulating the turnover of information payment resources. Specialists have drawn conclusions about the

significance, importance and role of using special wire transfers for the business community in California and the State government, based on a study of various official documents, government regulations, information resources regulations, and electronic payment systems. They have also analysed the security of e-money in different sectors of public life. This group of scholars and practitioners came to an interesting and important conclusion that in today's world, blockchain technology has moved far beyond the interests of the "computer scientists" and public advocates of cryptocurrency that initially caused its emergence and formation (TANIRBERGENOVA et al., 2021; MYTROFANOV et al., 2022). Nowadays, electronic money influences the distribution of power in society, promotes decentralised administration, supports the development of "sovereign identity" and "confidentiality of personal data", and transforms credit banking and other legislation in various countries and regions (TRUSOVA et al., 2021; GHARAIBEH et al., 2012).

Another specialist from the USA, M. Muhetaer (2021), has studied the stability and state regulation of government monetary policy. He has analysed and investigated in depth the impact of cryptocurrency on the state of the country's banking sector. According to this scholar, the welfare of the USA depends directly on defining the nature and role of electronic money circulation in the modern banking system. Therefore, it is necessary to modernise the regulatory framework for this type of modern money. The impact of e-finance on government monetary policy lies in the modernisation of lending and monetary instruments through the development of special official instructions in this area, which have a legal basis for the regulation of financial processes in the country.

A team of experts from the University of Alabama at Birmingham and a practitioner from the Department of Plastic Surgery at a New York hospital are studying the impact of the legitimacy of cryptocurrency use in medical organisations as a means of paying for treatment. At the same time, they explain the nature and definition of this type of electronic means of payment: "it is a decentralised digital form of payment that is encrypted and protected by blockchain technology". There is also a study of the need for legal support regarding the circulation of electronic payments in the medical field in the USA. In 2018-2021, cryptocurrency as an electronic means of payment for services in this field "has been used by many medical specialities, including urology, plastic and reconstructive surgery, and dermatology" (ZAZA et al., 2021).

Within the framework of examining laws on foreign capital investment of businesses in the country, the possibility of investing electronic money in the Chinese economy, and regulations on the security of personal data in electronic circulation, Chinese banking expert M. Zhang (2020) makes a valid point about the shortcomings of regulations on intangible (virtual) money turnover in the

monetary policy of the Chinese. He notes the importance of legal directives from the State's Supreme People's Court to clarify and supplement legislative initiatives regarding the stabilisation of terminology and the legal enshrinement of the concept of "electronic money". German scholar P. Schwartz (2021) considers the problems of legal regulation of intervention by state and law enforcement agencies to examine confidential citizen data and control telecommunications networks. He raises the question of the universality and independence of electronic money from governmental regulations. The scholar also addresses issues of legal regulation of electronic money circulation in Germany, considering current changes to legal regulations to ensure the security of users of electronic payment systems and online banking.

Another scholar, W.M. Maurer (2021), has an interesting perspective on the specifics of regulation and state control of the movement of electronic payments via mobile devices and social media. He believes that the state should not restrict the developers of new payment information tools with any legal or control measures. According to him, the future of the world's paperless monetary system lies in these tools. He develops a peculiar terminology in the field of electronic money, modernising the current academic concepts of "mobile money" and "social currency", and giving them a certain value and risk content. In this context, one can state that the concept of "social currency" has been studied in science and law before, but there is still no general terminological, let alone legal, the definition of it.

Mobile money is recognised by many scholars as a multi-functional and innovative medium and a tool designed to make use of the most relevant financial services by transferring money through cellular and mobile phone operators using phones and other portable devices. M. Fourcade and J. Gordon (2020) consider the issues of the relationship between state regulation of the information and digital sphere and the development of new payment systems in the world. A Chinese expert from the University of California examines a specialised electronic means of payment and turnover in social global networks, Bitcoin, as the first decentralised cryptocurrency. In revealing its investment potential, he studies and notes particular aspects of the need for state regulation of money circulation regarding various electronic network platforms (XU, 2020).

A group of European academics sees the emergence of new electronic means of payment, particularly cryptocurrency, as an achievement of the entire European and global community. The scholars have studied the socioeconomic value of new electronic means of payment, the profitability of electronic payment systems, the significance of cryptocurrency in the financial market of goods and services, and normative regulation of virtual money instruments circulation system in the legislation of the European Union countries (REULE and HÄRDLE,

2021; MIETHLICH et al., 2022). Another group of European specialists is calculating selected indicators to clarify the importance of cryptocurrency in the European market and for the functioning of the legitimate and most widespread electronic payment systems. Cryptocurrency is also studied by the authors as a special investment vehicle, alongside traditional investment "portfolios". They also calculate the legal risks regarding the unstable legal regulation of electronic money turnover in certain European countries (PETUKHINA et al., 2021).

The diversity of ideas and reflections presented in the aforementioned studies shows that there is no consensus and no common scientific understanding of the increasing scale and direction of the e-money impact on the monetary system regulation. This is related to the wide variety of virtual money systems in which electronic means of payment represent different legal natures of financial products, and payment platforms have many varieties. Therefore, the development of a unified regulatory and legal approach to the concept and nature, role and content of electronic money as the most important virtual means of payment and instrument of modern high-tech information monetary turnover is necessary at the global and national levels.

CONCLUSIONS

One of the problems of legal regulation of electronic money turnover using different electronic payment systems is the lack of uniform terminology in different countries and in the international community and the scientific understanding of certain legal concepts related to the considered issues of the subject. According to the authors, the legal deficiency is the consolidation of the concept of "electronic money" in the legislation of Kazakhstan through the category of the law of obligations (as a type of obligation), rather than as a phenomenon of property nature, namely a special type of property with value and utility for civil circulation. Furthermore, amendments to certain provisions of paragraph 3, Article 25 of Law of the Republic of Kazakhstan No. 11-VI "On Payments and Payment systems" of 26 July 2016 are suggested. These include listing separately "transmission of electronic money" and use of "means of electronic payment", combining both categories in a single sub-paragraph.

Among the organisational and legal issues of reforming electronic money circulation in Kazakhstan, the problem of introducing digital national currency is raised. The study fully supports it, as it will increase the interoperability of money exchange by introducing digital technologies in the financial policy of the state; provide additional privacy and security measures for holders and owners of the mentioned digital currency; ensure the scale of movement and immediacy of transfers and flexibility in exchange rates. Therefore, it may be useful for studying the issues and areas of improvement of law-making and socio-economic policy of

the authorities of Kazakhstan. The study is aimed at forming a new legislative and regulatory framework for digitalisation and implementation of modern innovative concerning the development of electronic means of payment in the country.

REFERENCES

Ajevskis, V. & Vitola, K. (2010). A convergence model of the term structure of interest rates. *Review of Finance*, 14(4), 727-747.

Ajevskis, V. (2011). A target zone model with the terminal condition of joining a currency area. *Applied Economics Letters*, 18(13), 1273-1278.

Armenia. (2004). *Law of the Republic of Armenia No. ZR-150* "On Payment and Settlement Systems and Payment and Settlement Organizations". Available at: https://base.spinform.ru/show_doc.fwx?rgn=90246.

Auer, R., Cornelli, G. & Frost, J. (2020). *Rise of the central bank digital currencies:* drivers, approaches and technologies. Available at: https://www.bis.org/publ/work880.pdf.

Belarus. (2003). *Resolution of the Board of the National Bank of the Republic of Belarus No. 201*. "On approval of the Rules for conducting operations with electronic money". Available at: https://www.nbrb.by/legislation/documents/pp_201_199.pdf.

Belarus. (2008). *Law of the Republic of Belarus No. 455-Z* "On Information, Informatization and Information Protection". Available at: https://pravo.by/document/?guid=3871&p0=h10800455.

Blahuta, R. I., Kovalchuk, Z. Ya., Bondarchuk, N., Kononova, O. & Ilchenko, H. (2019). Financial resources and organizational culture as determinants for competitive strategy of enterprises. *International Journal of Economics and Business Administration*, 7(4), 471-482.

Crittenden, C. (2020). *Blockchain in California*: a roadmap. Available at: https://escholarship.org/uc/item/2j9596dp.

Fourcade, M. & Gordon, J. (2020). Learning like a state: statecraft in the digital age. *Journal of Law and Political Economy*, 1(1). Available at: https://escholarship.org/uc/item/3k16c24g.

Gharaibeh, B., Al-Refaie, A., Goussous, J. & Shurrab, M. (2012). Effect of CCMS on customer satisfaction and loyalty in Jordanian banks. *Information (Japan)*, 15(12 C), 6227-6237.

Hrynko, P., Grinko, A., Shtal, T., Radchenko, H. & Pokolodna, M. (2021). Formation of an Innovative Business Model of a Trade Organization in the Context of Economic Globalization. *Scientific Horizons*, 24(6), 92-98.

Idrysheva, S. K. (2021). Electronic payments and electronic money: legal bases and individual collisions in the legal understanding of terms. *Journal of Foreign Legislation and Comparative Jurisprudence,* 17(1), 68-85.

Kazakhstan. (2016). *Law of the Republic of Kazakhstan No. 11-VI.* "On Payments and Payment systems". Available at: https://adilet.zan.kz/rus/docs/Z1600000011.

Kazakhstan. (2020). *Resolution of the Board of the National Bank of the Republic of Kazakhstan No. 133*. "On approval of the Program for the development of the national payment system in the Republic of Kazakhstan until 2025". Available at: https://online.zakon.kz/Document/?doc_id=34607746&pos=13;-58#pos=13;-58.

Kazakhstan. (2021). *Report of the National Bank of the Republic of Kazakhstan for public discussions.* "Digital tenge". Available at: https://cutt.ly/YHXBHCO.

Kyrgyzstan. (2015) *Law of the Kyrgyz Republic No. 21*. "On the Payment System of the Kyrgyz Republic". Available at: http://cbd.minjust.gov.kg/act/view/ru-ru/205425.

Maurer, W. M. (2021). *Regulation as retrospective ethnography.* Available at: https://escholarship.org/uc/item/70f3942c.

Miethlich, B., Belotserkovich, D., Abasova, S., Zatsarinnaya, E. & Veselitsky, O. (2021). The Impact of COVID-19 on Digital Enterprise Management. *IEEE Engineering Management Review*, 49(4), 16-29.

Miethlich, B., Belotserkovich, D., Abasova, S., Zatsarinnaya, E. & Veselitsky, O. (2022). Transformation of Digital Management in Enterprises Amidst the COVID-19 Pandemic. *Institutions and Economies,* 14(1), 1-26.

Muhetaer, M. (2021). *Essay on monetary policy and bank regulation.* UC Riverside. Available at: https://escholarship.org/uc/item/3v32c1xm.

Mytrofanov, O., Proskurin, A., Poznanskyi, A., & Zivenko, O. (2022). Determining the power of mechanical losses in a rotary-piston engine. *Eastern-European Journal of Enterprise Technologies*, 3(8-117), 32-38.

Petukhina, A., Trimborn, S., Härdle, W. K. & Elendner, H. (2021). Investing with cryptocurrencies – evaluating their potential for portfolio allocation strategies. *Quantitative Finance*, 1-29. Available at: http://dx.doi.org/10.2139/ssrn.3274193.

Proskurnina, N. V., Shtal, T. V., Slavuta, O. I., Serogina, D. O. & Bohuslavskyi, V. V. (2021). Omnichannel Strategy of digital transformation of retail trade enterprise: From concept to implementation. *Estudios de Economia Aplicada*, 39(6). https://doi.org/10.25115/eea.v39i6.5238

Reule, R. & Härdle, W. K. (2021). Rise of the machines? Intraday high-frequency trading patterns of cryptocurrencies. *European Journal of Finance*, 27(1-2), 23-24.

Schwartz, P. (2021). *German and U.S. telecommunications privacy law:* legal regulation of domestic law enforcement surveillance. Available at: https://escholarship.org/uc/item/41s8v90m.

Tanirbergenova, A., Orazbayev, B., Ospanov, Y., Omarova, S. & Kurmashev, I. (2021). Hydrotreating unit models based on statistical and fuzzy information. *Periodicals of Engineering and Natural Sciences*, 9(4), 242-258.

Trusova, N. V., Hryvkivska, O. V., Yavorska, T. I., Prystemskyi, O. S., Kepko, V. N. & Prus, Y. O. (2020). Innovative development and competitiveness of agribusiness subjects in the system of ensuring of economic security of the regions of Ukraine. *Rivista di Studi sulla Sostenibilita*, 2020(2), 141-156.

Trusova, N. V., Melnyk, L. V., Shilo, Z. S. & Prystemskyi, O. S. (2021). Credit-investment activity of banks of the Ukraine: Financial globalization, risks, stabilization. *Universal Journal of Accounting and Finance*, 9(3), 450-468.

Xu, Y. (2020). *Bitcoin price forecast using LSTM and GRU recurrent networks, and hidden Markov model.* Available at: https://escholarship.org/uc/item/70d9n5sd.

Zaza, T., Boudreau, H. S. & Boyd, C. J. (2021). The utilization of cryptocurrency as financial reimbursement in dermatology practices. *Dermatology Online Journal*, 27(10). Available at: https://escholarship.org/uc/item/2pn9n8tz.

Zhang, M. (2020). Change of regulatory scheme: China's new foreign investment law and reshaped legal landscape. *UCLA Pacific Basin Law Journal*, 37(1). Available at: https://escholarship.org/uc/item/5xh829ms.

The Law, State and Telecommunications Review / Revista de Direito, Estado e Telecomunicações

Contact:
Universidade de Brasília - Faculdade de Direito - Núcleo de Direito Setorial e Regulatório
Campus Universitário de Brasília
Brasília, DF, CEP 70919-970
Caixa Postal 04413

Phone: +55(61)3107-2683/2688

E-mail: getel@unb.br

Submissions are welcome at: https://periodicos.unb.br/index.php/RDET

The Concept of Cyber Insurance as a Loss Guarantee on Data Protection Hacking in Indonesia

Submitted: 18 July 2022
Reviewed: 3 November 2022
Revised: 2 December 2022
Accepted: 3 December 2022

Article submitted to blind peer review

Jufryanto Puluhulawa[*]
https://orcid.org/0000-0001-7090-9699
Mohamad Hidayat Muhtar[**]
https://orcid.org/0000-0002-1728-683X
Mellisa Towadi[***]
https://orcid.org/0000-0002-9237-5250
Vifi Swarianata[****]
https://orcid.org/0000-0003-2257-9677
Apripari[*****]
https://orcid.org/0000-0001-5508-2136

DOI: https://doi.org/10.26512/lstr.v15i2.44206

Abstract

[Purpose] This research departs from the legal vacuum regarding data protection insurance in Indonesia. In terms of regulation, Law Number 40 of 2014 concerning Insurance has not regulated all about cyber insurance, and Indonesia still needs to have a law that regulates data protection.

[Methodology/Approach/Design] This research is categorized into the normative legal research type based on the issues and themes raised as a research topic. The research approach used is the conceptual approach, philosophical approach, and analytical approach. The research focuses on analyzing the concept of cyber insurance in protecting data and a study of the urgency of regulating cyber insurance in Indonesia to minimize the impact of losses due to data hacking.

[Findings] The results show that the concept of cyber insurance in personal data protection began in the 80s and increased in the early 2000s due to digitization in all areas of people's lives. This significant development was not followed by Indonesia, with a legal vacuum regulating cyber insurance in data protection. Therefore, several things that

[*]Jufryanto Puluhulawa, Assistant Professor, Universitas Negeri Gorontalo. Law Science Department, Faculty of Law Universitas Negeri Gorontalo, Jend. Sudirman Street no. 6, Gorontalo City, 96128, Gorontalo, Indonesia. E-mail: jufryantopuluhulawa@ung.ac.id.
[**]Mohamad Hidayat Muhtar, Lecturer, Universitas Negeri Gorontalo. E-mail: hidayatmuhtar21@ung.ac.id.
[***]Mellisa Towadi, Assistant Professor, Universitas Negeri Gorontalo. E-mail: mellisatowadi@ung.ac.id.
[****]Vifi Swarianata, Lecturer, Universitas Negeri Gorontalo. E-mail: vifiswarianata@ung.ac.id.
[*****]Apripari, Lecturer, Universitas Negeri Gorontalo. E-mail: apripari@ung.ac.id.

Indonesia must do, namely Revision of the Law of the Republic of Indonesia Number 40 of 2014 concerning Insurance, Establishment of implementing regulations, need new normalization in overriding the Civil Code.
[Practical Implications] This study has legal implications for norming. In addition, it has implications for changes in the concept of insurance in Indonesia because, so far, cyber insurance services are still conventional.
[Originality/Value] On an Indonesian scale, this research is the first to comprehensively discuss cyber insurance for data protection.

Keywords: Cyber Insurance. Data Protection. Legal Void.

INTRODUCTION

Attention to data protection in Indonesia, in general, has been emphasized in the 1945 Constitution of the Republic of Indonesia ('UUD'). In particular, Article 28G paragraph 1 states that everyone has the right to personal protection, family, honor, dignity, and property under his control and has the right to a sense of security and protection from the threat of fear to do or not do something which is the proper human rights. In line with the constitution's substance, personal data is now like a valuable asset, which in M. Arsyad Sanusi's view, is like a commodity with high economic value SANUSI, 2004, so it must be maintained and appropriately managed in today's digitalization world.

In several international instruments, such as the OECD Guidelines and the Data Protection Convention from the Council of Europe, personal data is information about an identified or identifiable natural person. Another definition of personal data is data in the form of identity, code, symbol, letter, or a number of a person's marker that is private and confidential SAUTUNNIDA, 2018.

Society's dependence on information technology is increasing, so the risk is higher NAPITUPULU, 2017. The digital revolution has created an innovative capacity to acquire, store, manipulate and transmit volumes of data in real-time, vast and complex. Therefore, the digital revolution is often considered synonymous with the data revolution. These developments have encouraged the collection of various data, no longer dependent on considerations of what data might be helpful in the future.

However, almost all data is collected, the government and the private sector are competing to increase their data storage capacity, and data erasure is becoming less and less frequent. They discover new value in the data, treated like a tangible asset. This new era of data management is commonly referred to as Big Data. The interaction of digital society in using the internet depends on the availability, integrity, and confidentiality of information in cyberspace.

Although insurance companies have insured all types of disaster products and events for hundreds of years, cyber insurance, which covers corporate losses

and costs stemming from cyber-attacks, is a relatively new concept that Lloyd's of London (Lloyd's) insurance company started as one of. The first company to sell policies for cyber-attack-related incidents in 1999. Twenty years later, cyberattacks have become a daily occurrence, and one successful breach can cost an organization/company hundreds of thousands, even millions of dollars TALESH, 2018. This opens the horizon of thinking that most people think that digitalization, on the one hand, brings benefits to civilization, but on the other hand, digitalization brings new problems as well as challenges in this era of the Industrial Revolution 4.0 PULUHULAWA, PULUHULAWA e KATILI, 2020.

Cybercrime is one of the most critical business risks for companies worldwide in the 21st century. Cyber risk can be defined as 'any risk arising from using information and communication technology (ICT) that compromises the confidentiality, availability or integrity of data or services. Operational technology (TO) damage ultimately causes business disruption, infrastructure damage (critical), and physical property damage. Generally, breaches of obligations and confidentiality regarding data protection, business interruption, and data theft can result in financial damage and reputational loss WREDE, STEGEN e GRAF VON DER SCHULENBURG, 2020.

According to McAfee and the Center for Strategic and International Studies, cybercrime consumed at least $600 billion in 2017 of the entire global economy, or nearly one percent of the global GDP lost to cybercrime each year. Data breach security incidents have become commonplace annually and cost hundreds of millions. As a result, the market for insuring these losses has proliferated in the last decade. Cyber insurance is a broad term for insurance policies that cover first and third-party losses due to computer-based attacks or damage to company information technology systems. Examples include hacking or other incidents of unauthorized persons illegally gaining access to computer systems and attacks on systems by viruses or other malware ROMANOSKY, ABLON, *et al.*, 2109.

The losses above are caused by the increasing number of human activities controlled by technology and the internet. Coupled with the large amount of data stored by internet technologies, there is an increased risk of cyberattacks, defined as deliberate and malicious acts intended to damage an organization's critical ICT infrastructure via the internet. The economic consequences of these cyberattacks can be far-reaching as companies must repair or replace equipment and pay additional labor to upgrade cybersecurity programs and equipment, cover consultant fees, and even pay heavy regulatory fines for failing to protect confidential information to comply with breach reporting requirements—data or to implement necessary privacy or security measures.

Privacy is a complex concept consisting of 'three independent and reduced elements: confidentiality, anonymity, and solitude. Each of these elements is independent. Therefore, loss or violation may occur due to the intrusion of any of the three elements GAVISON, 1980. In addition, significant data breaches often lead to costly litigation and cross-litigation between multiple parties due to their interdependence, resulting in high costs for cybercrime losses NIEVAS, 2020.

Usually, cyber insurance provides 2 (two) types of coverage: the first party, which covers damage to the insured due to cyber incidents. Furthermore, third-party coverage protects liability provided in the event of a cyber incident that harms the client or related parties. These types usually include coverage for any expenses related to public relations, legal fees, and business interruptions. Cyber insurance policies are generally written on a claims-made basis, while the insured must notify the claim during the policy period KRISNAREINDRA, 2021.

