ISSN 2713-2749

Legal Issues in the DIGITAL AGE

Вопросы права в цифровую эпоху

2/2023

Volume 4

Legal Issues in the **DIGITAL AGE**

Publisher
National Research University Higher School of Economics

2/2023

ISSUED QUARTERLY VOLUME 4

Articles

Comment

Review

Legal Issues in the **DIGITAL AGE**

Legal Issues in the **DIGITAL AGE**

ISSUED QUARTERLY

"Legal Issues in the Digital Age" Journal is an academic quarterly e-publication which provides a comprehensive analysis of law in the digital world. The Journal is international in scope, and its primary objective is to address the legal issues of the continually evolving nature of digital technological advances and the necessarily immediate responses to such developments.

The Digital Age represents an era of Information Technology and Information Communication Technology which is creating a reliable infrastructure to the society, taking the nations towards higher level through, efficient production and communication using digital data. But the digital world exposes loopholes in the current law and calls for legal solutions.

"Legal Issues in the Digital Age" Journal is dedicated to providing a platform for the development of novel and analytical thinking among, academics and legal practitioners. The Journal encourages the discussions on the topics of interdisciplinary nature, and it includes the intersection of law, technology, industry and policies involved in the field around the world.

"Legal Issues in the Digital Age" is a highly professional, double-blind refereed journal and an authoritative source of information in the field of IT, ICT, Cyber related policy and law.

Authors are invited to submit papers covering their state-of-the-art research addressing regulation issues in the digital environment. The editors encourage theoretical and comparative approaches, as well as accounts from the legal perspectives of different countries.

The journal is registered in the Federal Service of Supervision of Communications, Information Technology and Mass Media. Certification of registration of mass media серия Эл № ФС77-83367

ISSN 2713-2749

Address: 3 Bolshoy Triohsviatitelsky Per.,
Moscow 109028, Russia
Tel.: +7 (495) 220-99-87
https://digitalawjournal.hse.ru/
e-mail: lawjournal@hse.ru

Legal Issues in the Digital Age. 2023. Vol. 4. No. 2.
Вопросы права в цифровую эпоху. 2023. Том 4. № 2.

Articles

Research article
УДК: 347.1
DOI:10.17323/2713-2749.2023.2.4.25

Digital Currency in Modern Russia: Legal Essence and Place in Turnover

Alexander Ivanovich Goncharov[1], Andrey Nikolaevich Sadkov[2], Vitaly Andreevich Sadkov[3], Davud Akhmedovich Davudov[4]

[1, 2, 4] Volgograd State University, 100 University Avenue, Volgograd 400062, Russia.
[3] Volgograd Academy of the Internal Ministry, 130 Historical Str., Volgograd 400075, Russia.
[1] goncharov@volsu.ru, GAI-AlexanderGoncharov@yandex.ru
[2] sadkov@volsu.ru
[3] wrendek@mail.ru
[4] davudov@volsu.ru

Abstract

The information society of our time is characterized by large-scale and intensive use of computer technologies in most areas of economic relations. Many procedures of interaction between people and business entities are computerized and digitized. Remote technologies used on the Internet allow groups of people, in particular, to perform mathematical calculations and use the data obtained in the interests of participants in such collective calculations. The totality of such electronic data in the Russian Federation is legitimized as a digital currency. The legal content and place of digital currency in property turnover and the system of its state regulation seems to be an actual object of research and development. The article solves the following tasks based on the study of domestic legislation and academic publications: the legal content of digital currency as encrypted information and the type of other property is substantiated; legislative constructions providing for the functioning of digital currency as a means of payment and investment are analyzed; qualitative features of digital currency inherent in the object of civil rights are identified. Digital currency is studied as a set of electronic data and information, the author's definition of digital currency

is presented. Digital currency in circulation is disclosed as encrypted information, settlement and exchange equivalent and investment asset. The fallacy of the legislative recognition of digital currency as a means of payment is argued. The legal constructions on the possibility of using digital currency as an investment are critically evaluated. The features of turnover and the development of regulatory regulation of digital currency in the Russian legal order are analyzed. A legal analysis of the parliamentary bill on the "mining" of digital currencies is being carried out. The essence is substantiated; the definition of activities aimed at obtaining digital currencies by mathematical calculations on private computers is formulated. Digital currency is considered as a kind of other property, the conclusion is made about the possibility of recognizing the "coin" of digital currency as an object of civil rights. The article examines the modern doctrinal developments of mainly Russian researchers on the subject of exploration, as well as encyclopedic and normative sources. Proposals are being made to improve the legal regulation of public relations in the field of property turnover of digital currency.

Keywords

digital currency; information technologies; mathematical calculations; information in electronic form; Internet; legislation; property turnover; other property.

Acknowledgements: The study was prepared in accordance with a grant from the Russian Science Foundation (project No. 23-28-00475).

The paper is published within the project of supporting publications of authors of Russian educational and research organizations in the HSE academic publications.

For citation: Goncharov A.I., Sadkov A.N., Sadkov V.A., Davydov D.A. (2023) Digital Currency in Modern Russia: Legal Essence and Place of Turnover. *Legal Issues in the Digital Age,* vol. 4, no. 2, pp. 4 –25. DOI:10.17323/2713-2749.2023.2.4.25

Introduction

About 14 years ago groups of anonymous individuals acting on a proactive basis and using specific computer programmes for rather unusual purposes began appearing on the Internet. And one such group began to make extensive use of a software programme called 'Bitcoin', which provides for the calculation of 21 million special 'coins'. Each member of this group could, using an appropriate software algorithm on special computer equipment, mathematically compute a 'coin' which, in consensus with the software algorithm and on the approval of all other members of that group, would be added to the chain of 'coins' already computed. Thus, the chain is getting longer every year, the computations are slowing down, and approximately by the year 2140 all 21 million 'coins' of 'Bitcoin' will have been calculated. Inside their group, the anonymous actors record the data on

the calculated 'coins' into special 'electronic wallets' and then use them as a payment instrument, as monetary surrogates. There are ATMs in some foreign embassies in Moscow exchange said monetary surrogates for US dollars, and payment service providers publish offers in Internet to exchange Bitcoin coins and other digital currencies for Russian roubles.

The software algorithms and the subsequent transmission of data within Internet communications must involve encryption, also called cryptoprotection. This is how, without any legitimate basis, the term 'cryptocurrency' was born about 10 years ago and has become globally widespread. However, the 'coins', the monetary surrogates calculated within groups of anonymous actors, do not belong to state currencies. By 2023, the term 'digital currency' has already been legitimised in a number of jurisdictions, although the application of both the first part of the term, i.e., 'digital', and the second part of the term, i.e., 'currency', is highly controversial. 'Digital' is apparently supposed to reflect the binary code of the software algorithms which use two digits, 0 (zero) and 1 (one). 'Currency' is apparently to meant to refer to the use of these monetary surrogates as a means of payment in exchange for the goods, works, services, etc. Federal Law No. 259-FZ of 31 July 2020 'On Digital Financial Assets, Digital Currency and Amendments to Certain Legislative Acts of the Russian Federation' (henceforth Federal Law 259-FZ) legitimated the disputed term. According to Article 1 (3) of the Law, digital currency is a collection of electronic data. The words 'digital code', 'digital sign' may be used along with the basic term. The legislator emphasises from the very first article of the law that digital currency, although it may be accepted as a means of payment and as an investment in certain local information systems of individuals, cannot replace public money and is not an international currency or unit of account.

The legislator also defines in the said Law main uses of digital currency as an object of property turnover: first, digital currency may be offered and may be accepted as a means of payment, e.g., for the calculation of digital currency 'coins' themselves; second, digital currency may be offered and may be accepted as an investment. The above legislative provisions raise questions: why and who needs in these new unofficial means of payment; and, is digital currency itself an object of investment or is digital currency a new investment instrument? In this context, we consider the legal content and place of digital currency in the system of state regulation of property turnover in present-day Russia to be an important object of scientific research. It should be clarified that 'cryptocurrency' does not represent any

interest from a scholar and legal point of view and is not explored in this paper, because it does not exist here in Russia as a legal category.

Based on Russian law and doctrine, the article substantiates the legal content and understanding of digital currency as encrypted information, a special kind of property, and an object of civil rights. The study aims to develop knowledge about digital currency in the interpretation of Russian law and achieves this aim by solving the respective tasks: first, substantiate the legal content of digital currency as encrypted information and a type of other property; second, assess legislative constructions providing for the functioning of digital currency as a means of payment and investment; third, identify the qualitative features of digital currency inherent in an object of civil rights. Authors have carried out the study on the basis of materialistic positivism combined with the application of general research, special research and special methods of knowledge. In particular, were used special methods of legal science that included historical and retrospective method, comparative legal method, systematic research one, formal legal one.

1. Digital Currency as a Collection of Electronic Data and Information

According to the Bank for International Settlements, in 2022 more than 80% of national central banks developed terms and procedures for the introduction of public digital currencies in their national jurisdictions. Digital currencies of central banks currently operate in at least 10 countries. Notably, the Commonwealth of the Bahamas and Cambodia pioneered this path in 2020. In Russia, the central bank's digital currency was not yet legally regulated as of February 2023[1].

Federal Law 259-FZ stipulates in Clause 3, Article 1 on the subject of regulation and the scope of the law that digital currency is recognised as a set of electronic data. The legislator gives in brackets two more synonyms for the definition of digital currency as identical to this data set: digital code; digital symbol. These electronic data (digital codes and symbols) are recorded and exist in a special information system. Then, the law stipulates two ways to use such electronic data (digital codes and symbols): they may be offered and accepted as a means of payment, or, alternatively, without

[1] Central Bank of Russia. Cryptocurrencies: trends, risks, measures. A report. Available at: URL: htpp.:www.cbr.ru.content/document/file/132241/ consultant_paper_20012022pdf (accessed: 22.02.2023)

being offered first, may be accepted as a means of payment (e.g., for performing mathematical computations); they may be used as an investment. The legislator has clearly stipulated that such a means of payment is not public money of the Russian Federation, nor is it the monetary unit of a foreign state, nor is it an international monetary unit or unit of account.

The legislator gives a 10-line long definition that contains the fiduciary description, and describes the ways in which digital currency emerges and exists. We can see that in relation to sets of electronic data (digital codes and symbols) there is no person with an obligation before each holder of such electronic data. However, the text of the law is contradictory because it clarifies that there are still persons with an obligation, and that can be either of the following, or two together: information system operator; information system nodes. Also, the text gives an exhaustive list of their obligations. The persons in question are to ensure that the following parameters comply with the information system regulations: the procedure for issuing these electronic data (digital codes and symbols); the procedure for entering (altering) these entries (digital codes and symbols) in such an information system. Let us further elaborate on the legal content of digital currency by analysing parts of the legislative definitions.

Federal Law No. 149-FZ of 27 July 2006 'On Information, Information Technologies and Information Protection'[2] (henceforth Federal Law 149-FZ) stipulates in Article 2 on the main concepts used in the law that information is data (messages) irrespective of the form in which it is presented. Consequently, from a legal point of view, digital currency is information in electronic form. This information can be presented as a collection of data, as numerical codes, or as numerical symbols. Information is organised and stored in the computer memory as encrypted records in databases. It may be visually reflected on the computer monitor by a string of numbers, letters, or other graphic symbols in an archive folder with some unique name, maybe in the form of images of 'coins'. It is into these archived folders in computer databases in their group that anonymous actors record information about calculated 'coins' as they fill their 'electronic wallets' with digital currency.

The question arises: Who is the recognised and authoritative custodian of encrypted records in 'electronic wallets', and on what computer are such

[2] Federal Law No. 149-FZ of 27 July 2006 "On Information, Information Technologies and Information Protection" // Corpus of Legislation of the Russian Federation 2006. No 31. (Part 1). Art. 3448.

databases located? According to Federal Law 149-FZ, the holder of information is a person who has independently created such information or obtained the right to authorise or restrict access to information under the law or an agreement. The fundamental feature is that encrypted information about the 'currency' (newly added digital currency in collective circulation) is created, and access to it is restricted or allowed with the mandatory participation of all members of the group of anonymous actors and on every computer on that network. The way the algorithm works is that the consent of each group member is exercised as a duplication of the current state of the database with each member. A special computer programme and equipment is used for this purpose, which means that these people act coherently, in a coordinated and systematic way. We are dealing here with the functioning of an information system: information is systematically recorded into databases by means of special information technology. The whole process is conducted by special machines, which require electricity and Internet connection.

2. Digital Currency in Circulation as Encrypted Information, Settlement and Exchange Equivalent and Investment Asset

Digital currency, in each of its discrete units, i.e., a 'coin', is a unique group of symbols, a set of data in electronic form. This data is encrypted and stored in the memory of all the computers that are linked together in a local area network via the Internet and work together according to a specific digital currency software programme that certain people in that local area network want to obtain. Each computer has its own individual Internet address, hence such a node in a local network also becomes non-repeating and unique. Earlier we proposed quite a meaningful term: 'cryptocurrency'. And we believe this understanding of digital currency is still quite acceptable today, too. If the mathematical computations are successful, they culminate in new crypto records appearing in the 'electronic wallets' of the computer owners in such a network. Over time, the number of digital 'coins' of anonymous participants in this computation grows.

To be able to identify the legal content properly, let us talk in theory and imagine each discrete unit of digital currency as a QR code all covered with black and white squares that are connected by rectangularly twisting black and white lines between them. This QR code is generated only once and will never be repeated again as long as it appears in this local information

system. If these QR codes are materialised by printing each one onto small pieces of paper of the same size, quasi cash (monetary surrogates) will be created. If people within a particular group agree to mutually accept such monetary surrogates in exchange for material values, what we get is fiduciary quasi-money with limited circulation within that group. But what was the reason for the legislator to propose the formula "a set of electronic data contained in an information system that ... may be accepted as a means of payment" in Federal Law 259-FZ?

Many goods (work, services, property rights) are, for a number of reasons, most often not sold immediately for cash. This happens due to the current ability of customers, service recipients, tenants etc. to pay. This gives rise to the need for the purchase and sale of goods (work, services, property rights) without paying at the time of receipt, i.e., paying in instalments, or by deferred payment, i.e., buying on credit. If the manufacturer (contractor, service provider, lessor) can act as the seller of the goods (contractor, service provider, lessor) before the counterparty can confirm its status as the buyer (customer, service recipient, tenant) by paying money, they enter into a credit relationship. Money as a means of payment begins to function when a creditor-debtor legal relationship arises between the agents. The legal category of a 'payment' only applies in connection with the legal category of 'money'. In view of this we ought to agree completely with A.V. Gabov that "digital currency is not the rouble" and that "the rouble is not money" [Gabov A.V., 2021: 58, 59]. Hence, digital currency is not money.

Money realises its function as a means of payment in a specific way that is reflected in the following formula: Good (Performance of work, rendering of services, granting of property rights) on credit (Debt) → Obligation to repay the debt → Performance of the debt obligation on time → Money. Here, the movement of goods (work, services, property rights) and money does not occur as a counter-movement, but at different points in time. The repayment of the debt obligation coincides with the end of the sale transaction (performance of work, rendering of services, granting of property rights) exactly through the repayment of the debt via the payment of money. It should be noted here that the gap in time between the transfer of goods and the receipt of money for these goods determines the probability (risk) that the debtor (buyer/customer/service recipient/tenant) does not pay to the creditor (commodity producer/contractor/service provider/lessor), because the solvency of the counterparty may deteriorate dramatically during the performance of the debt obligation. The functioning of money

as a means of payment is the basis for the emergence of a special form of money, namely, credit money.

Credit money is used very heavily in the economy of modern Russia. Digital information technology, in particular remote banking, makes it possible to solve questions of lending to borrowers with a positive credit history in a matter of hours within a single working day. There is a broad range of credit instruments available to individuals, such as mortgage, car loans, emergency loans, student loans, payday loans, home repair loans, point of sale loans, etc. The same applies for corporations: There are industrial mortgage loans, working capital loans, business development loans, overdrafts to cover cash flow gaps, etc.

It has a sense to ask here a valid question: How important to modern society are the activities of groups of people who anonymously compute a digital currency, which they then upload to their 'electronic wallets' on their computers in the form of crypto-records? All their activities are anonymous. They operate in unknown jurisdictions and outside state control. Consequently, all this has zero relevance and significance for society. On the other hand, if there are no violations of any law, people are free to dispose of the crypto-records computed in the algorithm of the special computer programme as they see fit. But why would the legislator recognise digital currencies created by anonymous calculators as a means of payment? Is there any social relevance to identify in the law an array of electronic data with the instrument of a credit relationship and a means of payment?

We believe that the words "a set of electronic data contained in an information system that ... may be accepted as a means of payment" are no more than a statement of fact. This formula does not work; it does not and cannot influence in any way the behaviour of people who compute digital coins and then dispose of them as items of their property, possibly using them as quasi-money in their local network group. By a long stretch of imagination we could imagine that the period of computation of yet another discreet unit of digital currency may be represented as deferred payment (you receive the coin when the computation is over, and you will not receive it before that moment in time). However, what is quite special about this situation is that there is no debtor, and the proactive volunteer computing the digital currency is not a creditor, either. Thus, the legislator has made a mistake by failing to understand the function of money as a means of payment, which can only be realised within the legitimate framework of the relationship between the creditor and the debtor. The relationship that

people have when they calculate digital currencies in an anonymous environment on local computer networks on the Internet cannot be regulated in any way even if the legislator recognises digital currencies as a means of payment. A single 'coin' computed within the group of anonymous persons is a block of encrypted information standardised within that group, which can be used in that group on a mutual trust basis as an electronic equivalent for settlements. And this will always occur spontaneously, each time on the unique terms of the current situation and depending on the material interests of the parties participating in the exchange. At the same time, Russian law does not prohibit people from using such electronic equivalents for mutual, private (local-network) settlements and exchanges.

The second line defined by legislator in Federal Law 259-FZ is the use of digital currency in property circulation: "...may be offered and may be accepted as an investment." This legal formula raises just as many questions as the previous one. What would it mean to offer digital currency as an investment? Let us assume that the legislator meant "as investment capital". This means that the owner of the digital currency offers the business entity that initiates a project to record a set of cryptocurrencies in the name of that initiator in a certain 'electronic wallet' as the currency owner's investment in that project. It may happen that this project initiator has ideas as to how to use such a crypto-investment for the benefit of the project. We believe it is worth clarifying that, on a relatively small scale, such projects to attract individual digital currencies as investment capital can be found on the Internet. However, we believe there is no option to legitimately invest digital currency as investment capital with interest under a bank deposit agreement, as only public money can be used in this legal construct; nor is there an option for a loan agreement (money, fungible goods, or securities). Nor is it legal to make a digital currency payment from the employer to an employee under a contract of employment.

Let us assume that what the legislator meant was to offer digital currency as an object of investment (investment asset). We agree that this is the area that attracts the attention of profit mongers the world over. Most of the analyses we know about the so-called capitalisation of digital currencies (e.g. Bitcoin, Bitcoin Cash, Dash, Ethereum, Ripple) over the past five to ten years reflect the surveys of the fluctuations in the 'prices' of these investments relative to the US dollar. For example, from our own observations, we can see that in the year 2011, one Bitcoin was worth $1; in 2013, it was 1000$; on 17 December 2017, it was 19,483$; and on 09 November

2021, 68,300$. On 21 February 2023, one Bitcoin was available for purchase for cash remotely on the website https://currency.com at $24,581. It is obvious that since the said digital currency, Bitcoin, has changed its price thousandfold against the US dollar over the 10-12 year horizon, it is a high-risk speculative investment asset. According to foreign authors, the rapid development of digital currencies specifically as investment assets is confirmed by the growth of crypto-investor accounts on crypto-intermediary websites from 45-48 million in 2016 to 190-200 million in 2020 [Blandin A., Pieters G. et al., 2020]. Russian authors confirm our view that investors look at digital currencies precisely as targets for short-term investments of public money, with an inevitable return from digital currencies back into public money, for the purpose of speculative gain. At the same time, digital currencies are of little interest as quasi-money in real crypto practice [Lunyakov O.V., 2021]; [Umyarov K.S., 2021]. We obviously come to the conclusion again that the legislator's wording, which states the facts of an established relationship and informs us that digital currency can be offered and can be accepted as an investment, has no regulatory relevance. At the same time the fact that people use digital currencies as an electronic settlement and exchange equivalent, an investment instrument, an object of investment, including a number of grounds listed below, allows to recognise digital currencies as a type of other property under Article 128 of the Russian Federation Civil Code[3] on the composition of objects of civil rights.

3. Special Features of Digital Currency Circulation and Regulation

Federal Law 259-FZ highlights the figure of the information system operator as the obliged person. According to Federal Law 149-FZ, the information system operator is the user that can be both an individual and a legal entity. This person operates the information system, which includes processing the information stored in this system's databases. Fundamentally new for legal regulation is that an 'information system node' is presented as the 'person with an obligation'. This is clearly a natural person, a human. But, due to this person's anonymity, it is impossible to define their legal standing more specifically. The person's age is unknown, their intellectual and physical state and their jurisdiction are unknown.

[3] Part One, RF Civil Code of 30 November 1994 No. 51-FZ // Corpus of Legislation of the Russian Federation. 1994. No. 32. Art. 3301.

What does the legislator mean by the category of 'a person with an obligation before each holder of such electronic data'? The term 'category' is the most appropriate here because we cannot use the more specific term 'subject'. Assuming, one day a member of the collective of the anonymous computers group (or a profiteer) finds out that the records of some or all 'coins' in their 'electronic wallet' have disappeared. For such a situation, the legislator specifies the defendant against whom the aggrieved person can lodge a claim for protection of their rights and compensation for damages. Hypothetically, this claim could be realised against the operator of the information system operator. But can one lodge a material claim against the node(s) of an information system? No, one cannot. We are dealing here with a fundamental contradiction. On the one hand, there is an information technology of distributed node-by-node entry of new data into the database (or of making changes in the existing data), where trust is eliminated and replaced by mathematical computation in the operation of a computer algorithm. On the other hand, the creation of encrypted 'currency' information implies there must be trust and readiness of all members of the anonymous group to respond positively to all offers to use the existing and/or newly created digital currency as a means of payment and as an investment, as well as their full trust in the operation of the computer algorithm.

What exactly is the task of the 'person with an obligation before each holder of such electronic data'? In the legislator's view, this person's task is to maintain order. This means: firstly, electronic data (numerical codes and symbols) must be released in accordance with the rules of the information system; secondly, the procedure for making (changing) entries regarding electronic data (digital codes and symbols) in the information system must also comply with its rules. It is extremely sad to see the legislator's passive approach to the attempts to regulate anonymous relationships in this area. A person, acting of their own free will and interest, joins a group of anonymous individuals who, on a voluntary and proactive basis, buy with public money, generate and encrypt information and, from time to time, modify in the database records belonging to certain holders, who appear in this respect on the Internet as 'electronic wallet' addresses with unique logins and passwords. The entire process uses a computer programme and is highly automated. Therefore, a properly functioning algorithm for such a programme is the very rules of the information system that must be followed. Consequently, non-compliance with the order only occurs as a result of improper operation of the software programme.

Such issues can take place due to a variety of causes, both technical and man-made. A technical failure may occur, or a computer programme may have been 'hacked' with malicious intent. However, preventing distortions in the algorithm of such a programme is not and cannot be part of the skills of an information system operator (according to the law, it any citizen and any legal entity can be an operator). Members of a group of anonymous actors, each on their own computer (in their own node) also have no influence whatsoever on the operation of such a programme's algorithm. Hence, the 'person with an obligation before each holder of such electronic data' cannot discharge their obligations. The legislator's formula in the fragment of Federal Law 259-FZ in question is nothing more than a good wish that the computer algorithm in the relevant group of anonymous users should work properly, both in terms of the mathematical computation of digital currency and in terms of the mode of entry of records about the digital currency into the database.

This naturally raises a series of straightforward questions. What is the role of the brilliant author of the computer programme that the groups of anonymous actors use in full trust to compute and record digital currency on a voluntary and proactive basis? Because the group may number in the tens of millions. How does this person behave in space and time? Can this person, for whatever reason, influence the algorithm of their brainchild, causing a global collapse of the entire information system? Clearly, this risk is totally real and this negative event could take place. Figuratively speaking, the entire group of anonymous actors that compute digital currency on a voluntary and proactive basis and conduct settlement and exchange transactions with this currency is hostage to this brilliant author. It is therefore the obligation of the government to take legislative measures to prevent potential conflicts and to develop a mechanism to protect the rights of participants in this area of social relations.

Hopes for progress in regulating the area of social relations in question appeared owing to Draft Law No 237585-8 submitted to the State Duma in November 2022. It is with deep disappointment that we must admit that our hopes have not been fulfilled. The law-making by a group of parliamentarians in this draft law is directly related to digital currency in terms of taking certain practical steps to obtain it. This draft law does not use the Russian word for 'mining', but the English loan word. It uses the following definition: "Digital currency *mining* is understood to be the activity of performing mathematical computations by operating computing devices and hardware and software complexes to make entries in an information

system using distributed ledger technology, with the purpose of creating digital currency and/or receiving remuneration in digital currency."[4]

We call digital currencies (a set of electronic data) monetary surrogates because money is issued by the central banks of states. Groups of users generate cryptocurrency data, i.e. digital currencies, as their computers perform computations by using algorithms. A special programme is installed on the computer of a volunteer member of the group, and it does not matter where on the planet this computer is located. This programme performs computations and finds a unique hash function to attach a new block to the block chain. In the course of millions of iterations, the group member's computer picks up a single hash (the result of some mathematical transformation of a block from the previous block in the chain), thus making it possible to 'attach' one more block to the block chain. When a block is 'attached', the group member whose computer was the first to solve this mathematical problem receives a reward, namely a collectively recognised cryptocurrency 'coin', which is written into their 'electronic wallet'. These records are generally referred to as 'cryptocurrency' (although, for no reason whatsoever), which is why the words 'amount in digital currency' are constantly used in this relationship. The terms 'wallet' and 'amount' are intrinsic to the concept 'money', but we have proven above that digital currency is not money. User groups that have gathered around cryptocurrencies with various exotic 'coin' names (such as Bitcoin, Bitcoin Cash, Dash, Ethereum, Ripple, etc.) have different computational features and time horizons for years to come. But in any event, to participate in such 'entrepreneurial activity' a person needs: one, certain intellectual and physical abilities; two, special computer hardware and software; three, uninterrupted and stable connection of their computer to the Internet; four, sufficient electric power for the functioning of the whole hardware and software complex.