In this regard, cyber insurance in Indonesia has yet to become something urgent. This is based on information from the executive director of the Indonesian General Insurance Association (AAUI), who stated that until the end of 2017, there were no more than ten cyber insurance companies, primarily foreign ones. Some of them are PT Asuransi Tokio Marine Indonesia, PT AIG Insurance Indonesia, and PT Chubb General Insurance Indonesia SANDY, 2019. In addition, according to Google Trends, Indonesia has not found sufficient data that discusses cyber insurance, as described in the following picture:

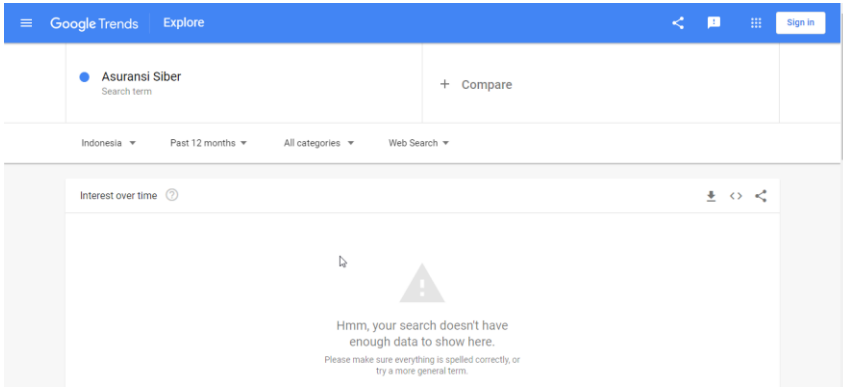


Figure 1 – Graphic Data that Discusses Cyber Insurance.

The lack of interest in cyber insurance in Indonesia is because this type of insurance is still relatively new and is different from conventional insurance. In particular, the legal framework for cyber insurance still needs to be stronger. Ni Gusti Ayu Putu Nitayanti confirmed this, and Ni Made Ari Yuliartini Griadhi in conventional periscopes, in general, that until now, Indonesia has no special rules governing the protection of personal information. Regulations regarding the protection of personal information are still separate in several laws and regulations, so a special arrangement regarding the protection of personal information is needed to create legal certainty NITAYANTI e GRIADHI, 2014.

Regarding insurance regulation, Indonesia has Law (UU) Number 40 of 2014 concerning Insurance, but the Act and implementing regulations need to explain the concept of cyber insurance specifically. Therefore, it is essential to regulate more strictly about cyber insurance in Indonesia to minimize the risks that arise when there is a theft or breach of company data MADAMBA, PULUHULAWA, *et al.*, 2021.

One example occurred on April 17, 2020, when an international hacker with the nickname 'Why So Dank' managed to hack Tokopedia. According to @underthebreach, the hacked data contained emails, passwords, and usernames with 91 million accounts and 7 million merchant accounts hacked. The perpetrators sold the data for US $ 5,000 or around Rp. 74 million FATHUR, 2020. Tokopedia is also experiencing legal problems over this data leak with a claim for compensation of 100 billion Rupiah.

The right to privacy is one of the rights inherent in everyone. The right to privacy is the dignity of every person that must be protected. Personal data relates to a person's characteristics, name, age, gender, education, occupation, address, and position in the family MAHIRA, YOFITA e AZIZAH, 2020. Therefore, the weak regulation of cyber insurance in Indonesia harms business development because companies, in the event of data hacking, will face several risks: claims for compensation, reputational damage, and the risk of temporary operational termination.

PROBLEM STATEMENT

The problems studied in this paper are focused on analyzing the concept of cyber insurance in protecting data, as well as a study of the urgency of regulating cyber insurance in Indonesia to minimize the impact of losses due to data hacking.

METHOD

This research is categorized into the normative legal research type based on the issues and themes raised as a research topic. The research approach used is the conceptual approach, philosophical approach, and analytical approach. It ends with the conclusion that aims to generate new findings as answers from the subject matter that has been set as well as will be analyzed with the descriptive-analytical method, namely by describing the laws and regulations that apply to the legal theory and practices of law enforcement positively related to the problem MARZUKI, 2014.

DISCUSSION

The Concept of Cyber Insurance in Protecting Data

Conventional insurance is not designed to cover cyber risks. Such policies, for example, general commercial liability, director's and officers' errors and omissions, and data theft and ransoms, usually do not contain express coverage for these risks in conventional insurance KISLOFF, AHUJA e BANK, 17.

Cyber insurance has been around since the late 1970s, with the market growing out of risk from technological developments/errors and negligence. In the 1980s, policies regarding cyber insurance were first introduced, designed primarily for financial institutions and blue-chip organizations. The number of insurance providers offering products has gradually grown due to technological developments CAMILLO, 2017. There is a growing awareness that cyberspace only sometimes matches conventional insurance coverage.

To avoid uncertainty about coverage for cyber risk, cyber insurance offers policies to manage potential losses from data breaches, ransomware attacks, theft or loss of unencrypted assets, business email intrusion, cloud misconfiguration exploits, and other cybercriminal activities. Personal data breaches and security incidents have become commonplace, with thousands of cases occurring each year and some costing hundreds of millions of dollars. Case in point: A cyber researcher from Singapore, DarkTracer, reported a leak of credential data from over 49 thousand government sites worldwide. In addition, as many as 40,629 internet users in Indonesia were infected with Stealers such as Redline, Raccoon, Vidar, and others. In addition, there are 502 thousand more credential data for access to the .id domain (dot id), which was leaked and distributed through dark sites ASHARI, 2022.

In essence, this phenomenon is not in line with the idea of The Right to Privacy or the right not to be disturbed. Warren and Brandheis are of the view that with the development and advancement of technology, there is a public

awareness that there has been awareness that there is a person's right to enjoy life LATUMAHINA, 2014.

The massive number of personal data breaches and security incidents implies that the market for insurance against losses has snowballed in recent decades. Cyber insurance is a broad term for insurance policies that cover first and third-party losses due to computer-based attacks or malfunctions of company information technology systems.

Increased crime using information technology has been identified since 2003, for example, carding crimes (credit card fraud), ATM/EDC skimming, hacking, cracking, phishing (internet banking fraud), malware (viruses/worms/trojans/bots), cybersquatting, pornography, online gambling, transnational crime (drug trafficking, mafia, terrorism, money laundering, human trafficking, underground economy). Cybercrime is a hacking event or another occurrence of an unauthorized person gaining access to a computer system, an attack on the system by a virus, or other malware ROMANOSKY, ABLON, *et al.*, 2109.

The initial concern over this was the spread of viruses and other types of malwares that could potentially lead to legal liability. However, the increased appreciation of cyber vulnerabilities sometimes translates into demand for cyber insurance. Most of the company's spending during the late 1990s and early 2000s focused on loss mitigation and network security. Meanwhile, insurers grappling with these emerging risk areas are reluctant to offer significant line sizes for largely untested products and where there is a dearth of historical loss data to measure and price risk. There is a feeling among insurance and corporate risk buyers that the cyber insurance market remains a niche area, lacking the coverage and capacity they need ROMANOSKY, ABLON, *et al.*, 2109.

Apart from this, the development of cyber insurance has progressed quite rapidly, accompanied by the increasing number of human activities that intersect with the internet. The coverage of protection provided by cyber insurance is as follows:

(1) Post-incident forensic investigations;
(2) Data retrieval and recovery, including negotiation and payment of ransomware requests;
(3) Notice of breach to comply with legal and contractual obligations;
(4) Credit monitoring and identity theft protection services for those affected by the incident;
(5) Management of public relations and communications to reduce potential reputational damage;
(6) Network business disruption; and

(7) Attorney's fees related to the notification of infringement.

If you look at the explanation above, the existence of cyber insurance to minimize losses from cybercrime is one of the preventive ways that can be done. Preventive legal action can be interpreted as the protection provided by the government to prevent violations that can cause harm ASRI, 2018. Unfortunately, in Indonesia, the regulations and concepts of cyber insurance have yet to be comprehensively regulated in the legislation. Even in the general context of the protection of personal data itself, no specific regulation covers it.

The Urgency of Cyber Insurance Regulations in Indonesia to Minimize the Impact of Losses Due to Data Hacking

Indonesia is one of the countries with the most significant number of internet users worldwide. Internet users in 2017 touched 143.26 million people. That number has increased a lot compared to previous years, namely, 2016, which counted 132.7 million people, and 2015, which was 110.2 million people PUTRA, 2021. Currently, internet users in Indonesia are approximately 73.7% of the total population in the 2019-2020 period (Q2) GUNAWAN, AULIA, *et al.*, 2021.

The number of internet users of that size has a considerable risk of cybercrime regarding data protection. If you look at it from a broader perspective, this crime has attacked several large companies, especially those engaged in online buying and selling (Electronic Commerce / E-commerce), by hacking user data to be traded illegally. Some of these companies, namely Tokopedia and Bukalapak, were hacked, and millions of user data were stolen/taken and traded freely in cyberspace.

This certainly causes losses for users and companies with a significant loss of value. Not to mention the issue of the company's credibility and also lawsuits against the company. Therefore, the importance of cyber insurance in Indonesia is part of the adaptation of technological developments and legal protection. The absence of a guarantee that e-commerce transactions are free from attempts to destroy/manipulate data will undoubtedly impact decreasing public trust in this system. Whereas in business transactions in the current global era, legal certainty and security are the pillars supporting the development of economic activity. It should be noted that personal data or information has become very valuable and vulnerable as a commodity. Hence, it poses a risk of vulnerability to misuse or theft of personal data FAD, 2021.

Theoretically, from a legal point of view, insurance is a: risk coverage agreement between the insured and the insurer that promises to pay for the loss caused by the insured risk to the insured. The concept is that the insurer aims to

obtain payment of a premium as a reward while the Insured aims to be free from risk and obtain compensation if a loss occurs in his interests NAVISA, 2020.

What he understands is that any risk that arises and is capable of causing harm to the insured's interests can be used as an object of insurance or, in other words, can be insured. This means that all forms of transactions in electronic commerce should be ensured to ensure legal certainty and security in transactions and minimize the risk of losses that may occur. Legal certainty will bring justice, which is when there is legal certainty. If viewed from the perspective of the grand theory of the civil law system, legal objectives can be realized in the form of justice, certainty, and benefit. If viewed from the perspective of utilitarian legal theory, personal data insurance is essential to provide the maximum benefit to the most significant number of people.

Unfortunately, the current regulations in Indonesia do not regulate the existence of insurance related to the term cyber insurance. Synergistic with this condition, Gio Arjuna Putra said, the high number of Internet penetration and social media users in Indonesia is inversely proportional to the progress of legal and technological development. This can be seen from the stipulation of a legal product at the level of the law that explicitly regulates the protection of personal data PUTRA, 2021, especially regarding personal data insurance.

Therefore, it is crucial to establish cyber insurance regulations to protect personal data. This is following the discovery of laws and the creation of new laws by the goals of the State, which is a mandatory value to be implemented to achieve legal supremacy and justice MUHTAR, 2019. The legal vacuum in personal data protection is undoubtedly very sad, considering the need for a Personal Data Protection Law to be crucial in this era of digital disruption FATHUR, 2020. So, a progressive legal approach is needed to emphasize legal breakthroughs so that harmonizing regulations and community conditions can run well. Do not let there be a stigma that the law is left behind by the society it governs TAMPI, 2018.

On the other hand, the root of the problem is the stagnation of regulations regarding the protection of personal data, especially regarding personal data insurance, partly because the State of Indonesia is still using the old laws and regulations inherited from the Netherlands of concordance. The articles that regulate insurance or coverage issues in the Commercial Code (KUHD) are articles 246 to 308 of the KUHD. Article 246 of the Commercial Code (KUHD) states insurance or coverage is an agreement in which the insurer binds himself to the insured by obtaining a premium to provide him with compensation for a loss, damage, or not getting the expected profit, which may be suffered due to an uncertain event.

Furthermore, article 247, it is stated that the coverage can include, among others: fire hazards; (KUHD 287) the dangers that threaten unharvested agricultural products; (KUHD) the soul of one or more persons; (KUHD 302) the dangers of the sea and the dangers of slavery; (KUHD 592) the dangers of transportation on land, in rivers and inland waters. (KUHD 686).

The Law of the Republic of Indonesia Number 40 of 2014 concerning Insurance does not mention the type of cyber insurance. If you refer to the Commercial Code, the types of insurance in Indonesia are:

(1) Loss Insurance: Loss insurance is an insurance agreement in which the insurer provides services to cover the risk of loss or loss of benefits to the insured. In this case, the object of loss insurance can be in the form of houses, buildings, factories, and movable objects such as motorized vehicles, ships, and movable objects contained in or as part of the relevant fixed object MUHAMMAD, 2006.

(2) Life Insurance: Life Insurance is a business that provides risk management services that provide payments to policyholders, the insured, or other entitled parties if the insured dies or remains alive or other payments to policyholders, the insured, or other entitled parties at a specific time regulated in the agreement, the amount of which has been determined and/or is based on the results of fund management. In connection with the explanation above, there is still a legal vacuum in the regulation of cyber insurance in Indonesia. Cyber insurance cannot be categorized as loss insurance because it is so complex concerning cybercrime data hacking. Indonesia still needs to establish definite rules and standardization concerning cyber insurance policy coverage. The ambiguity of this arrangement is principally at risk of legal uncertainty and losses caused by data hacking.

Based on this, the concept of cyber insurance in Indonesia must be regulated with various considerations, including:

(1) Revision of Law of the Republic of Indonesia Number 40 of 2014 concerning Insurance: This revision of the Insurance Law is mandatory so that cyber insurance arrangements can have a clear legal basis by including a particular chapter on cyber insurance, such as loss insurance or life insurance.
(2) Need for Implementing Arrangements: Implementing regulations are regulated through government or ministerial regulations relating to

substantial matters that need a complete description. This implementing regulation is regulated regarding cyber insurance coverage, policies, premiums, and the obligation to use cyber insurance for e-commerce companies and other arrangements according to cyber insurance needs.

(3) There is a need for norms that override the Civil Law Code: This needs to be done because the legal norms, especially those that regulate insurance in the Civil Code, which was made in the colonial period, are no longer following the development of the times and current technology. This urgency should be done so that in its application later, there will be no different legal interpretations that can hinder the implementation of cyber insurance in Indonesia.

Based on this, the author argues that with the increasingly complex development of technology and world crimes related to data hacking. Indonesia needs to prepare itself, especially in terms of cyber insurance regulations, in order to minimize the risk of loss from data hacking and provide legal certainty and protection for cyber-crimes.

CONCLUSIONS

The complexity of the times has brought the development of an increasingly advanced insurance world. Conventional insurance related to data hacking and cybercrimes can no longer protect against losses. As one of the countries with the most significant internet users, Indonesia should design a cyber-crime protection system, one of the regulations regarding cyber insurance. Therefore, in this case, Indonesia needs to pay attention to several things:

(1) Revise the Law of the Republic of Indonesia Number 40 of 2014 concerning Insurance.
(2) There is a need for implementing regulations regarding cyber insurance and
(3) There is a need for norms that override the Civil Code.

In addition, in the aspect of personal data protection, it is necessary to normalize a special law that regulates the protection of personal data. This is important because, until now, Indonesia does not have a law that explicitly regulates personal data.

REFERENCES

Ashari, M. (2022). Belajar Dari Kebocoran Data Kredensial: Data Yang Paling Berharga adalah Data Pribadi. *Kementerian Keuangan Republik Indonesia,* 22 Maret 2022. Available at:

https://www.djkn.kemenkeu.go.id/kpknl-kisaran/baca-artikel/14838/Belajar-Dari-Kebocoran-Data-Kredensial-Data-Yang-Paling-Berharga-adalah-Data-Pribadi.html.

Asri, D. P. B. (2018). Perlindungan Hukum Preventif Terhadap Ekspresi Budaya Tradisional di Daerah Istimewa Yogyakarta Berdasarkan Undang-Undang Nomor 28 Tahun 2014 Tentang Hak Cipta. *JIPRO: Journal of Intellectual Property*, 1, 1, 13-23.

Camillo, M. (2017). Cyber Risk and the Changing Role of Insurance. *Journal of Cyber Policy*, 2, 1, 53-63.

Chotimah, H. C. (2019). Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara [Cyber Security Governance and Indonesian Cyber Diplomacy by National Cyber and Encryption Agency]. *Jurnal Politica*, 113-128.

Fad, M. F. (2021). Perlindungan Data Pribadi Dalam Perspektif Sadd Dzari'ah. *Muamalatuna*, 13, 1, 33-69.

Fathur, M. (2020). *Tanggung Jawab Tokopedia Terhadap Kebocoran Data.* National Conference on Law Studies (NCOLS). Jakarta: Fakultas Hukum Universitas Pembangunan Nasional "Veteran" Jakarta, 43-60.

Gavison, R. (1980). Privacy and the Limits of Law. *The Yale Law Journal*, 89, 3, 421-471.

Google Trends. Explore "Asuransi Siber". *Google Trends*, 9 July 2022. Available at: https://trends.google.com/trends/explore?geo=ID&q=Asuransi%20Siber.

Gunawan, R. (2021). Adiksi Media Sosial dan Gadget bagi Pengguna Internet di Indonesia. *Techno-Socio Ekonomika*, 14, 1, 1-14.

Kisloff, M., Ahuja, J. & Bank, A. (2021). Looking for Cyber Insurance? Legal Terms, Issues to Know. *Bloomberg Law*, 2021 September 17. Available at: https://news.bloomberglaw.com/us-law-week/looking-for-cyber-insurance-legal-terms-issues-to-know.

Krisnareindra, K. (2021). The "PDP Law" Era and Cyber Protection Urgency. *IndonesiaRe*, 15 June 2021. Available at: https://indonesiare.co.id/id/article/the-pdp-law-era-and-cyber-protection-urgency.

Latumahina, R. E. (2014). Aspek Hukum Perlindungan Data Pribadi di Dunia Maya. *Gema Aktualita*, 3, 2, 14-25.

Madamba, P. (2021). Application of Territorial Principles Against Pedophile Criminal Act Perpetrators Perpetrated by Foreign Citizens. *Jurnal Legalitas*, 14, 1, 77-84.

Mahira, D. F. F., Yofita, E. & Azizah, N. L. (2020). Consumer Protection System (CPS): Sistem Perlindungan Data Pribadi Konsumen Melalui Collaboration Concept. *Jurnal Legislatif*, 3, 2, 287-302.

Marzuki, M. P. (2014). *Penelitian Hukum:* Edisi Revisi. Jakarta: Prenadamedia Group.

Muhammad, A. K. (2006). *Hukum Asuransi Indonesia.* Bandung: Citra Aditya Bakti.

Muhtar, H. M. (2019). Model Politik Hukum Pemberantasan Korupsi Di Indonesia Dalam Rangka Harmonisasi Lembaga Penegak Hukum. *Jambura Law Review*, 1, 1, p. 68-93.

Napitupulu, D. (2017). Kajian Peran Cyber Law Dalam Memperkuat Keamanan Sistem Informasi Nasional. *Deviance Jurnal Kriminologi*, 1, 1, 100-113.

Navisa, F. (2020). Karakteristik Asas Kepentingan (Insurable Interest) Dalam Perjanjian Asuransi. *Negara dan Keadilan*, 9, 2, 188-204.

Nievas, A. M. (2020). Cyber Insurance Today: Saving It before It Needs Saving. *Catholic University Journal of Law and Technology*, 29, 1, 111-144. Available at: https://scholarship.law.edu/jlt/vol29/iss1/4?utm_source=scholarship.law.edu%2Fjlt%2Fvol29%2Fiss1%2F4&utm_medium=PDF&utm_campaign=PDFCoverPages.

Nitayanti, N. G. A. P.; Griadhi, A. Y. N. M. (2014). Perlindungan Hukum Terhadap Informasi Pribadi Terkait Privacy Right Berdasarkan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. *Kertha Negara: Journal Ilmu Hukum*, 2, 5, 1-6.

Parker, D. B. (2007). The Dark Side of Computing: SRI International and the Study of Computer Crime. *IEEE Annals of the History of Computing*, 29, 1, 3-15.

Puluhulawa, F. U., Puluhulawa, J. & Katili, M. G. (2020). Legal Weak Protection of Personal Data in the 4.0 Industrial Revolution Era. *Jambura Law Review*, 2, 2, 182-200.

Putra, G. A. (2021). Reformulasi Ketentuan Pengelolaan Data Pribadi sebagai Ius Constituendum dalam Menjamin Perlindungan Data Pribadi Pengguna Layanan Media Sosial. *Jurnal Hukum Lex Generalis*, 2, 8, 684-700.

Putra, W. (2021). Aspek Cybercrime dalam Paylater. *Jurist-Diction*, 4, 2, 791-812.

Romanosky, S. (2019). Content analysis of cyber insurance policies: how do carriers price cyber risk? *Journal of Cybersecurity*, 5, 1, 1-19.

Sandy, O. P. (2019). Asuransi Siber di Indonesia Masih belum Diminati. *Cyberthreat.id*, 10 May 2019. Available at:

https://cyberthreat.id/read/418/Asuransi%20Siber%20di%20Indonesia%20Masih%20belum%20Diminati%20https:/cyberthreat.id/read/418/Asuransi-Siber-di-Indonesia-Masih-belum-Diminati.

Sanusi, M. A. (2004). *Teknologi Informasi dan Hukum E-commerce.* Jakarta: Dian Ariesta.

Sautunnida, L. (2018). Urgensi Undang-Undang Perlindungan Data Pribadi di Indonesia: Studi Perbandingan Hukum Inggris dan Malaysia. *KANUN: Jurnal Ilmu Hukum*, 20, 2, 369-384.

Talesh, S. A. (2018). Data Breach, Privacy, and Cyber Insurance: How Insurance Companies Act as "Compliance Managers" for Businesses. *Law & Social Inquiry*, 43, 2, 417-440.

Tampi, M. M. (2018). Menakar Progresivitas Teknologi Finansial (Fintech) Dalam Hukum Bisnis Di Indonesia. *Era Hukum-Jurnal Ilmiah Ilmu Hukum*, 16, 2, 246-281.

Wrede, D., Stegen, T. & Graf Von Der Schulenburg, J. (2020). Affirmative and silent cyber coverage in traditional insurance policies: Qualitative content analysis of selected insurance products from the German insurance market. *Geneva Pap Risk Insur Issues Pract*, 45, 4, 657-689.