In our opinion, such global computer calculations of mathematical formulas for adding the next block to the existing chain of blocks in a computer programme have no socially useful function and bring no economic growth. Clearly, at the same time computer equipment is improved, Internet services are developed, and electricity companies increase their sales. Along with this, opportunities for laundering money linked to criminal offences increase, illegal consumption of electricity rises sharply, and hundreds of millions of computers are involved in mathematical computations

[4] The State Duma. Zakonotvorchestvo (Law-making) State Automated System. Available at: URL: https://sozd.duma.gov.ru/bill/237585-8 (accessed: 22.02.2023)

that have no positive influence on human progress. E.g., in 2019, Interregional Distribution Grid Company of the North Caucasus discovered the theft of electricity worth RUB 130 million in the village of Plievo in Ingushetia. Its engineers found a site near the village where unidentified persons had illegally installed 2 transformers that supplied power to over 1,600 mining farms. Illegal miners have been detected at a Ukrainian nuclear power plant, and a officer of the Ukrainian Security Service told they could not rule out that not only plant employees but also National Guard officers who were guarding the plant were mining cryptocurrency.[5]

In essence, the result of such 'entrepreneurial activity' is turning electricity into cryptocurrency records in the 'electronic wallet' of the electricity consumer. In this connection, we do not consider it possible to use either the English loan word 'mining' or its Russian equivalent 'dobycha' ('mining') to define mathematical computation of digital currency. The Great Soviet Encyclopaedia states that "mining is the extraction of solid, liquid and gaseous minerals from the earth's interior. The process of mining consists of excavating minerals and transporting them from the face of the mine to the surface. Solid minerals are extracted by open-pit and underground mining. Peat is extracted from the surface with full mechanisation of the main production processes. Liquid minerals and natural gas are increasingly extracted by means of surface-drilled wells. Production of solid minerals (gold, tin, diamonds, zircon, monazite, ilmenite, etc.) and oil from the seabed has been developing since 1960s.[6]

As noted above, the member of the group of 'miners' whose computer first solves the mathematical issue for attaching next block to an existing block chain gets a certain number of crypto-'coins' of digital currency into their 'electronic wallet'. To increase the likelihood of success in these computations, the owners of the computers involved in the computations began to agree to link their computers in local networks, e.g., of 100 computers. Clearly, such a local pool of 'miners' will compute the single correct hash faster. In this way, 100 users within their local association will be able

[5] Sekret Firmy. Media registration certificate El No. FS77-68947 / Mining, the Caucasus Way. Bitcoin Hunter from Ingushetia Steals RUB 130M Worth of Electric Power. Available at: URL: https://secretmag.ru/news/.maining-po-kavkazski-okhotnik-za-bitkoinami-iz-ingushetii-ukral-elektroener giyu-na-130-mln-rublei-04-09-2019.htm (accessed: 22.02.2023). RosBiznesKonsulting. Available at: URL: https://www.rbc.ru/crypto/news/637e3 dfb9a7947082e0569b8 (accessed: 22.02. 2023)

[6] The Great Soviet Encyclopedia. 3rd ed. Moscow, 1969. Available at: URL: https://www.booksite.ru/fulltext/1/001/008/053/ 584.htm (accessed: 22.02.2023)

to 'attach' another block to the existing block chain in the course of combined computer operation with significantly higher likelihood and faster than each of them individually. In this draft law, unfortunately, we again see another fact of the Russian legislator's adherence to Anglo-Saxon terminology. E.g., such a term as 'association of miners' has been proposed: "A mining pool is the pooling of the capacity of several computing devices that belong to different owners (hereinafter, 'mining pool participants') and are used for mining purposes, which results in the distribution of the resulting digital currency among the owners of the said computing devices.'[7]

However, if one takes a close look, a 'mining pool' is not at all an association of people owning computers, or an 'miners association'. The draft law clearly refers to a classic asset package: a combination of the capacities of several computing devices that belong to different owners. This raises an avalanche of questions: Is it joint indivisible ownership of common property? Or is it shared divisible ownership of interconnected property? Or is it an association of businessmen like a general partnership? Or is it a membership-based production cooperative with one vote for each member? But parliamentarians do not care about such subtleties of civil and business law. The draft law is primarily driven by fiscal interest.

As a first approximation, one could imagine taxation of the property itself, as regulated, for example, under the transport tax, i.e., based on one horsepower of the car engine. But in real life, it is impossible to know reliably how many computers are looped into one pool, and the computers themselves may be scattered over several jurisdictions. And since it is impossible to tax, e.g., 100 computers located in different countries and looped into a local network, the legislators, in a somewhat naive and light-minded way, shift the duty of good faith reporting of taxable objects to the 'miners' themselves, leaving the practical tax administration to the Russian government. "In the event of receipt of digital currency as a result of mining, the person engaged in mining, including the participant of a mining pool, shall provide information on receipt of digital currency, and information on the unique sequence of symbols used to record transactions with digital currency credited as a result of mining to the person engaged in mining (address identifier), in accordance with the procedure and within the time limits established by Russian legislation on taxes and levies."[8] But the root of the issue here is that every anonymous individual plunges into

[7] Available at: URL: https://sozd.duma.gov.ru/bill/237585-8 (accessed: 23.02. 2023)

[8] Ibid.

the depths of the crypto-world via the Internet precisely in order to enrich themselves in a shadowy manner, so that no one will ever know the intensity and extent of their transactions, and certainly without the intention of paying taxes to any state or regularly sending their truthful statements to the tax authorities.

In connection with the Russian parliamentarians' initiatives, it should be noted that the share of China, which until recently was the world's largest mining hub, has fallen from 46% to zero. This drop is explained by imperative regulatory measures that have led to a total ban on cryptocurrency mining in China since autumn 2021. As a result, digital currency mining companies had to move to other jurisdictions. China has imposed a total ban on cryptocurrency transactions, recognising them as illegal financial activity. We believe that the government of the People's Republic of China clearly sees more important areas for application of the country's electricity resources that are not so abundant in China. At the same time, according to our estimates, there is a surplus of generated electricity in Russia today, especially in the areas around the eight hydro-electric power plants and 12 nuclear power plants. Mathematical computations can be organised under public-private partnerships and special legal regulations.

4. Digital Currency as a Type of Other Property and an Object of Civil Rights

Studying doctrinal judgments on the topic we found no fundamental and sharp contradictions to our views regarding the legal content of digital currency. What we did find was confusion in the statements made by some authors. The most widespread mistake is the confusion of the terms 'cryptocurrency' and 'digital currency'. We believe this is unacceptable at the legal level. For example, E.R. Vergeles claims that Federal Law 259-FZ "says nothing about cryptocurrency and blockchain. Moreover, according to the said federal law, cryptocurrencies are not digital money whose circulation is allowed in the Russian Federation, due to the fact that there is no definition of cryptocurrency itself" [Vergeles E.R., 2022: 37]. We do not believe that one should look in Federal Law 259-FZ for an interpretation of cryptocurrency in the places where there should be none, as Article 1 on the subject of regulation and the scope of the law clearly states the limits and categories of regulation. K.O. Boykova classifies all types of cryptocurrencies according to their degree of financial security: cryptocurrency (monetary surrogates) and the digital rouble [Boykova K.O., 2022: 189]. We believe it is a mistake

to classify the digital rouble (one of the legitimate monetary units of the Russian Federation) as a cryptocurrency. Furthermore, the term 'degree of financial security' needs a separate scientific justification. E.A. Mosakova erroneously claims, contrary to the current legislation of most developed countries, that cryptocurrency is "the new form of money", "a new word in monetary circulation", and "will allow cryptocurrencies to become one of the world currencies in the medium term" [Mosakova E.A., 2021: 2–4, 6,7]. M.M. Dolgiyeva correctly points out the mathematical principles of digital currency generation and its automatic management by means of software [Dolgiyeva M.M., 2022: 128-129]. V.D. Kuligin comes to a conclusion with which we cannot agree: "Cryptocurrency is private money. Such money has always been present in the circulation of any country in the form of bills of exchange, coupons and certificates, etc." [Kuligin V.D. et al., 2022: 151]. Firstly, there is no such money in circulation, and secondly, bills of exchange, coupons and certificates have never been and cannot be a form of money.

The scholarly findings of a number of prominent Russian legal scholars deserve close attention. Professor I.I. Kucherov believes that "it is necessary to extend the range of objects of civil rights by adding a new object which could include cryptocurrency. In the author's view, documented information could be such a type" [Kucherov I.I., 2018: 189]. Corresponding Member of the Russian Academy of Sciences A.V. Gabov quite rightly points out that "the system of objects of civil rights is therefore not static, but rather quite fluid; the legislator must respond to changes in the outside world and reflect them in the law in time." [Gabov A.V., 2021: 63]. The work closest to our topic is that of Professor L.Y. Vasilevskaya. In our view, owing to the depth and breadth of this work, it should be considered the best specifically on the subject of digital currency as of early 2023. Our views concur on a number of points: "Cryptocurrency is the antipode of the digital rouble, since it circulates within an inherently global, decentralised digital payment system of individuals extending beyond the territory of any state». On the other hand, we cannot agree with her that "digital currency should be qualified as a digital financial asset" [Vasilevskaya L.Y., 2023: 16, 17]. This is not possible, because, at the very least, the legislator makes the distinction in the title of Federal Law 259-FZ.

Around 50 years ago Soviet scholars described in the Great Soviet Encyclopaedia the legal understanding of property as: the totality of things and tangible assets in a person's possession...; the totality of things and property

rights to receive them from other persons...; the totality of things, property rights and obligations which characterise the property status of their bearer. Currently the Russian legislator in Article 128 of the Civil Code on the composition of objects of civil rights, develops and details the interpretation of property: things (including cash and certificated securities), other property, including property rights (including non-cash funds, uncertificated securities, digital rights); results of work performed and services provided; protected intellectual products and similar means of individualisation (intellectual property); intangible goods.

From a formal legal point of view, things include cash and securities — special documents on sheets of paper. No doubt, in addition to these two types, things include a whole huge world of material goods whose list would not fit into any code. Other property includes property rights and everything that can be attributed to other property for a reason that does not contradict the law. We cannot find any restrictions on classifying digital currency, i.e., the encrypted information existing in electronic form, as a type of other property that belongs to objects of civil rights in the context of the above provisions of Article 128 of the Civil Code. We share A.V. Gabov's position that "The object of civil rights is, above all, a certain idea that emerges by abstracting features of various phenomena (objects) of the external world that are not attributable to its subjective part, and 'marking' a certain group of objects by a single generic concept". We also fully agree with his concern "What if, in the form of digital currency, we are dealing with a play on words that obscures meaning?" [Gabov A.V., 2021: 62, 64].

V.D. Kuligin and his co-authors formulate conclusions that resonate with ours: "Bitcoin is a digital, informational structure designed to perform an exchange" [Kuligin V.D. et al., 2022: 151]. We support the position of R.M. Yankovskiy that "regulating cryptocurrency rights as an absolute right will require a new object of civil rights to be described in the law, similar to the special legal regime for uncertificated securities." We also agree with the him that "although the RF Civil Code does not define 'other property', given the current realities and level of technology, this concept may be interpreted as broadly as possible, in particular by including cryptocurrency as part of property" [Yankovskiy R.M., 2020: 50, 52].

A single 'coin' computed within the group of anonymous persons is a unique block of encrypted information standardised within that group, which can be used in that group on a mutual trust basis as an electronic equivalent for settlements and as an investment. Each digital currency 'coin'

is discrete and individual. It is a cipher that is never repeated — a block of information in electronic form; it is always assigned to a specific person and can circulate by being transferred between 'electronic wallets', which are maintained on the computers of the participants in this settlement (investment). And this digital currency 'coin' is continually assessed in terms of public money, usually of US jurisdiction. The steady, long-standing practice of using digital currency 'coins' as settlement equivalents, investment instruments and investment targets allows us to treat digital currency as a type of other property, and digital currency 'coins' as an object of civil rights in the context of Article 128 of the Civil Code.

Conclusion

The steady, long-standing practice of using digital currency 'coins' as settlement equivalents, investment instruments and investment objects allows us to treat digital currency as a type of other property, and digital currency 'coins' as an object of civil rights in the context of Article 128 of the Civil Code. Network nodes are created through the free affiliation of new members to the existing group, which increases the package of technical facilities functioning according to a specific programme for the benefit of the entire group. From the point of view of investments and economics, we define this growing network as a financial pyramid, a Ponzi scheme. It is compulsory for a member of the local network to connect their node (computer) via an individual address to the Internet and to a source of power. Information (digital currency as a set of electronic data) is recorded, generated and modified via a mathematical computation algorithm on each computer within such a local network. The 'person with an obligation before each holder of such electronic data' cannot discharge their obligations to upkeep order. There is a real risk of external interference with the proper operation of the mathematical computation algorithm, in particular by the author of the software programme. In this regard, we propose to introduce a compulsory by law state registration of the author of such intellectual products and to formalise the author's obligation to conduct supervision over the proper functioning of the corresponding algorithm of mathematical calculations. In addition, a legal regime of state control corresponding to the said obligation of the software author is necessary.

Russian jurisprudence regulating property turnover describes the place of digital currency as *terra incognita*. On the one hand, the legislator mentions digital currency in virtually a few phrases, merely stating the fact that

it exists in information systems. Legal regulation of digital currency currently in force in Russia is so far presented in its most general, initial form in the federal law on digital assets. The law stipulates this encrypted information in electronic form can be offered as a means of payment and as an investment. We believe that the fact that the legislator recognises digital currencies as a means of payment will in no way regulate the relationships that develop among people who interact anonymously on an extraterritorial basis when they compute digital currencies on local computer networks within the global Net. The legislator's statement that digital currency may be offered and may be accepted as an investment has no regulatory value. Digital currencies are high-risk speculative investments. On the other hand, digital currency appears in Russian tax law as an object of taxation, in bankruptcy and enforcement laws as an object of recovery, in family law as joint property of spouses, and in inheritance law as property. In the context of Article 128 of the Civil Code, digital currency must be classified as other property and the digital currency 'coin' is an object of civil rights.

It is regrettable that the legislators use the verb 'may' in Federal Law No. 259-FZ with reference to digital currency. The Dictionary of the Russian Language states, inter alia, that "may" is "...an expression of uncertain confirmation, probably, apparently...". And "perhaps" is the very first synonym in the list of synonyms. So we see here a failed, uncertain attempt by the legislator to approach the regulation of shadow circulation of digital currencies, which is decentralised and free of any law, and the relationships within this circulation. But the first steps, the most difficult ones, have already been made. Doctrinal development of the legal content and place of digital currency in the system of state regulation of property turnover, and the formation, accumulation and scholar understanding of judicial practice on this issue should continue.

References

1. Blandin A., Pieters G. et al. (2020) CCAF 3rd global crypto asset benchmarking study. *SSRN Electronic Journal*. DOI: 10.2139/ssrn.3700822.

2. Boikova K.O. (2022) Problematic aspect of determining legal nature of digital financial assets and digital currency in investigation of crimes with their turnover. *Kriminalistika: vchera, segodnya, zavtra*=Criminalistics: yesterday, today, tomorrow, vol. 22, no. 2, pp. 181–192 (in Russ.)

3. Dolgieva M.M. (2022) Operations with cryptocurrencies: issues of application of criminal law. *Aktualnye problemy rossiyskogo prava*=Issues of Russian Law, no. 4, pp. 128–139 (in Russ.)

4. Gabov A.V. (2021) The digital ruble of the Central Bank as an object of civil rights. *Aktualnye problemy rossiyskogo prava*=Issues of Russian Law, no. 4, pp. 55–65 (in Russ.)

5. Haentjens M., de Graaf T., Kokorin I. (2020) Failed hopes of disintermediation: Crypto-Custodian insolvency, legal risks and how to avoid them. Available at: URL: http://dx.doi.org/10.2139/ssrn.3589381.

6. Jianqiang G. et al. (2022) Data element embedding and firm performance: the influence of ESG investment. *Frontiers in Environmental Science,* vol. 10, art. 974399. DOI: https://doi.org/10.3389/fenvs.2022.974399.

7. Kochergin D.A. (2022) Cryptoactives: economic nature, classification and regulation of turnover. *Vestnik mezhdunarodnyh organizations*=Bulletin of International Bodies, no. 3, pp. 75–130 (in Russ.) Available at: https://doi:10.17323/ 19967845-2022-03-04.

8. Kucherov I.I. (2018) Legal approaches to the legitimization of cryptocurrency. *Vestnik Nizhegorodskoy akademii Ministerstva vnutrennikh del*=Bulletin of the Nizhny Novgorod Academy of Internal Ministry, no. 2, pp. 183–193 (in Russ.)

9. Kuligin V.D. et al. (2022) Evolution of money in the direction of digital currency. *Vestnik Universiteta*=Bulletin of the University, no. 4, pp. 146–152 (in Russ.)

10. Mosakova E.A. (2021) Risks of using cryptocurrencies as the newest form of money in the digital economy. *Informatcionnoye obschestvo*=Information Society, no. 3, pp. 2–8 (in Russ.)

11. Nagl L. (2022) Digital technology: reflections on the difference between instrumental rationality and practical reason. *Kantian Journal,* no. 1, pp. 60–88. DOI: https://doi.org/10.5922/0207-6918-2022-1-3.

12. Objects of civil rights (2019) Collection of studies. A.I. Goncharov (ed.) et al. Moscow: Yurayt; Volgograd: Volga Publishers, 567 p. (in Russ.)

13. Oluyeju M. (2022) Legal protection of investors from the corporate malfeasance of insider dealings: A South African-Canadian comparative review. *BRICS Law Journal,* no. 9, pp. 136–167.

14. Ushakov D.N. et al. (1990) Explanatory dictionary of the Russian language. Available at: URL: https://biblioclub.ru/index.php?page=dict&termin= 1153 382 (accessed: 22.02.2023) (in Russ.)

15.Vasilevskaya L. Yu. (2023) Digital ruble: a civilian view at the issue. *Russkiy zakon*=Lex Russica, vol. 76, no. 1, pp. 9–19 (in Russ.) DOI: 10.17803/1729-5920.2023.194.1.009-019.

16. Vergeles E.R. (2022) Crypto assets: a place in modern legislation. *Academicheskaya Mysl=Academic Thought*, no. 18, pp. 35–37 (in Russ.)

17. Yankovsky R.M. (2020) Cryptocurrencies in Russian law: surrogates, “other property” and digital money. *Pravo. Zhurnal Vysshey shkoly ekonomiki*=Law. Journal of the Higher School of Economics, vol. 12, no. 4, pp. 43–77 (in Russ.)

Information about the authors:

A.I. Goncharov — Doctor of Sciences (Law), Professor.

A.N. Sadkov — Candidate of Sciences (Law), Associate Professor.

V.A. Sadkov — Candidate of Sciences (Law), Lecturer.

D.A. Davudov– Candidate of Sciences (Law), Associate Professor.

The article was submitted to editorial office 22.02.2023; approved after reviewing 09.03.2023; accepted for publication 28.04.2023.

Legal Issues in the Digital Age. 2023. Vol. 4. No. 2.
Вопросы права в цифровую эпоху. 2023. Том 4. № 2.

Research article
УДК: 336.221
DOI:10.17323/2713-2749.2023.2.26.45

Features of Tax Regulation of the IT Industry in the Russian Federation and EAEU states

Maria Aleksandrovna Perepelitsa[1], Victoria Viktorovna Mironchukovskaya[2]

[1, 2] Yeletsky Bunin State University, 28 Kommunarov Str., Yelets 399770, Russia,
[1] perepelitsa.doc@gmail.com, https://orcid.org/0000-0003-4648-1789
[2] bosfor4878@mail.ru, https://orcid.org/0000-0001-7658-2375

Abstract

The article discusses the features of the application by the Russian Federation and the member countries of the Eurasian Economic Union (EAEU), Republics of Belarus, Kazakhstan, Kyrgyzstan, mechanisms of tax incentives for the development of the domestic IT industry. Tax incentives, a simplified taxation system and the taxation regime in the territory of the Special Economic Zones (SEZ), High-Tech Park (HTP) are analyzed. Special attention is paid to the consideration of the procedure for access and accreditation of companies for the opportunity to work in the territory of the SEZ or HTP with the use of a preferential tax regime. The article concludes that states as a whole apply all tax incentive mechanisms in a complex: tax incentives, a simplified taxation system, SEZ, HTP, however, there are differences in their use, which ultimately affects the level of stimulation of domestic IT industries. Russia uses a selective and differentiated approach, that is why most companies in the field are cut off from the preferential tax regime. The EAEU countries have developed more positive experience in this matter due to the simplification of the registration procedure required to enter the preferential zones, both for domestic and foreign IT companies and the admission to the HTP and SEZ of individuals specialists. The access of foreign companies from friendly countries as residents in the territory of the Russian SEZ will facilitate the introduction of new information technologies and the exchange of experience with domestic companies. The thesis is also substantiated that for a holistic and systematic stimulation of the development of the domestic IT industry, it seems inappropriate to differentiate companies into Software Company (companies specializing in high technologies) and companies not specializing in such technologies. Special attention is drawn to the need to expand the list of types of IT-activities that provide access to

domestic companies to the mechanism of preferential taxation. The article notes that the experience of tax incentives for the IT industry in the EAEU countries shows that the approach used makes it possible to unite the majority of domestic companies and specialists — individuals in the territory of a separate free economic zone or HTP, that is beneficial both for the companies themselves and individuals from — for preferential taxation, and to the state, which keeps them records and records of their IT products and discoveries. In the Russian Federation IT companies, unless they are included in the SEZ, are fragmented and more difficult to control in this sense. In general, it is concluded that in Russia it is necessary to ensure the uniform application of tax incentives for the domestic IT industry throughout the territory, which will contribute to its development and growth of competitiveness in the international market.

Keywords

IT-industry; IT-company; tax regulation; taxation; special economic zones; high technology park.

Acknowledgments: the paper is published within the project of supporting the publications of the authors of Russian educational and research organizations in the Higher School of Economics academic publications.

For citation: Perepelitsa M.A., Mironchukovskaya V.V. (2023) Features of Tax Regulation of IT Industry in the Russian Federation and EAEU States. *Legal Issues in the Digital Age,* vol. 4, no. 2, pp. 26–45. DOI:10.17323/2713-2749.2023.2.26.45

Introduction

Coming of information technologies into various spheres of human life promotes the transition to a new, higher quality level of development of the industries and areas of the public sector such as economy, security, energy, medicine, education, ecology, culture, and other equally important areas of public life. According to the Strategy for the Development of the Information Technology Industry in the Russian Federation for 2014–2020 and until 2025, this industry must be developed to ensure the transition to a new post-industrial technological paradigm of society.[1] Such development is possible when various legal incentives are used, the tax incentive being one of them.

Most states offer various preferential regimes, exemptions, investment clusters, free economic zones, special economic zones and hi-tech parks.

[1] Decree of the Government of the Russian Federation No. 2036-p of 1.11.2013 'Strategy for the Development of the Information Technology Industry in the Russian Federation for 2014-2020 and until 2025.' Available at: URL: https://www.digital.gov.ru>uploaded>-files (accessed: 03.02.2023)

Russian Federation has to compete for IT professionals and encourage the development of the IT sector, too. Among other things, this need has been reinforced by the current international situation: many well-known companies have decided to cease operations in Russian, and some professionals have left the Russian market. Moreover, there are problems in tax regulation of the Russian IT sector because approach to taxation is unstructured and inconsistent. Not all companies can obtain access to tax-heaven arrangements. This makes it difficult to achieve the goal set forth in the 'Strategy for the Development of the Information Technology Industry in the Russian Federation for 2014-2020 and until 2025' and in other documents pertaining to this sector that the state adopts. In view of the above it would be appropriate to draw the reader's attention to the experience of the member countries of the Eurasian Economic Union because their IT sectors have been growing and demonstrating good results in areas related to products, projects, start-ups, and services. Hence, consideration of the proposed topic is relevant and timely.

Subject of study: study tax exemptions, simplified tax system and legal regimes in the free economic zones, special economic zones and hi-tech parks of Russia and the EAEU member countries, and their comparative analysis.

Purpose of study: research the experience of applying tax incentives in the IT sector in the Russian Federation and Eurasian Economic Union, and justify of the need to introduce in Russia legal norms stimulating the development of the domestic sector.

Special methods of research have been used in studying the legal norms governing taxation of the IT industry in the EAEU jurisdictions like: comparative law, legal interpretation method, and formal-legal method.

1. Fiscal regulation concept: the main instruments used in the IT industry in the Russian Federation and EAEU states.

The tax law science determines tax regulation is government regulation of tax relations [Krasyukov A.B., 2007]; [Lazarev V.I., 2009]; [Morozov A.A., 2011]. In analysing the contents of fiscal regulation, scholars include in it such concepts as tax policy, tax mechanism, tax administration, tax planning and forecasting, tax strategy, tax control, taxation [Aliyev B.K., 2008]; [Serdyukov A.E., Vylkova E.S., 2008]; [Stepanenko V.V., Ermakova E.A., 2012]. We share this position of the scholars: to be able to

influence the behaviour of subject involved in tax relations (both public and private), fiscal regulation must include the above tools and methods listed by the researcher. They are not used separately from each other, but in an integrated manner and to achieve a certain goal. The main purpose of fiscal regulation is to ensure a level of operation of the tax system where tax revenues would be collected on time, in full and with a view to making the best use of the financial potential of the national economy in the future. This purpose can be reached through the fiscal function of the tax, the essence of which is to fill the revenue side of the state budget.

However, depending on the industry or sector of the economy, fiscal regulation may differ or even have the opposite objective. The right approach to fiscal regulation of a sector of the economy implies the state's legal influence on the operations of agents in that particular sector through the application of the taxation mechanism in order to implement the fiscal or regulatory (incentive) functions of the tax, based on the principle of priority development of this sector in the interests of the state. In other words, the state, proceeding from the need to reach the country's development goals, applies different taxation instruments to the relevant industry (sector), increasing or decreasing the role of the fiscal or regulatory (incentive) functions of the tax. So, depending on the means of intervention and the legal instruments applied, government fiscal regulation may aim to encourage or discourage the development of a particular industry.

Tax law scholars suggest that tax incentives are a motivation mechanism based on a low-tax policy, optimisation of the composition and structure of the tax system, the level of tax burden, the rates of individual taxes, or on the use of a tax exemption system [Zhigunova E.N., 2014]. This type of tax incentive has a positive effect on certain areas or sectors of the economy. Tax deterrence is a less common form of state fiscal regulation because its aim is to restrain the development of certain sectors of the economy and investment activity; it is based on a policy of high taxes, general and selective high tax rates, increasing the list of tax payments, abolishing tax exemptions, etc. [Barulin S.V. et al., 2008]. E.g., in order to reduce a segment of the entertainment services industry such as gambling business, it would be sufficient to strengthen the fiscal function of taxation by raising the tax rate, expanding the tax base, complicating the licensing procedures (introducing the need to obtain additional permits), increasing the grounds for tax control, etc. All such actions would indicate that the fiscal function of the tax prevails over the regulatory (incentive) function.

Tax regulation is effected through the use of the relevant tools. As we have noted above, these are: tax policy, mechanism, administration, planning and forecasting, strategy, control, and taxation. The latter, i.e., taxation as an individual fiscal regulation tool, includes the tax subject (taxpayer), tax object, tax base and tax rates, sources of fiscal payments, benefits, sanctions, schedules, tax credits, tax holidays, tax clusters, special taxation regimes, tax amnesties, tax deductions, tax deferrals and tax instalments, ways of enforcing the tax obligation, and other elements. Depending on what elements prevail in the taxation process, fiscal or incentive, we can talk of tax incentives, tax deterrence or general fiscal regulation.

IT taxation mechanisms in Russia and the EAEU states are incentive-based because they use a fairly wide range of tax incentives and preferences. These include tax exemptions, special tax regimes, moratoriums on tax audits, preferential terms in the performance of tax obligations, free economic zones, special economic zones and hi-tech parks. Russian, Belarus, Kazakhstan, and Kyrgyzstan use the above tax incentives in some way or another, but there are differences in the procedures and grounds for their application that brings different results.

2. Fiscal regulation of the IT industry in the Russian Federation

According to Decree of the Government of the Russian Federation No. 2036-p of 1.11.2013 (hereinafter Decree 2036), the information technology industry is understood as the totality of Russian companies involved in the following activities: development of mass-market software products; service provision in the IT sphere; development of hardware and software complexes with high added value of the software part; remote information processing and provision in various environments, including the Internet[2]. From the tax law perspective, this definition enables identifying the tax subject (tax payer) and the taxation object. In a general sense, the idea is to include individual IT professionals into the IT sector, too, because in 2021 there were approximately 1.7 Million individuals making a specialty out of IT.[3] Today, they account for a significant share in the Russian IT sector, while also being taxpayers. Ac-

[2] Decree of the Government of the Russian Federation No. 2036-p of 1.11.2013 'Strategy for the Development of the Information Technology Industry in the Russian Federation for 2014-2020 and until 2025.' Available at: URL: https://www.pravo.gov.ru (accessed: 11.03.2023)

[3] Statistics on outflow of IT professionals from Russia in 2023. Available at: URL: https://www.inclient.ru>outflow (accessed: 15.02. 2023)

cording to Article 19 of the Russian Tax Code, organisations and individuals charged with the obligation to pay taxes, levies and insurance payments respectively are recognised as taxpayers, levy payers and insurance payers in accordance with this Code[4]. This means that not only organisations but also individuals may be regarded as taxpayers in the field. The mechanisms for preferential taxation of individuals and legal entities working in the IT industry are different, because individuals work under a special tax regime, the simplified taxation system, while legal entities are entitled to benefits under the general taxation system.

Before looking at the specifics of preferential taxation of IT companies and individual IT professionals, one must define the object of taxation in the industry that would be is universal for both the Russian Federation and the EAEU states. The object of taxation of revenues from information services provided or products made is manifold and therefore internally structured. Different tax and legal regulations apply to the object of taxation in the sphere, depending on the type of its manifestation.

Information collection, processing and distribution services are provided through information technologies whose efficacy determines the performance of other sectors of economy, companies, and individuals. The industry offers a wide range of information products intended to provide relevant information to subjects (clients and users). On the whole, the variety of information products can be categorised into the following areas of activity: software installation and configuration; mobile application development; IT outsourcing; infrastructure subscription services (software maintenance, hosting, programming, testing, etc.); Internet access services; website creation and software development; training and certification; cloud and virtual services[5]. The Russian Classification of Economic Activities (OKVED) gives a more detailed description of IT services.[6] According to the OKVED, these services list includes: software installation and configuration; mobile application development; outsourcing; infrastructure subscription services including software maintenance, hosting, programming, testing, etc.; Internet access services; website creation and software

[4] RF Tax Code No. 117-FZ. 05.08,2000 // Collection of Laws of the Russian Federation. No. 32, 2000, P. 3340.

[5] IT Company / OKVED codes. Available at: URL: https://www.regfile.ru>okved-nabor>it-kompaniya (accessed: 15.02. 2023)

[6] Russian Classification of Economic Activities OKVED No. 14 26.07.2022. Order of the Federal Agency on Technical Regulating and Metrology Rosstandard. Available at: URL: https://www.classifikators.ru>okz (accessed: 15.02. 2023)

development; training and certification; cloud and virtual services. Each of the areas (groupings) has its own further breakdown into types, and the list is quite long, with over 80 types. E.g., 62.01 — development of computer software; 62.02.1 — planning and design of computer systems; 63.11.1 — database creation and use, etc. The eligibility for tax incentives, and therefore the amount of the tax liability of the IT company, will depend on the type of information service or product provided.

According to Para 1, Article 56 of the Russian Federation Tax Code, tax and levy benefits are benefits provided to certain categories of taxpayers and levy payers as envisaged by the laws and regulations on taxes and levies in comparison with other taxpayers or levy payers, excluding the possibility of not paying tax or levy or paying it in a smaller amount[7]. Tax incentives are provided to taxpayers in various forms: tax exemption in perpetuity or for a certain period (tax holidays); exemption from taxation when certain types of income are removed from the object of taxation; reduced tax rate; tax deductions. Tax incentives in the IT industry include tax holidays, reduced tax rates and exemption of certain types of income from taxation. This variety of tax incentive forms demonstrates the state's commitment to support development of the Russian industry.

But how easy it for all Russian companies to get access to tax incentives and can any company have a subjective right to various forms of such incentives? Moreover, the very definition of an IT company in the Russian Federation may lead to the erroneous conclusion that any company engaged in IT activities is entitled to preferential tax treatment by virtue of this fact alone: in accordance with Para A, Part 4 of the Regulation on State Accreditation of Russian Organisations Acting in the Field of Information Technology[8], a domestic company is a Russian organisation carrying out activities related to information technology. This impression could also be due to the fact that public policy has lately been proclaiming support for the IT industry as a whole, without dividing it into sectors. E.g., the Presidential Address of 23.06. 2020 announced the intention to support the Russian IT industry with tax incentives[9]; the Budget, Tax and Customs

[7] RF Tax Code. // Collection of Laws of the Russian Federation No. 32, 2000, P. 3340.

[8] Regulations on State Accreditation of Russian Organisations in the Field of Information Technology: RF Government Decree No. 1729. 30.09.2022. Available at: URL: https://base.garant.ru/405366137/#blok_1100 (accessed: 15.02.2023)

[9] Available at: URL: http://kremlin.ru/events/president/news/63548 (accessed: 11.03. 2023)

and Tariff Policy Guidelines for 2022 and for the planning period 2023 and 2024 also referred to the establishment of incentives for information technology companies[10]; furthermore, the Strategy for the Development of the Information Technology Industry in the Russian Federation for 2014-2020 and until 2025 itself largely focuses on stimulating the domestic industry. But in fact, the government takes a selective approach in regulating the industry taxation. Such selective and double taxation policies may result in under-achieving domestic industry development goals and falling behind those jurisdictions and countries that apply a consistent approach in taxing the national sector.

Upon analysing the law with respect to the payment of corporate income tax for Russian companies it may be concluded that some services and works are not included in the exempted category. Moreover, the rules for accessing the tax exemption are quite stringent, both in terms of obtaining and maintaining it. Para 1.15 of Article 284 of the Tax Code establishes a list of activities (operations) that give Russian IT-industry organisations the right to a tax exemption. These include the sale of copies of programmes and databases, granting and transfer of rights to use them, development of custom-made programmes and databases, their installation, testing, maintenance, etc. Such activities are considered to be more high-tech in relation to other information works and services. The list is exhaustive. But, only doing the activities from this exhaustive list is not enough to obtain an income tax incentive. The legislator sets out a number of other requirements that must be met at the same time: IT-company in question must have a state accreditation in the field of information technology, obtained by procedure established by the Government of the Russian Federation; revenues from the specified exhaustive list must account for at least 90% of the taxpayer's total revenue (which forces the latter to constantly prove its right to the benefit and, if it is lost, to honour the income tax obligation in full, possibly even with a penalty); the company must have at least seven employees in the accounting (tax) period. Only if all of the above requirements are met the company is entitled to an income tax exemption. The benefit itself can be characterised as actively incentivising, as it is presented in forms of tax holidays: 0% income tax payable to the federal budget and a reduced tax rate: 3% income tax payable to federal budget. As a result, the very idea of

[10] Main directions of budgetary, tax and customs and tariff policy for 2022 and the planning period 2023 and 2024. Available at: URL: http://www.minfin.gov.ru (accessed: 11.03. 2023)

this tax incentive is highly positive, but access to this benefit is significantly limited. So what we have here is only a partial and very narrow incentive for the Russian industry–more precisely, for an individual segment of it (termed *Software Companies*–companies specialising in high technology). A similar situation exists regarding insurance payments[11] (Article 427 of the Tax Code). This excludes from preferential taxation a broad range of IT companies that provide other, no less important information services and products: website support services, distribution and maintenance of information materials on the Internet, information search; outsourcing, outstaffing, consulting, and advertising platforms; dealing services, marketplaces, PC installation and set-up services, crash recovery, software installation, etc. E.g., information companies develop products (mobile and web applications, online services, social media, anti-viral software). Outsourcing companies develop application software commissioned by third parties and provide them with technical support. Outstaffing companies 'lease out' technical specialists to work on the client's individual projects. Consulting companies help put ready-made software into operation and provide software servicing. In our opinion, such activities of IT companies are important for the development of the Russian IT product/service market and need tax support measures, just like activities of hi-tech IT companies.

It has a sense also to remember an company operating in the field of IT services and technology should not exclusively focus on getting the benefit (which should be a secondary task) or keep adapting its activities to that end.

In discussing the profit tax concessions for IT companies, we should make one important point: they will only be in effect until 2024. This also raises questions because just one year is left. It is clear that within a specific fiscal year, tax exemptions are inversely related to tax revenue: the more significant and longer-lasting the tax incentives are, the lower are the state budget's tax revenues, i.e. in terms of the budget, the tax exemptions are on the expenditure side. But the Government's stated strategic goal of stimulating the Russian IT industry cannot be achieved in such a short term. Nor is it sufficient for the taxpayer to scale up its business. It would be correct to provide such a benefit for five years or longer.

Consequently, this selective and differential approach used by the state violates the principle of equitable taxation to effectively bar most compa-

[11] Collection of Laws of the Russian Federation, 2000, No. 32, Art. 3340.

nies from the preferential regime. In the future, that may slow down the development of the Russian IT industry.

Tax benefits for individual IT professionals in Russia is effected via a special tax regime, a simplified taxation system. As rightly noted by A.N. Kozyrin, 'the existence of a general tax regime and a special tax regime helps create more favourable conditions for the taxpayers engaging in economically and socially significant activities. In that case, a taxpayer is usually left with a choice: to continue on the general regime or switch to a special one' [Kozyrin A.N., 2021]. Information technology represents a socially significant economic sector. It will be correct to agree with the researchers who note that special tax regimes have a beneficial effect on the economy by reducing the tax burden on the taxpayer and by streamlining taxation and raising its efficiency for both parties (the tax authority and the payer) [Nogina O.A., 2017]; [Muradkhanova Z.S., Musayeva Kh.M., 2019]; [Gromov V.V., 2022]. That is especially relevant when it comes to taxing the incomes of IT start-ups (we mean natural persons working in the sector).

A simplified taxation system is more advantageous for the above category of taxpayers than any concessions made available under the general system, as it enables them to start their activities without the high tax pressure, which is the case under general taxation. Here we should remember that a newbie start-upper may not yet have such experience and as many clients as the one who has been worked in the IT service market for some time. So, the simplified system is for him/her the only way to start a business without bearing increased tax costs (including the mandatory insurance payments). The funds thus saved on taxes can be invested in the development of one's start-up or project. The general taxation system is unfavourable for an IT start-upper working individually, for it forces him/her to pay all the taxes in full (13% natural persons' income tax plus VAT) and to bear all the tax accounting and reporting duties. It is only natural that few IT experts use that system. And under the simplified system, the tax payments depend on income. The rate varies from region to region between 1 and 6 % (compared with the general tax system's rates, these are considered preferential and stimulative); a single tax is paid in advance, on a quarterly basis before the 25th day of the month. Besides, there is no duty to do tax accounting, with only the revenue to be recorded as the taxable base. The tax reporting duty is also simplified: one has to file a tax return once a year, by 30 April of the following year. So the simplified system is the simplest and most lucrative taxation system for individual professionals.

Individual professionals are also in demand as freelancers in the service market. Freelancer servicers are attractive to corporate clients as they do not have to bear the tax and social insurance duties and costs for hired employees, nor assume additional obligations and responsibility for any non-compliance. Such legal relations are of interest to the freelancers as well: they mean unconstrained work and ability to distribute one's time, choose among clients, do as much as one can, and work remotely. A professional can provide outsourced services. Outsourcing in IT means full or partial transfer of IT infrastructure development, support and testing functions and/or other tasks in this area to an IT company or individual professional [Gadzhiyeva Ye. Yu., 2018]. Outsourcing in the field of information technology reduces the clients' costs and enables them to concentrate on their core activities [Lukoyanov I.V., 2015]. Outsourced IT services are in demand, so either a legal entity providing services or an individual may be an outsourcer. The revenue from the service provided is taxable.

A special tax regime, in the form of the simplified taxation system, is thus in place for individual professionals working in the IT sector of the Russian Federation as a tax incentive for their activities.

In addition to using the tax incentives and a simplified taxation system, companies of the Russian industry (RF residents) may operate in Special Economic Zones (SEZs). The SEZs are parts of the Russian Federation territory as defined by the Russian Federation Government where there is a special regime for doing business, and a free economic zone customs procedure may also apply.[12] As researchers note, SEZs are established to address the strategic, economic, social, foreign trade, and/or scientific and technological tasks faced by the country as a whole or some part of it [Panskov V.G., 2018]. The Russian Federation sets these very tasks as it decides to establish SEZs in its territory. Depending on the type of residents' activities permitted in the respective SEZ, these are subdivided into industrial and manufacturing, tourist and recreational, technology development and implementation, and port zones. IT industry companies, as residents conducting high technology activities, belong to technology development and implementation SEZs, which includes innovative activities, development and implementation of computer programmes, databases, integrated circuit topographies, information systems, etc. E.g., the SEZs in Petersburg and Tatarstan are innovative technology development and

[12] On Special Economic Zones in the Russian Federation. Federal Law No. No. 116-FZ 22.07.2005 / Collection of Laws of the Russian Federation, 2005, No. 12, P. 2147.

implementation ones that focus on knowledge-intensive and information-related technology.[13]

A SEZ is established for a 49-year period, and this is one of its advantages, especially when it comes to tax benefits for the Russian IT sector.[14] The point is that long-term tax incentives (incentives) help IT companies accumulate their funds released from taxation and then invest them in new and promising projects and information technology, which ultimately benefits the state. E.g., in the *Technopolis Moscow* SEZ, companies specialising in information protection have invested RUB 3 Billion in their projects; the Russian company IVA Technologies from the IT cluster of the Moscow SEZ has managed to substitute foreign IT giants' products and to offer a free license to its video conferencing platform, and S-Terra CSP, a Moscow SEZ resident, has created its own innovative products for information protection and virtual private networking that protect data transferred via communication channels. And such impressive results were achieved within a year's time. Of course, should the preferential SEZ tax regime remain in place for a longer period (49 years), the Russian IT sector has every chance to become the most sophisticated one in the global IT industry.

In a SEZ there is a special regime that fosters the growth of its residents' activity. Tax incentives are used to attract them to work in the SEZ. IT companies receive considerable tax relief on all the main taxes and contributions. Analysis of the taxation of residents suggests that SEZs use a differential approach to setting their tax rates. The tax relief may differ. Thus, in the *Innopolis* SEZ, the preferential profit tax is 2% for the first five years; income tax, 1%; and property taxes, 0% for the first ten years; in *Technopolis Moscow* –7% profit tax for the first five years; in the territory of the *Skolkovo* SEZ, 0% for ten years after getting participant status; in the Republic of Crimea and Sevastopol, 2% in the first three years after the company is entered in the SEZ residents' register, etc.[15] The different approaches to setting the preferential regime results from the fact that there are few SEZs in

[13] CNews Names Russian Regions Where IT Companies Pay the Smallest Taxes. Available at: URL: https://base.garant.ru/405366137/#blok_1100 (accessed: 18.03.2023)

[14] But that is not to say that the duration of the tax benefit is the same. 49 years is the operating period of the SEZ itself, and the benefit in its territory may be provided for a shorter term. For example, preferential VAT rates are provided to Skolkovo residents. Residents are exempted from that tax for ten years. Anyway, a preferential regime for IT companies within a SEZ exceed the duration of a similar regime outside it.

[15] Special Economic Zones for IT and Innovative Projects. Available at: URL: https://sezinnopolis.ru (accessed: 15.02. 2023)

Russia whose tax benefits have been established under the Tax Code. The existence of a preferential taxation regime in an individual SEZ may also be governed by a special regulation applicable in that zone only (e.g. the Federal Law 'On the Skolkovo Innovation Centre'[16] establishes a tax exemption for the participants in that SEZ).

Social insurance benefits also have a positive effect on IT companies' development in SEZs (the reduced insurance contribution rate is 7.6%, including 6% for compulsory pension insurance, 1.5% for compulsory temporary disability and maternity insurance, and 0.1% for compulsory medical insurance). Resident IT companies dealing with information technology and products, unlike manufacturing resident companies, bear no significant capital expenses. Their main expenditure item is remuneration for their employees (highly skilled and thus well-paid IT professionals). To reduce such costs, lowered insurance contribution rates are established for IT companies; that helps accumulate funds and invest them in start-ups.

However, to become a SEZ resident, a company must pass accreditation under the new rules that have become more difficult and complicated. So some Russian companies have limited access to the SEZs, which leaves them outside the tax stimulation area. That generally precludes systematic support for the development of the Russian industry. It would be more appropriate to ensure uniform application of tax incentives in taxing the national IT industry in the whole territory of the Russian Federation.

3. Experience of EAEU Member Countries in Taxing IT Industry: Belarus, Kazakhstan, Kyrgyzstan

3.1. IT Industry in Belarus

From the international perspective, the Belarusian IT market is considered 'young', as more than 50% of Belarusian IT companies have been working for not longer than five years, and 31% have been providing their services for six to ten years. Only 17 % of companies have more than eleven years' experience in the market. Prominent among major companies in the market of Belarus are Science, Soft, EPAM, Belhard, IBA, and Belsoft. The information and computer services sector comprises more than 971 companies, of which only 24 (less than 2.5%) are state-owned. Most of compa-

[16] On the Skolkovo Innovation Centre, see Federal Law No. 244-FZ 28.09. 2010 // Collection of Laws of the Russian Federation, 2010. No. 40, P. 4970.

nies are located in Minsk (more than 90%). The IT industry of Belarus is special in that most of its IT companies work on the grounds of the High Technology Park (HTP), with its preferential tax regime. For those Belarusian companies that are not residents and not eligible to switch to the simplified taxation system, the profit tax rate is 18%. The HTP was established in Belarus in 2005 by a Presidential Decree, and is considered one of the largest IT clusters in Central and Eastern Europe. The cluster's legal regime includes a broad range of preferences and exemptions in the tax, foreign economic, and migration areas. To become a participant, a company must have resident status and follow a simple registration procedure.

The companies working in HTP employ 24,000 programmers who implement high technology projects for clients from 61 countries. Its residents account for more than 80% of the industry. For five consecutive years, Belarus has been one of the world's top economies showing the most dynamic growth of IT indices, which reflects not only its modern and advanced information and communication infrastructure, but also shows how it is used by its society, business, and state.[17] Over the past ten years (since 2013), export of IT services from Belarus has grown more than 50-fold. The software developed by the HTP is supplied to 67 countries, with half of the exports going to West Europe, and a little less, to the United States. Besides, HTP residents have entered the markets of the Philippines, Vietnam, Turkmenistan, and Mexico for the first time [Turban G.V., 2018]. In the meeting between the Presidents of Russia and Belarus on 18 February 2023, President Aleksandr Lukashenko confirmed that Belarusian IT companies had received orders from Russia worth more than USD 300 million.[18] That attests to efficient co-operation with Russia as well.

All those data testify to a dynamic growth of the Belarusian IT market, which is only possible if considerable tax preferences are in place. Since 2005, an HTP with a preferential tax regime for companies has functioned in Belarus. HTP residents do not pay: VAT (20% rate), profit tax (18%), land tax on plots within the HTP, real estate tax on fixed assets located in the HTP, VAT on goods import into the custom territory, or customs duty (the rate for these taxes is zero). The Presidential Decree 'On the Development of Digital Economy' of 21 December 2017 established an even more

[17] Support to IT Countries in the EAEU. Available at: URL: https://grataned.com>laravel>filemanager>files (accessed: 15.02. 2023)

[18] RF Companies Order Products Worth USD 300 Million from Belarusian IT Sector. Available at: URL: https://www.9111.ru (accessed: 19.02. 2023)

preferential tax regime for IT activities in the Republic of Belarus and extended the pre-existing favourable tax regime till 2049. The positive experience of Belarus in taxing the IT industry consists, firstly, in its simple registration procedure for HTP residents that enables most of the Belarusian IT industry to work in a preferential zone and know its long-term prospects. And, secondly, it means complete exemption from the main taxes, which comprehensively encourages the industry's development.

3.2. IT Industry in Kazakhstan

The Kazakh IT industry has been actively developing and now includes big, medium and small business segments. The major companies in Kazakhstan are Yandex, Aviata, Tickets.kz, Documentolog, Glovo, inDirver, Wolt, Ticketon, Logicom, Asia-Soft, and EPAM. One well-known IT start-up project is the Chocofamily group of companies that offers e-commerce and other IT services in various areas. The state encourages the development of the IT industry by adopting various programmes that include tax support measures, in particular. The Government of the Republic of Kazakhstan developed a *Digital Kazakhstan* State Programme, under which an *Astana Hub* International Technopark for IT start-ups was founded in 2018. The Technopark performs a broad range of functions, including those related to IT activities.

The IT companies in the Technopark are fully exempt from the corporate tax, individual income tax, VAT and social tax on non-residents, land tax and property tax. Unlike in Russia and Belarus, foreign IT companies are also allowed to work in the Astana Hub, subject to a simple registration procedure. Since early 2021, 70 foreign companies have been registered in Astana Hub and have become part of its system to develop start-ups in Kazakhstan. They represent countries such as Russia, Kyrgyzstan, Belarus, Israel, UAE, South Korea, China, Japan, Singapore, the UK and the US.[19] Astana Hub co-operates with foreign IT companies and attracts them as members of the technopark with tax resident status that entitles them to the same tax benefits as those granted to domestic IT companies. That became possible after the Government established a procedure for registering foreign legal entities on an extra-territorial basis, i.e. the IT company is no longer required to be located in the national territory, while the procedure

[19] Astana Hub Advises 468 Foreign Companies on Relocation to the Republic of Kazakhstan. Available at: URL: https://kapital.kz (accessed: 17.02.2023)

itself may be passed on the eGOV.kz portal, which takes one to two days.[20] A foreign company may also work in Kazakh territory in the tax non-resident status and then pay its taxes on a non-preferential basis.

Kazakhstan has thus established a fairly streamlined regime of registration and working in the Technopark for its domestic IT sector as well as foreign IT companies, both attracted by preferential taxation. It should say that the IT industry follows the rule that greater openness is better for the country, for the entry of a foreign component into the domestic IT market will only strengthen the country's position in the sphere.

In this connection we see the situation in the Russian Federation is different. Firstly, there is nothing of this kind in Russia. Under the national tax law, a foreign company is recognised to be a tax non-resident from the outset and already has no access to a preferential tax regime. Secondly, amid the international sanctions many well-known foreign IT companies have decided to cease their activities in Russia: Microsoft suspended its sales of goods and services; Oracle — a developer of database management and analytics software; Cisco –a network solutions provider that held some 50% of the market of network infrastructure; Nokia, a leading global manufacturer of telecommunication equipment; Apple–services; Adobe–developer and seller of Photoshop, Premiere, and Lightroom software. Acronis, Arbor, Citrix, Docker, ESET, Unity, Miro, Pearson VUE, Zabbix, Matlab and some other companies have also announced that they leave the Russian IT market or suspend their activities.[21] Russian-made analogues of those companies can certainly be developed (which is being done), but that will take time. So it would be appropriate to use Kazakhstan's experience in this area. A streamlined extra-territorial procedure should be adopted for foreign IT companies from friendly countries to register in resident status, which will give them access to preferential taxation in the SEZ.

3.3. IT Industry in Kyrgyzstan

It is export-oriented. 84% of its IT services are export products that go to countries like the USA, Kazakhstan, Russia, Australia, Singapore, Kuwait, Ireland, the UK, etc. In 2013, a High Technology Park was established in Kyrgyzstan. Its main purpose is to support the software development sector

[20] Ibid.

[21] They Quit for Good: which IT Companies Left Russia. Available at: URL: https://hightech.fm>it-companies-went-away (accessed: 17.02. 2023)

of the IT industry. The HTP now includes 100 resident companies, most of them foreign IT businesses.[22] It is a zone with a special tax law regime that for its residents. This special tax regime exempts the residents from taxes and provides insurance contribution benefits for 15 years since the HTP was created (i.e. till 2028). HTP residents pay 0% profit and sales taxes, a 5% income tax and make deductions of 1% of revenue to maintain the HTP ecosystem.

Access to those tax preferences is provided by HTP resident status. Registered as resident may be a national or foreign legal entity or individual who/that derives at least 90% of their income from IT activities listed in the HTP Rules. Yet, the Kyrgyz law provides for a lengthier procedure of getting one than in Kazakhstan. It starts with primary registration for six months, with a certificate issued to this effect. After six months, the IT company is expected to submit a report on tis activities and confirm the grounds for getting a permanent HTP resident status. If the HTP's management body, the Directorate, finds the company's activities conducted during the (six-month) primary registration period to have been proper, the entity will be finally registered as an HTP and a report to this effect will be entered in the register of HTP residents. Final registration is of unlimited duration and is confirmed by certificate. Foreign individuals and legal entities may be registered as residents irrespective of their location. Such a favourable tax policy boosts both national companies' and foreign IT businesses' interest in the HTP in Kyrgyzstan. The number of residents grows from year to year. In our opinion, a broad list of IT activities that permit entry into the HTP is another tax incentive for the Kyrgyz IT industry. Here the legislator does not distinguish between Software Companies (specialising in high technology) and other IT activities. In other words, the state provides full and uniform support in the field.

So, it will be appropriate to take into account both the Kyrgyz and Kazakh experience in designing tax benefits for the Russian IT industry. This includes a simpler registration procedure for both domestic and international IT businesses as zone residents; allowing individual professionals to register in the SEZ (in Russia, only IT companies have access to the SEZ). And, no less importantly for the Russia — also along the lines of Kyrgyz law, this means a wider list of IT activities (works/services) that permit state accreditation and granting SEZ resident status. In Kyrgyzstan their list is broader, which naturally facilitates IT businesses' access to a favourable taxation regime, encourages the development of the national IT industry and makes it more competitive in the international IT industry market.

[22] Support for IT Companies in EAEU…

Conclusion

In taxing IT industry, Russia and EAEU countries use a set of tax benefit mechanisms such as tax incentives, a simplified taxation system, special economic zones, and HTPs. The Russian Federation uses a selective and differentiated approach to tax benefits for its IT industry that separates most companies from the preferential taxation regime. In the future, that may lead to weak and slow development of the Russian IT industry. It should ensure uniform use of tax incentives in taxing IT industry in the whole territory of the Russian Federation.

Positive experience of taxing the sector in Belarus consists, firstly, in a simple registration procedure for HTP residents that enables most of the Belarusian industry to operate in the preferential zone in the long run, and, secondly, in complete exemption from the main taxes combine to stimulate the Belarusian industry. In Russia, the procedure for entering the SEZ is rather complicated and requires accreditation of an IT company,that includes a set of strict and imperative conditions and actually weakens overall development of the IT industry.

It will be proper for the Russian Federation to take into account the Kazakh experience of streamlining the procedure for the registration of foreign IT companies from friendly countries in resident status, on an extra-territorial basis, that will provide access to preferential taxation in the SEZ. Foreign companies' resident access to SEZ in Russia promotes implementation of new information technology and exchange of experience with Russian IT companies.

The positive experience of Kyrgyzstan in tax benefits for its IT industry consists in a simplified procedure for registration and access to its HTP established for national and international IT companies and individual IT professionals and in a broad list of IT activities that does not distinguish between Software Companies (specialising in high technology) and those not specialising in such technology. In Kyrgyzstan, their list is broader, which improves IT businesses' access to a favourable tax regime, encourages the development of the industry and makes it more competitive internationally. Such rules should be used to stimulate the domestic IT industry.

The experience of tax benefits for the IT industry in the EAEU countries shows that the approach used helps bring most of the national IT companies and individual IT professionals together in a special economic zone or HTP, which is beneficial both for those companies and individuals, due

to preferential taxation, and for the Government that takes stock of them and the products and discoveries they make. In the Russian Federation, IT companies are fragmented and more difficult to monitor in this respect, unless they work in the SEZ.

References

1. Aliyev B.K. (2008) Tax system: concept, structure and parameters. *Nalogi*=Taxes, no. 3, pp. 16–18 (in Russ.)

2. Barulin S.V. et al. (2008) Tax management. Manual. Moscow: Omega, 269 p. (in Russ.)

3. Gadzhieva E.Yu. (2018) Outsourcing in IT technologies. *Vestnik Yuzhnogo institute upravlenia*=Bulletin of Southern Institute of Management, no. 1, pp. 35–37 (in Russ.)

4. Gromov V.V. (2022) Special regime of taxation of Russian IT companies: from the choice of preferences to the tax maneuver in the industry. *Finansovyi zhurnal*=Financial Journal, vol.14, no. 3, pp. 9–27 (in Russ.)

5. Katsman F.M. (2007) Special economic zones. *Ekonomika i financy*= Economics and Finance, no. 8, pp. 22–26 (in Russ.)

6. Kouam J., Asohgu S. (2022) Effects of taxation on social innovation and implications for achieving sustainable development goals in developing countries. *International Journal of Innovation Studies*, vol. 6, pp. 259–275.