The Law, State and Telecommunications Review / Revista de Direito, Estado e Telecomunicações

Contact:
Universidade de Brasília - Faculdade de Direito - Núcleo de Direito Setorial e Regulatório
Campus Universitário de Brasília
Brasília, DF, CEP 70919-970
Caixa Postal 04413

Phone: +55(61)3107-2683/2688

E-mail: getel@unb.br

Submissions are welcome at: https://periodicos.unb.br/index.php/RDET

Digital Transition, Sustainability and Readjustment on EU Tourism Industry: Economic & Legal Analysis*

Submitted: 19 August 2022
Revised: 13 December 2022
Reviewed: 18 December 2022
Accepted: 22 December 2022

Article submitted to peer blind review

Antonio Sánchez-Bayón**
https://orcid.org/0000-0003-4855-8356
Luis M. Cerdá Suárez***
https://orcid.org/0000-0002-3909-8805

DOI: https://doi.org/10.26512/lstr.v15i2.44709

Abstract

[Purpose] To explain why the tourism sector is so relevant for European economies (specially in Spain), but there are many failures and paradoxes in its public management during the digital transition (from Welfare State Economy to Wellbeing Economics), with more troubles because the COVID-19 crisis and the Ukraine war.

[Methodology/Approach/Design] This is a heterodox review on Political Economy, Macroeconomics, Labor Economics and Business Management, focused on the readjustment effect into the tourism industry due to the impact of the digital transition and its aggravation with the COVID-19 crisis and the Ukraine war. The objective of this review is to try to explain the current situation (not to predict anything), so it is applied the theoretical and methodological frameworks of the heterodox synthesis, mixing the genetic-causal approach by Austrian Economics with the historical-comparative approach by New-Institutional Economics.

[Findings] This review explains the failures and paradoxes in the public management of the tourism sector transition because there is a resistance to change, and there is not an adaptation in the production process and its economic structure. In an overview, the resistance is observed in the switch of economic model (from Welfare State Economy to Wellbeing Economics) and labor relations (from repetitive-technicians directed to talent collaborators with autonomy). Focused in the tourism industry, the digital transition can help to offer better travel experiences.

[Practical Implications] The readjustment effect can help to improve the European economies, specially for the Spanish case, where the tourism industry is the main sector

*Acknowledgments to the research group GESCE-Universidad Rey Juan Carlos (URJC) & INES-Universidad Internacional de la Rioja (UNIR).
**Assoc. Prof. Applied Economics at Universidad Rey Juan Carlos (URJC), researcher at INES-UNIR & PhDc. in Economics & Business at Univ. Málaga, Spain. E-mail: antonio.sbayon@urjc.es.
***Luis M. Cerdá Suárez, PhD in Finance. Prof. Marketing and director of academic programs at Universidad Internacional de la Rioja-UNIR. Research Group Fellow at INES-UNIR. E-mail: luis.cerda@unir.net.

of its economy. With this proposal is possible to take the digital advantage and its changes to become more productive and profitable, with greater wellbeing level for workers and society.
[Originality] This review introduces the heterodox synthesis, moving from econometric foundations (based on statistical approach to get predictions and equilibrium point), to mainline foundations (based on principles and empirical evidence on incentives, efficiency and institutional-quality).

Keywords: Digital Transition. Sustainability. Readjustment Effect. Tourism Industry. European Union. New Political Economy.

INTRODUCTION

This review is different, in relation with the economic mainstream papers, which seek statistical support and equilibrium modeling; this is a critical review, based on the recognition of the change process and its real adaptation, as proposed from heterodox approaches (Sánchez-Bayón, 2022), like Austrian Economics-EAE (Huerta de Soto, 2000 and 2009), New-Institutionalism-NEI (i.e. Law & Economics, Public Choice, Constitutional Economics, Posner, 1973; Buchanan y Tullock, 1962; Anderson, 1986) or Cultural Economics (i.e. Evolutionary Economics, Behavioral Economics, Diamond et al, 2012; Thaler, 2016). It turns out that the ongoing socio-economic transformations in the underlying reality are becoming more frequent, deep, rapid and interconnected (Valero et al, 2018). For this study, the accelerants of change have been the globalization and the digitalization: they have stimulated the transit between worlds, eras and technological revolutions, with new scenarios and rules of the game (see figure 0 & 3). Therefore, a review of the present reality and available knowledge is urgent (Sánchez-Bayón, 2020a and 2021). Our review will also cover the approaches of Economics and its relationship with other related social sciences (Law, Politics and Sociology, above all, as has been carried out since EAE and the neo-institutionalism of the *New Political Economy*-NEP, Sánchez-Bayón et al, 2022).

Economic System: from industrial and developed capitalism (of material acquisition), to capitalism of talent (of immaterial enjoyment);
Economic Model: from welfare state economy-WSE or state welfare economy (articulated from top to bottom, interventionist, bureaucratic and rigid), to *wellbeing economics*-WBE or personal welfare state economy-WSE or welfare economics (from bottom to top and entrepreneurial, creative and flexible);
Economic Activity: from one mean-oriented and focused on the increase in incomes, (e.g. increase in GDP, and fragmented in stagnant sectors), to another

focused in outcomes (concentrated in satisfaction, e.g. happiness management, and interconnected via dynamic networks)
Business Culture Shift: from rigid, centralized and hierarchical corporations, results-oriented and attentive only to hygienic measures, towards more agile and holacratic companies, promoting sustainable 5P (profit-planet-people-peace-partnership) and motivational relationships (seeking greater satisfaction and wellbeing)
Labor Relations Transformation: from the utilitarianism and mechanisms of human resources (given the massification and replication of workers required by the first phases of industrial capitalism), to the entrepreneurial dynamism of talent management (differential assets of capitalism based in talent)

Table 1 – Change Levels and recognition (Hermeneutic Turn and Copernican Revolution)[1]. Source: Own Elaboration

A closer attention to the transformation levels (with their awareness and hermeneutic turn), it lets to study the evolution of labor and business relations in the digital economy, as well as the model of *wellbeing economics*-WBE (see figure 1). This study seeks to refute the postulates contrary to technological progress, since digital transformation does not destroy so much employment as it was initially forecasted. On the contrary, employment adapts, evolves and gives rise to new expressions and work opportunities, according to the Ricardo effect, also called readjustment effect (reviewed by García-Vaquero et al., 2021; Sánchez-Bayón, 2021; Sánchez-Bayón el al., 2021). Through digital transformation, new opportunities emerge to change both structure and production processes: from rigid and unproductive companies -with high volume of unskilled and duplicated workers - to more flexible companies that required diverse and talented collaborators (profiles demanded for the tourism sector in the digital economy). As a result, the economic-cyber paradox takes place: the more the technology increases, the more human become labor relations, under the condition that the principles of WBE are also observed. Nonetheless, our proposal of review seems to pose another paradox when applied to the European tourism sector, especially to the Spanish one (see section 4).

[1] The hermeneutic turn makes reference to the change of approach (from the macro econometric to the micro and socio-economic) reconnecting the economy with the rest of the social sciences (Sánchez-Bayón, 2020a & 2022). That can be seen in the Copernican shift in the Nobel Prizes in Economics (i.e. Hayek and the EAE return; Simons, Kahneman, Thaler or Diamond and Behavioral Economics advances; Stigler, Becker, Buchanan, Coase or Ostrom and Williamson in the NEP & new-institutionalism revival; Fogel and North with Cliometrics and also neo-institutionalism (Sánchez-Bayón, 2020a & 2021).

REVIEW OF THEORETICAL AND METHODOLOGICAL FRAMEWORKS

This study is part of a socio-economic research program (Lakatos, 1978) on the impact of digital transformation on labor and business relations (Sánchez-Bayón, 2020b & 2021), applying to the reconversion of the tourism sector of the European Union-EU (Arnedo et al, 2021. González et al, 2021). In this case, attention is paid to the paradox of tourism in the EU and, in particular, to the Spanish case, due to the lack of the readjustment effect, and given the vulnerabilities of its Small & Medium Enterprises-SMEs and entrepreneurs after the last crises (from the 2008 Recession to COVID-19 pandemic), which contribute to discredit former *mainstream* approaches (Levy et al, 2022; Bagus et al, 2021 & 2022; Huerta de Soto et al, 2021)[2]. In order to achieve the objectives of our proposed review, there is a mix of EAE (analytical-deductive, subjectivist and individualist) and the New-Institutionalism of NEP (empirical-inductive and institutional-quality analysis), because their theoretical and methodological frameworks help to recognize the changes in the social reality.

It is worth remembering something fundamental in economic science (Boettke et al, 2016): there are several schools, classified between mainstream or dominant (orthodoxy) and heterodox (complementary and with possibilities to become also mainstream, see figure 1). Thus, it is possible to understand the succession of theoretical and methodological frameworks in economic research, according to their ability to formulate functional and widely accepted paradigms. In this regard, the problem lies in the fact that the current mainstream -also called neoclassical synthesis- is a kind of hybridization, between the neoclassical schools of Lausanne and Cambridge, with fiscal interventionism (or Keynes way) and monetarist (or Friedman way), seeking a pretended *positive economy*, following Chicago School (neoliberals or *Chicago boys*), and also excessively econometric that has ended in regulations, following

[2] Those crises have also had second-round effects , growing over time and extending to other areas and giving way to other EU crises: bankruptcies and bailouts of European states (i.e. Greece up to three times, requiring help of the International Monetary Fund-IMF); the relocation of Syrian refugees and illegal immigration from the South, which compensates the demographic crisis related to the aging of the European population and the entrepreneurial deficit (Navajas et al, 2013 and 2014); the excruciating *Brexit* negotiations (dragging on for several years) and the internal fragmentation into blocks with divergent strategic visions on the future of the EU. Consequently, the EU is in the process of reviewing its project (VV.AA., 2010) and its narrative (Del Valle, 2013. Moreno, 2013), under institutional review since 2017 (Le Gales & King, 2017), with Junker Commission and the white-book on *the future of the EU* (European Commission, 2017).

New-Keynesian School (*MIT boys*), with expansive public spending and correction of market failures. In this sense, an attempt has been made to transmute economics from social science into natural science and engineering, via econometrics followed up to present days with the natural experiments (Card & Kruger, 1995 – with origin in Friedman & Schwartz, 1963). In this sense, we can speak of the error of Friedman (1953), given his preference for models more predictive than realistic, in addition to the error of excessive mathematization or *mathiness* (Romer, 2015). In turn, this error is heir from others, such as the error of Walras (1883), when trying to equate economics and physics, with its mathematical models of equilibrium. Additionally, Walras´error started from another previous misconception: the *methodenstreit* or methodological dispute between EAE and its principles (Menger, 1871 & 1883) and the Institutional Approach-EI or German Historicist School (Schmoller, 1900). To overcome all these mistakes and build bridges between the different schools and returning to economic fundamentals, it is convenient to go back to the second generation of EAE (Menger's doctoral students): Böhm-Bawerk, Wieser and Fetter. All of them reconnected EAE and EI, providing socio-cultural keys to the economy. The work of Fetter was especially important (Rothbard, 1977; Kirzner, 1987). It extended EAE in the United States of America, in universities such as Indiana, Cornell or Princeton, and collaborating with Veblen and Davenport (representatives of EI in the USA). This movement gave rise to American Psychological School, overcoming the EAE-EI tensions. This connection has been re-edited later by the neo-institutionalists of NEP, comprising: Law & Economics or economic analysis of law (Coase, 1937 and 1960; Posner, 1973 and 1979); Public choice (Buchanan & Tullock, 1962); Constitutional Economics (Brennan & Buchanan, 1985. Buchanan, 1986, 1987 and 1990); Possibilism (Hirschman, 1970 and 1993), etc.

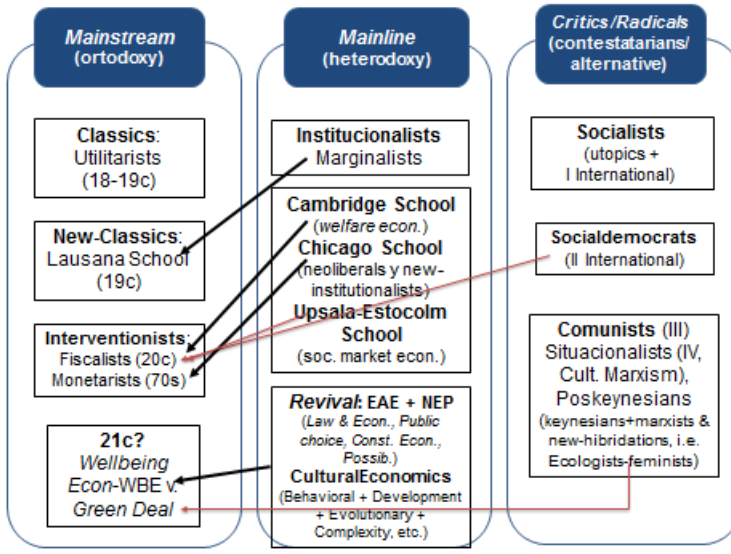


Figure 1 – Relations among Economic Mainstream-Mainline-Critics.
Source: Own Elaboration.

This review has combined compatible heterodox contributions (EAE and NEP), applied to the development of WSE models in the EU and their common targeted policies (including tourism since 2009, European Parliament, 2022). This management is carried out by the EU institutions according to strategic agendas and in financial and multi-year timeframes. This was Monnet's initial project for the European Communities and later recovered by Delors since 1988 (see Figure 2). This strategy of directed and planned development of the EU does not arouse great criticism from mainstream approaches (especially the dominant neo-Keynesian in the Public Economy). In order to have another perspective that allows us to detect problems and solving them, this revision has resorted to Mises's theorem on the impossibility of socialism (Mises, 1922, 1929, 1933 and 1944), revised by Hayek (1944 and 1988, beyond the economic and the political), then extended to any type of centralized coercive interventionism and repressor of freedom, according to Hoppe (1989) and Huerta de Soto (1992). Mises's theorem has the corollary of the Buchanan-Tullock theorems on public choice , affirming the end of political romanticism and the concept of paternalistic public sector, because there are many power games in collective decisions, with collateral effects such as *rent-seeking, clientelism, crony capitalism, unfinished and inclusive agendas, logrolling, pork barrel, omnibus laws,* etc., as well as the problem of the endless agenda (Buchanan & Tullock, 1962). Another key idea to consider is Hayek's thesis on

spontaneous order (developing Smith's invisible hand, 1776), in favor of evolutionary social institutions (Hayek, 1946 and 1952a-b) – ergo not designed, as neo-Keynesians defend. This thesis is complemented with the Mises-Huerta de Soto theorem on dynamic efficiency (Mises, 1949; Huerta de Soto, 2009). In methodological terms, EAE offers various resources since its inception, with its *methodenstreit* ,or dispute over the method (Menger, 1871 and 1883; Mises, 1929 and 1933; Huerta de Soto, 1992 and 2007. Hoppe, 1995). This revision extends to other complementary contributions, such as the case studies of Grice-Hutchinson (1976) and the modeling of Machlup (1954) and Garrison (2001).

EU Macroeconomics & Multiannual Financial Framework – MFF

- *1st Financial Framework (1988-1992, Delors Agreement I):* Prioritizes Internal Market and R+D+I.
- *2nd Financial Framework (1993-1999, Delors Agreement II):* Prioritizes Social Politics, Cohesion and Introduction to Euro.
- *3rd Financial Framework (2000-2006, Agenda 2000):* Focus on Expansion and Integration.
- *4th Financial Framework (2007-2013, Digitalization & Entrepreneurship):* Focus on Sustainable Growth and Competitiveness (Employment Promotion).
- *5th Financial Framework (2014-2020, Single Market Re-Enforced):* Focus on Future of EU + Digital and Wellbeing Economics.
- *6th Financial Framework (2021-2027):* Green Deal (UK New Green Deal/Rifkin) and Next Generation.

[*] *Objections: a) Mises´ Theorem (Impossibility of Interventionism) and Buchanan-Tullock´S Theorems (Unfinished Agenda et al.). Narrative and Strategic Agenda (G7: Climate Change, WEF: Global Reset and H2030+H2050)*

Table 2 – Evolution of the EU's Strategic Agenda in Multiannual Financial Periods.
Source: Own Elaboration

Coming back the preliminary question of this review: changes and adaptation to them, attention is drawn to the mainstream, based on theories of resistance to change, such as new-Luddism and technological unemployment (Keynes, 1930 and 1937, already criticized by Hazlitt, 1946), plus the great decoupling and the digital paradox of employment (Brynjolfsson & McAfee, 2014). It is possible to clarify the phenomenon of resistance to change and the cost of learning (information and communication technologies-ICT and learning

and knowledge technologies-LKT), which hinders the transition that we want to study. This resistance is due to the high cost of learning to adapt to changes, as well as the fear of the loss of the benefits identified in the current model. However, changes have taken place and continue to occur, and the longer it takes to adapt the more costly the process will be, due to its greater discontinuity in time.

Among the multiple dimensions of the WBE model of digital economy (enabler of the transition to talent capitalism), we address the transformation of labor and labor relations, with new dynamic concepts such as *emprosumer* -*entrepreneur+productor+consumer*- and *knowmands* –knowledge+nomads- (Sánchez-Bayón, 2020a-b & 2021b; Sánchez-Bayón & Trincado, 2020). In particular, attention is paid to the digitalization-work relationship, which is clarified through the readjustment effect and other complementary resources (see above).

The research question is: do the various waves of digital transition mean job destruction and technological unemployment in WSE or -on the contrary- do they serve as a stimulus for techno digital intensification and talent development that allows transitioning towards talent capitalism? We can anticipate that, according to the data of international organizations and forums, both scenarios coexist. On one hand, traditional jobs of low qualification and remuneration are obsolete while others of high qualification and better working and professional conditions are created. The question is to recognize that the digital transformation of the economy goes through labor re designing, which in turn requires deep educational transformations (upskilling ad re-skilling). Quite possibly, this is the key factor that explains the paradox of the Spanish tourism sector (see above).

PARADIGMATIC CHANGE AND READJUSTMENT EFFECT

The combination of globalization and digitalization has generated profound socio-economic changes (Brynjolfsson & McAfee, 2014. Sánchez-Bayón, 2021. Suresh, 2010), which is part of the broader development of capitalism and its changes, which affects labor and professional relations, following the subsequent industrial, technological and energy revolutions (see figure 3). Among the most relevant changes that we should mention:

(1) Eras: from an agonizing, rigid and protected by the nation-state (including the economic sphere), to an emerging, flexible and coordinated by international organizations and forums;
(2) Worlds: both latitudes (with their geographies and cultures), moving from the Atlantic area (as the epicenter of soft-power or

white/economic power) to the trans-Pacific area (which includes the American Pacific coast, Oceania and Southeast Asia), where more income is being generated at the moment; as well as means of interaction, from the physical to the virtual world;

(3) Technological revolutions: we are moving from the 4th industrial and technological revolution (based on mobile and exponential technology) to the 5th, based in the singularity (Kurzwell, 2005), starting from Horizon 2030 (UN-GA, 2015. EU-Horizon Europe, 2021) and where WBE that is, the economy of personal wellbeing (which is also psychosocial and environmental), has been implemented (Sánchez-Bayón et al, 2021).

(4) Wealth: it is moving from predominance of material goods (the age of the production and acquisition of goods) to its immaterial tendency (the era of satisfaction/happiness and access to experiences, thanks to knowledge and talent); etc.

1st Revolution or Mechanization (Circa 1750-1870, in Atlantic Europe): energy via coal and steam engine; communication via telegraph and telephone (local); transport via train and steamboat; it goes from rural countryside to urban workshops (being textile industry one the most relevant reference), with civil contracts of services (by days and agreed benefits). Combination: Slows down the progress of guilds and similar institutions
2nd Revolution or Electrification (Circa 1880-1950, in Europe, USA and Japan): energy via oil and electricity; telephone communication (continental); transport by air; production via assembly line, it is passed from the workshops to the factories (one of its main sectors being the automobile), with working contracts (under labor regulations). Its evolution is altered throughout wars and state interventions, balancing between accelerations and recessions.
3rd Revolution or Computerization (Circa 1960-2000, in the West): nuclear energy; communication via mobile telephony and the internet; multiple transport and hubs; transformation caused by computer science and robotization. We move from factories to centralized techno-bureaucratic headquarters and delocalized production and sales modules, plus the emergence of malls or shopping centers, with a diversity of labor relations and employability (civil and commercial contracts, labor, civil servants, etc.). State interventions continue to alter its progress (it is the golden era of Welfare State Economy).
4th Revolution or Digitalization (Circa 2008-2030 – Post-Globalization - Global): mixed energies (including renewables); communication via multimedia applications; accelerated transport and relocation; prevalence of programming (especially, Blockchain since 2009, thanks to Satoshi Nakamoto -actually an alias of collaborative intelligence-) and mobile (as an integrated office). It is the era of social networks, apps & everywhere commerce-ewc, emerging of the *emprosumer* (see above), plus the arrival of top professionals (knowmads vs freeriders, see *above*), who can be commission agents, freelancers, affiliates, etc.

New modalities of labor relations arise, i.e. click-pay, flexicurity or part-time jobs mix). It is also the period of the emergence of the smart-contracts & DAO (smart contracts, such as cloud codes, whose parts are artificial intelligences, operating from the stock market to driverless driving). In this way, not only is the ED in its gig or *bowling* phase, but also a new stage of capitalism emerged. It is the era of talent, supported by the concept of happiness management.
5th Revolution or Connectivity (From 2030): total connectivity and interoperability (combined energy, communications, and transportation) are possible thanks to the implementation of 5G and the arriving of uniqueness (with the superiority of AI processing)

Table 3 – Revolutions of Industry, Technology & Energy with an Impact on Labor Relations. Source: Own Elaboration.

All this has changed the rules of the game (UN, 2012. OECD, 2012): from the type of economic agents and their role in the economy (emerging new and dynamic combinations, since there are no longer rigid and immutable separations, i.e. *emprosumer*), through the renewal of economic activities and sectors (i.e. consumer-to-consumer relations through social networks), where the physical world coexists with the virtual one, operating in a *glocal* way (global+local); up to the rules of distribution and the financial instruments (i.e. digital currencies). Already Robinson (1962), advanced the change of values (Suresh, 2010. Valero et al, 2018); Galbraith (1958) and Keynes (1936) even warned of the difficulty of changing values due to the burden of previous thinkers and their economic postulates.