7. Kozyrin A.N. (2021) Tax law. Moscow: Higher School of Economics, 487 p. (in Russ.)

8. Krasyukov A.V. (2007) Reception of private law mechanisms in tax regulation. *Vestnik Voronezhskogo universiteta*=Bulletin of Voronezh State University, no. 2, pp. 255–267 (in Russ.)

9. Lazarev V.I. (2009) Legal regulation of tax relations in the Russian Federation. *Trudy Rossiyskoy Akademii advokatury i notariata*=Scholar Works of the Russian Academy of Advocacy and Notaries, no. 3, pp. 79-82 (in Russ.)

10. Lukoyanov I.V. (2015) IT outsourcing in Russia. *Sovremennye issledovania sotcialnyh* problem=Modern Studies in Social Issues, no. 4, pp. 379–388 (in Russ.)

11. Morozova A.A. (2011) Economic and organizational and managerial aspects of tax regulation. *Terra economicus*, vol. 9, no. 1, pp. 126–129 (in Russ.)

12. Mukherjee A., Singh M., Zaldokas A. (2017) Do corporate taxes hinder innovation? *Journal of Financial Economics,* vol. 124, pp. 195–221.

13. Muradkhanova Z.S., Musaeva Kh. M. (2019) Special tax regimes: advantages and disadvantages. *Ekonomika i biznes*=Economics and Business, no. 12, pp.134–136 (in Russ.)

14. Nogina O.A. (2017) Concept and signs of a special tax regime. *Aktualnye problemy rossiyskogo prava*=Issues of Russian Law, no. 11, pp. 68–73 (in Russ.)

15. Panskov V.G. (2018) Special economic zones: results and development prospects. *Aktualnye problemy ekonomiki*=Issues of Economics, no. 7, pp. 39–53 (in Russ.)

16. Serdyukov A.E., Vylkova E.S. (2008) Taxes and taxation. Manual. Saint Petersburg: University Press, 704 p. (in Russ.)

17. Stepanenko V.V., Ermakova E.A. (2012) Tax control in Russia: organization and directions of development. Saratov: State Socio-Economic University Press, 132 p. (in Russ.)

18. Turban G.V. (2018) Development of IT services in Belarus. *Ekonomicheskyi vestnik universiteta*=Economic Bulletin of University, issue 22, pp. 1–7 (in Russ.)

19. Zhigunova E.N. (2014) The content of tax regulation and its main tools. *Vestnik Rossiyskogo kooperativnogo universiteta*=Bulletin of the Russian University of Cooperation, no. 1, pp. 44–49 (in Russ.)

Information about the authors:

M.A. Perepelitsa — Doctor of Sciences (Law).

V.V. Mironchukovskaya — Candidate of Sciences (Philosophy).

The article was submitted to editorial office 21.02.2023; approved after reviewing 09.03.2023; accepted for publication 28.04.2023.

Legal Issues in the Digital Age. 2023. Vol. 4. No. 2.
Вопросы права в цифровую эпоху. 2023. Том 4. № 2.

Research article
УДК: 34.07
DOI:10.17323/2713-2749.2023.2.46.77

Talent Acquisitions and Lock-in Agreements: Antitrust Concerns

Aleksey Yurievich Ivanov[1], Olga Andreevna Nikolaenko[2]

[1, 2] National Research University Higher School of Economics, 20 Myasnitsky Str., Moscow 101000, Russia,
[1] aivanov@hse.ru
[2] oagavrilova@hse.ru

Abstract

In recent years companies are paying more and more attention to the promising ideas and researchers within their fields. In various pharmaceutical sectors, most part of the firms is buying talent but not a customer base and products. When a company is acquiring a controlling stake in a smaller research and development-focused firm, the vendor is often the leading researcher and she are retained by non-compete clauses, confidentiality clauses and other forms of obligations that will keep the person working exclusively for the target. Acquisitions and strategic collaborations with far-reaching lock-in effects have suffered from underenforcement of competition law, and that neither United States antitrust agencies nor the European Union Commission, nor the competition authorities of the BRICS countries have sufficiently addressed the innovation concerns raised in these regards. Our proposal, which we admit requires further analysis and development, is to view researchers and key individuals as innovation assets — and to recognise these assets on the input markets or R&D markets that they *de facto* are active on. This would enable analysis of whether large corporations are essentially vacuuming the relevant research and development markets and creating dead zones devoid of any new ideas.

Keywords

acquisition; talents; innovation asset; competition law; antitrust enforcement; research and development market; non-compete clause.

For citation: Ivanov A.Yu., Nikolaenko O.A. (2023) Talent Acquisitions and Lock-in Agreements: Antitrust Concerns. *Legal Issues in the Digital Age,* vol. 4, no. 2, pp. 46–77. DOI:10.17323/2713-2749.2023.2.46.77

Introduction

It seems that there is a general consensus that the benefits of unfettered innovation far exceed the potential gains of making markets more competitive by driving prices closer to marginal costs. In light of this, one obvious issue should be, whether competition authorities should take innovation and the disbursement of research and development (R&D) capabilities into consideration, perhaps even as the ultimate goal when screening concentrations under merger law or collaborations as regards anti-competition agreements.

Globally there is a booming start-up trend, where entrepreneurs are encouraged to pursue their ideas and nascent business strategies and where large incumbent firms are paying close attention to the promising ideas and researchers within their fields of business. In various industries, such as Big Tech, biotech and pharma, incumbent firms are purchasing ideas and talents in the form of start-ups, rather than a customer base and products. Cases where companies make merger and acquisition (M&A) deals to acquire specific R&D projects are currently common within the digital economy and all industries with a strong innovative component. In research-driven organisations, the employees controlling and developing the research or business strategies are considered highly valuable assets. When incumbent firms buy R&D or tech start-ups, they usually want to acquire the ideas, knowledge and research methodology held by the key employees [Zingales L., 2000: 29].

Generally, the incentive for an incumbent firm to purchase a start-up is matched by an equal incentive for the entrepreneur to be purchased. Many entrepreneurs today seek not to 'innovate to compete' with incumbent firms, but rather to 'innovate for sale'. They seek not to enter the market as a competitor of the incumbents, often larger firms — instead providing a nascent business potential or even threat to the incumbent firms. The ultimate goal is to be purchased. Indeed, in several industries, it seems that incumbent firms purchase research or management teams' ideas and talents. They have as a strategy to accumulate the valuable assets constituted by the key employees' goals, research, tacit knowledge and experience. This can

strengthen an incumbent firm's competitive advantage in the market. Innovation, in a broad sense, is acquired and competitive threats are neutralised. However, the competitive threat is mainly contained in the entrepreneurship of the key employees, and to neutralise this threat, key employees often need to stay on in the firm for some time after the purchase. The entrepreneurs may agree to this because they have launched the start-up with the aim to sell it to an incumbent for remuneration, rather than to compete with the incumbent.

Restrictions on entrepreneurs and key employees may negatively affect the economy in general and the development of innovations, especially in the digital, pharmaceutical or biotech sectors. When unique entrepreneurial and research assets are locked in, they are not sufficiently used in society, causing welfare losses.

The article presented deals with the issue identified above, and authors intention is to consider whether large firms' strategy of 'talent acquisitions' may lead to antitrust concerns. The authors start with addressing how incumbent firms may purchase, retain and lock in talent through acquiring firms and start-ups. They will also address the conduct of incumbent firms to neutralise nascent ideas and talents through various lock-in efforts. How are such restrictions addressed as ancillary agreements to mergers, and how can the parties to a merger circumvent restrictions found to violate merger or competition law? The article also address the neighbouring and equally important issues of whether firms can lock in and neutralise competitive threats and talent through strategic alliances, R&D collaborations and license agreements[1].

It is of interest show that the conduct of incumbent firms to lock in and neutralise nascent ideas and talent is not addressed under competition law. These set-ups are very rarely scrutinised, even though large incumbent firms are capable — through transactions and collaborations — exclusively obtain relevant research results and unique business ideas, while locking in researchers and inventors. Lastly, it is proposed in the article how the analysis under competition and merger law may be adapted so it addresses

[1] In a recently published FTC report focusing on mergers in the digital sector, several forms of relevant transaction were identified: Voting Security (Control); Voting Security (Minority); Asset transactions; Patent Acquisition; Hiring Event; Non-Corporate Interest (Control); Non-Corporate Interest (Minority); License agreements and transaction in reference to Economic Interest. Cf. 'Non-HSR Reported Acquisitions by Select Technology Platforms, 2010-2019: An FTC Study' 2021. Available at: https://www.ftc.gov/system/files/documents/reports/non-hsr-reported-acquisitions-select-technology-platforms-2010-2019-ftc-study/p201201technologyplatformstudy2021.pdf (accessed: 01.11.2022)

these concerns, to more adequately encourage innovation and competition. Author's proposal (that authors freely admit requires further analysis and development), is to view researchers and key individuals as innovation assets — and to recognise these assets on the R&D markets that they *de facto* are active on. This would enable analysis of if incumbent firms are essentially vacuuming the relevant R&D markets and creating dead zones devoid of any new ideas.

1. Talent Acquisition

In recent years companies are paying more attention to the promising ideas and researchers within their fields. In various technology and pharmaceutical environments, firms are buying talent — rather than a customer base and products. Cases where companies make M&A deals to get a management or R&D team are common on digital markets and markets with a strong innovative component. For example, Google and Apple have the tendency to acquire both talent and technology at a share that exceeds 70%. Microsoft acquired technology in approximately 99% of its acquisitions, but it acquired talent in approximately 50% of its M&A deals. On the other hand, Facebook, tended to acquire talent through its acquisitions, at a rate of more than 92%, while technology transfer only occurred about half the time [Parker G., Petropoulos G., Van Alstyne M., 2021: 1316].

The Merriam-Webster Dictionary defines an asset as a valuable person or thing[2]. Talent employees are the key intangible asset. In 1999 the management guru Peter Drucker drew conclusion that the most valuable asset of a 21st-century institution (whether business or nonbusiness) will be its knowledge employees [Drucker P., 1999: 91]. Those talents refer to more than just investment but also the ability to manage and grow an asset management business [Haitao L. et al., 2011: 60]. The main argument of this article is that talent acquisition leads to significant assets concentration and may harm innovations and competition.

It seems that when a company purchases research or management team talent, it accumulates one of the most valuable assets in the digital economy era — the key employees' research, tacit knowledge and experience. This can strengthen a company's competitive advantage in the market. The company often gains new knowledge and takes a step up the knowledge ladder, getting closer to marketing for example new drugs or tech services

[2] Available at: https://www.merriam-webster.com/dictionary/asset (accessed: 14.11.2022)

to their customer base. When such practices are common, it may negatively affect the economy and development of innovations, especially in the digital, pharmaceutical or biotech sector. Big companies can acquire the talent from their competitors or potential competitors (with highly substitutable technologies) in order to protect their market position and eliminate the market competition threat[3]. This section describes how talent acquisition may lead to antitrust concerns, killer acquisitions or even dead zones in the markets.

Axel Gautier and Joe Lamesch in considering the large companies' strategies found that most acquisitions were undertaken to strengthen innovation efforts by purchasing R&D talent. The empirical study showed that 60% of start-up acquisitions led to a discontinuation of the purchased brand's service. These results clearly indicated that companies were buying talent, rather than a customer base [Gautier A., Lamesch J., 2020: 4]. Moreover, they showed that many purchasers created benefits and welfare for both the parties involved and society at large. Researchers, focusing on corporate and start-up collaborations, outlined that the practice of acquiring a company specifically to access its talent has become a crucial acquisition strategy in digital businesses, more so than acquisition of technology or other assets. Sometimes they identified hiring talents one of the factors motivating start-up acquisitions. Castanias and Helfat emphasised top management as a key resource for sustained competitive advantages for a firm [Castanias R., Helfat C., 1991: 155].

Still, considerable evidence suggests that large companies use acquisitions to consolidate their position on the market, gaining competitive advantages[4]. The acquiring firms, purchasing management teams and key researchers, increase their market power. Jaclyn Selby and Kyle Mayer, showing distinct benefits of talent acquisitions, relied on the hypothesis that firms were increasingly engaging in acquisitions of start-ups with the intention to acquire talented employees to help solve problems needing innovative solutions [Selby J., Mayer K., 2013: 5]. Acquisitions within core and adjacent markets, to complement internal innovations, can provide access to cutting-edge technology[5], while neutralising potential competitive threats. Since a start-up firm's most valuable asset is its human capital,

[3] Ibid.

[4] Why do Companies Merge with or Acquire other Companies? February 7, 2022. Available at: https://www.investopedia.com/ask/answers/why-do-companies-merge-or-acquire-other-companies/ (accessed: 22.10.2022)

[5] 'How to Innovate the Silicon Valley Way'. 2016. Available at: https://www2.deloitte.com/content/dam/insights/us/articles/tapping-into-silicon-valley-culture-of-innovation/DUP_3274_Silicon-Valley_MASTER.pdf (accessed: 22.10.2022)

acquiring a start-up company serves as an alternative way to capture new talent. It seems that talent acquirers obtain the following significant competitive advantages:

First, hiring by acquisition may save money and time, particularly when hiring or training is costly or slow, when a firm is seeking employees with unique or valuable skills, or when bringing in teams has advantages over hiring employees individually on the labour market. Some companies systematically engage in acquisition to obtain a larger skilled workforce [Ouimet P., Zarutskie R., 2011: 2].

Second, acquiring companies gain employees with particular skills to create a product that interests consumers. This includes not only specific mental and social abilities, but also tacit knowledge. Coff suggests that general human assets can be a valuable source of business advantages if they are rare, have no strategic substitutes, and the firm can retain them over time [Coff R., 1997: 378]. Talent acquisition enables the buyer to leverage the skills of its new, experienced employees to enter a new space quickly, even if the buyer is inexperienced in that market.

Third, start-up acquisitions allow the purchaser to strategically select a team of employees who have proven theirs ability to work together productively. According to several studies, having a well-matched team may increase employee retention. Companies prefer purchasing teams over purchasing individuals due to the manifold benefits of established and highly skilled teams. Growing evidence on peer effects and 'co-mobility' suggests that co-workers often prefer to continue working together [Marx M., Timmermans B., 2017: 1120]. Thus, acquisition of an entire team can lead to higher retention of employees [Selby J., Mayer K., 2013: 7, 18]. Firm-specific skills often include tacit knowledge of interpersonal relationships or corporate culture. These are elements of social complexity. Talent teams contribute to competitive advantages thanks to their inimitability, which is based on their intangible, firm-specific and socially complex nature [Hatch N., Dyer J., 2004: 1155]. Coyle and Polsky point out that talent acquisition allows a company to obtain many talents at once. It also allows the buyer to obtain well-functioning team of individuals who will often continue to work as a team, with expertise in a particular field — as opposed to assembling such a team from scratch [Coyle J., Polsky G., 2013: 294, 302].

Indeed, there is a large volume of academic research that points to the fact that talent acquisitions are beneficial for the, often larger, purchaser,

which efficiently acquires entrepreneurial and research skills and simultaneously defuses potential competitive threats. However, can we match these research to practice? Do we see talent acquisitions in, for example, the digital economy and the pharmaceutical industry?

For two decades, a significant number of top technology talent acquisitions in the digital economy have been observed. Facebook, Amazon, Apple, Microsoft, and Alphabet have performed multimillion-dollar acquisitions, most recently to acquire AI-powered businesses with great technical minds employed[6].

Looking only at the first half of 2020, in the biotechnology and pharma sectors, there are many revealing transactions, such as the purchasing by the American multinational pharmaceutical company Merck (also known as MSD) of the privately-held company Themis, focused on vaccines and immune-modulation therapies for infectious diseases and cancer[7]; the acquisition of Stratos Genomics, an early-stage sequencing technology company by Swiss cancer giant Roche[8]; the purchasing of the USA-based medical technology firm Valeritas Holdings by Danish biotech Zealand Pharma[9]; and the acquisition of the specialty pharmaceutical company Correvio Pharma Corp by global pharmaceutical company Advanz Pharma[10]. Many or all of these transactions had the clear aim to acquire promising research and researchers.

---

[6] How Big Tech Got so Big: Hundreds of Acquisitions. Available at: https://www.washingtonpost.com/technology/interactive/2021/amazon-apple-facebook-google-acquisitions/ (accessed: 22.11. 2022)

[7] Merck to Acquire Themis. Available at: https://investors.merck.com/news/press-release-details/2020/Merck-to-Acquire-Themis/default.aspx (accessed: 25.11.2022)

[8] Roche Acquires Stratos Genomics to Further Develop DNA Based Sequencing for Diagnostic Use. Available at: https://www.roche.com/media/releases/med-cor-2020-05-22b.html (accessed: 25.10.2022)

[9] Available at: https://www.globenewswire.com/news-release/2020/05/22/2037818/0/en/Zealand-Pharma-announces-FDA-acceptance-of-New-Drug-Application-for-the-dasiglucagon-HypoPal-rescue-pen-for-treatment-of-severe-hypoglycemia.html (accessed: 25.11.2022)

[10] Limited to Acquire Specialty Pharmaceutical Company Correvio Pharma Corp. Available at: https://www.advanzpharma.com/news/2020/advanz-pharma-corp-limited-to-acquire-specialty-pharmaceutical-company-correvio-pharma-corp# (accessed: 25.11.2022). Mark Corrigan, Correivo Chief Executive Officer, noted 'talented employees from the two organizations together will deliver increased scale, depth of commercial capability, breadth of geographical reach and complementary business models to bring important medicines to patients across the globe'.

2. Antitrust Harm

As addressed by Eric Posner and Cristina Volpin several years ago, NCAs enable employers to cartelise labour markets[11]. There are growing concerns about the potential for concentrated market power on labour markets[12,] especially in niche segments where entrepreneurs and researchers cater to a certain business or technology. As has been shown by this article, concentration and lock-ins in reference to such individuals can moreover harm innovation and the development of a specific industry. If an incumbent firm uses 'carrot and stick' packages that include lock-in covenants such as *de jure* or *de facto* NCAs when purchasing or collaborating with new R&D-driven firms, that will deter other firms and investors from entering the relevant labour and innovation market because they will have trouble hiring the individuals who could produce innovations for the future. Furthermore, the individual researchers will be locked in and cannot pose a relevant competitive threat to the incumbents. The incumbent firms will, with this strategy, control the development of the innovations in the business segment, especially if they continuously purchase or enter into new collaborations with promising new R&D start-ups. Thus, NCAs may be used to consolidate or expand power in the labour market [Naidu S., Posner E., Weyl E., 2018: 596], and may, together with other lock-in mechanisms such as delayed milestone remunerations, hamper and stall the relevant input market for innovations and R&D by locking in the key R&D assets, i.e., innovators and researchers.

It should be underlined that the differences between the US and EU are shrinking as regards the matter of identifying antitrust harm in competition in innovation. Both the US agencies and the European Commission have actively considered innovation in a series of recent merger cases. In the EU, these have involved, for example, exploring the possibilities that horizontal mergers would lead to a loss of innovation by eliminating a strong innovator already present on the market or that would likely have entered existing markets or that would have created entirely new value chains, thus preventing consumers from gaining increased choice and variety[13].

[11] Available at: https://www.concurrences.com/en/review/issues/no-4-2020/droit-et-economie/eric-a-posner (accessed: 27.11.2022)

[12] Available at: https://rooseveltinstitute.org/2018/03/05/a-new-study-of-labour-market-concentration/ (accessed 27.11.2022)

[13] US cases: Complaint, Amgen Inc., 134 FTC. P.333, 337–339 (identifying a research and development market for inhibitors of cytokines that promote the inflammation of hu-

It could be argued that the same development may be detected in US case law[14]. In a recent paper written by the current and former chief economists

man tissue); Wright Med. Tech., Inc., Proposed Consent Agreement with Analysis to Aid Public Comment, 60 Fed. Reg. 460, 463. Jan. 4, 1995 (identifying a research and development market for orthopaedic implants for use in human hands); American Home Prods. Corp., Proposed Consent Agreement with Analysis to Aid Public Comment, 59 Fed. Reg. 60,807, 60,815. Nov. 28, 1994 (identifying a research and development market for, among other things, rotavirus vaccines). See also Statement of the FTC in the Matter of Nielsen Holdings N.V. and Arbitron Inc., File No. 131-0058, September 20, 2013; and FTC Press Release, 'FTC Puts Conditions on Nielsen's Proposed $1.26 Billion Acquisition of Abritron, September 20, 2013; DOJ press release April 27, 2015. Available at: http://www.justice.gov/opa/pr/applied-materials-inc-and-tokyoelectron-ltd-abandon-merger-plans-after-justice-department; DOJ Complaint, USA vs Bayer AG and Monsanto Company, May 29, 2018, para 61.

EU cases: COMP/M. 5675 — Syngenta/Monsanto's Sunflower Seed Business, Commission decision of 17 November 2010, para 248, 200, 207 (finding that farmers would have suffered from reduced choice); COMP/ M.6166 — Deutsche Börse/NYSE Euronext, Commission decision of 1 February 2012, section 11.2.1.3.4, confirmed by Case T-175/12, Deutsche Börse AG v. Commission, ECLI: EU: T: 2015: 148; Case No COMP/ M.7326, Medtronic/ Covidien, Commission decision of 28 November 2014; Case No COMP/M.7275, Novartis/ GlaxoSmithKline's oncology business, Commission decision of 28 January 2015; Case No COMP/ M.7559, Pfizer/Hospira, Commission decision of 4 August 2015 Case No COMP/ M.7278, General Electric/Alstom (Thermal Power- Renewable Power & Grid Business), Commission decision of 8 September 2015. CASE M.7932 — Dow/DuPont, Commission decision of 27 March 2017.

[14] See: Statement of the FTC in the Matter of Nielsen Holdings N.V. and Arbitron Inc., File No. 131-0058, September 20, 2013; and FTC Press Release, 'FTC Puts Conditions on Nielsen's Proposed $1.26 Billion Acquisition of Abritron' September 20, 2013. See DOJ press release of April 27, 2015, available at <http://www.justice.gov/opa/pr/applied-materials-inc-and-tokyoelectron-ltd-abandon-merger-plans-after-justice-department>. See DOJ Complaint … May 29, 2018, para 61. The DOJ was specifically concerned about loss of innovation competition in the 'bundle' of traits and herbicides, recognising the importance of complementarities across these two areas ('Bayer is motivated to pursue trait research in part because successful commercialisation of a trait will generate additional returns through the sale of the associated herbicide, and vice versa' (DOJ Competitive Impact Statement, para 22). See also DOJ complaint, para 36 ('Going forward, competition between Bayer and Monsanto to develop next-generation weed-management systems is likely to increase.'). According to a Bayer strategy document, the company's number one 'Must Win Battle' is to '[e]stablish Liberty Link as a foundation trait for broadacre [row] crops and position Liberty herbicide as the superior weed management tool.' (Liberty is the commercial name of Bayer's herbicide, and Liberty Link is the name of its genetically modified seeds.) In expressing these concerns, the DOJ specifically emphasised the role of contestability absent the merger, and of greater cannibalisation after the merger: 'Absent the merger, Bayer and Monsanto would have each incentive to pursue these competing pipeline projects [in next-generation weed management systems] because any new innovation developed would help win market share from the other. In contrast, the merged firm will have different incentives due to heightened concerns that new innovation would simply cannibalize sales.'DOJ Competitive Impact Statement, para 10.

of the US and EU competition authorities, Giulio Federico, Fiona Morton and Carl Shapiro seem to endorse that there is a general test for establishing whether innovation in the industry as a whole would decrease due to a merger. This could be done, for example, by dividing horizontal pharma merger cases into different groups: product-to-pipeline overlaps; pipeline-to-pipeline overlaps, and, more generally; competition in innovation (e.g., overlap in innovation capabilities). The last group of cases is a result of a general approach where the lessening of innovation in the industry as a whole has been scrutinised [Federico G., Morton F., Shapiro C., 2019: 12].

We propose that the above test can be used when analysing whether lock-in clauses for key researchers, representing R&D assets and innovation capabilities, concentrate competition in innovation or on innovation markets, when used in mergers, strategic alliances, R&D collaborations or license agreements. Long-term lock-in covenants where researchers and other key employees risk losing substantial investments in the project should be regarded as potentially restricting competition in innovation, while making the innovation market and the labour market of researchers and key employees less dynamic and flexible.

Talent acquisitions are a reality seems clear — but what effects do such acquisitions have on the vendor, management and key employees?

3. Non-Compete Provisions and Deferred or Conditional Compensation for the Acquired Firms' Founders and Key Employees

There are concerns in academic community that systematic talent acquisition in a particular market sector and retention of workers using covenants, such as non-compete and confidentiality clauses, can lead to market concentrations [Marinescu I., Hovenkamp H., 2019: 1056]. Further, when the buyer integrates prominent start-ups and their market developments, this affects the input market of new ideas where it has its core business.

These concerns seem not to be purely academic. According to a recently published report entitled 'Nearly a Decade of Unreported Acquisitions by the Biggest Technology Companies', authored by the FTC, where more than 600 transactions in the digital economy were screened, most target firms were found to have been established less than five years before their purchase. The report set out to scrutinise whether non-compete provisions and deferred or conditional compensation to the acquired firms' founders

and key employees could be identified. More than 75 percent of the analysed transactions included non-compete clauses for the founders and key employees of the acquired entities. Higher value transactions were more likely to involve non-compete clauses[15]. This positive correlation was mainly driven by transactions of $25 million or less. When smaller firms were acquired, the likelihood that employees were transferred to the acquirer was also significantly higher than in other mergers[16]. Based on the report, it seems feasible to draw the conclusion that start-up firms were often acquired by large tech firms that demanded non-compete covenants, with key employees often agreeing to be transferred.

It is clear that entrepreneurs are increasingly aiming to be acquired, instead of running their own competing businesses. Selling a nascent company to for example Google or Facebook could be more attractive than running a business in competition with these firms. However, it should be noted that in order for the entrepreneur/innovator to receive an attractive price, and for there to be strong long-term driving forces to develop new innovations, there must be sufficient competition over each business and its innovations. However, if large incumbent firms gain a reputation of either purchasing all start-ups in a specific field of innovation at a low price or otherwise trying to exclude them from the market, that can make other investors shun start-ups in that field. This would create a so-called killing or dead zone [Rizzo A., 2021: 4]. A dead zone represents a concentration of the purchasing market of start-ups in a specific field of business, but also a concentration of a research field, if the start-ups represent a R&D pole or R&D avenue. This is common in the pharma or biotech sectors, but concentration in input markets can be seen in other areas too.

Labour market concentration, when a small number of companies dominate hiring on the market, is becoming increasingly common in some areas and frequently escapes the attention of antitrust authorities. Concentration resulting from acquisitions of promising firms and start-ups with talented researchers and their retention by large companies may have adverse effects in the economy. Lack of competition on the labour market for researchers or on the R&D market has the same negative effect on production as a

[15] Non-HSR Reported Acquisitions by Select Technology Platforms, 2010-2019: An FTC Study. Available at: https://www.ftc.gov/system/files/documents/reports/non-hsr-reported-acquisitions-select-technology-platforms-2010-2019-ftc-study/p201201technologyplatformstudy2021.pdf (accessed: 09.11.2022)

[16] Ibid.

lack of competition on the commodity market. The antitrust mechanisms of market definition, concentration measurement and primary case management based on concentration effects and consumer welfare assessments can be adapted to mergers affecting labour markets [Marinescu I., Hovenkamp H., 2019: 1063].

In turn, a company's dominant position in the labour market allows it to accumulate research teams. Predatory takeovers of R&D teams on one product market will allow the company to concentrate this market's leading research. Such a high competitive advantage, which may not be expressed in money, can lead to dominance on the input market. It can also lead to dead zones[17]. An example of both killer acquisitions and talent acquisition is the case in 2010 when Facebook bought the file-sharing service Drop.io, or more precisely, most of Drop.io's technology and assets. Sam Lessin from Drop.io was also moved to Facebook. Drop.io supported saving of all kinds of document types (pictures, video, audio, documents, and more) on a server, for transfer to other users. The company soon shut down all accounts. Also in 2010, there was another case of a killer acquisition of start-up talent. Facebook acquired the social activity and 'check-in' service provider Hot Potato. The start-up shut down all operations in about a month and deleted all data. The deal was made with the aim to bring in more talent, rather than to expand a product line[18].