Consequently, a paradigmatic review is urgently needed to appraise the economy as a whole and, above all, its growth and development model (UN-SG, 2012. UN-SNDP, 2013. UN-UNDP, 2013. UN-GA, 2015. OECD, 2019. EU-Consillium, 2019; plus Florida, 2010. Sánchez-Bayón, 2016. Valero et al, 2018. Llena-Nozal et al, 2019. Schwab & Malleret, 2019). This revision has intensified since the Great Recession of 2008, and has achieved a change of system from industrial and developed capitalism towards capitalism of talent, with new emerging labor relations (i.e. knowmads, riders, and other working modalities of the so-called *gig* economy). Not pursuing the paradigmatic transition -due to resistance to change- implies a growing gap between the available academic knowledge and the progress of the underlying reality, with the initiatives of international organizations and forums, plus the professional and business practices in progress. However, given the excessive scope of a thorough paradigmatic review, this study and its thesis starts from such a context to focus on the WBE model (as the next stage of ED, Garcia-Vaquero et al, 2021. Sánchez-Bayón et al, 2021), analyzing how the digital transition has affected the development of labor relations. Thus, the stance of resistance to

change based on the risk of technological unemployment (Keynes, 1933, 1936 and 1937) and traditional labor protectionism (Keynes, 1930) is refuted. It turns out that, in the digital transition, it is not a matter of the competition of man against the machine (Luddites and socialists of the First International), or even a question of humans following the pace with technology (Keynesians and socialists of the Second International). It will be sufficient that human labor will adapt to technological changes. The explanation is simple: for each position destroyed by the technological growth, and thanks to those technological advancements, at least 4 types of related positions are generated: the designer, the manufacturer, the user and the reviewer or maintainer.

Some authors such as Gómez (2019) consider that there will be no work scarcity in capital-intensive countries. Greater preparation will be necessary, hence the importance of education, for technical specialization and related talent development. This argument is supported by the Big-Tech companies that fail to fill up many of the positions they offer. This was also recently measured in a study by Oxford Economics and SAP with their 2020 workforce, a survey of almost 5,500 employees and executives in 27 countries.

As for the figure, we want to highlight that, right before COVID-19, there have never been so many people working in the US (and almost all over the Western World). The most digitized countries with the highest robotic density had had lower unemployment rates. Moreover, they did not fill the new digital vacancies due to lack of talent; hence, the transition from trade wars to talent wars has not been achieved. The social employment contract had to be revised, since the life expectancy of the companies had fallen to 15 years, so they cannot offer contracts for the entire working career of a person -being 30 years or even more with the ageing of the world population. Between the COVID-19 crisis and the war in Ukraine, the trend has recovered, accentuating the differences between the digitized countries and those that are not, drawing a K-shaped recovery model: In the ascending vector the digitized and observers of WBE, while in the descending one there are less digitized and obstinate in *Welfare State Economy*-WSE or *Economics of Welfare* (Pigou, 1920).

Faced with future crises, such as possible job destruction and mass unemployment, empirical evidence seems to indicate that a transformation similar to that of past transitions is actually taking place. An example is the one that occurred in the 1880s, with the shift from commercial to industrial capitalism, making disappear half of the jobs in the primary sector, but generating more than double in industry and services. In this sense, it is proposed as a complementary objective the exposition and explanation of the revised Ricardo effect -or readjustment-, which is raised here (in addition to enunciating paradoxes such as economic-cybernetic or happiness, to be

developed in other works) to facilitate in the end an overview of the theory of capital, economic cycles, the structure of production, and the evolution of social institutions (Menger, 1871; Hayek, 1952).

The following is a synthesis of approaches to the Ricardo effect or readjustment: its name, Ricardo effect, according to EAE[3], was defined by Hayek (1935 and 1939) in honor of the classical economist D. Ricardo -already mentioned- and his proposal about savings-wage relations (Ricardo, 1817). This refers to the microeconomic rationale according to which variations in savings have an impact on the level of real wages[4]. Hayek assessed its consequences, such as the possible replacement by capital goods, if wages rose above market productivity, causing a necessary readjustment of the labor factor. From there, he then connected this effect with the theory of capital and business cycles, observing that the same thing happened if there was a credit expansion (even without savings, but inflationary). Thus, using his triangle of the productive process (see figures 4), Hayek incorporated the Ricardo effect, to explain the distortions in the process and the productive structure, due to wage variations, especially those not based on the increase in productivity but by the effect of savings and investments, and the worst, by credit expansions without support in savings (then with distortion in prices and therefore in economic activity). This proposal was debated by Wilson (1940), Kaldor (1942) and many others. It was called the Ricardo or concertina effect controversy (Moss & Vaughn, 1986). Steele, 1988). Later, other EAE authors have developed the concept (Birner, 1999. Garrison, 2001. Gerhke, 2003. Huerta de Soto, 2006 and 2009.

[3] This point is key and moves away from a still persistent assumption by part of the academy (e.g. Ricardians, Marxists, some Keynesians): to offer a theory of distribution (e.g. wages), one must start before a theory of value, and here follows the one already announced by the marginalist revolution of the 1870s (from Jevons for the Cambridge School, or Walras for the Lausanne School, and Menger for EAE). EAE's approaches are of a subjective value theory. In ED there is a revival of marginalism. Thus, the great convenience of starting from EAE is clear

[4] The Ricardo effect is usually understood as the increase in wages over investment in capital. As wages grow, labor is replaced by capital, so the productivity of labor grows, and with it higher wages can be paid, while the period of production is extended (the economy is capitalized, in addition to increasing the phases of the productive structure and the terms of profitability of investments). This may cause some technological unemployment in the short term (as the Keynesians argue. Keynes, 1930, 1933, 1936 and 1937); however, as other authors of the business cycle have already advanced, it could be corrected in the medium and long term (Kuznets, 1930, 1933a-b and 1934), suffice with a readjustment in the productive process and structure (Hayek, 1935 and 1939). Thus, it is the investment in capital that grows (if saving equals investment, then savings will grow), 1939). Thus, it is the investment in capital that grows (if saving equals investment, then savings will grow), but there can also be an alternative and/or complementary reading, as offered here.

Klausinger, 2012. Ruys, 2017). Synthesizing these revisions and in a reformulation for ED, it would be possible to explain the Ricardo effect as a readjustment of the production process, with the use of relocation[5] for the development of talent, in accordance with the principles of WBE (García-Vaquero et al., 2021; Sánchez-Bayón et al, 2021): when wages are artificially raised in the phases closest to consumption (above all, by credit expansion and inflation), this will cause the replacement of workers (employees) by capital goods, freeing up the labor factor, which will be relocated to phases of production further away (even new ones), being able to provide more value, thanks to the development of talent, and therefore, earning more salary and better working conditions, in addition to achieving greater satisfaction (i.e. better schedule, more creative work, etc.), in line with WBE. To illustrate how the production process and structure is understood from EAE, several representations are given in the following figures[6]:

[5] On the contrary of other mainstream economists (tax interventionists or monetarists), relocation is not used because it is not a magical or instantaneous process. It has been preached, for example, of the positive effects as a result of layoffs associated to the raising of the minimum inter-professional wage or MIW (Sánchez-Bayón, 2021c), since workers are only relocated to other phases of production when they are able to discover and exploit their talent, which in turn requires technical training or digital specialization.

[6] In summary, regarding the figures related to the Hayekian triangle, it is enough to emphasize that Hayek considered the production process and its structure in the form of a triangle, whose base corresponded to the production time and its phases, while the inclination corresponded to the interest rate (increasing according to the phases). The representation of the triangle has been varying its orientation (by Ruys and Huerta de Soto, in an inversion of Garrison´s proposal, see figure 4). The fact is that if any of these phases is distorted, the whole productive structure is affected. Then, the issuance of new money without the backing of savings, will send erroneous signals to investors, who believe that there will be future consumption and assume the risk of investing in more distant phases (since it accumulates more returns throughout its various phases). The problem is that signals will be incorrect: by distorting prices economic bubbles will be generated that later will cause a destruction of wealth. Thanks to the triangle it is also possible to observe why in the closest phase to consumption is more difficult to add value. When prices are raised artificially (i.e. legal increase in the IMW), then it will be preferred to replace the low-skilled worker with machines or AI. The key is to help relocate those workers, in addition to facilitating their transformation, discovering their talents and developing their technical skills, thus, becoming talented collaborators in phases further away from consumption, which being more capital-intensive, will allow them to be more productive and with greater labor well-being (that is, the Ricardo effect or readjustment).

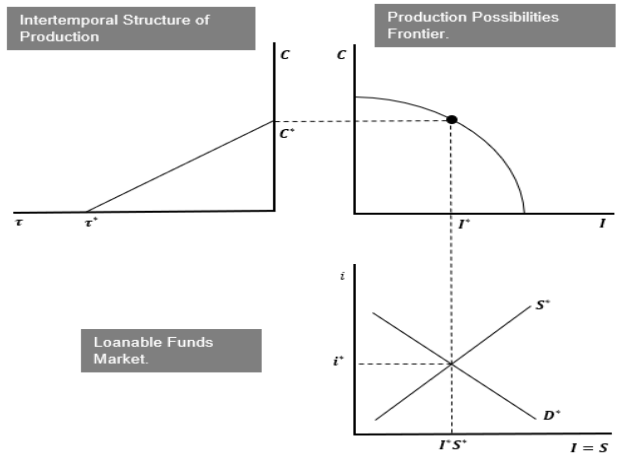


Figure 2 – Ricardo Effect Inter-Temporally in Economics (Hayekian Triangle+ Frontier of Possibility of Production+IS-LM).
Source: Garrison, 2001.

Below is a simplified version of its formulation and graph.

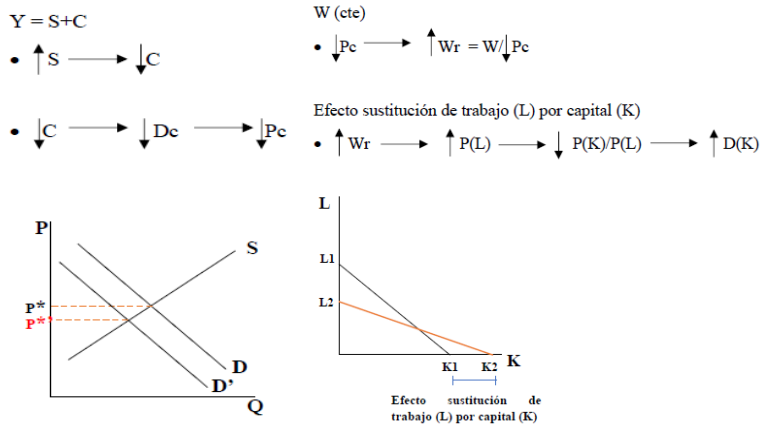


Figure 3 – Formulation & Its Graphical Representation of the Ricardo Effect (Readjustment)[7].

[7] Basically, the rule is that if savings increase consumption and with it prices fall, so that the real wage increases (having greater purchasing power). Now, if there are no savings but artificial credit expansion; then, in addition to distorting the interest rate (which will fall), a wrong signal will also be sent to investors, who will think that it is time to replace the worker with capital goods. That is why it seems that the base of the triangle is lengthened, pretending to increase the productive structure, but this is not the case, because there is no real demand behind it. It will then be understood that it is urgent to

Source: Own Elaboration

The novelty of this study is not so much in the synthesis offered, as well as in its formulation and graphic representation, but in the proposal of new definition, going from Ricardo -or concertina effect-[8] to readjustment effect, which is not mere relocation -as has already been clarified. This is justified for several reasons, mostly to avoid confusion, or encourage false polemics:

(1) Any allusion to Ricardo leads to an objective theory of value, not compatible with EAE, which defends subjective value -according to its marginal revolution, today revitalized with ED. On the other hand, it is part of the boy of knowledge of socialist economics (Marx considers Ricardo as one of his referents, Marx, 1867);
(2) Ricardo's approaches are utilitarian, not being compatible with the postulates of WBE: wellbeing must be authentic and personal, making the economy more human and less instrumental.
(3) Ricardo writes thinking about the capitalism of his time (during the transition from commercial to industrial capitalism), so he gives priority to the land factor and considers the labor factor accordingly, ergo, intensive, unskilled, mechanistic, and linked subordinate labor, which leads to a reasoning of diminishing returns. Such an statement, again, has nothing to do with talent capitalism or the WBE model (by relying on creativity, entrepreneurship, talent, etc., giving rise to a dynamic and open processes). It also coincides that there is another Ricardo effect, also called Ricardo-Barro equivalence (on savings and taxation), hence a new description of readjustment effect is proposed:
    a. By the relocation of unskilled workers close to consumption, with a minimum wage -given their low value contribution and reduced productivity-, being released and transferred to levels and phases further away in the productive structure after technical training and talent development, where talented collaborators are required, with better remuneration, since they

deal with the Ricardo effect or readjustment, to understand how to take advantage of the current situation of the digital transition to improve the production process and its structure, in addition to facilitating the transition in labor relations according to WBE.

[8] Concertina effect was the one that was reviewed by his critics, especially Kaldor (1942). He had a very limited vision, because the economy is not an accordion in the hands of the public sector that can stretch and shrink, since production processes can also be lengthened, fattened and create new ones (as well as the opposite), according to the needs and demands of the market (provided that the public sector does not distort prices, especially the interest rate).

add value and are more productive, in addition to enjoying greater well-being in schedules, tasks, organizational health, etc.

b. By the reorganization of the production process, purging the bad investments, which will also release factors of production, thus being able to reach the most appropriate phases (where talented collaborators are demanded);

c. By economic restructuring, thus improving the level of wealth and development, with greater human and environmental wellbeing , with an increase in creative and motivating tasks, as well as less polluting jobs).

In short, Hayek was very generous with Ricardo, when trying to update his approach; however, the Ricardian theory is intended for a commercial capitalism, not even industrial, which will arrive from the 1880s, with the 2nd industrial and technological revolution, and it is based on an objective value theory (surpassed with the marginalist revolution of Jevons-Walras-Menger), which considered costs as a determinant in price fixing and therefore wages. Such an approach is not valid in ED and, even less, in WBE and talent capitalism, which is about to come with the 5th. industrial and technological revolution planned for H2030, with the singularity and the latest wave of the digital transition.

In this research, and beyond the present study that will be developed in a more extensive program in which the hypotheses and theses previously mentioned are found, we propose to connect the readjustment effect with other economic principles and propositions, such as the Brunel effect and the Hicks compensation variation among others. Nonetheless, in order to make this combination to work, it is essential that the Public Sector will not interfere, except to facilitate the educational conditions of technical transformation, thus avoiding a distortion, especially by fiscal measures such as tax increases, even forcing robots to pay taxes and with greater public spending, ergo, more deficit and indebtedness. Those measures would cause effects such as the aforementioned Ricardo-Barro equivalence, the crowding-out effect, etc.

With regard to the resulting paradoxes (with the application of the readjustment effect), there are several, but three are addressed here:

(1) Economic-Cybernetic Paradox: it consists in that the more technology increases, the more human the economy is, since the human being is freed to perform tasks of his own nature, being able to be more creative and social. That is, developing the orange economy and the entire industry of emotions. An example of this paradox is provided by the

case of Israel, which after making the desert productive, intensified in technology, becoming a start-up nation or entrepreneurial country, with such an increase in wealth, that a set of transfers could be tested (as a kind of universal income), favoring the *haredíes* (Orthodox Jews), who dedicated themselves to the study of the Torah, in addition to reproducing and reaching today the status of majority- minority of the country and whose vote is key to the economic policies to be developed. Obviously, the generation of so much wealth (also called abundance of ED is only feasible. if technology is not taxed -as has been warned- (Diamandis & Kotler, 2014. Fernández, 2015). Otherwise the digital transformation would be stopped; transferring the new wealth to the State and leaving the private sector without incentives, so that any possible progress would be slowed down (remember the Brunel effect and the variation of Hicks compensation).

(2) Paradox of Happiness (Easterlin, 1974 and 2010): during the stagflation of the 70s, R. Easterlin researched the evolution of the income level of Americans, and whether this increased their level of perceived subjective well-being or happiness. He found that, once a satisfactory standard of living was reached, with all basic needs met, the level of well-being did not change, at least, not in the material aspects (welfare), but attention was required to the intangible aspects (wellbeing). Thus, a new field of study has emerged from the economics of happiness, based on the international indexes that have been developed, (e.g. OECD, UN, WEF). Attention has been paid to the level of human development (education, health, hope and quality of life, leisure, etc.). Even studies have been carried out recommending the change of public policies in this regard – and as it has been postulated by WEAII: we must stop paying attention to production and the increase in incomes (and promoting less concentration to macro data such as GDP) to concentrate into the quality of life of citizens in relation to their social environment (as intended with the European Green Deal, García-Vaquero et al, 2021; Trincado et al, 2020 & 2021).

(3) Jevons Paradox: marginalist author from which it takes its name. This author from the end of. 19th century enunciated this paradox. According to that theory, the search for greater energy efficiency would lead to a greater consumption. As far as WBE is concerned, one of the components that is still scarce is precisely the energy. However, as soon as digitalization will achieves it, not only zero marginal cost will also be reach but also a higher quality of life, with greater respect for the social and natural environment (observing 5P relationships). Instead, the official EU narrative on Green Deal (European Commission, 2019; European Parliament, 2022; Trincado et al, 2021) and given the EU energy transition plan with the primacy of renewables in detriment of others, it is causing a problem of scarcity and a subsequent rising in prices (with inflationary effects worsened by war in Ukraine, due to European dependence from Russian energy).

All this is applicable to the tourism sector, as long as it ceases to be produced according to the parameters of industrial capitalism and its WSE. Massive, standardized and intensive services are not required in low or medium skilled jobs which the most common in tourism industry. Facing the relevance of digital transition, tourism industry has to move towards the orange economy of the emotion industry, with higher focus in tailor-made /personalized experiences (García et al, 2021).

EUROPEAN TOURISM SECTOR PARADOX: SPANISH CASE

As it has already been mentioned, the paradox of the tourism sector within the EU: despite its importance (for its contribution to GDP and employment, assuming more than 10%, TRAN Commission, 2019; European Parliament, 2022), and despite being considered a common policy objective, European tourism industry does not yet have its own budget line (European Parliament, 2022). Additionally, recognition about its relevance in European economies has been late and incomplete (since 2009, after legal framework of the Treaty of Lisbon). Furthermore, when tourism has begun to be considered as a theme on the strategic agenda for EU's multiannual financial periods, its results have been worse. Is it due to the second-round effects of the COVID-19 and war crises in Ukraine? This could not be sustained, since other non-EU countries, such as Iceland and Norway have increased their results in tourism. Within the EU it is worth mentioning Ireland and Estonia. What all of them have in common is their success on the digital transition and observation of the WBE model. In the case of Spain, the paradox is more intense: until 2018, tourism generated 147,946 million euros, representing 12.3% of Spanish GDP, in addition to 2.62 million jobs, representing 12.7% of total employment (INE, 2019). Nowadays, and despite being a priority target for the reception of Next Gen funds, Spanish tourism only generated 61,406 million euros, or 5.5% of GDP, and only 2.2 million jobs have been maintained and thanks to wide furlough agreements, being more serious the situation of the self-employed that could not apply for any kind of subvention (INE, 2022).

At first, tourism in the EU began to be supported by the European Regional Development Fund (European Commission, 2014) to support the competitiveness, sustainability, and quality of the sector at regional and local level. However, given the EU's negative experience with the Common Agricultural Policy-CAP in the World Trade Organization-WTO and the penalties fees charged for bad practices such as subsidizing European farmers, thereby generating greater barriers for entry to producers in developing countries. Later, European Green Deal was used to fragment and rename

objectives using an ecological approach to diversify the allocated funds (Trincado et al, 2021), thus, avoiding penalty fees or criticism by international public opinion. In this way, the design of the Next Gen funds is understood: they were planned for the recovery of the sector more impacted by the confinement, as was the case of tourism, as international mobility was severely restricted. On the other hand, and in addition to digitalization, the requirement of conversion and increase of Green Jobs or green jobs was added (Arnedo et al, 2021; García-Vaquero et al, 2021). In this way, the conversion model initially planned for the energy sector has been extended to other sectors (García-Vaquero et al, 2021). Nevertheless, the expected results have not been achieved, at least in Spain, due to lack of transparency in the management of funds and the scarce digitalization, limited to the compatibility of teleworking and furloughs. The opportunity to undertake the readjustment has not been faced in crucial actions such as talent development, offering training in technical subjects, which would allow workers to looking for job opportunities in higher stages and with better working conditions. On the contrary, the concept of "social shield" (Government of Spain, 2021) has been coined, which actually meant keeping workers expecting to recover their old jobs, already out of date, due to lack of digitalization, instead of favoring a readjustment effect.

Back within the EU, despite the funds allocated for the recovery of the tourism sector, its recovery to pre-COVID-19 levels is not expected until 2023 (European Parliament, 2022). 30 million jobs were lost, half of which were recovered thanks to digitalization and hybrid systems (combination of face-to-face and virtual work). It turns out that the resolutions and communications of the European institutions during the COVID-19 crisis were mainly oriented to health to the detriment of the economy, so it has caused not only the aggravation of the effects of the pandemic but its condition of *syndemic* (Sánchez-Bayón et al, 2021b and 2022). Applying the theoretical framework of EAE and NEP, Mises's theorem and Buchanan-Tullock corollaries are confirmed: centralized management of the COVID-19 crisis by EU has been less efficient than the decentralized one, as has happened in Taiwan, Singapore, Australia, New Zealand, etc., according to ICT & LKT. The route of mass confinements and the bureaucratization of purchases of sanitary materials and vaccinations was not chosen in those countries where personalized digital response was preferred (thanks to tracking apps, preferential vaccinations, etc.).

In summary, in order to recover the pre-pandemic levels of EU tourism sector and even exceed them, it is fundamental to stop spending recovery funds just as mere subventions. It is more rational to design those funds as investments oriented to increase training in digital and technical skills and global talent management initiatives based in re-skilling and up-skilling in the tourism sector.