A purchasing company may nudge an acquired research team to continue working on a start-up project within the company or may complete all the developments of the purchased start-up. Project closure does not always accompany talent acquisition. Sometimes, a team is bought with the intention to acquire a project and continue it. This notwithstanding, there is a group of mergers where incumbent companies buy target start-ups and talents of innovative start-ups to kill theirs research projects and retain the researchers. In recent years, there has been a significant amount of merger activity involving large firms buying highly valued start-ups, especially in the technology, pharmaceutical and biotechnology sectors. Research has shown that these purchasers have aimed to terminate the research projects and prevent the researchers from continuing to conduct the competing re-

[17] See for detail: 13 Acquisitions Highlight Big Tech's AI Talent Grab. Available at: https://venturebeat.com/2020/12/25/13-acquisitions-highlight-big-techs-ai-talent-grab-in-2020/ (accessed: 9.09. 2022)

[18] Confirmed Hot Potato: Yup, Facebook Bought 'Em, Will Soon Shut Them Down. Available at: https://techcrunch.com/2010/08/20/facebook-buys-hot-potato/?_ga=2.236007427.367507840.1635507570-1920559926.1633516617 (accessed: 9.09. 2022)

search[19]. One or more large companies on a market can accumulate the talents of innovative start-ups and discontinue their innovation projects, thus pre-empting future competition[20]. As shown above, recent economic research of M&A activities led to the conclusion that the concept of 'killer acquisition' should perhaps be viewed even more broadly than the definition suggested by Cunningham et al. [Cunningham C. et al., 2020: 31].

Below, the contractual tools available for incumbent firms to purchase start-ups and neutralise competitive threats through killer acquisitions and by creating dead zones are discussed. Thereafter, authors of the article explore, how Big Pharma and Big Tech engage not only in share deals for the acquisition of start-ups, but also in asset deals and in long-term strategic alliances that can include license agreements and R&D collaborations. The research teams of small companies are being poached by pharmaceutical and tech giants and involved in their R&D projects, which may simply be another way to neutralise potentially disruptive technology. Covenants that lock in acquired talents, which will be discussed below, are not only an exacerbating factor in reducing competition, but might also open for killer acquisitions and dead zones.

4. Ancillary Agreements to Mergers Whereby \ Key Employees Are Locked in

An argument that could be put forward in reference to why mergers in R&D-driven industries do not represent a potential antitrust harm is that researchers holding the competition-relevant knowledge can always leave. If they disapprove of a merger, key employees can use their feet and start working for a competitor. However, is that a feasible line of argumentation, or are researchers locked in and retained by Big Pharma firms? Does this occur to such a degree that lock-ins could restrain research or prevent new innovations in a field of R&D?

A rarely researched issue in reference to the regulation of mergers is the lock-in efforts imposed on the vendor and the target's management, including leading researchers[21]. When a larger pharma or Big Tech firm

[19] OECD. Competition Committee. Start-Ups, Killer Acquisitions, and Merger Control. Available at: https://one.oecd.org/document/DAF/COMP/WD(2020)17/en/pdf (accessed: 01.11.2022)

[20] Ibid.

[21] It should be clear that the vendor and the leading researcher and management can be the same person. The Commission has accepted longer non-compete provisions if a vendor retains a stake in the business being sold, or when a vendor stays on and becomes part

is acquiring a controlling stake in what is often a smaller R&D-focused firm, the vendors are usually represented in the management and are often key employees in the start-up. They can be retained by covenants in the agreements with the purchaser, requiring them to stay with the company for a certain time after the control of the firm or the relevant research has been transferred to the purchaser. Often, the management is encouraged to invest in or will hold a minority share of the target after the purchaser has obtained control. Having the management act as investors has many advantages. It make them co-investors and co-owners of the success or failure of the company, while also making it possible — through covenants in shareholder agreements — to encompass them with non-compete clauses, confidentiality clauses and other forms of obligations that keep them working exclusively for the target. Indeed, notwithstanding the findings of Cunningham et al., it seems common when a big firm has identified some key employees in a target (often including the inventor) that such individuals are pursued with both carrot and stick to keep working for the target after the merger. Often, the purchaser wants the key individuals not only to hold some shares in the firm, but also to enter into option programmes or purchase options in the firm. Such investments should be perceived as 'substantial' by the key individuals, but without them gaining any form of control over the firm. The key employees should thus be presented with a carrot, in the form of an option programme, as well as a stick, in the form of a large personal investment. This will keep them in the firm, while ensuring that the R&D avenues are determined by the purchaser.

When entering such agreements, the individuals can be encompassed, either personally or through holding companies, by non-compete and confidentiality covenants in shareholder agreements or similar collaboration contracts for the joint ownership of the target [Domeij B., 2016: 249]. They will usually commit to staying on in the firm for a period of time, or risk the loss of milestone payments or the personal investments made in share and option programmes. The idea is that the individual should be offered a lucrative programme that will be paid out after a certain period of time (or in milestones) when the firm, the molecule or drug is proven successful, but that the individual also makes a substantial personal investment in this result.

---

of the new management (for example has a position on the board of the target). See M.1298 *Kodak/Imation* 23 October 1998. M.57 *Digital/Kienzle* (27 February 1991) or M.105 *ICL/Nokia Data* 17 July 1991. See also XXI *Report on Competition Policy* 1991; also C-42/84 *Remia*, pp. 18–20.

The two ingredients — non-compete clauses and having the key employee investing their own money through a holding company in the project — can work very effectively to keep or lock in key individuals when a target is purchased by a larger firm. The individuals will through their investments be subjected to shareholder agreements that may include non-compete and confidentiality clauses that often go beyond what is in accordance with national labour laws and principles. At the same time, they can be viewed as owners rather than employees of the target under national corporate rules and merger and competition law [Hansen J., Lundgren Ch., 2014: 537].

5. Non-Compete Covenants in M&A Transactions

Given the above, it has a sense to take a closer look at the legal instruments to retain highly skilled talents and prevent researchers from developing their research elsewhere. In accomplishing an acquisition deal, it is common practice to conclude several agreements, including restrictive covenants designed to reinforce retention. Often, this will be done in confidentiality and non-competition agreements (NCAs), but such covenants can also be embedded in attractive retention programmes. NCAs are contractual provisions that normally prohibit vendors, shareholders and employees from working for a competing company or forming a new firm as a competitor in specific industries, with a certain geographical scope for a specified period. Further, not only the employment agreement, but also the shareholder agreement may include non-compete obligations and confidentiality clauses. Non-compete clauses in shareholder agreements impose restrictions on the purchased entity's owners' conduct, to prevent a decrease of the acquired business value [Domeij B., 2016: 249].

This raises a question: does this practice promote or reduce competition in the market? In the development of niche or highly advanced technologies and the formation of a crucial role for R&D teams, the retention of researchers may become a significant concern for competition in innovation. Jonathan Pollard (2020) underlined that NCAs must be assessed primarily in terms of antitrust law. If it is unreasonable and unnecessary to protect legitimate business interests, it is illegal and raises an antitrust concern. In some cases, such restraints have a clear goal: to eliminate competition[22].

[22] Employee Non-Compete Agreements as Section 1 Antitrust Violations. 2020. Pollard PLLC. Available at: https://www.pollardllc.com/non-compete-agreements-section-1-antitrust-violations/ (accessed: 21.11.2022)

The cited above research of Eric Posner and Cristina Volpin indicates that NCAs enable employers to cartelise labour markets. There are growing concerns about the potential for concentrated market power to harm innovation and the economy[23]. Also, if a company uses NCAs, new firms will be deterred from entering the labour market because they will have trouble hiring. Thus, NCAs can be used to consolidate or expand power on the labour market [Naidu S., Posner E., Weyl E., 2018: 596]. The lock-in effects of NCAs thus affect not only individual entrepreneurs, being coerced into not starting competing companies, but also the relevant input market for key employees for the industry as a whole. It is necessary to consider, in more detail, what approaches antitrust authorities in different jurisdictions are developing to regulate non-compete covenants and assess their impact on competition.

In the USA non-compete covenants in employment contracts, from an employment law perspective, are regulated at the state level. A very interesting development in that regard is that in California, where non-compete covenants in employment agreements have been declared illegal *per se*. The prohibition was enacted specifically to encourage more interaction, innovation and competition, and has a profound impact in the high-tech sectors present for example in Silicon Valley[24].

However, there are US antitrust cases concerning non-compete covenants. Several cases and arguments appear to be in favour of non-compete covenants being regarded as potential violations of Section 1 of the Sherman Act, which prohibits agreements between two or more individuals or independent entities that 'unreasonably restrain trade'[25]. Thus, the United States

[23] Available at: https://rooseveltinstitute.org/2018/03/05/a-new-study-of-labor-market-concentration (accessed: 9.09. 2022)

[24] California offers by far the most restrictive reading of NCAs in the US due to public policy concerns. California Business and Professions Code in the section 16600 states: 'Except as provided in this chapter, every contract by which anyone is restrained from engaging in a lawful profession, trade or business of any kind is to that extent void.' The Supreme Court of California stated that the inclusion of a non-compete agreement creates a significant public policy harm insofar as: 'Every individual possesses as a form of property, the right to pursue any calling, business, or profession he may choose. A former employee has the right to engage in a competitive business for himself and to enter into competition with his former employer, even for the business of those who had formerly been the customers of his former employer, provided that such competition is fairly and legally conducted.' Cont'l Car-Na-Var Corp. v. Moseley, 148 P.2d 9, 12–13 (Cal. 1944).

[25] Section 1 of the Sherman Act. Glossary. Available at: https://uk.practicallaw.thomsonreuters.com/9-502-0833?transitionType=Default&contextData=(sc.Default)&firstPage=true (accessed: 01.12.2022)

Court of Appeals, Second Circuit, in the case *Newburger*, 563 F.2d 1057 (2d Cir. 1977), considering an antitrust counterclaim, stated that if Section 1 of the Sherman Act were to be applied, two lines of inquiry seemed relevant. First, would a restrictive agreement operate in circumstances where the former employer's actual business interests were not at stake? Post-employment competition restrictions that do not serve a legitimate purpose when adopted are null and void[26]. Second, even if the provision was not overbroad *per se,* it might still be subject to a rigorous check for unreasonableness. Are the restrictions so burdensome that their anti-competitive purposes and consequences outweigh their justification[27]? Restraints that fail this balancing test might be removed under a rule of reason[28]. One of the most revealing cases was a high-tech employee antitrust litigation[29]. When restrictive covenants in employment agreements raise antitrust concerns, they can also be assessed under Section 5 of the Federal Trade Commission (FTC) Act[30], which prohibits 'unfair competition methods'. That provision empowers the FTC to initiate complaints and investigate and enter orders to prevent unfair competition methods[31]. Especially in cases where the market is dominated by the employer requiring non-competition, antitrust claims involving NCAs are more likely to succeed where the employee is highly specialised, in high demand and short supply. It is considered likely that the non-compete restriction harms a public interest in such cases[32]. Here, the FTC's decision of September 13, 2019 (Nexus Gas Transmission/ DTE Energy) is pivotal. Although a transaction did not in itself raise anti-

[26] See *Northern Pacific Ry. Co. v. United States*, 356 U.S. 1, 5, 78 S.Ct. 514, 2 L.Ed.2d 545 (1958).

[27] See *Golden v. Kentile Floors, Inc*., 512 F.2d 838, 844 (5th Cir. 1975); *United States v. Addyston Pipe Steel Co*., 85 F. 271, 281 (6th Cir. 1898), modified aff'd, 175 U.S. 211, 20 S.Ct. 96, 44 L.Ed. 136 (1899); *Lektro-Vend Corp. v. Vendo Co.*, 403 F.Supp. 527, 532–33 (N.D.Ill. 1975), aff'd, 545 F.2d 1050 (7th Cir.), cert. granted, 429 U.S. 815, 97 S.Ct. 55, 50 L.Ed.2d 74 (1976).

[28] *Newburger*, 563 F.2d 1057 (2d Cir. 1977). Available at: https://casetext.com/case/newburger-loeb-co-inc-v-gross (accessed: 16.11.2022)

[29] DOJ 'Complaint, US v. Adobe Systems Inc. et al'. December 2013. Available at: https://www.justice.gov/atr/case-document/file/483451/download (accessed: 9.10. 2022)

[30] Section 5 of the Federal Trade Commission Act. Available at: https://uk.practicallaw.thomsonreuters.com/w-007-7584 (accessed: 16.11.2022)

[31] Antitrust Considerations in Employment Agreement Non-Compete Clauses. Available at: https://uk.practicallaw.thomsonreuters.com/w-002-2106?transitionType=Default&contextData=(sc.Default)&firstPage=true#co_anchor_a000012 (accessed: 16.11.2022)

[32] Ibid.

trust issues[33], the FTC required the parties to renegotiate their agreement to sell the pipeline and remove the non-competition clause, which was not reasonably narrow in scope. The FTC barred the parties from entering into a deal before the sales agreement was amended. In its decision, the FTC emphasised that antitrust scrutiny of non-competes in M&A transactions is becoming more important[34]. Another crucial case started on January 3, 2020, when the FTC issued an administrative complaint challenging Axon Enterprise, Inc.'s finalised acquisition of its body-worn camera systems competitor VieVu, LLC, as well as specific non-compete clauses contained within the parties' transaction documents[35]. The clauses included provisions that prohibited VieVu's owner, Safariland, LLC, from competing (i) in regards to various products and services that Axon supplied, some of which the FTC alleged had no relation to the business being sold, and (ii) for Axon's customers. These covenants extended ten or more years, which was 'longer than reasonably necessary' and, in some cases, were worldwide in scope[36]. According to the complaint, Axon's May 2018 acquisition reduced competition on an already concentrated market[37]. On 9 January 2020, during a workshop dedicated to examining antitrust and consumer protection issues, the FTC emphasised that 'a non-compete covenant is unreasonably in restraint of trade if (1) the restraint is more significant than is needed to protect the business and goodwill of the employer; or (2) the promise's need is outweighed by the hardship to the promisor and the likely injury to the public'[38]. Also, the FTC noted that non-competes

[33] Gillis D., Tierney J. Merger Non-Compete Clauses — Be Lawful or Be Gone. Orrick Blogs. Antitrust Watch. Available at: https://blogs.orrick.com/antitrust/2019/09/18/merger-non-compete-clauses-be-lawful-or-be-gone/ (accessed: 16.11.2022)

[34] FTC Approves Final Order Imposing Conditions on NEXUS Gas Transmission, LLC's Acquisition of Generation Pipeline LLC. Available at: https://www.ftc.gov/news-events/press-releases/2019/09/ftc-puts-conditions-nexus-gas-transmission-llcs-acquisition (accessed: 17.11.2022)

[35] The Complaint, In the Matter of Axon Enterprise, Inc. and Safariland, LLC, FTC File No. 181-0162. 2020. Available at: https://www.ftc.gov/system/files/documents/cases/d09389_administrative_part_iii_-_public_redacted.pdf (accessed: 19.11.2022)

[36] FTC Targets M&A Agreements in Continued Campaign Against Non-compete and No-Poach Clauses. Available at: https://www.sidley.com/en/insights/newsupdates/2020/02/ftc-targets-merger-agreements-in-continued-campaign-against-noncompete-and-no-poach-clauses (accessed: 9.10. 2022)

[37] Axon Enterprise and Safariland, Matter of 2020. Available at: https://www.ftc.gov/enforcement/cases-proceedings/1810162/axonvievu-matter (accessed: 19.11.2022)

[38] FTC Workshop 2020. Available at: https://www.ftc.gov/system/files/documents/public_events/1556256/non-compete-workshop-slides.pdf (accessed: 19.11.2022)

fall under Section 2 of the Sherman Act, according to which it is illegal to 'monopolize, or attempt to monopolize, … any part of the trade …'[39]. The latest state enforcement in the USA is moving towards a more proactive position on this issue and increasingly considers NCAs to disrupt competition in markets[40]. Currently, regulators in the United States exercise close supervision of M&A transactions that significantly reduce competition and create conditions for monopolies. This trend is seen at both state and local levels in the USA. On 19 July 2019, an antitrust complaint was filed to the US District Court for the District of Colorado. It asserted violations under Section 2 of the Sherman Act. The complaint argued that Vail Health had monopolised the market for physical therapy services in Vail Valley, Colorado, which led to increased prices and obstructed competition[41]. In particular, considering the barriers to entry faced by potential competitors, it was noted that Vail Health had linked about 70% of the Vail Valley labour market for physical therapists, who are saddled with restrictive non-solicitation or non-compete covenants in their employment contracts with Vail Health[42]. The adverse impact of Vail Health's anticompetitive behaviour on competition and consumers was illustrated by the fact that over the preceding three years, three of Vail Health's competitors have closed their offices in Vail (see below).

In January 2023 the FTC has proposed banning non-compete provisions that prevent employees from working for their employer's competitors for a certain amount of time after termination. Specifically, the FTC's new rule would make it illegal for an employer to:

---

[39] Ibid.

[40] See '*WeWork Co.* (2018): Settlement with New York AG required WeWork to release 1400 employees nationwide from non-compete agreements and narrow the scope of hundreds more. *Check Into Cash* (2019): Settlement with Illinois AG prohibits Check Into Cash from requiring non-competes for store-level employees. *Law360* (2016): Settlement with New York AG requires Law360 to release all but their top executives from non-competes'. Source: 'Antitrust Update on No-Poach and Non-Compete Agreement Enforcement'. Available at: https://www.gibsondunn.com/wp-content/uploads/2020/02/WebcastSlides-Antitrust-Update-on-No-Poach-and-Non-Compete-Agreement-Enforcement-27-FEB-2020.pdf (accessed: 21.09.2022)

[41] Vail Health Hit with Monopoly Suit over Physical Therapy Services. PaRR Global (2019). Available at: https://app.parr-global.com/intelligence/view/prime-2874175 (accessed: 22.11.2022)

[42] Case 1:19-cv-02075. Complaint in the US District Court for the District of Colorado. Available at: <https://app.parr-global.com/files/cases/1858116/Complaint%20July%202019%20-%20Sports%20Rehab%20Consulting%20Llc%20et%20al%20v.%20Vail%20Clinic%20Inc%20Dba%20Vail%20Health.pdf (accessed: 22.11.2022)

enter into or attempt to enter into a noncompete with a worker;

maintain a noncompete with a worker; or

represent to a worker, under certain circumstances, that the worker is subject to a noncompete[43].

The non-compete provisions are "exploitative" and unfairly restrict the ability of 30 million Americans[44]. According to a study by economists, nearly 20% of workers in the US. have non-compete clauses in their contracts[45]. According to experts, in the case of highly skilled employees and workers from high-tech sectors of the economy, this number could reach 50%. The FTC is seeking public comment on the proposed rule, which is based on a preliminary finding that non-competes constitute an unfair method of competition and therefore violate Section 5 of the Federal Trade Commission Act[46].

The approach of antitrust authorities of European Union member states to non-competition agreements cannot be tailored to each particular case. Thus, under for example Decision n°18/01931 of the Paris Court of Appeal on 19 May 2020, an employer should prove that the company can suffer practical harm if an employee carries out professional activities in a competing company[47].

Under EU competition law, the addressees of the prohibition of anti-competitive agreements and abuse of dominance are most commonly undertakings (firms). However, there are cases where a vendor and/or management has retained a stake in the business being sold and where NCAs have been addressed by the authorities.[48] It can also be considered individuals as undertakings when autonomously offer their services on the labour

[43] FTC Proposes Rule to Ban Non-compete Clauses, Which Hurt Workers and Harm Competition. January 5, 2023. Available at: https://www.ftc.gov/news-events/news/press-releases/2023/01/ftc-proposes-rule-ban-noncompete-clauses-which-hurt-workers-harm-competition (accessed: 23.11.2022)

[44] Available at: URL: https://www.vox.com/recode/2023/1/5/23540951/ftc-lina-khan-non-compete-ban (accessed: 21.09. 2022)

[45] Available at SSRN: https://ssrn.com/abstract=2625714 (accessed: 23.11.2022)

[46] FTC Proposes Rule to Ban Non-compete Clauses, Which Hurt Workers and Harm Competition. Available at: https://www.ftc.gov/news-events/news/press-releases/2023/01/ftc-proposes-rule-ban-noncompete-clauses-which-hurt-workers-harm-competition (accessed: 23.11.2022)

[47] Available at: https://www.dechert.com/content/dam/dechert%20files/knowledge/publication/practical-law--french-q-as-regarding-restrictive-covenants-clauses/2020/RestrictiveCovenantClausesQAndAFrancePracticalLaw.pdf (accessed: 26.11.2022)

[48] See generally the EU Jurisdictional Notice 2004.

market. An article 101 TFEU could be applied to non-compete clauses that restrict (potential) self-employed activities as an employee will be affected in her capacity as a potential undertaking[49].

According to EU competition law, NCAs have been cleared as being ancillary to a merger, during the period that the vendor/management retains a stake in the target and for two or three years thereafter. Similar covenants have been accepted for vendors when they have been retained a right to pick a board member[50]. The NCAs need to encompass firms, while non-compete covenants for individuals are normally addressed only under labour law. However, non-compete covenants can be included in shareholder agreements and extend to individuals, who can sometimes be viewed as undertakings.

According to the Hungarian Competition Authority's decision regarding the restrictions related to the acquisition of the start-up Code Cool Kft, it was permissible to include restrictive covenants in the sales contract of a start-up enterprise that prevented the inventors and developers of the innovation from competing in the future based on the same idea, even though they did not retain a stake in the start-up. This permission was given to make it more attractive to invest in undertakings of a start-up type and maintain the incentive to innovate. The market value of an undertaking does not necessarily decrease after its sale[51]. On the other hand, in July 2020, the Portuguese Competition Authority issued a statement of objections to six companies and six board members of the waste management groups Blueotter and EGEO concerning an NCA[52]. In yet another example, on 29 November 2017, the Swedish Patent and Market Court ruled that five-year non-compete clauses included in share purchase agreements did not constitute an infringement of competition rules[53].

---

[49] See Judgment of the Court (Sixth Chamber) of 16 September 1999. Case C-22/98. Available at: https://curia.europa.eu/juris/liste.jsf?language=en&num=C-22/98 (accessed: 26.11.2022)

[50] See M.57 Digital/Kienzle (27 February 1991) and M.105 ICL/Nokia Data (17 July 1991); also XXI Report on Competition Policy 1991.

[51] Case VJ/19/2019. The GVH Facilitates Investment in Startups with a Guideline Decision (2020). Available at: https://www.gvh.hu/en/press_room/press_releases/press-releases-2020/the-gvh-facilitates-investment-in-startups-with-a-guideline-decision (accessed: 26.11.2022)

[52] AdC Issues Statement of Objections to Six Waste Management Companies for Non-Competition Agreement. Available at: http://www.concorrencia.pt/vEN/News_Events/Comunicados/Pages/PressRelease_202012.aspx (accessed: 29.11.2022)

[53] European Competition Network Brief. 'The Swedish Patent, and Market Court uphold Stockholm District Court's decision that Excessively Long Non-Compete Clauses

Currently, as presented brief comparative study shows, NCAs are lawful and enforceable in various jurisdictions as long as they fulfil the applicable conditions. There does not seem to be any criteria that precisely prevents competition from being influenced by talent buying. It seems possible to list the minimum conditions in the NCAs. In this case the antimonopoly authority in each specific case should analyze these conditions and conclude if it harms competition and innovations. Traditionally, provisions regarding non-compete agreements for individuals are enshrined in labour law and not regulated in merger or antitrust legislation. Thus, in India, the antitrust authority's approach is rather one of deregulation and non-assessment of if NCAs are reasonable. On 26 November 2020, the Competition Commission of India (CCI) amended its regulations, removing the NCA disclosure requirement from merger filings[54]. Earlier, on 15 May 2020, the CCI invited the public to comment on its proposal to remove non-competitive valuation as part of a merger review. The CCI clarified that this was due to such assessments not being practical given the dynamic business environment and the short time frame for considering a merger[55]. For comparison, it is necessary to analyse the CCI's decision in 2012, regarding the proposed sale by Orchid Chemicals and Pharmaceuticals Ltd (OCPL) of its betaculum API (active pharmaceutical ingredient) business, its manufacturing facilities, another manufacturing facility in Aurangabad and an R&D facility in Chennai, to Hospira Healthcare[56]. There was a significant roadblock to obtaining the CCI's requisite approval: the non-compete clause in the business transfer agreement. It stipulated that OCPL and one of its promoters could not conduct certain commercial activities concerning the 'transferred business' for eight and five years, respectively. The cov-

in Share Purchase Agreements do not Infringe Competition Rules by the Object' (Alfa Quality Moving) e-Competitions Art. N° 86359. Available at: https://www.concurrences.com/en/bulletin/news-issues/november-2017/the-swedish-patent-and-market-court-upholds-decision-by-stockholm-district (accessed: 29.11.2022)

[54] The Competition Commission of India (Procedure regarding business transaction relating to combinations) Amendment Regulations. Available at: https://www.cci.gov.in/sites/default/files/regulation_pdf/CCINonCompRegl261120.pdf (accessed: 29.11.2022)

[55] Chand A.et al. India: Non-Compete Covenants out of the CCI's Merger Control Net. Khaitan & Co. Available at: https://www.mondaq.com/india/antitrust-eu-competition-/1012828/non-compete-covenants-out-of-the-cci39s-merger-control-net (accessed: 29.11.2022)

[56] Orchid Chemicals gets CCI not for Hospira deal. Available at: https://economictimes.indiatimes.com/industry/indl-goods/svs/petrochem/orchid-chemicals-gets-cci-nod-for-hospiradeal/articleshow/17747201.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst (accessed: 29.11.2022)

enant also stipulated a restriction on the R&D of specific APIs for injectable formulations. The CCI requested that the duration of non-compete commitments be limited to four years for the domestic market in India and that OCPL should be allowed to conduct research, development, and testing of new molecules that could result in the development of new penem and penicillin APIs for injectable formulations, which were non-existent. Thus, in 2012, the CCI expressed a clear position on non-competitive provisions, demanding changes in order to approve a transaction[57].

However, this does not mean that NCAs for vendors, board members and shareholders cannot be subject to consideration in the antitrust field. Individuals autonomously offer their services in the labor market. They may be subject to antitrust law that follows from the fact that the purpose of regulating competition is the basic prohibition against monopolization of the market as a method of combating abuse of right. A company's employees can influence the company's position in the competitive market by their decisions. Therefore, the manipulation of NCAs in order to retain these individuals in the company can be considered from the perspective of competition law. Several antitrust concerns and adverse effects of NCAs on competition have been discussed above, as well as some indicative antitrust cases. It seems clear that a Big Pharma or Big Tech firm can neutralise a specific start-up as a competitive threat with smart M&A tactics and non-compete and confidentiality covenants. The purchaser could require the vendor to retain a minority share and have the leading inventor subject to a shareholder agreement or put on the board of the post-merger entity. In such cases, NCAs are considered benign by many, if not all, competition authorities, even if they are of long duration and lock in the inventor for an extended period of time[58]. Perhaps this does not pose a problem, and if an individual researcher or inventor agrees to be locked in, he or she should be free to do so. But, as will be discussed below, if this means that an indispensable or necessary R&D asset or inventor is taken out of the relevant research field or R&D market — such covenants should be considered anticompetitive and causing antitrust harm. Thus, there may be a deficit in

[57] CCI. Order under Section 31 (1) of the Competition Act, 2002. Available at: https://www.cci.gov.in/sites/default/files/C-2012-09-79_0.pdf (accessed: 12.12.2022).

[58] For example, in South Africa, the antitrust authority has requested companies to consider altering restrictive covenants affecting individuals by shortening the duration of restrictions at the subnational level to no more than three years. Available at: https://uk.practicallaw.thomsonreuters.com/2-504-5969?transitionType=Default&contextData=(sc.Default)&firstPage=true (accessed: 12.12.2022).

competition and merger law concerning regulation of non-compete covenants in these circumstances. On the other hand, antitrust authorities can, should they choose to do so, judge NCAs as not being ancillary to merger deals, within the adequate framework. Also, it is important to note that even when a transaction does not raise antitrust issues, antitrust agencies can still consider transaction agreements not to be ancillary to the transaction[59]. The antitrust authorities should be developing requirements that non-compete covenants should be reasonably 1) protective of the legitimate business interest and 2) limited in time, geographical scope and the market or types of economic activities/services encompassed. We can observe this approach to regulation in Brazil. In 2019, a Note was submitted for Item 4 of the 131st OECD Competition committee meeting on 5–7 June, according to which companies should ensure that non-competition provisions in transaction documents are business-fit and reasonable in duration and scope. According to this Brazilian Note, non-competition clauses can constitute labour market antitrust violations[60].

It appears that with the increase of the nascent practice of innovator acquisitions and its negative impact on competition, antitrust authorities may need to outstrip legislators and develop approaches for assessing the impact of NCAs on competition.

Based on the above, anti-competitive effects which arise as a result of NCAs might significantly hinder the economy's innovative development and outweigh any potential benefits (for instance, protection of trade secrets) [Lovells H., 2020: 25]. With digitalisation penetrating all spheres of society and the high value of advanced technologies, the supervision of M&A transactions has become somewhat strengthened. In several jurisdictions, antitrust authorities have begun to realise the significant impact on competition of buying and retaining talent. It is becoming essential to develop a new evaluation approach in competition law, based on practice, and pursue more thorough analysis of one of the leading talent retention instruments in M&A deals — non-compete covenants.

However, tying down of individuals or specialised R&D-driven firms through up-front or *de facto* non-compete covenants does not need to be

[59] Gillis D., Tierney J. Merger Non-Compete Clauses…

[60] Competition Issues in Labour Markets. Note by Brazil. This document reproduces a written contribution from Brazil submitted for Item 4 of the 131st OECD Competition committee meeting on 5–7 June 2019. Available at: http://www.oecd.org/daf/competition/competition-concerns-in-labour-markets.htm (accessed: 14.12.2022)

done through mergers. Big Pharma or biotech firms often do not need to resort to purchasing promising research results by merging with the often smaller R&D-driven firms. Indeed, there are several other forms of collaboration that the parties can enter where the larger pharma firm is still granted control of the promising research result, while neutralising the competitive threat represented by the start-up. While mergers are sometimes used to exclude certain parts of management (as shown by Cunningham *et al.*), they — like other forms of collaborations — may be built on the active inclusion of the inventor and the R&D start-up management. Then, the R&D start-up is controlled through covenants regarding *inter alia* R&D agreements, exclusive licenses, scholar boards and option programmes. In some jurisdictions, such control would trigger an obligation to notify the collaboration under the merger regime[61], while in others, this would scrutinised *ad hoc* under the prohibition on anticompetitive agreements[62]. Non-compete covenants are the most clear-cut way to control potential competition, but confidentiality agreements and acknowledgement of trade secrets may also be implemented to the same or similar effect.

6. Strategic Alliances, R&D Collaborations and License Agreements

As stated above, one of the results of the trend for specialisation by firms in the pharma and biotech sector is the great increase in the amount of technology transfer, licenses and collaborations entered into by independent parties [Robinson D., Stuart T., 2007: 559]. Today, not even the largest pharmaceutical firms conduct research, develop and market drugs and treatments in-house. Instead, we are seeing an increase in collaborations in the form of license agreements, R&D ventures and co-marketing agreements to develop and market new research result into drugs. Generally, pharma and biotech firms are collaborating more and more and thus are

[61] See for example the recently published FTC report focusing mergers in the digital sector, several forms of relevant transaction were identified: Voting Security (Control); Voting Security (Minority); Asset transactions; Patent Acquisition; Hiring Event; Non-Corporate Interest (Control); Non-Corporate Interest (Minority); License agreements and transaction in reference to Economic Interest. Cf. Non-HSR Reported Acquisitions by Select Technology Platforms, 2010-2019: An FTC Study 2021. Available at: https://www.ftc.gov/system/files/documents/reports/non-hsr-reported-acquisitions-select-technology-platforms-2010-2019-ftc-study/p201201technologyplatformstudy2021.pdf (accessed: 16.12.2022)

[62] For instance, under EU merger law.

entering into more and more agreements on the creation, facilitation and transfer of patents, molecules, knowledge and technologies. Such exchange or transfer of information and ideas, coupled with both complex agreements with terms, obligations and covenants that may exclude and restrict the parties and the market transparency due to the patent and market approval procedures, creates a rather distinctive setting for this industry [Arnold K. et al., 2002: 1085].

Often before any intellectual property rights have been established, agreements between parties needs to be adjoined with confidentiality obligations. Even after the intellectual property rights (often patents) have been established, confidentiality agreements are important for the protection of the 'know-how' that accompanies the patents and are usually included in technology transfer agreements when a substance or molecule is transferred between firms. However, know-how is often retained by key employees.

In the early to middle stages of the development of a molecule, the firms may enter into collaborations regarding R&D. The R&D agreements may be concluded for several reasons. There is a genuine need for a meeting of the minds of researchers to create something. Different firms may hold core knowledge in different parts of the innovation chain, with one firm having developed the research tools that a second firm needs to understand and use. Perhaps there are no intellectual property rights established yet, so any transfer and joint creation of knowledge needs to be boxed in by confidentiality covenants. Moreover, joint R&D agreements often focus on the mechanism for dividing the intellectual property rights once the collaboration has ended.

From the parties' perspectives, the basis for any form of collaboration in the pharma or biotech sector relies heavily on the 'license agreement'. In fact, there are numerous sorts of agreements that pharma and biotech firms may enter, but at the heart of them all, irrespective of what they are called, is often a right or license to use a patent covering a molecule or antidote, to develop and sell a drug or treatment, or an assignment to develop a research result and then license or assign the developed product further. Even share or asset transfer agreements of R&D firms often include elements of assignment of patent rights or licenses, since innovations are the main assets that a purchaser wants to acquire and control, often in conjunction with the transfer of the necessary know-how held by researchers. Indeed, remuneration for shares or assets is often exclusively connected to

milestones for the development of the research into a drug, e.g., clinical testing, successful phase I, phase II, etc.

This notwithstanding, it seems that license agreements with connected collaboration features, *inter alia* setting up a board of academic experts from both the Big Pharma firm (licensee) and the R&D start-up (licensor), are generally more popular than mergers for transferring promising research results[63]. In both license agreements and alliances, success hinges upon the setting up of a scientific board of experts, including the inventors and other researchers connected to the start-up. They are often retained and must commit to spending a certain number of hours in the strategic alliance and actively pursuing the R&D of the molecule and the project. They will also be encompassed by NCAs.

A licensing agreement in the pharma sector, though not implying a change of control over the firm, may thus often stipulate a transfer of the main assets (molecule and connected know-how) and an in-depth and lengthy collaboration between the parties, including specific covenants that the licensor make specific researchers available to spur the development of the drug. The smaller firm acts as a licensor, while the scientific board is granted the right to decide on the further development of the molecule into a drug. The larger firm is thereby *de facto* granted an exclusive license to develop the substance or molecule further, since they control the majority of the scholar board[64].

Still, the smaller firm needs to provide know-how and guidance by granting access to experts to serve on the research board/committee and oversee the development under the license agreement. The collaboration may last for a long period of time, possibly until the end of commercialisation of the drug in every relevant jurisdiction, while the licensee (the Big

[63] For example, a Deloitte report from 2015 showed that of all alliances reported between January 2011 to May 2012, 751 consisted of licensing, while 498 were M&A. Cf. R. Marcello and others. *Executing an Open Innovation Model: Cooperation is Key to Competition for Biopharmaceutical Companies*. 2015. It also showed that Open Innovation is more successful than Closed Innovation. See also A. Pavlou and M. Belsey, 'BioPharma Licensing and M&A Trends' 2005 4 *Nature Reviews Drug Discovery,* pp. 273–274. See also for example McKinsey. Available at: https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/whats-behind-the-pharmaceutical-sectors-m-and-a-push# (accessed: 16.12.2022)

[64] The licensee, the larger pharma or biotech firm, is generally not bound by a non-compete obligation. On the contrary, the agreements often explicitly state that the licensee is not bound by a non-compete.

Pharma firm) often holds the exclusive prerogative to determine whether, and at what speed, the research result is to be developed[65].

Interestingly, a license and collaboration agreement as presented above is generally more lucrative and less risky for Big Pharma to enter into than being forced to purchase and merge with smaller R&D-intensive firms to gain access to the interesting R&D results. With the use of the *de facto* exclusive license and a collaboration agreement including non-compete covenants, the larger firm will control the start-up, the molecule or substance. The lock-in effects for the R&D-focused firm are also substantial. Often, the Big Pharma firm does not need to transfer an up-front purchase sum when entering into a license agreement. It takes no risk. Instead, remuneration under the license agreement is transferred to the R&D start-up in dispersed milestone payments, connected to the various stages in the development of the drug. This creates incentives (both carrots and sticks) for the inventors and vendors in the start-up to keep working for the development of the molecule or drug, even when the molecule and patents have been exclusively licensed to the Big Pharma firm. Further, it gives the larger firm control over when remuneration has to be paid.

The collaborations falling short of being mergers may not need to be notified under the merger rules in certain jurisdictions, since it is not certain that they represent change of control and the exclusive license does not imply the transfer of a turnover source, as the research result is not yet generating any turnover[66]. They might under certain jurisdictions be required to be notified as joint ventures, if they are considered fully functioning or are concentrations (mergers). However, the requirements for 'fully

[65] The licensor should be made aware that it needs to enclose in the agreement hard milestones connected to future dates, so as to push forward the development of the research result. It should be noted that the licensee often has an obligation to return the exclusivity to the licensor should it decide not to pursue the development further. This notwithstanding, there are licensing agreement where there is no one-time up-front payment, with all remuneration to the licensor being triggered by milestones, which the licensee *de facto* decides when to meet.

[66] Only exclusive licenses can, in certain cases, trigger an obligation to notify under the EU Jurisdictional Notice 2008, see para 24. A transaction confined to intangible assets such as brands, patents or copyrights may be considered to be a concentration if those assets constitute a 'business with a market turnover'. In any case, the transfer of licences for brands, patents or copyrights, without additional assets, can only fulfil these criteria if the licences are exclusive, at least in a certain territory, and the transfer of such licences will transfer the turnover-generating activity. As regards non-exclusive licences, it can be excluded that they, *per se,* constitute a business with a market turnover. For an interesting decision in reference to this issue, cf. M.5727 *Microsoft/Yahoo!* Search business (18 February 2010).

functioning' joint ventures are high and hard to meet[67]. Moreover, even if they are notified, the great majority of the collaborations in the pharma sector — reflecting the above scenario — are generally *ex ante* viewed as beneficial for the parties, the industry and society at large. From a competition law perspective, analysing the agreements *ex ante*, such collaborations must often be deemed pro-competitive. Usually, they cannot be regarded anticompetitive — for several reasons. The research conducted by the R&D start-up may be in early stages and there can be great uncertainties regarding whether the research will actually result in an effective drug. The Big Pharma firm is needed to conduct the necessary testing and development of the drug, and the potential killing aspects of the collaboration cannot be detected based on the wording of the collaboration. However, a competition authority's conclusions in such a case may be based on using the wrong tests and not taking innovation into consideration to the degree needed, because the collaborations can hide efforts by Big Pharma to kill or shelve the promising research result and lock in the researchers. An analysis may reveal that the Big Pharma firm is in fact monopolising the input R&D market, creating a dead zone where no research is conducted. Indeed, such collaboration can be as detrimental to competition and innovation as killer mergers. This will be discussed below.

This notwithstanding, it should be pointed out that the terms and conditions of such collaborations reflect poor business acumen on behalf of the management and owners of the smaller R&D-driven firms, who are often innovators themselves or closely connected to the innovators. In the biotech and pharma industries, researchers often have their main employment at a university. The mergers or license agreements sometime reflects a clash between idealistic researchers and shrewd businessmen. What these collaborations will often *de facto* come to represent is an agreement of transferring know-how and research results with a guarantee from the small R&D-driven firm to exit the research area when the transfer has been completed and the researchers have proven if the molecule is successful or not. Indeed, what they represent from an *ex post* perspective is an agreement not to compete in the future, while the inventors are given remuneration during the period of time that the non-compete obligation is in effect. Of course, innovation for sale must be honoured, and competition authorities need to tread lightly so as not to discourage innovation — but collaborations of this type do not efficiently utilise innovations and researchers.

[67] See: EU Jurisdictional Notice 2008, para 91 et seq.

Moreover, especially in the pharmaceutical sector, researchers may hold highly unique knowledge and retaining such researchers under non-compete covenants may cause enormous welfare losses, especially if the aim of the R&D collaboration, from the perspective of the larger license, is to stall and eventually kill a potential competing drug.

Conclusion

From the above, it seems clear that acquisitions, licensing agreements and R&D collaborations with far-reaching NCAs have been under-regulated in competition law, and that neither US antitrust agencies nor the EU Commission have sufficiently addressed the innovation concerns raised in these regards. The research of Cunningham and his co-authors showed that killer acquisitions do occur, and as licensing and R&D collaborations are more common than mergers, one can presume that killer R&D collaborations and killer license agreements are commonplace. Moreover, the acceptance of large firms' M&A strategies causes dead zones to emerge, where very little or no entrepreneurial efforts are invested.

Ultimately, we would like to propose how the analysis under competition and merger law could be shifted to address the concerns raised, so as to pursue innovation and competition more adequately. Our proposal, which we freely admit requires further analysis and development, is to view researchers and key individuals as innovation assets — and to recognise these assets on the input markets or R&D markets that they *de facto* are active on. This would enable analysis of if incumbent firms are essentially vacuuming the relevant R&D markets and creating dead zones devoid of any new ideas. Since innovations, R&D and nascent tech service developments are often deployed in narrow R&D avenues, finding the key individuals who are able to pursue similar entrepreneurial efforts can be important. By analysing the labour or R&D asset markets in these narrow avenues, monopolisation or cartelisation of the same can be identified.

References

1. Arnold K. et al. (2002) Value Drivers in Licensing Deals. *Nature Biotechnology*, vol. 20, no. 11, pp. 1085–1089.

2. Castanias R., Helfat C. (1991) Managerial Resources and Rents. *Journal of Management*, vol. 17, no. 1, pp. 155–171.

3. Chesbrough H. (2003) *Open Innovation: The New Imperative for Creating and Profiting from Technology.* Boston: Harvard Business School Press, 222 p.

4. Coff R. (1997) Human Assets and Management Dilemmas: Coping with Hazards on the Road to Resource-Based Theory. *Academy of Management Review*, vol. 22, no. 2, pp. 374–402.

5. Coyle J., Polsky G. (2013) Acquire-Hiring. *Duke Law Journal*, vol. 63, no. 2, pp. 281–346.

6. Cunningham C. et al. (2020) Killer Acquisitions. *Journal of Political Economy,* vol. 129, no. 3, pp. 649–702.

7. De Jong G., Klein R. (2009) The Content and Role of Formal Contracts in High-Tech Alliances. *Innovation*: *Management*, *Policy & Practice*, vol.11, no. 1, pp. 44–59.

8. Domeij B. (2016) *Från anställd till konkurrent.* Stockholm: Wolters Kluwer, 473 p.

9. Drucker P. (1999) Knowledge-Worker Productivity: The Biggest Challenge. *California Management Review*, vol. 41, no. 2, pp. 79–94.

10. Federico G., Morton F., Shapiro C. (2019) Antitrust and Innovation: Welcoming and Protecting Disruption, Innovation Policy and the Economy. Wash.: National Bureau of Economic Research, pp. 1–50.

11. Garnier J. (2008) Rebuilding the R&D Engine in Big Pharma. *Harvard Business Review*, vol. 86, no. 5, pp. 68–70.

12. Gautier A., Lamesch J. (2020) Mergers in the Digital Economy. CES info Working Paper Series. No. 8056, pp. 1–34.

13. Haitao L. et al. (2011) Investing in Talents: Manager Characteristics and Hedge Fund Performances. *The Journal of Financial and Quantitative Analysis,* vol. 46, no. 1, pp. 59–82.

14. Hansen J., Lundgren Ch. (2014) Köp og salg af virksomheder. København: Nyt Juridisk Forlag.

15. Hatch N., Dyer J. (2004) Human Capital and Learning as a Source of Sustainable Competitive Advantage. *Strategic Management* Journal, vol. 25, no. 12, pp. 1155–1178.

16. Lovells H. (2020) Key Takeaways from the FTC's Non-Compete Workshop. Antitrust, Competition and Economic Regulation. Available at: https://www.hoganlovells.com/en/publications/~/media/8516b3f2a7d9486eb8be311ce44b9633.ashx (accessed: 19.12.2022)

17. Marinescu I., Hovenkamp H. (2019) Anticompetitive Mergers in Labor Markets. Legal Scholarship Depository, pp. 1031–1063. Available at: https://scholarship.law.upenn.edu/ (accessed: 30.11.2022)

18. Marx M., Timmermans B. (2017) Hiring Molecules, Not Atoms: Comobility and Wages. *Organization Science*, vol. 28, no. 6, pp. 1115–1133.

19. Naidu S., Posner E., Weyl E. (2018) Antitrust Remedies for Labour Market Power. *Harvard Law Review*, vol. 132, pp. 537–601.

20. Norbäck P., Olofsson Ch., Persson L. (2020) Acquisitions for Sleep. *The B.E. Journal of Economic Analysis & Policy,* vol. 20, no. 2, p.13.

21. Norbäck P., Persson L, Svensson R. (2016) Creative Destruction and Productive Pre-emptive Acquisitions. *Journal of Business Venturing,* vol. 31, no. 3, pp. 326–343.

22. Norbäck P. et al. (2019) Verifying High Quality: Entry for Sale' IFN Working Paper Institute för Näringslivsforskning, p. 1186.

23. Parker G., Petropoulos G., Van Alstyne M. (2021) Platform mergers and antitrust. *Industrial and Corporate Change,* vol. 30, no. 5, pp. 1307–1336.

24. Posner E., Volpin C. (2020) Labour Monopsony and European Competition Law. Available at: https://www.concurrences.com/en/review/issues/no-4-2020/droit-et-economie/eric-a-posner (accessed: 22.12.2022)

25. Rizzo A. (2021) Digital Mergers: Evidence from the Venture Capital Industry Suggests that Antitrust Intervention Might be Needed. *Journal of European Competition Law & Practice,* vol. 12, no. 1, pp. 4–13.

26. Robinson D., Stuart T. (2007) Financial Contracting in Biotech Strategic Alliances. *Journal of Law and Economics,* vol. 50, pp. 559–596.

27. Selby J., Mayer K. (2013) Startup Firm Acquisitions as a Human Resource Strategy for Innovation: The Acquire Phenomenon. Available at: https://mackinstitute.wharton.upenn.edu/wp-content/uploads/2013/04/Selby-Jaclyn-Mayer-Kyle_Startup-Firm-Acquisitions-as-a-Human-Resource-Strategy-for-Innovation-The-Acqhire-Phenomenon.pdf (accessed: 03.12.2022)

28. Starr E., Prescott J., Bishara N. (2021) Non-competences in the US Labor Force. *Journal of Law and Economics.* Available at: https://ssrn.com/abstract=2625714 (accessed: 24.12.2022)

29. Zingales L. (2000) In Search of New Foundations. National Bureau of Economic Research. Working Paper No. 77-06, pp. 1-52. Available at: https://ssrn.com/abstract=232092 (accessed: 16.12.2022)

Information about the authors:

A.Yu. Ivanov– LLM, Director.

O.A. Nikolaenko–Candidate of Sciences (Law), Researcher.

The article was submitted to editorial office 22.03.2023; approved after reviewing 28.04.2023; accepted for publication 18.05.2023.

Legal Issues in the Digital Age. 2023. Vol. 4. No. 2.
Вопросы права в цифровую эпоху. 2023. Том 4. № 2.

Research article
УДК: 342
DOI:10.17323/2713-2749.2023.2.78.121

Balancing Cyber-security and Privacy: Legal and Ethical Considerations in the Digital Age

Naeem Allahrakha

Tashkent State University of Law, 35 uy, Sayil ko ‘ch, Toshkent 100047 sh., Uzbekistan,

Chauharynaeem133@gmail.com, 0000-0003-3001-1575

Abstract

In today’s digital world the need to maintain cyber-security and protect sensitive information is more important than ever. However, this must be balanced against the right to privacy, which is also a fundamental human right. This article provides an overview of the legal and ethical considerations involved in balancing cyber-security and privacy in the digital age. It explores the challenges of implementing effective cyber-security measures while respecting privacy rights, and discusses the current legal framework for cyber-security and privacy in various jurisdictions. The article also considers the ethical implications of balancing these two important values and suggests ways in which cyber-security and privacy concerns can be reconciled in a general context. By highlighting the importance of a careful balance between cyber-security and privacy, this article aims to raise awareness of the need for ethical and legal considerations in the development of digital technologies and their regulation.

Keywords

cyber-security; privacy; digital age; legal considerations; ethical considerations.

For citation: Allahrakha N. (2023) Balancing Cyber-security and Privacy: Legal and Ethical Considerations in the Digital Age. *Legal Issues in the Digital Age*, vol. 4, no. 2, pp. 78–121. DOI:10.17323/2713-2749.2023.2.78.121

1. Introduction

In the contemporary world with the exponential growth of digital technologies, the need to maintain cyber-security and protect sensitive information is more crucial than ever. However, this must be balanced against the right to privacy, which is also a fundamental human right. The issue of balancing cyber-security and privacy is a complex one that requires careful consideration of legal and ethical implications. [Singer P., Tushman M., 2021]. The article explores the topic in detail, examining challenges of implementing effective cyber-security measures while respecting privacy rights, current legal framework for cyber-security and privacy in various jurisdictions, and ethical implications of balancing these two values. The aim of article is to raise awareness of the need for ethical and legal considerations in the development of digital technologies and their regulation. The introduction provides an overview of the article and highlights its significance in context of digital age.

1.1. Background

The advancement of digital technologies has revolutionized the way we live, work, and communicates. The widespread use of the Internet and digital devices has made our lives easier, but it has also created new challenges, particularly in the area of cyber-security and privacy. With the increasing amount of personal and sensitive information being stored online, protecting this information from cyber-attacks has become a critical concern for individuals, businesses, and governments. At the same time, the right to privacy is also a fundamental human right recognized by international law. Protecting individuals' privacy rights in the digital age has become a challenging task, as the collection and processing of personal data have become more widespread.

Balancing the need for reasonable cyber-security measures and privacy rights has become a critical challenge for policymakers, businesses, and individuals alike. This background highlights the importance of examining the legal and ethical considerations involved in balancing cyber-security and privacy in the digital age. Understanding the challenges and implications of this balance can provide insights into the development of effective cyber-security policies that respect privacy rights [Kshetri N., 2021].

1.2. Research Problem

The issue of balancing cyber-security and privacy in the digital age presents a significant challenge for policymakers, businesses, and individuals. While cyber-security is critical in protecting sensitive information from cyber-attacks, the collection and processing of personal data raises concerns about the violation of privacy rights. The challenge is to find a balance between cyber-security and privacy that allows for the protection of sensitive information without compromising individual privacy rights. This article seeks to address the research problem of how to balance cyber-security and privacy in the digital age. The article examines the legal and ethical considerations involved in this balance, explores the challenges of implementing effective cyber-security measures while respecting privacy rights, and discusses the current legal framework for cyber-security and privacy in various jurisdictions. By doing so, the article aims to provide insights into how to reconcile cyber-security and privacy concerns in a general context.

1.3. Objective of Research

The objectives of the author are to provide an overview of legal and ethical considerations involved in balancing cyber-security and privacy in the digital age, and to explore the challenges of implementing effective cyber-security measures while respecting privacy rights. The article aims to discuss the current legal framework for cyber-security and privacy in various jurisdictions and to consider the ethical implications of balancing these two important values. The article suggests ways in which cyber-security and privacy concerns can be reconciled in a general context, highlighting the importance of a balance between cyber-security and privacy. Ultimately, the objective of the article is to raise awareness of the need for ethical and legal considerations in the development of digital technologies and their regulation.

1.4. Literature

In recent years a growing number of scholars have explored the ethical and legal implications of balancing cyber-security and privacy in the digital age. For instance, the traditional dichotomy between security and privacy is a false one, and that the two are mutually reinforcing concepts that should be balanced together. Privacy is not just an individual right, but

also serves important social and democratic functions, such as protecting free speech and limiting government overreach [Pavlou P., Lewis K., 2020].

Similarly, scholars like Greenwald have highlighted the dangers of government surveillance and data collection, arguing that these practices can undermine individual privacy rights and erode trust in democratic institutions. Greenwald, for instance, exposed the extent of U.S. government surveillance activities through his reporting on the Edward Snowden leaks, revealing how the government collected vast amounts of data on private citizens without their knowledge or consent [Greenwald G., 2021: 78–86]. Other scholars have focused on the challenges of implementing effective cyber-security measures while respecting privacy rights. For example, Yoo [Yoo C., 2015: 129–137] argues that privacy protections can actually enhance cyber-security by reducing the risks of data breaches and identity theft. However, he also notes that overly strict privacy laws can inhibit law enforcement and national security agencies from accessing important data and preventing terrorist attacks. In addition to these legal and ethical considerations, scholars have also explored the economic implications of cyber-security and privacy. Among others,some people [Acquisti A., Grossklags, 2013: 1–32] argue that privacy as a valuable commodity can be traded in the marketplace, and that individuals should be able to control how their personal information is used and monetized by businesses. Meanwhile, Cavoukian has developed the concept of "privacy by design," that emphasizes the need for businesses and technology developers to incorporate privacy considerations into their products and services from the outset.[1]

Despite these contributions, however, there is still much debate over how to balance cyber-security and privacy in the digital age. For instance, some scholars argue that the focus on individual privacy rights can undermine the collective good, while others contend that government surveillance and data collection can actually harm national security by eroding public trust and limiting cooperation between citizens and law enforcement agencies [O' Harrow R., 2017: 95–113].

1.5. Methodology

The research methodology employed in the article is a qualitative analysis of literature and legal frameworks. The purpose of the study is to pro-

[1] Cavoukian A. 2017. Privacy by design: The 7 foundational principles. Toronto, 2017.

vide an overview of the legal and ethical considerations involved in balancing cyber-security and privacy in the digital age. The study will explore the challenges of implementing cyber-security measures while respecting privacy rights and discuss the current legal framework for cyber-security and privacy in various states. In addition, the author considers the ethical implications of balancing these two important values and suggests ways in which cyber-security and privacy concerns can be reconciled in a general context. That methodology is appropriate because the topic of balancing cyber-security and privacy is complex and multi-faceted. Qualitative analysis of literature and legal frameworks is a way to examine and synthesize the current state of knowledge in this area. The methodology enables the researcher to examine multiple sources of data, identify patterns and trends, and draw conclusions based on a comprehensive analysis of the available evidence.

The approach taken in this study is based on a systematic review of the relevant literature and legal frameworks. The systematic review method involves a comprehensive and structured search of literature to identify all relevant studies. The studies are then screened and evaluated based on pre-determined inclusion and exclusion criteria. The selected studies are then analyzed and synthesized to identify key themes and patterns. The article aims to establish a methodological connection between the research objectives and the data collection and analysis methods. Methods used are designed to ensure that the research is rigorous, transparent, and replicable, and that the findings are grounded in reliable evidence. The literature review will be conducted through a systematic search of databases such as JSTOR, PubMed, and Google Scholar. The search terms used will be "cyber-security," "privacy," "legal," "ethical," and "digital age." The inclusion criteria for the literature review will be based on relevance to the research questions, quality of research, and date of publication.