CONCLUSIONS

This study has sought to clarify the importance of change management, especially in the current era of volatility. This implies a paradigmatic revision, which in turn requires resorting to other visions, such as those offered by heterodox economic approaches and schools (which may become the mainstream future, if they prove their worth). For this review, the combination of contributions from EAE and the neo-institutionalists of NEP has been used. In this way, it has been possible to study the ED with its WBE model, without intending its reconversion to categories of WSE still supported by the neo-Keynesians. According to EAE, ED involves a change in the structure and production process, requiring a readjustment effect, so that the company culture and labor relations are efficiently redesigned. This implies facilitating that those rigid companies, with unskilled workers and monotonous jobs could be transformed into flexible companies with talented collaborators. Those are the profiles required for the future of tourism sector in the digital economy, since its workers and professionals must be able to offer better and more personalized experiences. The achievement of this readjustment not only consolidates the WBE model and the transition to talent capitalism, but also gives rise to the so-called economic-cybernetic paradox: the more technology increases, the more human the economy and labor relations are required, provided that the principles of WBE are followed.

In the digitalization-work relationship, the possible destruction of employment and digital unemployment will be compensated with the adaptation of jobs and the appearance of new ones: for each type of job that becomes obsolete and disappears, four new jobs are generated: the designer of the technology, manufacturers, users and technical supervisors. Certainly, to facilitate this transition, it is necessary to pay attention to the readjustment effect: unskilled, easily replicated and dependent workforce will be replaced by capital goods, being freed and urging a *geek* training or digital training of technological specialization, to discover their talent and apply them in ED. In this way, workers will be able to become talented collaborators, in higher phases further away from production level and in accordance with WBE, thus providing added value and in exchange receiving better salaries, working conditions and intangible assets. In short, they could be more productive, sustainable and with higher wellbeing.

In more specific terms, the necessary transformation of the European tourism sector and especially the Spanish case can lead us to conclude: central planning, via strategic agenda and in multiannual financial periods is not feasible, or the Mises' theorem and Buchanan-Tullock corollaries will be

fulfilled (as is already the case with the CAP and the agricultural sector). For the tourism sector recovery, being once again one of the engines of the European economy, there is an urgent need for a readjustment that would enable workers and professionals to offer better and more personalized experiences (as a comparative advantage over other lower-priced tourism proposals). It is no longer and only a question of quality but of continuous innovation. This requires *geeky* transformation and talent development (unlike the restrictions and dependencies of the Green Deal, according to the Mises and Buchanan-Tullock theorems). Achieving the readjustment effect is key to reactivating the tourism sector, in addition to influencing economic systems and their location in the K model of post-COVID-19 recovery.

REFERENCES

Anderson, M. (1986). *The Unfinished Agenda: Essays on the Political Economy of Government Policy in Honour of Arthur Seldon*. London: Institute of Economic Affairs.

Arnedo, E., Valero, J. & Sánchez-Bayón, A. (2021). Spanish tourist sector sustainability: Recovery plan, green jobs and wellbeing opportunity. *Sustainability*, 13(20), 11447.

Bagus, P., Peña-Ramos, J. & Sánchez-Bayón, A. (2022). Capitalism, COVID-19 and lockdowns. *Business Ethics, the Environment & Responsibility*-BEER, 31(SI), 1–11.

Bagus, P., Peña-Ramos, J. & Sánchez-Bayón, A. (2021). COVID-19 and the Political Economy of Mass Hysteria. *Int. J. Environ. Res. Public Health, 18,* 1376.

Birner J (1999). The Place of the Ricardo Effect in Hayek's Economic Research Programme. *Revue d'Économie Politique,* 109(6): 803–816

Boettke, P., Haeffele-Balch, S. & Storr, V. (2016). *Mainline Economics: Six Nobel Lectures in the Tradition of Adam Smith*. Arlington: Mercatus Center-George Mason University.

Brynjolfsson, E. & McAfee, A. (2014). *The second machine age: work, progress, and prosperity in a time of brilliant technologies.* New York: W.W. Norton & Co.

Buchanan, J. & Tullock, G. (1962). *The Calculus of Consent: Logical Foundations of Constitutional Democracy.* Ann Arbor: The University of Michigan Press.

Card, D. & Kruger, A. (1995). *Myth and Measurement: The New Economics of the Minimum Wage*. Princeton: Princeton University Press.

Comisión Europea. (2019). *Un pacto verde europeo.* Availabe at: europa.eu. (Un Pacto Verde Europeo | Comisión Europea).

Comisión Europea. (2014). *Turismo:* periodo de programación 2014-2020. Available at: europa.eu. (Turismo | Política Regional | Comisión Europea).

Comisión TRAN. (2019). TRAN Committee: European Tourism: Recent Developments and Future Changes. Available at: https://research4committees.blog/tran/ and at europa.eu.

Costanza, R., Caniglia, B., Fioramonti, L., Kubiszewski, I., Lewis, H., Lovins, L., McGlade, J., Mortensen, L., Philipsen, D., Pickett, K., Ragnarsdóttir, K., Roberts, D., Sutton, P., Trebeck, K., Wallis, S., Ward, J., Weatherhead, M. & Wilkinson, R. (2018). Toward a Sustainable Wellbeing Economy. *Solutions Journal* Available at: https://thesolutionsjournal.com/2018/04/17/toward-sustainable-wellbeing-economy, at https://www.resilience.org/stories/2018-05-11/toward-a-sustainable-wellbeing-economy and at https://weall.org/about.

Del Valle, A. (2013). Europa más allá de la Unión: pacto confederal y nuevo relato europeo. *Teoría y Realidad Constitucional*, 32: 341-355.

Diamond, P. & Kotler, S. (2014). *Abundance.* New York: Free Press.

Diamond, P. & Vartiainen, H. (2012). *Behavioral Economics and its applications*. Princeton: Princeton University Press.

Durán, F. (2013). *Repensar la cooperación al desarrollo*, Saarbrücken: EAE

Easterlin R (1974) Does Economic Growth Improve the Human Lot? David, P. & Reder, M. (Eds.). *Nations and Households in Economic Growth*, New York: Academic Press Inc.

Easterlin, R., Angelescu, M. L., Switek, M., Sawangfa, O. & Zweig, J. (2010). The happiness-income paradox revisited. *Proceeding of the National Academy of Sciences*, 107(52): 22463-68.

EU-Consilium. (2019). *The Economy of Wellbeing*: Going Beyond the GDP. Available at: https://www.consilium.europa.eu/en/infographics/economy-wellbeing/.

EU-Consilium. (2019). The Economy of Well-Being. Executive Summary of the OECD Background Paper on "Creating opportunities for People's Well-Being and Economic Growth". (10414/18 ADD 1). Available at: https://data.consilium.europa.eu/doc/document/ST-10414-2019-INIT/en/pdf.

EU-Horizon Europe. (2021). *What is Horizon Europe* Available at: europa.eu.

Fernández, I. (2015). *Felicidad organizacional*. Santiago: Ediciones B.

Fernández, S. (2015). *Vivir con abundancia.* Madrid: Plataforma Editorial.

Florida, R. (2010). *The Great Reset:* How New Ways of Living and Working Drive Post-Crash Prosperity. Toronto: Random House Canada

Friedman, M. (1953). *Essays in Positive Economics*. Chicago: University of Chicago Press.

Friedman, M. & Schwartz, A. (1963). *A Monetary History of the United States, 1867–1960.* Princeton: Princeton University Press.

Galbraith, J. K. (1958). *The Affluent Society*. Boston: Houghton Mifflin.

García, S. & Sánchez-Bayón, A. (2021) Gestión del cambio y del conocimiento en organizaciones cooperativas y de transformación social. *Revista Internacional de Organizaciones*, 27, 137-171.

García, D. & Sánchez-Bayón, A. (2021). Cultural consumption and entertainment in the Covid-19 lockdown in Spain: Orange economy crisis or review? *Visual Review*, 8(2),131-149.

García-Vaquero, M., Sánchez-Bayón, A. & Lominchar, J. (2021). European Green Deal and Recovery Plan: Green Jobs, Skills and Wellbeing Economics in Spain. *Energies*, *14(14)*, 4145.

Garrison, R. (2001). *Time and Money*. London: Routledge.

Gehrke, C. (2003). The Ricardo Effect: Its Meaning and Validity. *Economica*, 70(277), 143–158.

Gobierno de España. (2021). *Escudo Social*. Ministerio de Derechos Sociales y Agenda 2030. Available at: mdsocialesa2030.gob.es.

Gómez, P. (2019). *La riqueza de las naciones en el s. XXI.* Almería: Círculo Rojo.

González, E. & Sánchez-Bayón, A. (2021). Rescate y transformación del sector turístico español vía fondos europeos Next Gen EU. *Encuentros Multidisciplinares*, 23(69), 1-15.

Hayek, F. (1952). *The sensory order*. Chicago: University of Chicago

Hayek, F. (1939). Profits, Interest, and Investment, and other Essays on the Theory of Industrial Fluctuations. Hansjörg, K. (Ed.) (2012). *The Collected Works of F.A. Hayek*, 8, Business Cycles Part II.

Hayek, F. (1935). Prices and Production. Salerno, J. (Ed.) (2008). *Prices and Production and Other Works*. Auburn: Mises Institute.

Hazlitt, H. (1946). *Economics in one lesson.* New York: Harper & Row.

Huerta de Soto, J. (2009). *The theory of dynamic efficiency*, London: Routledge.

Huerta de Soto, J. (2006). *Money, Bank Credit, and Economic Cycles*. Auburn: Mises Institute.

Huerta de Soto, J. (2000). *La Escuela Austriaca*. Madrid: Síntesis.

Huerta de Soto, J., Sánchez-Bayón, A. & Bagus, P. (2021). Principles of Monetary & Financial Sustainability and Wellbeing in a Post-COVID-19 World: The Crisis and Its Management. *Sustainability*, 13(9), 4655, 1-11.

International Monetary Fund (IMF). (2020). *World Economic Outlook*. A Long and Difficult Ascent. Available at: imf.org.

Instituto Nacional de Estadística. (INE). (2019). *Turismo de España* (CSTE). Revisión Estadística 2019 Serie 2016 – 2018. Available at: ine.es.

Instituto Nacional de Estadística. (INE). (2022). *Turismo de España en 2020*. Revisado en 2022. Available at: ine.es.

Kaldor, N. (1942). Professor Hayek and the Concertina-Effect. *Economica*, 9(36), 359–382.

Keynes, J. (1937). The General Theory of Employment. *The Quaterly Journal of Economics*, 51(2), 209-223. Available at: https://www.jstor.org/stable/1882087.

Keynes, J. (1936). *The General Theory of Employment, Interest and Money*. London: Macmillan.

Keynes, J. (1933). The means to prosperity. *The Times* (Luego Desarrollado, como Planfleto y Publicado por Macmillan).

Keynes, J. (1930). Economic Possibilities for our Grandchildren. *Nation´s Business.* (1927) y Macmillan (1930, de manera póstuma incorporado en Keynes, J. M. (1963) *Essays in Persuasion.* New York: W.W. Norton & Co. ,358-373.

Klausinger, H. (2012). Introduction. Klausinger, H. (Ed.). *The Collected Works of F.A. Hayek*, 8, Business Cycles Part II, 1–43.

Kirzner, I. (1987). Austrian School of Economics, *The New Palgrave*: A Dictionary of Economics, 1, 145–151

Kurzweil, R. (2005). *The singularity is near*. New York: Penguin Group.

Kuznet, S. (1934). *National Income, 1929–1932*. 73rd US Congress, 2d session, Senate document no. 124. Washington DC: US Congress.

Kuznet, S. (1933a). National Income. *Encyclopaedia of the Social Sciences*. New York: Macmillan

Kuznet, S. (1933b). *Seasonal Variations in Industry and Trade*. New York: National Bureau of Economic Research.

Kuznet, S. (1930). *Secular Movements in Production and Prices:* The Nature and their Bearing upon Cyclical Fluctuations. Boston: Houghton Mifflin Co.

Lakatos, I. (1978). *The methodology of scientific research programmes*. Cambridge: Cambridge University Press.

Le Gales, P. & King, D. (2017). *Reconfiguring European States in Crisis.* Corby: Oxford University Press.

Levy, D., Mayer, T. & Raviv, A. (2022). Economists in the 2008 Financial Crisis: Slow to See, Fast to Act. *Journal of Financial Stability*, 60, 1-90.

Liadze, I., Macchiarelli, C., Mortimer-Lee, P. & Sanchez, P. (2022). *The Economic Costs of the Russia-Ukraine Conflict*. London: National Institute of Economic and Social Research (Policy Paper nº 32).

Macron, E. & Imbert, C. (2020). *The Macron Doctrine. Group d´études géopolitiques* Available at: geopolitique.eu.

Llena-Nozal, A., Martin, N. & Murtin, F. (2019). *The Economy of Well-being:* Creating opportunities for people's well-being and economic growth. SDD Working Paper No. 102. Paris: OCDE.

Lucas, R. (1972). Expectations and the Neutrality of Money. *Journal of Economic Theory*, 4(2), 103-124.

Lucas R (1975) An Equilibrium Model of the Business Cycle. *Journal of Political Economy*, 83(6): 1113-1144

Marx, K. (1867-94). *Das Kapital,* Kritik der politischenÖkonomie (3 Vols.). Hanover: Meisner.

Menger, C. (1871). *Grundsätze der volkswirtschaftslehre.* Leipzig: Duncker & Humblot.

Menger, C. (1883). *Untersuchungen uber die Methode der Socialwissenschaften und der Politischen Oekonomie Insbesondere*. Leipzig: Duncker & Humblot.

Mises, L. (1929). *Kritik des Interventionismus*. Jena: Gustav Fischer Verlag.

Mises, L. (1944). *Omnipotent Government: The Rise of the Total State and Total War*. New Haven: Yale University Press.

Moreno, A. (2013). El fin del relato europeo. La crisis del proceso de integración y su impacto sobre las narrativas europeas. *Revista de Derecho Comunitario Europeo*, 45, 607-630.

Moss, L. & Vaughn, K. (1986). Hayek´s Ricardo effect: a second look. *History of Political Economy*, 18(4), 545–565.

Navajas, V., López, C. & Sánchez-Bayón, A. (2014). Aprendizaje participativo en disciplinas duales mediante estudio de casos trasversales: una mirada a los problemas del emprendimiento en España. *Revista Universidad & Empresa*, 16(26), 173-190.

Navajas, V., López, C. & Sánchez-Bayón, A. (2013). Problemas del emprendedor inmigrante en España: evaluación de las políticas laborales y sociales españolas en el último lustro. *Revista Libre Empresa*, 10 (1), 13-49.

Organisation for Economic Co-operation and Development (OCDE). (2021). Measuring Well-being and Progress. Well-being Research. Available at: oecd.org.

Organisation for Economic Co-operation and Development (OCDE). (2021), Measuring Well-being and Progress. Working Papers. Available at: oecd.org.

Organisation for Economic Co-operation and Development (OCDE). (2019). *The Economy of Well-being:* Creating Opportunities for People's Well-being and Economic Growth. Paris: OCDE. Available at: oecd.org.

Organisation for Economic Co-operation and Development (OCDE). (2012). *Digital Economy.* Available at: oecd.org.

United Nations. (2015). *Transforming our World:* the 2030 Agenda for sustainable development. Gral. Assembly Resolution on Sept. 25, 2015 (A/RES/70/1).

United Nations. (2012). *Defining a New Economic Paradigm:* The Report of the High-Level Meeting on Wellbeing and Happiness. New York: ONU.

United Nations. General Assembly. (2015). *Transforming our World:* the 2030 Agenda for Sustainable Development (UN Resolution A/RES/70/1).

United Nations. Secretariat for the New Development Paradigm. (2013). Working Group Meeting in Bhutan. Available at: http://www.newdevelopmentparadigm.bt/category/resources/.

United Nations. Secretary-General (2012). *Secretary-General SG/SM/14204*. Message to Meeting on "Happiness and Well-being" Calls for "Rio+20" Outcome that Measures More than Gross National Income. Available at: http://www.un.org/News/Press/docs/2012/sgsm14204.doc.htm.

United Nations. Sustainable Development Goals Fund. (2015) *Goal 8:* Decent Work and Economic Growth. Available at: www.sdgfund.org/goal-8-decent-work-and-economic-growth.

United Nations Conference on Trade and Development. (2019). *Digital Economy Report*.

United Nations Development Programme. (2013). *A million voices - The World We Want:* A sustainable Future with Dignity for All Available at: http://www.worldwewant2015.org/millionvoices.

Parlamento Europeo. (2022) *El turismo.* Available at: europa.eu. (El Turismo | Fichas Temáticas sobre la Unión Europea | Parlamento Europeo).

Pigou, C. (1920) *Economics of Welfare.* London: Macmillan.

Posner, R. (1973) *Economic Analysis of Law*, Boston: Little Brown.

Ricardo, D. (1817). *On the Principles of Political Economy and Taxation.* London: J. Murray.

Romer, P. (2015). Mathiness in the theory of economic growth. *American Economic Review*, 105(5): 89-93.

Rothbard, M. (1977) Fetter the Radical (Preface & Introduction), en Fetter F (1905) *Capital, Interest, and Rent: Essays in the Theory of Distribution*. Kansas City: Sheed Andrews and McMeel, Inc.

Ruys, P. (2017) A Development of the Theory of the Ricardo Effect. *Quarterly Journal of Austrian Economics*, 20(4): 297–335.

Sánchez-Bayón, A. (2022). ¿Crisis económica o economía en crisis? Relaciones ortodoxia-heterodoxia en la transición digital. *Semestre Económico*, 11(1): 54–73.

Sánchez-Bayón, A. (2021). Balance de la economía digital ante la singularidad tecnológica: cambios en el bienestar laboral y la cultura empresarial. *Sociología y Tecnociencia*, 11(2). 53-80.

Sánchez-Bayón, A. (2020a). Renovación del pensamiento económico-empresarial tras la globalización, *Bajo Palabra*, 24: 293-318.

Sánchez-Bayón, A. (2020b). Una Historia de RR.HH. y su transformación digital, *Rev. Asociación Española de Especialistas de Medicina del Trabajo*, 29(3): 198-214.

Sánchez-Bayón, A. (2020c). Medidas de economía de bienestar que destruyen empleo en la economía digital. *Semestre Económico*, 23(55), 87-112.

Sánchez-Bayón A, García-Vaquero M, Lominchar J (2021) Wellbeing Economics: beyond the Labour compliance & challenge for business culture. *Journal of Legal, Ethical and Regulatory Issues*, 24(si). 1-13

Sánchez-Bayón A., Gonzálezo, E. & Andreu, A. (2022). Spanish Healthcare Sector Management in the COVID-19 Crisis Under the Perspective of Austrian Economics and New-Institutional Economics. *Frontiers in Public Health* 10:801525 (1-15).

Sánchez-Bayón, A. & Trincado, E. (2021). Rise and Fall of Human Research and the Improvement of Talent Development in Digital Economy. *Studies in Business and Economics*, 16(3): 200-214.

Sánchez-Bayón A. & Trincado, E. (2020). Business and labour culture changes in digital paradigm, *Cogito*, 12(3): 225-243.

Schwab, K. & Malleret, T. (2019). *COVID-19: The Great Reset*. Genova: WEF.

Schmoller, G. (1900). *Grundriss der allgemeinen volkswirtschaftslehre*. Leipzig: Duncker & Humblot.

Steele, G. (1988). Hayek's Ricardo Effect, *History of Political Economy*, 20(4): 669–672.

Suresh, R. (2010). *Economy and Society. Evolution of Capitalism*. Delhi: SAGE.

Thaler, R. (2016). Behavioral Economics: past, present, and future. *American Economic Review*. 106 (7): 1577–1600.

Trincado, E., Sánchez-Bayón, A. & Vindel, J. (2021). The European Union Green Deal: Clean Energy Wellbeing Opportunities and the Risk of the Jevons Paradox. *Energies, 14(14)*, 4148.

Valero, J. & Sánchez-Bayón, A. (2018). *Balance de la globalización y teoría social de la posglobalización*. Madrid: Dykinson.

VV.AA. (2010). *Proyecto europeo 2030: retos y oportunidades*. Bruselas: Consejo Europeo.

Walras, L. (1883). *Théorie mathématique de la richesse sociale.* Lausanne: Corbaz.

Wilson, T. (1940). Capital Theory and the Trade Cycle. *Review of Economic Studies*, 7(3): 169–179.

The Law, State and Telecommunications Review / Revista de Direito, Estado e Telecomunicações

Contact:
Universidade de Brasília - Faculdade de Direito - Núcleo de Direito Setorial e Regulatório
Campus Universitário de Brasília
Brasília, DF, CEP 70919-970
Caixa Postal 04413

Phone: +55(61)3107-2683/2688

E-mail: getel@unb.br

Submissions are welcome at: https://periodicos.unb.br/index.php/RDET

Identity of the Suspect in Cyber Sabotage

Submitted: 4 August 2022
Reviewed: 20 October 2022
Revised: 1st March 2023
Accepted: 3rd March 2023

Article submitted to blind peer review

Oleh Peleshchak[*]
https://orcid.org/0000-0002-2785-7464
Roman Blahuta[**]
https://orcid.org/0000-0002-8087-5995
Larysa Brych[***]
https://orcid.org/0000-0002-7079-3726
Nataliya Lashchuk[****]
https://orcid.org/0000-0001-9723-9824
Dmytro Miskiv[*****]
https://orcid.org/0000-0003-3710-0374

DOI: https://doi.org/10.26512/lstr.v15i2.44518

Abstract

[Purpose] The purpose of the study is to identify means and measures to counteract and prevent cyber sabotage.

[Methodology] The research is based on a systematic approach and logical tools (description, analysis, synthesis, induction, deduction, etc.). Special scientific, general scientific, and philosophical methods are applied.

[Findings] The study analyses the possible motives of the suspect in cyber sabotage and unifies classification approaches. Attention is focused on information support for the interrogation of a suspect in cyber sabotage by an investigator to learn the identity of the suspect. Certain features of the sources of obtaining information about a person suspected of committing cyber sabotage are noted. The general characteristics and features of the identity of a cyber sabotage suspect cannot be considered outside the context of other socially dangerous attacks in cyberspace. The development of mechanisms for countering cybercrime in Ukraine continues.

[Value] The practical significance of the study is determined in the list of measures and means proposed by the authors to reduce the risk of cyber sabotages and eliminate their harmful consequences.

Keywords: Criminal Identity. Forensic Characteristics. Cybercrime. Prevention. Cybercrime.

[*] Postgraduate Student, Department of Criminal Procedure and Criminalistic, Lviv State University of Internal Affairs, Lviv, Ukraine. E-mail: peleshchak8739@yahoo.com.
[**] PhD in Law, Professor, Lviv State University of Internal Affairs, Lviv, Ukraine. E-mail: ro-blahuta@gmail.com.
[***] Full Doctor in Law, Associate Professor, Head of the Scientific-Research Laboratory, Lviv State University of Internal Affairs, Lviv, Ukraine. E-mail: lbrych@outlook.com.
[****] PhD in Law, Head of the Department of Criminal Law Disciplines, Lviv State University of Internal Affairs, Lviv, Ukraine. E-mail: nat.lashchuk@aol.com.
[*****] PhD in Law, Lviv Branch, Department of Homeland Security of the National Police of Ukraine, Lviv, Ukraine. E-mail: miskiv5@outlook.com.

INTRODUCTION

Nowadays, cybercrime is the most dynamically developing type of socially dangerous attacks in the world and in Ukraine. Over the past ten years, there has been an increase in this type of crime exponentially. During 2020, more than 5000 cybercrimes were registered in Ukraine, 106 persons involved in criminal proceedings were detained (In 2020, the National Police…, 2021). The prerequisites for this increase are the availability of computer knowledge, a growing level of integration of technologies into the economy and public life, technological progress (improving the technical characteristics of equipment combined with reducing the price of it), insufficient level of security of information processes, cross-border (no state borders in cyberspace), an increase in the Internet, telecommunications, and other types of networks (the ability to connect to them via ordinary telephone lines), improvement of network technologies, an increase in the number of users (their low legal awareness, disregard for the rules of cyber hygiene, non-compliance with the policy of code (password) and information security), corruption component, hyperlatedness (fear of victims losing their reputation, revealing their security schemes, exposing their own illegal actions) etc (DE FRÉMINVILLE, 2020; GETMAN et al., 2019). Cyber threats against unauthorised interference, distributed denial-of-service (DDoS) attacks, the spread of malicious software (including one that can automatically type all alphanumeric combinations based on the principle of a random number generator for setting a password), internet fraud, the establishment of hidden access for the purpose of future control to the use of fake twin sites, simulation programmes, chatbots, cloud technologies, and many others are also being modified. In this context, cyber-attacks on the public sector are also increasing, which, considering modern threats and challenges, slow down positive development trends and threaten both society and the state. Illegal access or distortion of computer information can disrupt the operation of state security systems and lead to material damage and human casualties (RYCHKA, 2019).

Modern information technologies and the latest software not only affect economic processes, and therefore politics and overall society, but also provide new and more advanced opportunities for committing previously unknown offences, or committing traditional crimes by non-trivial methods and means. However, there is a limit of the law that is mandatory for both the real and virtual world (BILENCHUK, 2001). The identity of the criminal is the source of the crime, and therefore, the analysis of thinking, characteristics, and specific features of the person suspected of committing cyber sabotage play an important role in forming the trace picture of this crime. The study is significantly complicated by the lack of an unambiguous assessment of "cyber incidents" in national legislation (usually they are conditionally interpreted as a way of committing), the dispersion

of factual and objective information about these individuals in the reports of various law enforcement departments of Ukraine, the hyper-diversity and atypicality of ways and means of committing cyber sabotages (TACIJ et al., 2014). Therefore, the work of law enforcement agencies to detect, investigate, and prevent crimes in this area in a timely manner requires further adequate organisational, managerial, and forensic means and measures to counteract and intensively introduce innovations.

The above causes an urgent need for further study in this area to clarify certain scientific provisions in order to improve the methodology for investigating crimes of this category, establish productive interaction between law enforcement agencies, strengthen criminal legal protection, and criminal liability, require analysis and addition of the arsenal of countering the commission of cyber sabotages (DENYSOVA, 2003; LUTSENKO, 2017; BORYSOVA et al., 2019). Liability for criminal offences in the use of electronic computers (computers), systems and computer networks and telecommunication networks are provided for in Chapter 16 of the Criminal Code of Ukraine. If the violation of automated systems is associated with the commission of more serious crimes (for example, sabotage, espionage, theft of property, etc.), the actions of the perpetrators are qualified according to the totality of crimes (BORYSOVA, 2006). The purpose of the study is to identify means and measures to counteract and prevent cyber sabotage.

MATERIALS AND METHODS

The study applied special scientific, general scientific, and philosophical methods. This allowed comprehensively considering the subject matter. Using the dialectical method, the process of developing criminological knowledge about the identity of a cybercriminal in general and a person suspected of committing cyber sabotage, in particular, was considered. The use of a criminological approach to the investigation of a person suspected of committing cyber sabotage is complex, since it covers sociological, criminal-legal, psychological, and pedagogical aspects of scientific analysis. The use of methods of analysis, synthesis, induction, and deduction identified socio-demographic, criminal-legal, and moral and psychological features of a person suspected of cyber sabotage, forming a list of measures and means of countering and preventing cyber sabotages.

Criminological and criminalistic sources were analysed using various methods of legal interpretation and in the context of the hermeneutical method of scientific knowledge. This facilitated an in-depth analysis of the subject matter. The logical and semantic approach was used to analyse classification systems and types of cyber criminals. The scientific conclusions were confirmed using the statistical method.

The problems of characterising the face of a cybercriminal have been considered by many researchers since the beginning of the 21st century. Some aspects of this problem were investigated by: P.D. Bilenchuk (2001), O.O. Denysova (2003), L. Borysova (2006), K. Titunina (2006), V.B. Shkolnyi (2012), N.S. Kozak (2013), S.V. Yakimova and B.C. Borovikova (2016), O.Yu. Ivanchenko (2019), M.O. Gvozdetska and K.Yu. Izmaylov (2016), V.Yu. Shepitko and V.A. Zhuravel (2017), B.Yu. Chernikov (2018), O.Yu. Dovzhenko (2019), M.I. Maliy and P.D. Bilenchuk (2019), D.O. Rychka (2019), N.L. Pushina (2020), M.W. Kranenbarg, S. Ruiter, J.L. Van Gelder (2021), A.F. Karachka (2017), O.R. Peleshchak (2021).

RESULTS AND DISCUSSION

When qualifying crimes related to computer equipment, it is necessary to consider not only the general rules for qualifying crimes, but also some specifics of crimes inherent only in such acts. The object will be especially important for the qualification, that is, the identity of the criminal and their forensic characteristics. Computer criminals are colloquially referred to as "hackers", "software crackers", and "phreakers". A hacker is a highly qualified IT (information technology) professional who understands the intricacies of computer software. A cracker is an IT professional who hacks security systems (including software protection), software, creates or modifies hacking, and much more. The result of hackers is deliberate cracks, which are programmes that allow hacking software. Software crack is usually suitable for mass production. In fact, a crack is the epitome of a type of hacking, most often it is a general patch (information intended for automatically making certain changes to computer files). In most cases, software crack does not have the source code of the programme, so the disassembler and debugger investigate the programme using special utilities (MAYER LUX & VERA VEGA, 2020). A phreaker is a person who is engaged in phreaking. This term is also used for people who use the phone for their illegal actions in order to psychologically influence the end user.

Recently, phreaking is understood as various ways of hacking electronic systems, such as bank security systems and access control systems. As a consequence of the above, these individuals have special knowledge and practical skills in the field of computer technology and are at least computer users. In a computer information crime against a legal entity, the perpetrator or accomplice (accomplice) is usually an employee of this institution or organisation. These are computer operators, peripherals and communications equipment; programmers; system administrators; electronics engineers; database administrators; network security specialists, civil servants and other persons who have access to computer information and equipment, their networks. Competitors or industrial spies, and

professional criminals and cyberterrorists, can pose a serious threat to network security. Representatives of these groups are engaged in illegal activities from corporate espionage to extremely dangerous sabotage of computer systems of vital objects. In recent years, the investigation of the identity of a criminal in global computer networks has faced a significant increase in criminal activity on the part of hackers. Not only in identifying the fact of committing a cyber sabotage after the fact (according to experts, 90% of cases of crime detection are generally due to chance), but also in investigating this type of crime, there are certain difficulties. It is quite difficult to identify, record, and seize criminally significant information when performing investigative actions for use as material evidence (CHERNIKOV, 2018). Most of this information can be obtained by using profiling methods both when identifying a cybercriminal and to prevent illegal actions. Since a wide range of people are involved in cybercrime, the establishment of a database of typical profiles of cyber criminals and the study of their general features allows optimising the process of narrowing the circle of suspects.

Speaking about the personality of criminals, it is important to emphasise that this type of person is characterised by a high level of intellectual development, unusual thinking, professionalism, fanatical attitude to new computer technologies, ingenuity, rich imagination, and secrecy. As a rule, the criminal among the employees of the organisation is an exemplary employee with appropriate training. Such persons have not previously committed any criminal offences. Often these are managers of various ranks who have leadership roles, but are not directly responsible for specific areas of work with computer information. Most often, crimes in the field of computer information are committed by stable criminal groups that are characterised by mobility, high technical equipment, a clear distribution of roles, expressed self-serving motivation and a well-thought-out system for hiding traces of criminal activity (CHERNIAVSKYI et al., 2019). The greatest danger and difficulties for detection and disclosure are criminal groups, which include highly qualified specialists with special knowledge in the field of secret obtaining and protection of computer information. Most of the crimes committed by these subjects remain latent.

The vast majority of offenders are adults, with an almost uniform distribution by age. It should also be noted that the vast majority of those who have committed these types of offences have higher or secondary special education. As for the gender characteristics of the attacker, it can be stated that criminal offences in the field of computer information are committed mainly by men. In the current period, a large number of people, both non-professional and highly qualified specialists, will be involved in the commission of computer crimes. At the same time, all of them have different social status and level of education, which already allows them to be divided into two large groups – these

are both people who are in an employment or other employment relationship with the victim, and people who do not have a corresponding connection with the victim. The first group should include employees who abuse their position. These are different types of clerks, security guards, supervisors, people who deal with organisational issues, engineering and technical personnel.

Computer security experts believe that amateur hackers are the most numerous, but the least dangerous. They account for up to 80% of all computer attacks. But these people are not interested in a specific target, but in the attack process itself, and they enjoy overcoming defence systems. For the most part, their actions can be easily stopped, since amateur hackers prefer not to take risks and avoid problems with the law. Most people of this type were connected to computers at school. Knowledge of computer technology is limited to one or two programming languages. The installation of criminal behaviour among amateurs happens spontaneously, mainly under the influence of a random chain of successful and unsuccessful "hacks" of security programmes on other computers. The consolidation of this attitude occurs under the influence of the "authoritative opinion of senior comrades", which they express after communicating with the "newcomer" in the network "lobbies". As the level of professionalization increases, amateurs acquire a deeper, more systematic knowledge of computer technology, programming languages, solid skills and abilities in working with networks, software, etc. This is related to the actual acquisition of higher technical education. They are already specialists. People in this group are psychologically more balanced, have a well-developed system of thoughts and values, but are not yet very ambitious. In most cases, the criminal "career" of such a group of people is transformed from an amateur "career" or developed by entering the criminal environment, for example, with the help and support of "professional" friends. The main areas of criminal activity of "specialists" are network hacking, actions in operations to obtain confidential information using powerful data protection systems, economic and mental espionage.

One of the most important elements for identifying a cybercriminal is motivation, the definition of which can provide information about the needs, interests, and characteristics of the suspect. Motives can be the following: political, ideological (for example, as a form of protest, so-called "hacktivists"); hooligan motives; self-serving (commercial calculation, thirst, material interests); sexual motive; obtaining specific items that have a special value in the cyber world or a higher unofficial social status, competition, technical challenge, struggle between human and artificial intelligence; the desire to have fun, assert themselves, prove intellectual abilities, curiosity, game; research, experiments on the study of software and technical electronic devices, networks, search for weaknesses, opportunities for them use and elimination; manifestations of sadism, painful imagination, pathological predisposition to destructive influence on

society and public relations, obtaining moral satisfaction from the scale of destructive consequences; revenge (for example, for troubles at work), personal hostility; negligence, etc. (SHULZHENKO & ROMASHKIN, 2021). Sometimes the motives are complex or complementary to the main ones. The prerequisites for cyber sabotage are the following objective and subjective circumstances:

(1) Wide development of the high-tech industry and significant spread of computer technologies among the population;
(2) Availability of specialities in higher educational institutions that train students with the instillation of subject knowledge, programming skills, and knowledge;
(3) Influence of the family and non-family environment on the process of becoming the culprit of computer information;
(4) Actual impunity of persons who have committed computer crimes due to the high latency of these illegal actions, the lack of proper training of law enforcement officers involved in criminal proceedings on this category of crimes.

No less informative is the professional operation of investigative types of classifications of cyber criminals. For example, depending on their motives, they are divided into: hackers, criminals, vandals (In 2020, the National Police…, 2021). Depending on the purpose of committing a criminal offence, and the scope of application of professional skills, cyber criminals are conditionally divided into four groups: those who "crack" codes and passwords more through curiosity and self-affirmation, trying to find out what will happen for this (usually teenagers, students), by their actions they create serious obstacles to the normal operation of networks and computers; persons who are engaged in targeted theft of new software that is distributed for a fee. Characteristic of this category is the establishment of stable groups with a clear distribution of responsibilities among their members: some crack security codes and passwords, others are engaged in their implementation; computer hooligans who spread computer viruses that destroy software; criminals who hunt for confidential information, sometimes on order, receiving material remuneration for this.

In the specialised literature, there are a large number of other classifications of cyber criminals according to: age characteristics; professional and qualification characteristics (the most difficult to investigate are cases of combining professions); type of labour relations with the affected party; signs of employment; state of health, mental changes; gender characteristics; repeatability of criminal actions (recidivism); individual psychological traits; the ability to access information, the nature of encroachment on it; the method and purpose of committing; social status in society; the scope of crime; the state of awareness of

crime actions (often the criminal is not able to fully foresee the consequences of their actions, which depend on many subjective and objective factors. This applies to professional violators of the operating modes of equipment, whose unintentional actions can lead to less serious consequences than a planned cyber-attack); the number of performers, etc. At the stage of preparing for the interrogation of a cyber sabotage suspect, the investigator needs to conduct information support, investigate the suspect's identity and carry out planning. The main tasks of the interrogation are: identification of elements of the composition of cybercrime; establishment of its circumstances, method, motives, accompanying circumstances; identification of signs of cybercrime; establishment of the method of its concealment.

Next, the study considers the investigation of the identity of a suspect in cyber sabotage. Information is to be established by traditional investigative means: biographical data, previous activities (educational, labour); individual psychological characteristics (assigned forensic psychological and/or forensic psychiatric examination, visual observation is conducted, sources of open information are analysed for the study of professional interests, interests, hobbies, attitude to social phenomena, approval of criminal behaviour, etc. (sources of Information: groups in social networks, free ads); special and professional skills (pattern in crime of cyber criminals, which is expressed in certain ways, methods and techniques committing cybercrime, they can be detected by an involved specialist based on the analysis of the technology and method of obtaining illegal remote access (more often cyber criminals prefer to intercept information when transmitting it via telecommunications channels and computer networks, rather than directly entering the premises), establishing important technical data (IP (internet protocol), email address, mobile phone number); features of the subject of encroachment (for example, banking or commercial information); interaction with the victim or the affected organisation; time and place of the crime.

The investigator conducts research and compares data about a person from different sources. Thus, scientific studies on individuals who had information about those who committed cybercrime note that in 31% of cases other people had information about the plans of the criminal; in 64% of cases – colleagues, in 21% – friends, in 14% – family members, in 14% – accomplices (GVOZDETSKA e IZMAYLOV, 2016). Usually, cyber criminals think through their actions in advance and take measures to hide them. If the preparation for the commission of a crime takes place without the involvement of unauthorised persons, the search history in the browser or information from witnesses regarding the search for special literature or special software tools by the suspect may become informative. During the interrogation, as in a normal interview, the investigator should identify contradictions, lies in the testimony, identify the person's attitude to the crime and be prepared for intellectual opposition from the criminal. The investigator and

specialist should pay particular attention to the unsystematic unjustified destruction of obstacles (including in cyberspace), the absence of traces in places where logically they should be (staging), the nature of hacking (may indicate penetration from the inside of the room/internal server of the organisation). According to a study by IDG (International Data Group) Corporation, 88% of cases of information theft occur through employees of firms and only 12 % – through external penetration using special means (YAKIMOVA e BOROVIKOVA, 2016).

Therefore, the main danger is caused by internal users (or with their help). They commit 94% of crimes, while external crimes – only 6% (AIKOV e SEIGER e FONSTORCH, 1999). Notably, deliberate destruction of information is most often carried out by former employees or employees of the organisation in order to conceal other crimes or negligence. In cyber extortion, the criminal has access to information that is used when threatening the victim. The peculiarities of the interrogation of a perpetrator of cyber sabotage are the high intellectual level, the special psychological make-up of the interrogators, and the complex technical nature of the questions to be clarified. Recently, there has been a tendency to complicity in group cyber-attacks. Judicial practice shows that 38% acted independently, 62% – as part of organised groups and terrorist communities (SHEPITKO e ZHURAVEL, 2017). The most dangerous due to the ability to organise and commit cyber sabotage are organised groups of corrupt representatives of various state structures, special services that have almost unlimited financial capabilities, independently regulate and control Internet traffic, highly professional, educated, can enjoy the support of legislation and local authorities.

In order to prevent cybercrime, including cyber sabotage, the following technical and organisational measures can be implemented: periodic inspection of equipment for unauthorised access, statistical analysis of traffic to detect anomalies (with the help of a specialist or special software); maintaining a register, database of cyber criminals; introducing mandatory identification and verification of the Internet users; limiting the circle of intermediaries; constant testing and improvement of programmes for the state of protection of users' rights, especially in the field of public services; improving the protection of electronic digital signatures of users; informing internet users about the rules of cyber hygiene, risks and possible cyber threats (including in the cloud environment); establishing rules on the tactics of internet users' actions for typical, atypical and suspicious actions of unauthorised persons in cyberspace (recommendations); establishing technical and other types of restrictions (for example, setting network filters, using a virtual private network), etc. High requirements are also imposed on the investigator of the fact of cyber sabotage, they must have training at the level of a professional programmer or system administrator, be able to use the

appropriate software, understand the internal mechanisms of systems and networks, be able to use certified software tools during a search and when collecting physical evidence.

CONCLUSIONS

Cybercrime is becoming more and more global, the latest technologies are turning real criminals into anonymous ones, and the ease of getting rich quickly attracts more and more people to join this criminal activity. Lack of demand for creative potential combined with ignorance of all the consequences of illegal actions – on the one hand, cold professionalism – on the other. These are just common features of cyber criminals. Their technical armament, knowledge, and skills far exceed the capabilities of law enforcement agencies, so improving law enforcement systems is becoming more difficult and expensive. Since the conditions of cyberspace differ significantly from real ones, in order to establish the process of occurrence of criminal intent, its nature, and the degree of public danger of the criminal, there is also a need to classify criminals depending on various subjective and objective factors. Prevention of cybercrime is based on measures aimed at reducing the risk of committing such crimes and neutralising harmful consequences for society and the public and private sectors. Effective counteraction combines a complex of legal (legislative), technical, organisational, and informational measures.

At the legislative level in Ukraine, many issues in the field of countering cybercrime remain unresolved. These are, first of all, gaps in the current legislation in the field of: information technologies, electronic proof, prevention and counteraction to the legalisation of proceeds from cybercrime, and the lack of sufficient investigative and judicial practice in criminal cases on the fact of cyber sabotage and single information and legal space that ensures legal awareness of all structures of society and each citizen separately. Advanced legal regulation can also be provided by: highlighting cyber sabotage and other crimes committed using computer technologies (cyber sabotage, unauthorised collection of information, cyber stalking, cyber investigation) in a separate group of illegal acts in the criminal law, strengthening criminal liability for cybercrime; improving the mechanism for recognising electronic documents and other data as an evidence base in the investigation of cybercrime; clear regulation of interaction between law enforcement agencies. Difficulties in obtaining the necessary amount of information about the identity of the criminal are associated with their high latency, as noted above. These issues are rarely brought to the attention of law enforcement agencies, which allows tracking the characteristics of the criminal introduced in the form of technical developments. However, it is possible to use the above to create a portrait that meets modern realities. Paradoxically, attracting

hackers to socially useful work can also help law enforcement agencies, as one of the measures to prevent computer crimes and solve those already committed.

REFERENCES

Aikov, D., Seiger, K. & Fonstorch, W. (1999). *Computer crimes:* A guide to combating computer crimes. Moscow: Mir.

Bilenchuk, P. D. (2001). Questions of social and criminological characteristics of a computer criminal. *State and Regions*, 4, 16-22.

Borysova, L. (2006). Subject (person) of transnational computer crime: forensic and psychophysical aspects. *Current Issues of State and Law*, 1, 76-81.

Borysova, V. I., Ivanova, K. Y., Iurevych, I. V. & Ovcharenko, O. M. (2019). Judicial protection of civil rights in Ukraine: National experience through the prism of European standards. *Journal of Advanced Research in Law and Economics*, 10(1), 66-84.

Cherniavskyi, S.nS., Holovkin, B.nM., Chornous, Y.nM., Bodnar, V.nY. & Zhuk, I.V. (2019). International cooperation in the field of fighting crime: Directions, levels and forms of realization. *Journal of Legal, Ethical and Regulatory Issues*, 22(3), 1-11.

Chernikov, B. Y. (2018). Criminological characteristics of cybercrime. *Young Scientist*, 11(63), 941-944.

De Fréminville, M. (2020). *Cybersecurity and decision makers:* Data security and digital trust. Wiley: ISTE

Denysova, O. O. (2003*). Information systems and technologies in legal activity*. Available at: http://ukrkniga.org.ua/ukrkniga-text/817/.