1.6. Data Collection, Analysis, Limitations

The data collection is primarily based on a comprehensive review of literature, including books, journal articles, and other relevant publications. The literature review serves as the primary method for collecting data to support the arguments and analysis presented in the article. Author conducted a systematic search of various academic databases to identify relevant literature on the topic of balancing cyber-security and privacy in the

digital age. He used a combination of keywords and search terms related to cyber-security, privacy, digital technologies, legal and ethical considerations, and related topics to identify relevant publications. It also relied on secondary sources, including government reports, policy documents, and other relevant publications to supplement the literature review. These sources were used to provide additional insights into the current legal and regulatory frameworks for cyber-security and privacy in different countries.-

The information is reviewed and analyzed to identify the legal and ethical considerations related to cyber-security and privacy in the digital age. The analysis is conducted in a qualitative manner, where the data is grouped and categorized based on the themes and sub-themes that emerge from the literature review. The information is analyzed to identify the challenges of balancing cyber-security and privacy, the current legal framework for cyber-security and privacy in various jurisdictions, and the ethical implications of balancing these two values. The analysis is also used to identify potential ways to reconcile cyber-security and privacy concerns in a general context. The synthesis of the literature review is then presented in the article, with key findings and conclusions drawn from the analysis. The findings are presented in a logical and coherent manner with arguments and evidence to support the conclusions.

There are limitations to the study that must be acknowledged. Firstly, the study relies solely on secondary data sources, such as books, journal articles, government reports, and policy documents, and did not involve primary data collection methods, like surveys or interviews. While secondary sources provide a comprehensive overview of the topic, they may not be as nuanced as primary data sources in providing insights into specific perspectives or experiences of individuals or groups. The study focuses on legal and ethical considerations of balancing cyber-security and privacy and does not delve into technical aspects of cyber-security measures.

Future studies could explore the technical challenges of implementing strict cyber-security measures while respecting privacy rights.

Furthermore, the study focuses mainly on the Western legal framework, and more research is needed to explore the legal and ethical considerations in other parts of the world, especially in developing countries where digital technologies are rapidly growing. However, the article does not provide recommendations or solutions to the challenges identified in the study.

2. Cyber-security and Privacy: Definitions and Importance

2.1. Define Cyber-security and Privacy

Cyber-security refers to the practice of protecting computer systems, networks, and sensitive digital information from unauthorized access, theft, damage, or other malicious acts.[2] In the context of this article, cyber-security is especially important due to the proliferation of digital technologies and the increasing amount of sensitive data being collected and transmitted over the internet. The risks associated with cyber-attacks, data breaches, and other forms of digital crime are significant, and the consequences can be severe for individuals, organizations, and even entire countries. Cyber-security measures are essential for protecting privacy rights and maintaining the integrity of digital systems, but they must also be balanced against the need to respect fundamental human rights such as privacy and freedom of expression [Fisher D., 2021: 2129–2149].

The term "privacy" in the article refers to the right of individuals to control their personal information and to be free from unwanted or unwarranted surveillance or intrusion.[3] In the digital age, privacy concerns have become increasingly complex due to the vast amount of personal data that is collected, stored, and shared by individuals and bodies. This data may include sensitive information like financial records, medical histories, and personal communications, making it critical to ensure that privacy is protected. The article explores the legal and ethical considerations involved in balancing the need for privacy with the need for cyber-security measures, highlighting the importance of striking a careful balance between these two values [Stevens A., 2022: 45–77].

2.2. The Importance of Cyber-security and Privacy in the Digital Age

Cyber-security and privacy now are two fundamental values that are essential for individuals, businesses, and governments. Cyber-security is

[2] Rouse M. What is cyber-security? Definition, best practices & job titles. 2018. Available at: https://searchsecurity.techtarget.com/definition/cybersecurity (assessed: 18.04.2023)

[3] Universal Declaration of Human Rights, specifically Article 12: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation."

important because it involves protecting sensitive information, such as personal data, financial records, and intellectual property, from unauthorized access, theft, or damage [Luiijf E., Douma A., 2019: 3–14]. Without proper cyber-security measures in place, individuals and organizations are vulnerable to cyber-attacks, which can result in financial loss, reputational damage, or legal liability. Privacy, on the other hand, is equally important because it involves protecting an individual's right to control their personal information and how it is used. In today's digital age, individuals generate and share vast amounts of personal information online, through social media, e-commerce platforms, and other digital channels. This information can be used by companies and governments for various purposes, such as targeted advertising, market research, or national security. However, it can also be misused, leading to identity theft, stalking, or other forms of harassment. [4] Balancing cyber-security and privacy is crucial because these two values often conflict with each other. For instance, implementing strong cyber-security measures may require collecting and analyzing large amounts of personal data, which could infringe on an individual's privacy rights. Conversely, protecting an individual's privacy may require limiting the collection and use of personal data, which could compromise cyber-security [Rosenzweig P., 2015: 318–329].

Therefore, finding right balance between cyber-security and privacy is essential to ensure that individuals and organizations can benefit from the opportunities offered by digital technologies, while also protecting their rights and interests. This requires a careful consideration of legal, ethical, and technical issues, as well as the development of policies and regulations to guide the use of digital technologies in a responsible and ethical manner.

2.3. Potential Conflicts between Cyber-security and Privacy

The challenge in balancing cyber-security and privacy is to find the right strategy between maintaining a high level of security while also respecting individuals' privacy rights. This requires a multi-faceted approach that involves implementing security measures, educating users on cyber-security risks, and developing a legal and regulatory framework that protects both cyber-security and privacy. Potential conflicts can arise between cyber-security and privacy because both concepts have distinct goals that can sometimes clash. Cyber-security focuses on protecting computer systems

[4] Singer N., Helft M. Your data is crucial to a $200 billion industry. Available at: https://www.nytimes.com/2019/03/30/opinion/sunday/data-privacy.html (assessed: 18.04.2023)

and networks from unauthorized access, theft, or damage. This involves implementing various measures such as firewalls, encryption, and access controls to prevent cyber-attacks. On the other hand, privacy is concerned with protecting personal information, such as individual identities, financial details, and online activities, from unauthorized disclosure, surveillance, or exploitation.[5]

However, cyber-security measures can potentially compromise privacy by collecting or disclosing sensitive information without the user's knowledge or consent. For example, a company might use tracking cookies to monitor a user's online behavior in order to improve their cyber-security, but this could also violate the user's privacy rights. Similarly, governments might use surveillance techniques such as wiretapping or data interception to detect potential cyber-threats, but this could also infringe on individuals' privacy rights [Villeneuve E., 2022: 495–511].

Another potential conflict is the trade-off between security and convenience. Often, cyber-security measures such as multi-factor authentication or password complexity requirements can be seen as cumbersome and time-consuming for users. This can lead to frustration and may result in users bypassing security measure altogether, which in turn compromises security. Alternatively, reducing security measures to enhance convenience can make systems vulnerable to attacks and increase the risk of data breaches.

2.4. Legal Framework for Cyber-security and Privacy

The legal framework varies across different jurisdictions, but there are some common principles and regulations that are widely recognized. In the United States, for example, the main legislation governing cyber-security and privacy is the Cyber-security Information Sharing Act (CISA)[6] and the Electronic Communications Privacy Act (ECPA).[7] The European Union has implemented the General Data Protection Regulation (GDPR), which provides a comprehensive framework for data protection and pri-

[5] Iqbal M. Cyber-security vs. privacy: Protecting both in the digital age. Available at: https://www.forbes.com/sites/forbestechcouncil/2019/09/24/cybersecurity-vs-privacy-protecting-both-in-the-digital-age/?sh=3d01f7af5e11 (assessed: 18.04.2023)

[6] Cyber-security Information Sharing Act of 2015. Pub. L. No. 114-113, 129 Stat. 2242. Available at: https://www.congress.gov/bill/114th-congress/senate-bill/754 (assessed: 18.04.2023)

[7] Electronic Communications Privacy Act. Pub. L. No. 99-508, 100 Stat. 1848.1986. Available at: https://www.govinfo.gov/content/pkg/STATUTE-100/pdf/STATUTE-100-Pg1848.pdf (assessed: 18.04.2023)

vacy.[8] Other countries have also enacted laws and regulations to protect personal data and secure digital infrastructure, such as the Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada and the Cyber Security Law in China.[9] [10]

2.5. Current Legal Framework for Cyber-security and Privacy in Various Jurisdictions

In the US there are several laws and regulations that govern cyber-security and privacy. The most significant legislation is the Cyber-security Information Sharing Act (CISA) enacted in 2015 to encourage information sharing between the government and private entities regarding cyber threats. Other important laws include the Electronic Communications Privacy Act (ECPA), which regulates the interception of electronic communications, and the Health Insurance Portability and Accountability Act (HIPAA), establishing privacy standards for health information.[11] The Federal Trade Commission (FTC) has been active in enforcing privacy and data security regulations, particularly with regard to consumer protection.[12] The legal framework for cyber-security and privacy in the United States is complex and evolving, with a mix of federal and state laws, regulations, and guidelines that apply to different industries and sectors.

The current legal framework for cyber-security and privacy in Europe is primarily governed by the General Data Protection Regulation (GDPR),

[8] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN (assessed: 18.04.2023)

[9] Government of Canada. 2018. Personal Information Protection and Electronic Documents Act (PIPEDA). Available at: https://laws-lois.justice.gc.ca/eng/acts/P-8.6/ (assessed: 18.04.2023)

[10] National People's Congress. 2016. Cyber Security Law. Available at: http://www.npc.gov.cn/englishnpc/c23934/201706/a9a818170f9247d2b7294fe4cd20fadd.shtml (assessed: 18.04.2023)

[11] USA. Department of Health and Human Services (n.d.). Health Insurance Portability and Accountability Act (HIPAA). Available at: https://www.hhs.gov/hipaa/index.html (assessed: 18.04.2023)

[12] Federal Trade Commission. (n.d.). Privacy & Security. Available at: https://www.ftc.gov/tips-advice/business-center/privacy-and-security (assessed: 18.04.2023)

in effect in May 2018. The GDPR applies to all businesses operating within the European Union (EU) and regulates the processing of personal data of individuals within the EU. The regulation outlines strict requirements for obtaining consent, data breach notifications, and the right to be forgotten, among other provisions. The Network and Information Systems Directive (NIS Directive) requires EU member states to implement cyber-security measures for critical infrastructure and digital service providers, and to report major security incidents to national authorities.[13] The EU Cyber-security Act also establishes a framework for the certification of information and communication technology products and services. The legal framework in Europe prioritizes the protection of personal data and cyber-security while balancing these interests with the needs of businesses and national security concerns.[14]

In the United Kingdom main legislation governing cyber-security and privacy is the Data Protection Act of 2018[15], incorporating the General Data Protection Regulation (GDPR) into UK law. The GDPR provides a comprehensive framework for protecting individuals' personal data and sets out strict rules for the collection, storage, and processing of such data by organizations. The act also establishes the Information Commissioner's Office (ICO) as the regulator for data protection in the UK, with the power to enforce compliance and issue fines for non-compliance.[16] The UK has the Computer Misuse Act 1990 [17], that criminalizes unauthorized access to computer systems, hacking, and other cyber-related offences. The UK government has also recently introduced the National Cyber Security Strategy, which sets out a comprehensive approach to enhancing the country's

[13] European Commission. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. Official Journal of the European Union, L 194/1. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN (assessed: 18.04.2023)

[14] European Union. Cyber-security Act. Available at: https://eur-lex.europa.eu/eli/reg/2019/881/oj (assessed: 18.04.2023)

[15] Data Protection Act 2018. Available at: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted (assessed: 18.04.2023)

[16] ICO. 2018 Guide to the General Data Protection Regulation. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/ (assessed: 18.04.2023)

[17] UK Computer Misuse Act 1990. Available at: http://www.legislation.gov.uk/ukpga/1990/18/contents (assessed: 18.04.2023)

cyber-security capabilities and protecting against cyber-attacks.[18] The UK has a robust legal framework for cyber-security and privacy that seeks to balance the need for strong security measures with the protection of individuals' privacy rights.

In Canada the Personal Information Protection and Electronic Documents Act (PIPEDA) [19] is the primary legislation governing the collection, use, and disclosure of personal information by private sector organizations. It requires organizations to obtain an individual's consent before collecting, using, or disclosing their personal information, and to take reasonable measures to safeguard that information from unauthorized access, use, or disclosure. Canada's Anti-Spam Legislation (CASL) [20] regulates the sending commercial electronic messages, and the Digital Privacy Act [21] introduced several amendments to PIPEDA, including mandatory breach notification requirements for organizations. Office of the Privacy Commissioner is responsible for enforcing PIPEDA and promoting privacy rights. [22]

The United Arab Emirates (UAE) has implemented several legal measures to regulate cyber-security and privacy. One of the key instruments in this regard is the UAE Cybercrime Law criminalizing various cyber offenses, such as hacking, phishing, and spreading false information online.[23] The law also outlines punishments for violating the cyber-security of individuals or organizations, including fines and imprisonment. In addition, the UAE has established the National Electronic Security Authority (NESA), which is responsible for securing the country's critical information infra-

[18] HM Government. National Cyber Security Strategy 2016-2021. Available at: https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021 (assessed: 18.04.2023)

[19] Personal Information Protection and Electronic Documents Act. 2000. Available at: https://laws-lois.justice.gc.ca/eng/acts/p-8.6/index.html (assessed: 18.04.2023)

[20] Government of Canada. CASL of 2021. Available at: https://www.canada.ca/en/industry-canada/topics/information-communication-technology/protect-your-privacy/anti-spam-law.html (assessed: 18.04.2023)

[21] Digital Privacy Act, S.C. 2015. Available at: https://laws-lois.justice.gc.ca/eng/AnnualStatutes/2015_32/page-1.html (assessed: 18.04.2023)

[22] Canada. Office of the Privacy Commissioner. Available at: https://www.priv.gc.ca/en/about-the-opc/ (assessed: 18.04.2023)

[23] Federal Decree Law No. 5 of 2012 on Combating Cybercrimes. Available at: https://www.adjd.gov.ae/EN/MediaCenter/Publications/Pages/FederalDecreeLawNo5of2012onCombatingCyberCrimes.aspx (assessed: 18.04.2023)

structure and developing national cyber-security policies. [24] The UAE also recently enacted a data protection law, which regulates the processing of personal data and requires organizations to implement adequate measures to protect the privacy of individuals.[25] Despite these legal frameworks, concerns have been raised about the lack of transparency and due process in some cases related to cyber-security and privacy in the UAE.

In Singapore cyber-security and privacy are governed by a range of laws and regulations. The Personal Data Protection Act (PDPA)[26] is the main piece of legislation that regulates the collection, use, and disclosure of personal data in Singapore. The PDPA requires organizations to obtain individuals' consent before collecting, using, or disclosing their personal data and to take reasonable steps to protect that data.[27] The Cyber-security Act,[28] introduced in 2018, establishes a framework for the regulation of critical information infrastructure (CII) and provides for the sharing of information between CII owners and the government in the event of a cyber-attack.[29] The Computer Misuse Act[30] criminalizes various types of cyber-crime, including unauthorized access and hacking. The Monetary Authority of Singapore also issued a set of guidelines on technology risk management, that sets out best practices for financial institutions to manage cyber-risk. [31]

---

[24] National Electronic Security Authority. Available at: https://nesa.gov.ae/about-us/ (assessed: 18.04.2023)

[25] Federal Authority for Government Human Resources. 2020. UAE Federal Law No. (2) of 2019 on the Use of Information and Communications Technology in Health Fields. Available at: https://www.fahr.gov.ae/portal/en/about_fahr/news/28/3/2020/%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AD%D9%85%D8%A7%D9%8A%D8%A9-%D8%A7%D9%84%D8%B9%D8%A7%D9%85%D8%A9-%D9%84%D9%84%D8%A8%D9%8A%D8%A7%D9%86%D8%A7%D8%AA-%D8%A7%D9%84%D8%B5%D8%AD%D9%8A%D8%A9.aspx (assessed: 18.04.2023)

[26] Personal Data Protection Commission. Singapore. 2021. Personal Data Protection Act. Available at: https://www.pdpc.gov.sg/Legislation-and-Guidelines/Personal-Data-Protection-Act-Overview (assessed: 18.04.2023)

[27] Personal Data Protection Commission. Singapore. (n.d.). Personal Data Protection Act. Available at: https://www.pdpc.gov.sg/Legislation-and-Guidelines/Personal-Data-Protection-Act (assessed: 18.04.2023)

[28] Cybersecurity Act. Singapore Statutes Online. Available at: https://sso.agc.gov.sg/Act/CSA2018 (assessed: 18.04.2023)

[29] Ministry of Communications and Information. Singapore. Cybersecurity Act. Available at: https://sso.agc.gov.sg/Act/CSA2018 (assessed: 18.04.2023)

[30] Computer Misuse Act (Chapter 50A). (n.d.). Singapore Statutes Online. Available at: https://sso.agc.gov.sg/Act/COMPA1993 (assessed: 18.04.2023)

[31] Singapore's Cybersecurity Laws and Regulations. RHT Law Asia. Available at: https://www.rhtlawasia.com/singapores-cybersecurity-laws-and-regulations/ (assessed: 18.04.2023)

China has a complex legal framework for cyber-security and privacy, which is heavily influenced by the country's political and social context. The Cyber-security Law of the People's Republic of China,[32] in force since 2016, provides a comprehensive regulatory framework for cyber-security. The law requires network operators to take measures to protect the security of personal information and to report cyber-security incidents to the authorities. It also empowers the Chinese government to conduct cyber-security inspections and investigations, and to take measures to prevent and respond to cyber-security threats [Liu X., 2017: 1– 20].

However, concerns have been raised about the potential impact of the law on privacy and free speech, as well as the lack of transparency and accountability in its implementation. Also, China has a range of other laws and regulations related to cyber-security and privacy, such as the Criminal Law[33], the State Secrets Law,[34] and the Internet Information Services Regulation.[35]

In Japan legal framework for cyber-security and privacy is primarily governed by the Act on the Protection of Personal Information (APPI)[36] revised in 2020 to strengthen privacy protections for individuals. The APPI applies to both private and public sector organizations and sets out requirements for the collection, use, and disclosure of personal information, as well as the establishment of security measures to protect against unauthorized access, loss, destruction, alteration, or disclosure of personal information. In addition to the APPI, Japan has also implemented the Cyber-security Basic Act[37]; its aims are to ensure security of information and communications

[32] National People's Congress. Cyber-security Law of the People's Republic of China. Available at: http://www.npc.gov.cn/englishnpc/Law/2017-11/07/content_2039783.htm (assessed: 18.04.2023)

[33] Criminal Law of the People's Republic of China (1997, amended 2018). Available at: http://www.npc.gov.cn/npc/c30834/201807/d53b2ae7c2474f0faa8c6a312bffb3dd.shtml (assessed: 18.04.2023)

[34] National People's Congress. Law on Guarding State Secrets. Available at: http://www.npc.gov.cn/englishnpc/Law/2007-12/12/content_1383868.htm (assessed: 18.04.2023)

[35] National People's Congress. Decision of the Standing Committee of the National People's Congress on Maintaining Internet Security. Available at: http://www.npc.gov.cn/wxzl/gongbao/2000-12/15/content_5004607.htm (assessed: 18.04.2023)

[36] Ministry of Internal Affairs and Communications of Japan. (n.d.). Act on the Protection of Personal Information. Available at: http://www.soumu.go.jp/main_content/000327861.pdf (assessed: 18.04.2023)

[37] National Diet of Japan. 2014 Act on the Establishment of the Cybersecurity Basic Act. Available at: https://www.japaneselawtranslation.go.jp/law/detail/?id=3156&vm=04&re= (assessed: 18.04.2023)

networks, and the Act on the Protection of Specially Designated Secrets[38] regulating the handling of confidential information related to national security. The Japanese government has also established the Cyber-security Strategy Headquarters to promote cyber-security measures and coordinate efforts among relevant agencies and organizations.[39]

In South Korea the Personal Information Protection Act (PIPA) serves as the primary legislation governing data privacy and cyber-security.[40] The PIPA aims to protect personal information by regulating its collection, storage, use, and provision to third parties. It also mandates the implementation of appropriate security measures to prevent data breaches and requires prompt notification of affected individuals in case of any security incidents. In addition, the Network Act requires Internet service providers to retain user data for a certain period and grants law enforcement agencies access to this data under circumstances indicated in the Act.[41] It also prohibits cyber-bullying and the spreading of false information online. The South Korean government has also established the Ministry of Science and ICT and the Korea Internet & Security Agency to oversee and regulate cyber-security measures in the country.[42] [43] Despite these regulations, there have been concerns over government surveillance and censorship in South Korea, particularly in the context of national security.

Australia has a comprehensive legal framework for cyber-security and privacy. The Privacy Act of 1988 sets out the Australian Privacy Principles (APPs), which regulate the collection, use, and disclosure of personal information by government agencies and private organizations.[44] The Privacy

[38] National Diet of Japan. 2013 Act on the Protection of Specially Designated Secrets. Available at: https://www.japaneselawtranslation.go.jp/law/detail/?id=3157&vm=04&re= (assessed: 18.04.2023)

[39] Government of Japan. Cabinet Secretariat. 2013. Cybersecurity Basic Plan. Available at: https://www.nisc.go.jp/eng/pdf/CybersecurityBasicPlan_ver2.0.pdf (assessed: 18.04.2023)

[40] National Law Information Center. 2011 Personal Information Protection Act. Available at: https://elaw.klri.re.kr/eng_service/lawView.do?hseq=28399&lang=ENG (assessed: 18.04.2023)

[41] National Law Information Center. 2011 Act on Promotion of Information and Communications Network Utilization and Information Protection, etc. Available at: https://elaw.klri.re.kr/eng_service/lawView.do?hseq=29566&lang=ENG (assessed: 18.04.2023)

[42] Ministry of Science and ICT. (n.d.). About MSIT. Available at: https://english.msit.go.kr/english/main/main.do (assessed: 18.04.2023)

[43] Korea Internet & Security Agency. (n.d.). KISA Overview. Available at: https://www.kisa.or.kr/eng/main.jsp (assessed: 18.04.2023)

[44] Federal Register of Legislation. Privacy Act 1988. Available at: https://www.legislation.gov.au/Details/C2018C00243 (assessed: 18.04.2023)

Act also establishes Office of the Australian Information Commissioner responsible for enforcing the APPs and promoting privacy rights.[45] In addition, the Cyber Security Strategy 2020 outlines Australia's approach to cyber-security; it includes enhancing the resilience of critical infrastructure, promoting cyber-awareness, and strengthening law enforcement capabilities.[46] The Australian Signals Directorate (ASD) also provides guidance on cyber-security best practices for government agencies and critical infrastructure operators.[47] Australia's legal framework aims to balance the need for effective cyber-security measures with the protection of individuals' privacy rights.

The legal framework for cyber-security and privacy in South America states varies from one country to another. Brazil has implemented the General Data Protection Law to regulate the processing of personal data and protect privacy rights, which came into effect in September 2020.[48] The law applies to all businesses that process personal data, regardless of where the business is located. Mexico has the Federal Law on Protection of Personal Data Held by Private Parties, which also regulates the processing of personal data and gives individuals the right to access, correct, cancel, and object to the use of their data.[49] However, despite having legal frameworks in place, both countries still face challenges in effectively enforcing these laws and protecting the privacy of their citizens. Other South American countries such as Argentina and Chile also have legal frameworks for cyber-security and privacy, but the level of implementation and enforcement varies by country.

2.6. The Weaknesses of Legal Frameworks

One weakness of the legal framework for cyber-security and privacy in the USA is the lack of a comprehensive federal privacy law. While some laws and regulations (HIPAA and the Children's Online Privacy Protection

[45] Office of the Australian Information Commissioner (n.d.). Available at: https://www.oaic.gov.au/about-us/about-the-oaic/ (assessed: 18.04.2023)

[46] Department of Home Affairs. Australia's 2020 Cyber Security Strategy. Available at: https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy (assessed: 18.04.2023)

[47] Australian Signals Directorate. (n.d.). Cyber security guidance. Available at: https://www.cyber.gov.au/acsc/guidance (assessed: 18.04.2023)

[48] Brazilian Presidency of the Republic. 2018 Lei Geral de Proteção de Dados Pessoais (LGPD). Available at: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm (assessed: 18.04.2023)

[49] Mexican Congress. 2010 Federal Law on Protection of Personal Data Held by Private Parties. Available at: http://www.diputados.gob.mx/LeyesBiblio/pdf/316.pdf (assessed: 18.04.2023)

Act–COPPA), address specific privacy issues, there is no overarching federal law that provides a uniform standard for data privacy and protection.[50] [51]This may lead to confusion and inconsistency for both consumers and businesses. Another weakness is the fragmentation of laws and regulations across different industries and sectors. For example, financial institutions are subject to different regulations than healthcare providers or retailers. This is able to create challenges for businesses that operate across multiple industries or sectors, as they must comply with a patchwork of laws and regulations [Brennan-Marquez K., Hoffman S., 2022: 9–55].

Additionally, the legal framework may not keep pace with technological developments and new forms of cyber threats. As technology continues to evolve at a rapid pace, it is difficult for lawmakers and regulators to keep up with the latest trends and issues. It leads to gaps in the legal framework and potentially leave individuals and businesses vulnerable to cyber-attacks and privacy violations. There may be a lack of enforcement and penalties for non-compliance with cyber-security and privacy regulations. While the FTC has been active in enforcing privacy and data security regulations, there have been instances where companies have suffered data breaches or other privacy violations without facing significant consequences. It may create a perception that there is a low risk of punishment for non-compliance, which may not incentivize companies to prioritize cyber-security and privacy [Hickman L., Martin C., 2022: 73–132].

One potential weakness of the European legal framework in the field is that it may not be able to keep pace with rapidly evolving technologies and cyber threats. The GDPR, for example, was drafted prior to the widespread adoption of emerging technologies such as artificial intelligence and the Internet of Things, which present new challenges for data protection and cyber-security. The regulation has been criticized for being overly prescriptive and burdensome for businesses, particularly small and medium-sized enterprises. There is also concern that the GDPR may be difficult to enforce consistently across EU states; it could result in varying levels of protection for personal data and cyber-security in different countries. The legal framework may not be sufficient to address the challenges posed by cyber threats

[50] US Congress. Health Insurance Portability and Accountability Act of 1996. Available at: https://www.govinfo.gov/content/pkg/PLAW-104publ191/html/PLAW-104publ191.htm (assessed: 18.04.2023)

[51] US Congress. 1998 Children's Online Privacy Protection Act. Available at: https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule (assessed: 18.04.2023)

that originate from outside of the EU, highlighting the need for international cooperation and coordination on cyber-security and privacy issues [Purcell R., 2021: 135–148].

One weakness of the legal framework for cyber-security and privacy in the UK is the impact of Brexit on the applicability of the GDPR. While the Data Protection Act 2018 incorporates the GDPR into UK law, there is still uncertainty around how the UK's departure from the EU will affect the regulation's enforcement and application [White L., 2021: 8–10]. Additionally, the Computer Misuse Act 1990 has been criticized for being outdated and not providing sufficient protections against emerging cyber threats, such as those posed by nation-states or sophisticated criminal organizations. There is also the potential for conflicts between the UK's national security interests and individuals' privacy rights, which may lead to challenges in balancing the two priorities.[52] While the UK has a relatively robust legal framework for cyber-security and privacy, there is room for improvement and adaptation to meet the evolving challenges of the digital age.

One weakness of Canada's legal framework in the area is that PIPEDA only applies to private sector bodies, leaving government entities largely outside its scope. This means that government agencies may not be subject to the same strict requirements for data protection and privacy as private businesses.[53] While PIPEDA requires organizations to take reasonable measures to safeguard personal information, it does not provide specific guidance on what constitutes "reasonable measures," leaving room for interpretation and potential inconsistencies in compliance. Some critics have argued that Canada's privacy laws do not go far enough in protecting individuals' privacy rights, particularly in the face of evolving technologies and new threats to digital privacy [Rideout V., 2022: 83–85].