Dovzhenko, O. Y. (2019). On the question of tactics of interrogation in cybercrime cases. *Scientific Bulletin of the International Humanities University*, 37, 143-145.

Getman, A., Karasiuk, V., Hetman, Y. & Shynkarov, O. (2019). Ontological representation of legal information and an idea of crowdsourcing for its filling. *Advances in Intelligent Systems and Computing*, 836, 179-188.

Government Portal. *In 2020, the National Police exposed more than 5000 cybercrimes.* Available at: https://www.kmu.gov.ua/news/u-2020-mu-nacpoliciya-vikrila-ponad-5-000-kiberzlochiniv.

Gvozdetska, M.O. & Izmaylov, K.Yu. (2016). Criminological characteristics of cybercrime: Current state, structure and specifics of committing. *Current Challenges and Achievements in the Field of Cybersecurity*, 2, 52-53.

Ivanchenko, O. Y. (2019). Criminological characteristics of cybercrime, prevention of cybercrime at the national level. *Actual Problems of Domestic Jurisprudence*, 3, 172-177.

Karachka, A. F. (2017). *Technologies of information protection*. Ternopil: National University of Economics.

Kozak, N. S. (2013). Forensic characteristics of persons who commit computer crimes. *Scientific Bulletin of the National University of the State Tax Service of Ukraine (Economics, Law)*, 2(61), 186-191.

Kranenbarg, M. W., Ruiter, S. & Van Gelder, J. L. (2021). Do cyber-birds flock together? Comparing deviance among social network members of cyber-dependent offenders and traditional offenders. *European Journal of Criminology*, 18(3), 386-406.

Lutsenko, O. (2017). Bringing civil servants to liability for disciplinary misconduct in judicial practice of Ukraine, Poland, Bulgaria and Czech Republic. *Journal of Advanced Research in Law and Economics*, 8(1), 103-112.

Maliy, M. I. & Bilenchuk, P. D. (2019). *Cyberspace in the new millennium.* Who are they: cybercriminals? Available at: https://cutt.ly/UZmm0d9.

Mayer Lux, L. & Vera Vega, J. (2020). The crime of cyber espionage: Definition and delimitation. *Revista Chilena De Derecho y Tecnologia, 9*(2), 221-256.

Peleshchak, O. R. (2021). *Survey of the premises in the investigation of cyber diversions*. Madrid: Barca Academy Publishing.

Pushina, N. L. (2020). Forensic characteristics of a person who commits criminal offenses in the field of economic activity with the use of computer technology. *Scientific Notes of TNU named after V.I. Vernadsky*, 31(70), 121-126.

Rychka, D. O. (2019). *Peculiarities of the criminal-law qualification of crimes in the sphere of the use of electronic computers, systems and computer networks and telecommunication networks.* Dnipro: University of the State Fiscal Service of Ukraine.

Shepitko, V. Y. & Zhuravel, V. A. (2017). *Innovative principles of technical and criminalistic support of the activity of criminal justice bodies.* Kharkiv: Apostil.

Shkolnyi, V. B. (2012). Some reasons for the emergence and development of crime in the use of computers. *Law and Society*, 2, 222-227.

Shulzhenko, N. & Romashkin, S. (2021). Types of individual criminal responsibility according to article 25 (3) of rome statute. *Juridical Tribune*, 11(1), 72-80.

Tacij, V. J., Tjutjugin, V. I. & Grodeckij, J. V. (2014). Conceptual model establish responsibility for offense in the legislation of Ukraine (draft). *Criminology Journal of Baikal National University of Economics and Law*, 2014(3), 166-183.

Titunina, K. (2006). Characteristics of computer crimes committed using the Internet (analysis of questionnaires). *Fight against Organized Crime and Corruption*, 21, 307-313.

Yakimova, S.V. & Borovikova, B.C. (2016). Personality of an economic criminal. *Bulletin of the National University Lviv Polytechnic*, 837, 521-527.

The Law, State and Telecommunications Review / Revista de Direito, Estado e Telecomunicações

Contact:
Universidade de Brasília - Faculdade de Direito - Núcleo de Direito Setorial e Regulatório
Campus Universitário de Brasília
Brasília, DF, CEP 70919-970
Caixa Postal 04413

Phone: +55(61)3107-2683/2688

E-mail: getel@unb.br

Submissions are welcome at: https://periodicos.unb.br/index.php/RDET

Criminological Features of the Cybersecurity Threats

Submitted: 6 December 2022
Revised: 29 January 2023
Reviewed: 10 March 2023
Accepted: 15 March 2023

Viktor Anatolievich Shestak[*]
https://orcid.org/0000-0003-0903-8577
Alyona Dmitrievna Tsyplakova[**]
https://orcid.org/0000-0001-8564-0696

Article submitted to blind peer review

DOI: https://doi.org/10.26512/lstr.v15i2.45997

Abstract

[Purpose] Currently, novel tools have converted many traditional phenomena into cyber ones. The absence of a standardized terminology and classification of cybersecurity threats has raised significant concerns among researchers and lawmakers. Ignoring the emerging risks that necessitate appropriate responses is impracticable. Prior to devising countermeasures to combat cybercrime, it is imperative to accurately define the concept of cybersecurity threat and differentiate it from other related notions such as information security, computer security, cyberattack, cyberspace attack, cyber incident, cybersecurity incident, cyber threat, and cybersecurity event, whose definitions may be ascertained from the glossaries of various standardization institutes.

[Methodology/Approach/Design] This study presents a descriptive investigation of cybersecurity threats and their causes, utilizing genetic, systematic-functional, and systematization methods. Cyberattacks are identified as the primary threat, and data is represented through qualitative research and summarized in tables. The study also considers the historical background of concepts and cyber-criminality.

[Findings] The present study delves into a comprehensive analysis of distinct categories of cybersecurity threats, the trajectory of cybercrime, and the factors that underpin the emergence of new cybersecurity threats. The research scrutinizes both the general causes for cyber-criminality and the specific determinants for criminal activities that target the energy sector, a critical component of a state's infrastructure. The study reveals that the major sources of threats comprise terrorists, insiders (i.e., disgruntled employees), commercial spies, and black hackers or crackers, whose malicious acts are themselves considered threats to cybersecurity.

[*]Doctor of Juridical Science, Professor of the Department Criminal Procedure, Moscow Academy of the Investigative Committee of the Russian Federation (Moscow, Russian Federation). Address: 12, Vrubel Street, Moscow, Russia, 125080. E-mail: viktor_shestak@mail.ru.
[**]Bachelor of Laws (LL.B.), Master's Degree Student of the Department of Criminal Law, Criminal Procedure and Criminology of MGIMO University (Moscow, Russian Federation). E-mail: tsyplakova.a.d@my.mgimo.ru.

Keywords: Cybersecurity Threats. Criminology. Information Security. Cybersecurity. Determinants of Crime.

INTRODUCTION

Undoubtedly, it is the regulation of information and telecommunication technologies that arouses a lot of scientific interest. According to McKinsey Global Institute, more than half of operations will be automated in the next 20 years(Ovchinsky V. S., 2016: 9). According to Kaspersky Lab., the share of cyber aggression accounts for 49,48% (Kaspersky Lab., 2020). As to the short-term and medium-term risks, half of respondents rank cybersecurity as one of the top challenges, according to the World Economic Forum (World Economic Forum, 2021). Despite the fact that in the early 2000s fight against cyber threats was not considered primary, statistics show that most frequently committed crimes are cyberattacks, which can be committed within a company, a state and outside it. For instance, in the USA in September 2021, it was recorded that over the summer 77% of all companies in the fuel and energy sector were subject to employee data leakage. In 2020, the most popular scheme was DDoS attacks, and in 2021 it was phishing (in 65% of cases) (Nescout, 2021).

REVIEW OF KEY NOTIONS

Researchers have been elaborating the notion hierarchy, but it is treated as tentative. One may define information security (InfoSec) as the state of being secured vis-a-vis any information, regardless of its form of expression and medium. It is based on a triad of principles: integrity, availability and confidentiality. Cybersecurity is only an element of InfoSec and concerns the digital assets, including data in cyberspace and on any e-device. Due to the complexity of the digital world, the hardship arises with computer security that implies the use of such a specific device as computer, but it considers a narrow approach to the phenomenon in question.

Taking into account to the International Organization for Standardization, it is worth reviewing the standard ISO/IEC 27001: 2013 “Information technology — Security techniques — Information security management systems”. Cybersecurity is defined as actions and security controlling methods used to protect against cyberattacks. National Institute of Standards and Technology (NIST) Glossary provides broader interpretations of cybersecurity:

(1) Prevention of damage to, protection of and restoration of computers, electronic communications systems and services, wire and electronic communication, including information contained therein, to ensure its

availability, integrity, authentication, confidentiality and nonrepudiation;
(2) Process of protecting information by preventing, detecting, and responding to attacks;
(3) Ability to protect or defend the cyberspace against cyberattacks;
(4) Prevention of damage to, unauthorized use of, exploitation of the restoration of electronic information and communications systems (ICS) (if needed) and the information contained therein, in order to enhance the confidentiality, integrity and availability of these systems.

Cyberspace is described as the following:

(1) Global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems and embedded processors and controllers in critical industries;
(2) Complex environment which results from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it and does not exist in any physical form.

Nevertheless, one should take into account the fact that cybersecurity threats are far beyond cyberattacks, therefore, in the American researchers and policy makers broadly interpret the term cybersecurity, scrutinizing such notions as cyberattack, cyberspace attack, cyber incident, cybersecurity incident, cyberthreat, cybersecurity event.

A cyberattack is an attack committed via cyberspace and aimed at disrupting, disabling, destroying a computing environment or infrastructure; or destroying the integrity of the data or stealing controlled information. Meanwhile, a cyberspace attack has a more general characteristic, i.e., cyberspace actions that create various negative effects and manipulation leading to denial, however, it is insufficient to underline specific features of the phenomenon under consideration.

Actions that constitute a cyber incident are those taken through the use of an information system or network (IS/N) that result in an actual or potentially adverse effect on an IS/N and/or the information stored therein. The definition of the cybersecurity incident empathizes the necessity of response to the impact that actually or inevitably jeopardizes the triad of principles and constitutes a violation or imminent threat of violation of a law, security policy or acceptable use. The clarification of a cybersecurity event undermines consequences that have impact on the organization's activities, its capabilities or reputation. At the

same time, the concept of an incident can include not only deliberate attacks as a threat to obtain unauthorized access and data theft or falsification, but also unintended consequences, such as damage, incorrect operating systems and unauthorized changes to their configurations (Belous A. I., 2020: 229–230).

A cyberthreat is any circumstance, condition or event that may adversely affect the organizational operation, mission, functions, image, reputation, assets, or individuals, or other organizations, or the state, or the Nation through IS/N via unauthorized access, destruction, disclosure, modifications of information and/or denial of service. It is also considered undesirable potential loss.

As it is stated in the Glossary, regardless the specific term used, the basis constitutes all forms of (un)intentional, accidental or incidental, misuse or abuse, error, vulnerabilities, defect, fault and/or failure and their associated conditions. One may conclude that the concepts of cyber threat and cybersecurity threat are corresponding and reflect the features under consideration in full. The most famous cyberattacks on energy sector, military, transportation, entertainment banking and finance sphere are summarized in Table 1 (Desarnaud G., 2017; Livingston S., Sanborn S., Slaughter A., Zonneveld P., 2019; Kovacs E., 2018; Petcu A.G., 2022, Kaspersky E., 2017).

Year	Target	Act	Description and Consequences
1992	Ignalina nuclear-power station, (Lithuania)	Sabotage	Virus in the control system of a RBMK reactor.
1992	Emergency warning system at Chevron (USA)	Sabotage	An employee fired from the company hacked computers in charge of emergency warning system. A crash and explosion of toxic substances occurred at a refinery.
1999	Olympic (gas) pipeline in Bellingham (Washington D.C., USA)	Failure in SCADA (supervisory control and data acquisition system)	Oil spillage, 3 deaths and a number of injuries.
2001	Electricity operator (California, USA)	Sabotage attempt	Having got access to Independent Controlling System, the hackers failed.
2003	Davis-Besse	Cyberattack	Shutdown of the

	Nuclear power plant (Ohio, USA)	(Slammer)	parameter display system for 4 hours.
2008	Edwin I. Hatch nuclear power plant (Georgia, USA)	Human error (?)	Due to incorrect system update, there was an unintentional shutdown for 48 hours.
2008–2012	(Middle East)	Cyberattack (Narilam)	Data theft and small corruptions
2010	Natanz nuclear facilities (Iran)	Cyberattack (Stuxnet) by the Olympic Games	This type of sabotage damaged more than 900 uranium enrichment centrifuges.
2011	Energy industries (Iran, Sudan)	Cyberattack (Duqu)	Its operation relates to Stuxnet worm, but aims at gathering information (espionage) rather than destruction.
2011	Nuclear company Areva (France)	Cyberattack	Theft of non-critical data
2012	Energy companies (mainly, Middle East and North Africa, but also North America and Europe)	Cyberattack (Flame, Flamer, sKyWIper, Skywiper)	Espionage
2012	Saudi Aramco (Saudi Arabia) and RasGas (Qatar)	Cyberattack (Shamoon, W32.DistTrack)	Sabotage overwrote 30,000 hard disks, but had no impact on the operational network.
2012	Middle East	Cyberattack (Groove)	Time bomb
2013	Bowman Avenue Dam (New York, USA)	Cyberattack	Successful attempt to intrude in safety system. No consequences.
2013	Financial, military and media sectors (South Korea)	Cyberattack (Dark Seoul, Operation 1Mission) by Lazarus	32,000 frozen computer terminals terminated operation of 3 TV station, ATMs. Information leak of 200,000 citizens, 22,000 military personnel.
2013–2014	Energy and industrial	Cyberattacks (Energetic Bear)	Successful sabotage, data collection

	companies, aviation, education and healthcare system (USA and Europe)	using vulnerability of Windows and Citrix	(espionage).
2014	Sony (USA)	Cyberattack by Guardians of Peace	Related to Shamoon. Essential information leak.
2014	Korea Hydro and Nuclear Power, (South Korea)	Blackmail	Theft of plans and manuals of two reactors, electricity circuits, measures of radiation exposure in the zone, and data on more than 10,000 employees and 3 reactors closed.
2015–2017	250 energy American and European companies (electricity producers, electricity and oil distribution operators, equipment producers)	Phishing cyberattacks (Dragonfly)	Administrative operation under control, data collection (espionage), credit data theft and successful sabotage.
2016–2017	Government, industry, telecoms and transportation (Saudi Arabia)	Cyberattack (Shamoon 2)	Sabotage of 11 organizations. 35,000 computers collapsed.
2016–2017	Saudi Arabia and other countries of Middle East	Cyberattack (StoneDrill) by APT33 and Elfin	Related to Shamoon 2. Espionage.
2017	Saudi Arabia	Mamba Ransomware	Decryption of hard drives
2017	Petrochemical plants, power stations (Saudi Arabia)	Cyberattack (Trisis, Triton)	Sabotage that disables safety instrumented systems.
2018	Gas, oil and electricity operator (USA)	Cyberattack on cloud services	Stopping computers and ransom payment demand for encrypted files. At least, 5 companies stopped

			pipeline operation. Some big energy delivers had to stop transactions, under receiving or not receiving money due to miscalculated bills.
2018 – 2021	Oil and gas industry (Saudi Arabia, the UAE, India, Scotland and Italy)	Cyberattack (Shamoon 3)	Oil and gas services company Saipem reported that the malware wiped 300–400 servers and up to 100 PCs (4,000 machines).
2019	USA	Cyberattack (Dridex)	Banking trojan helped to steal more than 70 US dollars from victims' bank accounts.
2021	Natanz nuclear facilities (Iran)	Sabotage or cyberattack	A power blackout damaged machine. Authorities suspect cyber terrorism
2021	Colonial Pipeline (Texas, USA)	Cyberattack (data encryption) by Anonymous Group	13 states introduced emergency regime, 45% transit of East Coast was blocked for 6 days. A ransom in 75 bitcoins was paid (FBI succeeded in tracing and returning 66 bitcoins).

Table 1 – Most Commonly Known Cyberattacks Around the World.

National Cyber Threat Assessment from Canadian Centre for Cyber Security provides a shorter version with an intriguing ambiguity. A cyber threat is an activity intended to compromise the security of an information system by altering the availability, integrity or confidentiality of a system or the information it contains[1]. The security of an information system resembles of information security that protects data in general, while cybersecurity involves

[1] Canadian Centre for Cyber Security. *National Cyber Threat Assessment. An Introduction to the Cyber Threat Environment.* Available at: https://cyber.gc.ca/sites/default/files/cyber/publications/Intro-ncta-2020_e.pdf.

network, application, operational, cloud and IoT securities, which implies the processes and technologies as well (IT governance).

RESULTS AND DISCUSSION

Classification

The scholars note the lack of uniform terminology and unified classification of cybersecurity threats. The latter includes the activities of hackers (including hacktivists, botnet operators, phishers, spammers, authors of spyware and/or malware), insiders (commercial spies and disgruntled employees), cyber-terrorists, cyber-extremists, individual organized crime groups and even foreign intelligence services, as well as man-made disasters (See Table 2).

Type	Characteristics
Botnet	Hackers operating some systems to coordinate attacks and dissimilate phishing, spam and malwares
Organized Criminal Groups	Attacks often aim at monetary gain via spam, phishing, spy- or malware to steal personal data and e-fraud
Foreign Intelligence Service	One of the goals is information warfare and critical infrastructure decommission
Hackers (Including Hacktivists)	Applying malware or other instruments in order to cause failure and serious damage
Insiders	Disgruntled employees of an organization who do not obviously have specific knowledge in IT, but have access to ESM. The motive is often revenge which harms not only company's reputation, but critical infrastructure facilities
Phishing	Persons or small groups that steal personal data or information in general in order to take advantage via spam and spy- and/or malware software
Spammers	Persons or organizations that send e-mails with hidden or false information in order to sell produce, activate phishing, spy- or malware software and attacks on organization
The Authors of Spy- and/or Malware Software	Persons or organizations that create or dissimilate spy- or/and malware software, computer virus and worms which damage files and hard drives
Cyber-Terrorism and Cyber-Extremism	Persons or organizations that seek to destroy, disable or use critical infrastructure to compromise national security, weaken a nation's economy and use phishing schemes or spy- and/or malware to obtain funds or gather sensitive

	information
Commercial Spies	More professional approach rather than insiders and the motivation is private gain

Table 2 – Most Commonly Known Cyberattacks Around the World.

In the beginning, hacker had no destructive nature. Their experiments with the digital space in combination with the emerging idea of selectivity and elitism resulted in diving into white and black or crackers. The latter are the major deviants in the digital environment and are engaged in obtaining unauthorized access to ITS and information. Hacktivists pursue political goals while hacking, stealing, disseminating confidential information and attacking critical infrastructure in cyberspace (Ovchinsky V. S., 2016: 193, 194). There are also so-called thrill-seekers who get satisfaction being a cyber threat actor and shows the lowest level of sophistication (Canadian Centre for Cyber Security).

So-called pirates either use programs developed by hackers or work on their own and can be classified depending on their functions: couriers and distributors. Taking the spam as an example, one may assume that database spammers create lists of user addresses and cracker spammers create programs that organize data, which describes couriers. In general, spammers generate and send unsolicited, intrusive advertising messages with hidden or false information to sell products, carry out phishing scams, distribute spy- and malware, or facilitate cyberattacks on organizations and, inter alia, mailing spammers or distributors are involved in sending spam.

Therefore, phishing is a popular cyberattack that uses e-mail or a malicious website to literally infect a computer with malware or collect sensitive information. E-mails often prompt users to open a link or attachment containing malicious code, after which the phisher gains access to the information contained in the device and takes control over the system. Malware includes viruses and ransomware, spyware and banking trojans (U.S. Small Business Administration).

Some attacks indicate that hacker organizations also pursue apolitical venal goals. For instance, the DarkSide group committed a cyberattack on the Colonial Pipeline on May 7, 2021. They encrypted 100 GB of data, having previously bought 740 GB of data from the French branch of Toshiba and gained access to administrative networks, subsequently blocking the toll collection system. 13 states had to declare state of emergency, which accounted for the transit of 45% of the consumption of the U.S. East Coast to 260 delivery points was suspended (about 3 million barrels per day). In 6 days, gas prices broke the record of the last 6 years (Bowcut S., 2021). The cyberattack affected

not only the filling stations, but also school classes, which had to be online. After the paying approximately 4.4 million US dollars in cryptocurrency (75 bitcoins), on May 13, 2021, operation was restored. The U.S. Department of Justice discloses that FBI succeeded in partial returning the ransom, but there is no data about accurate sum (63,5–66 bitcoins). In April 2021, in Pennsylvania, hackers almost dropped critical doses of cleaning chemicals into the water supply (in February a similar incident occurred in Florida) (Rspectr, 2021). In 2017, hackers broke into the computer networks of 10 U.S. power plants, including the Wolf Creek Generating Station in Kansas (Vadimova E., 2021). As a result, cybersecurity crimes have been seen as elements of terrorist activity (Lewis J. A., 2002).

Insiders are technical personnel who commit computer offenses, causing a failure in the ITS or stopping the production, or deforming the software. At the individual psychological level, the motives are venal intent (as to commercial spies) and sabotage and revenge (as to employees). The second phenomenon is more common (Dolgova A. I., 2020: 836). Their methods include the following groups. Firstly, legally reprogramming via a trojan horse, a computer virus and worm. Secondly, data illegal activity includes a salami slice which implies using a fake account to charge small sums and impersonation which involves unauthorized use of a user profile to get access. Thirdly, such programs as super-zapping and a logic bomb that either replaces anti-theft systems or adds additional app (Misbrener K., 2019).

In the considered sphere American criminologists classify the offenses into 3 categories. Firstly, cybercrimes as white-collar offense. Secondly, such Internet crimes distributing sexual material, DDoS, illegal copyright infringement, internet security fraud, theft, Ponzi or pyramid schemes, non-delivery of goods or services. Thirdly, computer crimes are theft of services and software, unauthorized use of computers, data usage for personal gain, virus or worm (Siegel L. J., 2006: 429–432). Classifying computer-related crimes, one should take into account what a computer constitutes: object (theft of hardware or software), subject (attempt to interfere with the services provided by computers.) and instrument (while committing traditional crimes) (Kim, C., Newberger, B., Shack, B., 2012: 443–488). British scholars also focus on the role of a computer: whether it is an instrument and an aim or complement to increase scale or area, but they used to other notions, inter alia, online harm, but it deals only with the harm suffered by individuals (Department for Digital, Culture, Media & Sport, 2020). Saudi Arabia stands for traditional division into crimes against people, property and government depending on object of a crime (Alabdulatif A., 2018). First violations include cyber harassment, stalking, distribution of children pornography, spoofing, fraud, human trafficking,

identity theft and libel or slander and attacks against ICS, SCADA, DCS. The second one involves DDoS, hacking, virus transmission, cyber and typo squatting, cyber-vandalism, copyright infringement and IPR violations. The third type covers nnauthorized access to essential information, hacking, hacktivism, cyberwar, cyberterrorism, pirated software.

It is also worth mentioning that the terminology is still developing. Although the notion of computer crime originally emerged in the early 60s (Volevodz A. G. 2002: 17). However, the foundations of the study were laid by Donn B. Parker in the early 80s (Shestak V. A., 2020: 3). He formulated such a specific term as computer abuse which implies computer use for improper or illegal activities. Subsequently Computer Fraud and Abuse Act of October 16, 1986 was adopted. Taking into account the U.S. current legal framework, the scholars distinguish five forms of computer misconduct: unauthorized access, unauthorized use, dishonest manipulation or alteration of data, sabotage, and theft of information. However, this classification is also not exhaustive and the terms cybercriminal and computer criminal may replace each other (Dzafarli V. F., 2021: 14).

Causes and Environmental Reasons for Emerging Cybersecurity Threats

A system of social factors and environmental reasons involves internal and environmental causes that may be defined as following: a cause is socio-psychological determinant that is developing in specific circumstances as accelerator, contributing to crime situation (Kuznetsova N. F., 2004).

Criminologists outline general and specific causes, objective and subjective approaches, social and economic factors, taking into account psychological phenomena that shape the modern model of human behavior. As for delinquency in general, reasons include the aspirations and skills of the individual withal a real opportunity to fulfil them through a device, the ease and availability of acquiring necessary knowledge and tools, community indifference or approval, antisocial behavior, as well as organizational, legal and technical defects of both particular companies and service providers. For instance, in 2019–2020 more than 33 thousand of users were hacked via Microsoft Exchange and Orion of SolarWinds. Half of the data was leaked. A similar incident occurred to Kaseya July 2, 2021, but it was immediately detected and prevented (Willett, M., 2021).

Scholars single out also economic reasons related to it: artificially inflating prices for software products, unfair trade and, as a result, obtruding malicious and anti-virus software. Such slow are the detection and adjustment that they constantly incur additional costs (Bailey T., Maruyama A., Wallance

D. T. 2020). Modernization and remote monitoring have always been and will be expensive. For instance, in order to keep updated, American local energy company has to spend more than 100 million of US dollars annually (Dwight L.J., Duke E., 2019).

Despite large offer of necessary programs to ensure the enterprise or company operation, the quantity is likely to fail to satisfy in terms of quality. Some vendors use unsecured computers or unproven technologies while developing applications and updates and neglect cybersecurity, believing that it is not their responsibility.

Some companies prefer to use specialized devices developed by startups due to limited funds. This issue has been deteriorating more and more during the pandemic. Often is a built-in security system in charge of proper operation, but they are not always capable to prevent large-scale incidents. Also, the using models of different generations and from different manufacturers reduces the data security and access to it, according to the Cybersecurity and Infrastructure Security Agency (U.S. Department of Homeland Security). The continuing decentralized nature of management exacerbates the deplorable state of the cybersecurity (Bailey T., Maruyama A., Wallance D. T. 2020).

Neglecting the physical security of critical infrastructure utilities, outdated or unreliable software, the lack of proper control over personnel and criteria for sensitive information or OPS and access to it, failure to provide mechanisms for non-disclosure of trade secrets are the specific circumstances. It is worth noting that green energy utilities are more vulnerable. Recent wind farm security studies show that physical vulnerabilities as an easy-to-pick padlock and lack of network security allow to take control over the entire wind farm network in minute. It results in damage 10–30 thousands of US dollars per hour (or 252–720 thousands of US dollars per day) or even complete destruction of the turbines (Staggs J. 2017).

Objective determinants are the disproportion between countermeasures and rapid development of crime, inadequate cost of maintenance and, as a result, the low security of the utilities, whereas the subjective ones include social and psychological deprivation, irresponsibility or permissiveness, global spread of radical ideologies such as violence, hatred, mass antisocial consciousness (Kleymenov M. P., 2018: 69).

Remote access and digital space limits feedback and makes it possible to take full advantage of anonymity. What gives rise high online criminal rate is such special conditions as greater accessibility of virtual objects, no need for active physical actions, a sense of permissiveness and impunity, remoteness from the victim. Thus, it causes aspirations of the individual and the possibility to introduce through an electronic device. On this ground cybercriminals less

fear of being detected and have confidence in being beyond the reach. The so-called crisis of conscience was noted as early as the 70s in the United States due to systematic everyday violence, rooted even during the campaigns to exterminate the American Indians (Schur, E.M., 1969).

Cyberspace is a perfect environment for hiding criminal activity and engaging a wider range of individuals who used to be less likely inclined to commit a crime. One may portrait cybercriminal personality by tracing the following stages:

(1) Deep dive in e-world in which anonymity reigns;
(2) Emerging phenomenon of virtual personality;
(3) Escapism and loss of identity;
(4) Internet addiction or behavioral addiction as a form of deviant behavior;
(5) Getting into a specific subculture of cybercrime.

As a result, cybercriminals quickly make a fortune, that is why such a way to earn is becoming enticing (Dzafarli V. F., 2021: 56–60, 65, 85, 96–99).

Cybersecurity crime is often characterized by high latency or even ultra-high latency. Some researchers treat it as a means of achieving such inimical consequences as damage to national interests, crashes, environmental disasters, deaths or injuries and economic loss, thus encroaching on various objects of crime. They can be either organized or transnational, or local (Dolgova A. I., 2020: 831–833).

CONCLUSIONS

In conclusion, a cybersecurity threat is a complex phenomenon that includes any circumstance, condition and event that jeopardizes the object of the attack via the ITS, computer system or network through unauthorized access, destruction, disclosure, data modification and/or denial of equipment and results from (in)actions. Actions is responsibility of an offender, whereas apathy untimely response accounts for a victim. Unfortunately, it is impossible to consider in detail all the classifications of cybersecurity threats, however, authors have given a general description of particular types of the cyber threats and summarized it in Appendix B. Not only do incipient technologies change the social co-existence and complicate human interaction but are involved in evolving innovative crime and brand-new threats. Exacerbation of the criminogenic situation roots from a range of elements of an individual's social structure in interaction with the environment that have been examined by the authors.

At first, there was a lack of proper control, low security of the object of criminal encroachment, lagging counteraction. The intensive improvement of the various methods to commit a crime led to the failure to take sufficient measures in time. In order to ensure the security of operated computers, their systems and networks it would have taken too high costs. The lack of special units in law enforcement bodies also boosted crime situation in digital space. The more advanced technologies appear, the more sophisticated crimes become and more skilled personnel is on demand. Despite the efforts, a gap between the prevention measures and cyber criminality remains. On these grounds cybersecurity threats are one of the most acute problems throughout the world and should be studied more thoroughly.

REFERENCES

Alabdulatif, A. (2018). *Cybercrime and analysis of laws in Kingdome of Saudi Arabia*. [Master of Science in Information System Security, Technology of University of Houston]. Available at: https://uh-ir.tdl.org/bitstream/handle/10657/3107/ALABDULATIF-THESIS-2018.pdf?sequence=1.

Bailey, T., Maruyama, A. & Wallance, D. (2020). *The energy-sector threat: How to address cybersecurity vulnerabilities.* McKinsey & Company, 2020. Available at: https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/the-energy-sector-threat-how-to-address-cybersecurity-vulnerabilities.

Desarnaud, G. (2017). *Cybersecurity attacks and energy infractutures. Anticipating Risks.* Études de l'Ifri. Available at: https://www.ifri.org/sites/default/files/atoms/files/desarnaud_cyber_attacks_energy_infrastructures_2017_2.pdf.

Belous, A.I. (2020). *Cybersecurity of fuel and energy complex facilities.* Concepts, methods and tools for ensuring. Moscow, Vologda: Infra-Inzheneriya.

Black Kite (2021). *The 2021 ransomware risk pulse:* energy sector. Ransomware on the Rise Across Critical Infrastructure. Available at: https://blackkite.com/wp-content/uploads/2021/09/The-2021-Ransomware-Risk-Pulse-_-Energy-Sector.pdf.

Bowcut, S. (2021). C*ybersecurity in the energy industry.* Cybersecurityguide. Available at: https://cybersecurityguide.org/industries/energy/.

Canadian Centre for Cyber Security. N*ational Cyber Threat Assessment.* An Introduction to the Cyber Threat Environment. Available at: https://cyber.gc.ca/sites/default/files/cyber/publications/Intro-ncta-2020_e.pdf.

CISA. *Bad Practices.* Available at: https://www.cisa.gov/BadPractices.

Department for Digital, Culture, Media & Sport (2020). *Online Harms White Paper 2020*. Available at: https://www.gov.uk/government/consultations/online-harms-white-paper/online-harms-white-paper.

Duke Energy. (2019). *Accounting request related to cybersecurity informational technology–operational technology program*: letter to Kimberly D. Bose, US Federal Energy Regulatory Commission No. AC19-75-000. Available at: https://www.federalregister.gov/documents/2019/03/22/2019-05482/duke-energy-corporation-notice-of-filing.

Dolgova, A.I. (2020). *Criminology*. Moscow: Norma.

Dzafarli, V. F. (2021). *Criminology of cybersecurity: Criminological means of crime prevention in the field of information and communication technologies*. (S. Ya. Lebedeva, Ed.). Moscow: Prospekt.

IT Governance. *What is Cyber Security?* Definition and Best Practices. Available at: https://www.itgovernance.co.uk/what-is-cybersecurity.

Kaspersky, E. (2017). S*toneDrill:* We've Found New Powerful 'Shamoon-ish' Wiper Malware – and It's Serious. Official Blog of Eugene Kaspersky. Available at: https://eugene.kaspersky.com/2017/03/06/stonedrill-weve-found-new-powerful-shamoon-ish-wiper-malware-and-its-serious/.

Kaspersky Laboratory (2020). *Kaspersky Security Bulletin.* Statistics 2020. Available at: http://go.kaspersky.com/rs/802-IJN-240/images/KSB_statistics_2020_ru.pdf.

Kim, C., Newberger, B. & Shack, B. (2012). Computer Crimes. *American Criminal Law Review.* 49(2), 443-488.

Kleymenov, M. P. (2018). *Criminology*. Moscow: NORMA.

Kovacs, E. (2018). *Shamoon 3 Attacks Targeted Several Sectors.* Security Week. Available at: https://www.securityweek.com/shamoon-3-attacks-targeted-several-sectors.

Kuznetsova, N. F. (2004). *Criminology*. (N. F. Kuznetsova, V. V. Luneev, Ed.). Moscow: Wolters Kluwer.

Livingston, S., Sanborn, S., Slaughter, A., Zonneveld, P. (2019). *Managing cyber risk in the electric power sector.* Emerging threats to supply chain and industrial control. Deloitte. Available at: https://www2.deloitte.com/content/dam/insights/us/articles/4921_Managing-cyber-risk-Electric-energy/DI_Managing-cyber-risk.pdf.

Lewis, J. A. (2002). *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats Center for Strategic and International Studies.* Washington, D. C.

Misbrener, K. (2019). *Cyberattacks threaten smart inverters, but scientists have solutions.* Solar Power World. Available at: https://www.solarpowerworldonline.com/2019/04/cyberattacks-threaten-smart-inverters-but-scientists-have-solutions/.

Nescout. (2021). *Threat Intelligence Report 2021*. Available at: https://www.netscout.com/threatreport.

National Institute of Standards and Technology (NIST). *Cyber Attack*. Available at: https://csrc.nist.gov/glossary/term/cyber_attack.

National Institute of Standards and Technology (NIST). *Cyber incident.* Available at: https://csrc.nist.gov/glossary/term/cyber_incident.

National Institute of Standards and Technology (NIST). *Cyber Security.* Available at: https://csrc.nist.gov/glossary/term/cyber_security.

National Institute of Standards and Technology (NIST). *Cyber Threat.* Available at: https://csrc.nist.gov/glossary/term/cyber_threat.

National Institute of Standards and Technology (NIST). *Cybersecurity.* Available at: https://csrc.nist.gov/glossary/term/cybersecurity.

National Institute of Standards and Technology (NIST). *Cybersecurity event.* Available at: https://csrc.nist.gov/glossary/term/cybersecurity_event.

National Institute of Standards and Technology (NIST). *Cybersecurity Incident.* Available at: https://csrc.nist.gov/glossary/term/cybersecurity_incident.

National Institute of Standards and Technology (NIST). *Cyberspace*. Available at: https://csrc.nist.gov/glossary/term/cyberspace.

National Institute of Standards and Technology (NIST). *Cyberspace attack.* Available at: https://csrc.nist.gov/glossary/term/cyberspace_attack.

Ovchinsky, V. S. (2016). *Criminology of the Digital World*. Moscow: Norma. INFRA-M.

Petcu, A. G. (2022). *Emotet Malware Over the Years: The History of an Infamous Cyber-Threat.* Heimdal security. Available at: https://heimdalsecurity.com/blog/emotet-malware-history/.

Rspectr. (2021) *Bulk encryption weapons.* Available at: https://www.rspectr.com/articles/828/oruzhie-massovogo-shifrovaniya.

Schur, E. M. (1969). *Our criminal society:* the social and legal sources of crime in America. New Jersey: Prentice-Hall.

Shestak, V. A. (2020). Foreign experience in the legal regulation to counter cybercrime. SSRN, 2020 *Criminal Law:* development strategy in the XXI century. Materials of the XVII International Scientific-Practical

Conference, 23.01-24.01.2020. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3524513.

Siegel, L. J. (2006). *Criminology*. Thomson Wadsworth.

Staggs, J. (2017). *Adventures in attacking windfarm control networks*. Black Hat USA. Available at: https://www.blackhat.com/us-17/briefings/schedule/#adventures-in-attacking-wind-farm-control-networks-6394.

U.S. Small Business Administration. *Stay safe from cybersecurity threats.* Available at: https://www.sba.gov/business-guide/manage-your-business/stay-safe-cybersecurity-threats.

Vadimova, E. (2021). Digital against Fuel and energy complex. *Oil and Capital*. Available at: https://oilcapital.ru/article/general/29-06-2021/tsifra-protiv-tek.

Volevodz, A. G. (2001). *Combating computer-related crime:* the legal framework for international cooperation. Moscow: Yurlitinform.

Willett, M. (2021) Lessons of the SolarWinds Hack. *Survival*. 63(2): 7-26.

World Economic Forum. (2021). *The Global Risks Report 2021*. Available at: http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf.

The Law, State and Telecommunications Review / Revista de Direito, Estado e Telecomunicações

Contact:
Universidade de Brasília - Faculdade de Direito - Núcleo de Direito Setorial e Regulatório
Campus Universitário de Brasília
Brasília, DF, CEP 70919-970
Caixa Postal 04413

Phone: +55(61)3107-2683/2688

E-mail: getel@unb.br

Submissions are welcome at: https://periodicos.unb.br/index.php/RDET

Dados da Publicação

DOI: https://doi.org/10.26512/lstr.v15i2
SCOPUS Q3 - MIAR Index 9.6 - SJR H-Index 4

ISSN: 1984-9729 / **EISSN**: 1984-8161 - **Periodicidade**: (Mínima) Semestral.
Linha editorial: http://periodicos.unb.br/index.php/RDET/about
Avaliação das submissões: método de avaliação cega por pares (duplo cego), por intermédio de submissões eletrônicas administradas no sistema SEER, do IBICT, no link http://periodicos.unb.br/index.php/RDET/about/submissions, em que os manuscritos são distribuídos aos avaliadores sem identificação de autoria.
Política de arquivamento: sistema LOCKSS, da Universidade de Stanford (*Stanford University Libraries*), via Rede Brasileira de Serviços de Preservação Digital Cariniana, do IBICT; projeto de preservação de longo prazo do DOAJ (*Directory of Open Access Journals*); e Biblioteca do Senado Federal do Brasil.
Indexação em bases de pesquisa: SCOPUS (Elsevier); CROSSREF; ROAD; THE KEEPERS; LATINDEX (28283); EBSCO*host* research databases (EBSCO Publishing Inc.); Gale Group; AE Global Index; OAI (*Open Archives Initiative*) - DOAJ (*Directory of Open Access Journals*); WorldCat; Google Scholar; The European Library; CIEPS (Centre International d'Enregistrement des Publications en Série); Sistemas SEER e Diadorim, do IBICT.
Indexação em bibliotecas: Rede Virtual de Bibliotecas do Congresso Nacional (RVBI); Erasmus Universiteit Rotterdam; Universidade de Lisboa.
Endereçamento permanente: LexML e DOI.

Normas para Submissão de Manuscritos

Procedimento de submissão: http://periodicos.unb.br/index.php/RDET/information/authors
Data de publicação da RDET: anualmente, no mês de maio.
Data limite de submissões: submissões encaminhadas até 15 de janeiro serão consideradas para publicação no volume do ano correspondente, podendo-se estender o prazo a critério do Conselho Editorial.
Idiomas aceitos: português, inglês e espanhol.
Especificações de forma: os manuscritos deverão ser encaminhados por intermédio do sistema eletrônico de submissão constante do link acima (*procedimento de submissão*) em formato *Microsoft Word*, *LibreOffice* ou *iWorks*, em espaço simples, fonte Times New Roman 12 ou equivalente, com mínimo de três mil palavras (em torno de 15 páginas) e máximo de vinte mil palavras (em torno de 50 páginas), dele constando as referências bibliográficas segundo modelo de citação no próprio texto (AUTOR ano) ou em referências completas em notas de rodapé.
Resumo/Abstract: os manuscritos deverão ser precedidos de resumo em língua portuguesa de até 150 palavras e de sua tradução para a língua inglesa (*abstract*).
Palavras-chave/Keywords: o autor deve propor 5 palavras-chave em português e 5 em inglês.
Biografia: a biografia sintética do autor de até 5 linhas deverá ser preenchida no sistema de submissões online da RDET quando do encaminhamento do artigo para avaliação. A biografia encaminhada pelo autor será incorporada ao volume de publicação em caso de aprovação do manuscrito.
Modelos a serem seguidos para submissão:
- https://periodicos.unb.br/index.php/RDET/information/authors, inclusive resumo e abstract estruturados.

Journal Info

DOI: https://doi.org/10.26512/lstr.v15i2
SCOPUS Q3 - MIAR Index 9.6 - SJR H-Index 4

ISSN: 1984-9729
EISSN: 1984-8161
Periodicity: annual issues uninterrupted since May 2009 and two annual issues in May and October uninterrupted since May 2018.
Mission/Scope/Focus: http://periodicos.unb.br/index.php/RDET/about
Submission process: authors are requested to submit their papers following the instructions at http://periodicos.unb.br/index.php/RDET/about/submissions. The journal adopts the double-blind peer review process.
Archiving policy: LOCKSS-CARINIANA, DOAJ and Brazil's Senate Library.
Indexation: SCOPUS (Elsevier); CROSSREF; ROAD; THE KEEPERS; LATINDEX (28283); EBSCO*host* research databases (EBSCO Publishing Inc.); Gale Group; AE Global Index; OAI (*Open Archives Initiative*) - DOAJ (*Directory of Open Access Journals*); WorldCat; Google Scholar; The European Library; CIEPS (Centre International d'Enregistrement des Publications en Série); Sistemas SEER e Diadorim, do IBICT.
Permanent Web Identifier: LexML and DOI.

Manuscript Submission Process

Authors, please submit here: http://periodicos.unb.br/index.php/RDET/about/submissions
Submission time frame: The L.S.T.R. submission process is open all year round. Papers selected will be tentatively scheduled for publishing in the next issue.
Languages accepted: English, Spanish and Portuguese.
Formal requirements: The easiest way to follow this journal's formal requirements is to download the template in English from the L.S.T.R. website, in the section "Author Guidelines" and replace the content with your own material. The template file contains specially formatted styles (e.g., Normal, Heading, Footer, Abstract, Subtle Emphasis, and Intense Emphasis) that will reduce the work in formatting your final submission. The following instructions are already embedded in the template, but they are transcribed below in case you prefer to apply them directly to your paper. Please use the following coordinates for the page setup: Top (1.93 cm); Bottom (1.93 cm); Inside (1,93 cm); Outside (1,52 cm); Gutter (0,36 cm); mirror margins; page size customized for width (15,24 cm) and height (22,86 cm); different odd and even pages; Layout from Edge (Header: 0,89 cm; Footer: 0,76 cm). Right margins should be justified, not ragged. Please use a 10-point Times New Roman font or, if it is unavailable, another proportional font with serifs, as close as possible in appearance to Times New Roman 10-point. On a Macintosh, use the font named Times and not Times New Roman. Also, quotations of more than two lines should be written in Times New Roman, 10, scale 90%, line spacing exactly 10 pt. Legal texts should be cited as Times New Roman, 10, scale 80%, line spacing exactly 10 pt, "Don't add space between paragraphs of the same style" marked, indentation left 1.78 cm and right 1.78 cm. For reference purpose, please use the ABNT NBR style or APA.
Structured abstract: The L.S.T.R. adopts structured abstracts embedded in the template below.
Template: https://periodicos.unb.br/index.php/RDET/information/authors.