One weakness of the legal framework for cyber-security and privacy in the UAE is the lack of clarity and consistency in several laws and regulations. For example, the UAE Cybercrime Law has been criticized for its vague and broad language, which could lead to overreach and abuse of

[52] Henderson E. The UK's approach to cyber-security is weak — and now it's an international problem. The Guardian. Available at: https://www.theguardian.com/commentisfree/2022/jan/31/uk-cybersecurity-international-problem-britain-cyber-attacks. (assessed: 18.04.2023)

[53] Furuta K. Canadian privacy overhaul: what you need to know about Bill C-11. Harvard Business Review. 2021. Available at: https://hbr. org. 2021/02/canadas –privacy-overhaul-what-you-need-to-know-about-bill-c-11 (assessed: 18.04.2023)

power [Al-Fadhli N., 2021: 18–25]. In addition, while the data protection law is a positive step towards protecting individuals' privacy, some have raised concerns about the lack of a comprehensive regulatory framework and the potential for arbitrary enforcement. Another weakness is the limited transparency and due process in some cases related to cyber-security and privacy, which could undermine trust in the legal system and discourage individuals and bodies from reporting incidents or seeking justice [Abdul-Kareem A., 2021: 105488]. These shortcomings highlight the need for continued strengthening and refining legal frameworks in the UAE, with a focus on clarity, consistency, transparency, and due process.

While Singapore has implemented a comprehensive legal framework in the field, there are still some weaknesses to be addressed. One criticism of the PDPA is that it does not provide for a private right of action, which means that individuals cannot sue bodies for damages resulting from violations of the act [Dhamija R., 2022: 107937]. Another issue is that the government's powers under the Cyber-security Act have been criticized for being too broad and potentially infringing on individuals' privacy rights. Additionally, there have been concerns raised about the lack of transparency and accountability in the government's use of surveillance technologies.

These issues highlight the need for ongoing review and reform of Singapore's legal frameworks to ensure they strike an appropriate balance between protecting individuals' rights and promoting national security and economic interests.

Weakness of China's legal frameworks is the lack of transparency and accountability in their implementation. The Chinese government has broad powers to regulate and monitor online activity, and there have been concerns about the potential for these powers to be abused for political purposes [Zhang Y., 2021: 519–540]. The lack of clear and consistent enforcement mechanisms for cyber-security and privacy laws also raises questions about their effectiveness in practice. The strict regulatory environment in China can create barriers to innovation and entrepreneurship, as well as limit free expression and access to information online. The complex and often overlapping nature of China's legal frameworks for cyber-security and privacy can create confusion and uncertainty for both individuals and organizations operating in the country [Sun R., Xu Q., 2021: 103341].

One of the weaknesses of Japan's legal framework in the field is that the APPI's enforcement mechanisms may be insufficient to deter non-compliance. The APPI relies heavily on self-regulation and voluntary compliance

by organizations, with the Personal Information Protection Commission (PPC) responsible for enforcement. However, the PPC has limited powers to impose penalties on non-compliant organizations, and its authority to investigate violations is also restricted. In addition, the Cyber-security Basic Act and the Act on the Protection of Specially Designated Secrets primarily focus on protecting national security and critical infrastructure, which may limit their effectiveness in addressing broader cyber-security and privacy concerns. While Japan has made efforts to strengthen its legal framework for cyber-security and privacy, there may be room for further improvement in terms of enforcement and scope [Izumi K., 2021: 1–23].

South Korea has implemented various laws and regulations to regulate data privacy and cyber-security, nonetheless there are some weaknesses in the legal framework. One concern is the too broad surveillance powers granted to law enforcement agencies under the Network Act, which could potentially violate individuals' privacy rights. Another issue is the potential for government censorship, particularly in the context of national security, which could limit individuals' freedom of expression. There have been criticisms that the penalties for violating data privacy regulations under the PIPA are not severe enough to act as a sufficient deterrent. There have been concerns about the effectiveness of the regulatory bodies established to oversee cyber-security measures, particularly in the face of increasingly sophisticated cyber-threats [Kim M., Kim Y., 2021: 2675–2692].

Australia's legal framework is comprehensive; there have been concerns about its purpose in practice. One weakness is that the Privacy Act and APPs only apply to government agencies and private organizations with an annual turnover of more than AUD 3 million, meaning that smaller organizations may not be subject to the same level of regulation [Patterson M., 2021: 825–857]. In addition, there have been criticisms of the OAIC's enforcement powers and the adequacy of its resources to effectively regulate and enforce privacy protections. The Cyber Security Strategy 2020 has also faced criticism for being too focused on national security and not sufficiently addressing the broader cyber-security concerns of individuals and businesses. The effectiveness of the ASD's guidance on cyber-security best practices has been questioned, with some experts arguing that it may not be sufficient to address the evolving and sophisticated cyber threats facing Australia [Chia P., Teo T., 2021: 102307].

The weakness of the legal frameworks in the field in South America is the lack of strong enforcement mechanisms. While jurisdictions like Brazil

and Mexico have laws to protect personal data and privacy, there are challenges in enforcing these laws. This can be due to a variety of factors: limited resources for regulatory bodies, weak penalties for non-compliance, and lack of awareness and understanding of the laws by both individuals and businesses. The level of implementation and enforcement vary between different regions and sectors within a country. As a result, individuals and businesses may not feel compelled to comply with the regulations, leading to potential breaches of privacy and cyber-security threats. To address these weaknesses, there is a need for stronger enforcement mechanisms, as well as increased awareness and education about the importance of protecting personal data and privacy [Schaerer E., 2022: 111-125].

2.7. Gaps or Inconsistencies in the Legal Frameworks

One significant gap in the legal framework in the United States is the lack of comprehensive federal privacy legislation. While there are several laws that regulate privacy in specific sectors, such as HIPAA for healthcare and the Children's Online Privacy Protection Act (COPPA) for children's data, there is no overarching federal law that provides a comprehensive framework for privacy protection. This has led to a patchwork of state laws, such as the California Consumer Privacy Act (CCPA) and the Virginia Consumer Data Protection Act (CDPA), that have been enacted to fill the gap [Hu M., 2021: 501–534]. Another inconsistency is the tension between national security interests and privacy rights, particularly in the context of government surveillance programs. While CISA encourages information sharing to protect against cyber threats, it has also been criticized for potentially infringing on privacy rights. The legal framework for cyber-security and privacy in the US is fragmented and lacks a cohesive approach to privacy protection [Wessel M., van der Sloot B., 2021: 167–183].

In the legal framework for cyber-security and privacy in Europe is the lack of a unified approach to cyber-security and data protection across all member states. While the GDPR provides a comprehensive framework for data protection, the implementation and enforcement of the regulation can vary widely between member states. There is a lack of harmonization between the GDPR and other regulations, such as the NIS Directive that is able to lead to confusion and inconsistencies in compliance requirements [Van Eecke P., Oberschelp de Meneses A., 2021: 293–307].

Another potential gap is the lack of clear guidance on cross-border data transfers, particularly in light of the Schrems II decision by the European

Court of Justice invalidating the EU-US Privacy Shield Framework. These gaps can create challenges for businesses operating across borders and can lead to regulatory uncertainty and legal disputes [Hirila-Rus A., Borza A., 2022: 1–6].

One potential gap in the United Kingdom legal framework is the lack of specific regulations for the Internet of Things devices. As these devices become more prevalent, they may pose significant cyber-security risks and privacy concerns. Another potential gap is the limited scope of the Data Protection Act 2018, which applies only to data processing activities that are conducted within the UK. This may leave gaps in protection for individuals' personal data that is processed by organizations based outside of the UK. There have been concerns raised about the adequacy of fines imposed by the ICO for data breaches, which some argue may not be sufficient to deter non-compliance with data protection regulations [Thomas M., 2021: 6–9].

As for Canada, here PIPEDA applies to the private sector only, leaving government agencies and departments without a consistent privacy protection framework. There are concerns that PIPEDA may not provide sufficient protection for individuals' privacy rights in the face of swiftly progressing technology and cyber threats. Some critics have called for stronger enforcement powers for the Privacy Commissioner of Canada, as well as amendments to PIPEDA to ensure that it remains relevant and in protecting Canadians' privacy in the digital age.[54]

Gap in the field in the UAE is the possible conflict between the UAE Cybercrime Law and laws related to freedom of expression and human rights. Critics have raised concerns that the broad language of the law could be used to target individuals who express dissenting opinions or criticize the government. Additionally, there have been reports of individuals being detained or prosecuted for online activity that would be considered protected speech in other countries. Furthermore, the lack of transparency and due process in some cases raises concerns about the potential for abuse of power and infringement on individuals' rights to privacy and fair trial [Shafiq M., 2022: 14].

While Singapore has comprehensive legal frameworks in the field, some gaps and inconsistencies remain. For instance, the Cyber-security Act only

[54] Layton J. Privacy commissioner flags potential privacy gaps in the government use of AI. 2021. Available at: https://www. itworldcanada.com/article /privacy-commissioner-flags-potential-privacy- gaps-in government-use-of-ai (assessed: 18.04.2023)

applies to designated CII sectors, which excludes many bodies that could be vulnerable to cyber-attacks. This leaves gaps in the regulation of cyber-security measures for non-CII organizations. The PDPA has been criticized for being too lenient towards organizations that violate privacy laws, as fines for non-compliance are relatively low. Another potential inconsistency is the lack of clarity regarding the extent to which government agencies may access personal data for national security purposes. This could potentially lead to privacy violations if personal data is accessed without due process [Leong K., 2021: 105484].

In China one of the main gaps and inconsistencies in the legislation is the lack of transparency and accountability in its implementation. This has raised concerns about abuse of power by government authorities and the potential for violations of individuals' privacy and free speech rights. The Cyber-security Law grants broad powers to the government to regulate and control information flow online, which has led to criticism from human rights groups and tech companies alike. Some of the other laws and regulations related to cyber-security and privacy like the State Secrets Law, also have been criticized for their vague and broad definitions, which could be used to justify the persecution of individuals and groups for political or ideological reasons [Zheng Y., 2021: 102156].

While South Korea has made efforts to strengthen its legal frameworks, there are still gaps and inconsistencies that need to be addressed. One major concern is the potential for government surveillance and censorship, particularly in the context of national security. The Network Act grants law enforcement agencies access to user data under certain circumstances, which has raised questions about the extent of government surveillance in South Korea. Similarly, there have been cases where South Korean authorities have been accused of censoring online content, which raises concerns about the potential impact on freedom of expression. Furthermore, the efficiency of the PIPA in protecting personal data has been called into question, as data breaches continue to occur in the country. Therefore, there is a need for further reforms and improvements in South Korea's legal frameworks [Joo S., 2022: 23–27].

2.8. Challenges of Implementing Effective Cyber-security Measures While Respecting Privacy Rights

The increasing reliance on digital technologies and the internet has made cyber-security a critical concern for individuals, businesses, and gov-

ernments worldwide. However, it is equally essential to protect individuals' privacy rights while implementing strict cyber-security measures. This requires finding a balance between collecting the necessary data for cyber-security purposes and avoiding excessive data collection or misuse of personal information. It is crucial to determine which types of data are relevant and necessary for cyber-security purposes and ensure that sensitive data is protected adequately. Finding this balance is a complex task that requires collaboration of businesses, governments, and individuals to ensure that cyber-security and privacy are protected simultaneously [Xu H., Zhang R., 2021: 9–12].

In implementing cyber-security measures it is crucial to ensure that the collection and use of personal data are limited to what is necessary for cyber-security purposes. Excessive data collection or misuse of personal information could violate privacy rights, and it is essential to strike a balance between collecting enough information to protect against cyber threats while not infringing on privacy. Organizations should limit their data collection practices to the minimum necessary for cyber-security and implement appropriate safeguards to prevent misuse or unauthorized access to personal information. By doing so, they are able to protect both cyber-security and privacy rights and maintains trust with their customers or users.

Determining types of data necessary for cyber-security purposes is another challenge in implementing reasonable cyber-security measures while respecting privacy rights. While some information such as login credentials and IP addresses are essential for detecting and preventing cyber-attacks, other types of personal data such as browsing history or location data may not be necessary for cyber-security purposes and could be considered a violation of privacy rights. Bodies need to have a clear understanding of the data that they collect, the reasons for its collection, and how it will be used and stored. They should only collect data that is necessary for cyber-security purposes, and any personal data that is collected should be anonymized or encrypted to protect privacy.

Another challenge in implementing cyber-security measures while respecting privacy rights is finding a balance between the two, as privacy regulations and cyber-security needs often conflict with each other. For example, regulations such as GDPR and CCPA require companies to obtain user consent before collecting and processing personal data, while cyber-security measures may require continuous monitoring and analysis of user data to detect and prevent cyber-attacks. Companies must comply with these

regulations while still ensuring the protection of their cyber-security. This can be achieved by implementing privacy policies that outline data collection, use, and storage practices, obtaining user consent for data collection, and using technologies such as encryption and anonymization to protect personal data [Ghosh D., Scott M., 2022: 105666].

Implementing strict cyber-security measures while protecting sensitive data like medical records or financial information, is a significant challenge. These types of data require a higher level of protection due to the severe consequences that could result from a breach. However, ensuring the security of sensitive data must also be balanced with the need to respect privacy rights. Organizations must ensure that they are collecting only the necessary data for cyber-security purposes, using appropriate encryption and access controls to protect the data, and complying with relevant regulations such as HIPAA or PCI DSS. They must also provide transparency to users about how their data is being collected, stored, and used. By balancing these needs, organizations can ensure that sensitive data is protected while still respecting privacy rights.[55]

Implementing cyber-security measures while respecting privacy rights is a challenging task. It requires a thorough understanding of both cyber-security and privacy regulations and a collaborative effort of business, powers, and individuals. Organizations must collect only the necessary data for cyber-security purposes, protect sensitive data, and comply with relevant privacy regulations while still ensuring the protection of their cyber-security. Users must also be educated on the importance of cyber-security and privacy and provided with transparency about data collection and use practices. By working together and finding the right balance between cyber-security and privacy, organizations can protect against cyber threats while respecting individuals' privacy rights [Mangla S., 2021: 49–62].

2.9. Challenges Involved in Balancing Cyber-security and Privacy in Practice

One of the main challenges is limited resource. Many bodies, particularly small businesses, have a limited budget or staff to allocate to cyber-security and privacy measures. This can make it challenging to implement robust

[55] Fowler K. Balancing privacy and cyber-security when securing sensitive data. 2021. Available at: https://securityintelligence.com/articles/balancing-privacy-and-cybersecurity-when-securing-sensitive-data/ (assessed: 18.04.2023)

security measures that protect against cyber threats while also respecting privacy rights. Organizations may need to prioritize their resources based on their most significant security risks and compliance requirements. For example, they may choose to implement basic security measures such as strong passwords and regular software updates and focus on complying with relevant privacy regulations. It is crucial to allocate sufficient resources to cyber-security and privacy to ensure that both areas are adequately protected. [Kharraz A., Robertson W. et al. 2021: 13–23].

Another significant challenge in balancing cyber-security and privacy is navigating complex privacy regulations, such as GDPR or CCPA. These regulations can be challenging to understand and comply with, particularly for organizations with limited legal expertise. Compliance with privacy regulations is critical to protect individuals' privacy rights, but it can be challenging to implement effective cyber-security measures while complying with these regulations. Organizations may need to seek legal advice to ensure they are compliant while also implementing robust cyber-security measures that protect against cyber threats. It is crucial to have a clear understanding of privacy regulations to ensure that both privacy and cyber-security are adequately protected.[56]

Lack of awareness and education is another significant challenge in balancing cyber-security and privacy. Many individuals and businesses do not fully understand the importance of cyber-security or privacy, which can make it challenging to implement effective measures. Users may not be aware of the risks of cyber threats or the importance of protecting their personal data. This can result in poor security practices, such as weak passwords or sharing sensitive information with untrusted parties. Bodies may need to provide training and education to their employees to ensure they understand the importance of cyber-security and privacy and how to implement effective measures. Users may also need to be educated on best practices for protecting their personal data and privacy online, such as avoiding phishing scams and using strong passwords. Increasing awareness and education on these issues is critical to balancing cyber-security and privacy effectively.[57]

[56] Lee Y. et al. Can Privacy Regulations Improve Cyber-security? A Preliminary Empirical Study. 2021. Proceedings of the 54th Hawaii International Conference on System Sciences, pp. 3552–3561. Available at: https://doi.org/10.24251/HICSS.2021.440. (assessed: 18.04.2023)

[57] Madden M. et al. Parents, teens, and online privacy. Available at: https://www.pewresearch.org/internet/2013/05/21/parents-teens-and-online-privacy/ (assessed: 18.04.2023)

Technical complexity is another challenge in balancing. Implementing cyber-security measures may be technically complex and require specialized knowledge and expertise. It may be challenging for organizations to find the necessary expertise to implement robust cyber-security measures while also protecting privacy. Cyber-security measures may involve implementing complex technical solutions, such as firewalls, intrusion detection systems, and encryption, which require specialized knowledge and expertise to set up and manage adequately. Bodies may need to hire cyber-security professionals or outsource their cyber-security needs to third-party providers to ensure they have the necessary expertise to implement effective measures while also protecting privacy. It is crucial to have the technical knowledge and expertise necessary to implement robust cyber-security measures that protect against cyber threats while also respecting privacy rights [Rass S., Chiumento A., Engel T., 2021: 17].

Balancing privacy and security needs is one more challenge. There can be a tension between privacy and security needs, as the measures needed to protect against cyber threats may conflict with privacy requirements. For example, collecting and analyzing user data may be necessary for detecting and preventing cyber-attacks, but it may also raise privacy concerns. Similarly, encryption and other security measures may be necessary to protect sensitive data, but they may also make it challenging to access data for legitimate purposes [Gürses S., Troncoso C., 2022: 78–84]. Organizations need to find the right balance between privacy and security needs, ensuring that cyber-security measures work also respecting privacy rights. This may involve implementing technical and organizational measures that minimize the collection and use of personal data and ensuring that any data collected is used only for legitimate cyber-security purposes. It is crucial to find the right balance between privacy and security to ensure that bodies can effectively protect against cyber threats while also respecting privacy rights [Mendes R., Bonneau J., 2022: 78–89].

2.10. Potential Impact of Cyber-security Measures on Privacy Rights

That impact is a significant concern, as cyber-security measures often involve collecting and analyzing personal data that could be considered a violation of privacy rights. It can lead to concerns over the potential misuse of personal information or the creation of a surveillance state. For instance, the collection of internet activity data could reveal sensitive information

about an individual's political views, health conditions, or personal relationships, which could be exploited for nefarious purposes. Additionally, the use of facial recognition technology or other biometric data for authentication or security purposes could raise privacy concerns regarding potential misuse of sensitive information.[58]

The collection and processing of personal data for cyber-security purposes can have an enormous impact on privacy rights, as individuals may not be aware that their personal data is being collected, processed, and analyzed. This lack of transparency and consent can lead to concerns over the potential misuse of personal information. Furthermore, the storage and processing of personal data for cyber-security purposes may also raise concerns about data security. Cyber-security systems are not invulnerable to cyber-attacks, and if such systems are breached, personal data may be exposed, leading to significant harm and privacy violations. Therefore, it is essential to implement strong data security measures to protect personal data and ensure that privacy rights are respected [Choo K.-K., Tan H., 2021: 3–17].

While cyber-security measures may impact privacy rights, they can also help protect personal data from cyber threats and breaches. Cyber-attacks and data breaches can result in the exposure of personal data, leading to significant harm for individuals, such as identity theft or financial loss. Relevant cyber-security measures can prevent such attacks and breaches, ensuring that personal data is protected. The implementing strong cyber-security measures can increase user confidence in organizations' ability to protect their data, promoting privacy rights and enhancing trust in digital systems. Therefore, it is important to find a balance between cyber-security measures and privacy rights to ensure that both are adequately protected [Chakraborty R., 2021: 2727].

Balancing cyber-security and privacy is a hard task for organizations, and it requires a comprehensive approach that involves addressing the potential impact of cyber-security measures on privacy rights. By adopting a privacy-by-design approach, organizations can ensure that privacy is considered at every stage of the cyber-security process, from the design of security measures to the implementation and monitoring of security systems. That approach can help bodies to minimize the impact of cyber-security

[58] Chen B. Biometric data collection sparks privacy concerns. Wall Street Journal. 2022. Available at: https: //www.wsj.com/articles/biometric-data-cfollection-sparks-privascy-concerns-11647691800 (assessed: 18.04.2023)

measures on privacy rights, while still ensuring that personal data is adequately protected from cyber threats. Ultimately, balancing cyber-security and privacy requires a collaborative effort between organizations, individuals, and governments, and it is essential to find the right balance between these two critical areas [Koops B., Newell B. et al., 2021: 1–19].

3. Ethical Concerns Related to Cyber-security and Privacy

There are several ethical concerns related to the theme of the study. The use of surveillance technologies for cyber-security purposes creates ethical concerns as it raises questions about the appropriate level of monitoring that is necessary to ensure security. While surveillance technologies can help prevent cyber threats and ensure safety, the use of these technologies can also raise concerns about civil liberties and individual privacy. Organizations need to carefully consider the ethical implications of using surveillance technologies, ensuring that any monitoring is proportionate and limited to what is necessary for cyber-security purposes. The transparency and accountability measures should be in place to ensure that individuals' privacy rights are respected [Koops B. et al., 2021: 93–109].

One more ethical concern related to cyber-security and privacy is the potential misuse of personal data by organizations or individuals. Personal data collected for legitimate cyber-security purposes may be misused for other purposes, such as marketing or profiling. It raises concerns about the unauthorized use of personal data and the potential for individuals to be harmed or exploited as a result. The use of personal data in cyber-security measures could lead to a lack of transparency and accountability in how organizations handle and protect personal data, raising ethical concerns about the responsibility of organizations to protect individuals' privacy rights [Taddeo M., Floridi L., 2021: 53–54].

Data breaches and cyber-attacks are ethical concerns in cyber-security and privacy as they may result in the loss, theft, or misuse of personal data. This could lead to identity theft, financial fraud, reputational damage, and other harmful consequences for individuals. In addition, bodies that fail to adequately protect personal data may be seen as negligent and unethical, as they have a responsibility to safeguard the personal information of their customers and users. The potential harm caused by data breaches and cyber-attacks highlights the importance of ethical cyber-security practices

and the need for organizations to prioritize the protection of personal data [Kshetri N., 2021: 326–334].

Accountability and responsibility are critical ethical concerns. Organizations that collect and store personal data must be accountable for protecting that data from cyber threats and breaches. If a breach occurs, organizations must take responsibility for it, and individuals affected by the breach must be notified promptly. Failure to do so can lead to a loss of trust between the organization and its customers, and may raise ethical concerns about the body's commitment to protecting personal data. The organizations should be transparent about their cyber-security and privacy practices to maintain the trust of their customers and other stakeholders [Gross A., Acquisti A., 2021: 102260].

3.1. Ethical Implications of Balancing Cyber-security and Privacy

That issue highlights the need for organizations to find a balance between protecting personal data and respecting privacy rights. This involves implementing cyber-security measures that minimize the collection and use of personal data while ensuring that any data collected is used only for legitimate cyber-security purposes. Organizations must also be transparent about their cyber-security practices and take responsibility for any breaches that occur, promoting trust and accountability. It is essential to strike a balance between cyber-security and privacy to ensure that individuals' rights are respected while protecting against cyber threats [Vadlamudi P., 2022: 1–18].

Furthermore, organizations must also ensure that their cyber-security measures are not discriminatory and do not unfairly target or discriminate against certain individuals or groups. They must take steps to prevent data breaches and protect personal data from unauthorized access, use, or disclosure. At the same time, they must balance these considerations with the need for cyber-security measures to protect against cyber threats. This involves finding a balance between security and privacy that is ethical and respects the rights and interests of all bodies and human persons involved. The ethical implications of balancing cyber-security and privacy require organizations to take a comprehensive and nuanced approach to cyber-security that accounts for the diverse needs and concerns of all stakeholders involved [Bergmann M., Grohmann B., 2022: 197–207].

Addressing potential biases in cyber-security measures is necessary to ensure fairness and avoid discrimination. Bodies must implement mea-

sures to identify and mitigate any biases in algorithms and other tools used for cyber-security purposes. This may involve regular monitoring and testing to identify any patterns of bias and taking steps to correct them. Additionally, involving diverse perspectives and input in the development and implementation of cyber-security measures can help ensure that biases are identified and addressed. By doing so, organizations can ensure that their cyber-security practices are fair and just for all individuals, regardless of their demographic characteristics [López-Pozuelo J. et al., 2022: 1146–1162].

The increasing use of digital technologies and collection of personal data has significant ethical implications for society as a whole, as it affects individual rights and freedoms, as well as broader issues such as social justice and equity. There is a need to balance the benefits of technological innovation and cyber-security measures with potential risks and adverse impacts on privacy rights and other ethical considerations. It is crucial to engage in open and transparent discussions and policymaking processes that address these issues and ensure that cyber-security and privacy measures are fair, just, and equitable for all members of society [Floridi L., 2021: 20200242].

Balancing cyber-security and privacy is a complex task that requires organizations to weigh the benefits of cyber-security measures against their potential impact on privacy rights. To do so, organizations must take into account a range of ethical principles and values, including fairness, transparency, accountability, and respect for individual rights. By adopting ethical frameworks that prioritize these principles, bodies can ensure that their cyber-security measures are both strong and respectful of privacy rights. Ultimately, the ethical implications of balancing cyber-security and privacy extend beyond individual organizations to society as a whole, and it is important to consider these implications as we continue to rely on digital technologies to protect our data and infrastructure.

3.2. The Ethical Implications of Balancing Cyber-security and Privacy

The balancing raises several ethical considerations that organizations must address to ensure that they protect personal data while respecting individuals' privacy rights. One of the most significant ethical implications is the need to combine security and privacy in a fair and just manner. Organizations must consider the potential impact of their cyber-security measures on individuals' privacy rights and take steps to minimize any adverse

effects. They must also be transparent about their cyber-security practices and take responsibility for any breaches that occur [Barnes D., Liang X., 2022: 103598].

The potential for bias in cyber-security measures raises important ethical concerns, as it can result in unfair treatment and discrimination against individuals or groups. Algorithms and other tools used to identify potential cyber threats may use biased data or rely on assumptions that reflect societal biases, leading to incorrect assessments and unequal treatment. This can have serious consequences for individuals' rights and opportunities, and undermine the principles of fairness and justice. Therefore, organizations must ensure that their cyber-security measures are designed and implemented in a way that minimizes bias and discrimination and promotes equity and inclusivity. They must also be transparent and accountable for any biases that arise and take steps to address them. [59]

The increasing reliance on digital technologies and the collection of personal data in today's society have profound ethical implications for cyber-security and privacy. The widespread use of technology means that individuals' personal data is increasingly vulnerable to cyber threats, including data breaches and cyber-attacks. This creates a growing need for organizations to prioritize cyber-security measures to protect personal data. However, as these technologies become more prevalent, it is essential to consider their broader ethical implications for society as a whole. For instance, the collection and use of personal data by tech companies raise concerns about surveillance, privacy, and control over individuals' data. Thus, organizations must balance their cyber-security measures with ethical principles and values that uphold the privacy rights of individuals while ensuring security of personal data [Warren M., Brandeis L., 1890: 193–220].

Balancing cyber-security and privacy is a complex task that involves a range of ethical considerations. On the one hand, bodies have a responsibility to protect personal data from cyber threats that requires strict cyber-security measures. On the other hand, individuals have a right to privacy must be respected even in the context of cyber-security. They must carefully consider potential ethical implications of their cyber-security measures, such as privacy invasion and discrimination, and take steps to minimize any adverse effects [Axelsson A.-S., Söderberg J., 2022: 105639].

[59] Buolamwini J., Gebru T. Gender shades: Intersectional accuracy disparities in commercial gender classification. 2018. Conference on Fairness, Accountability and Transparency, pp. 77-91. Available at: https://doi.org/10.1145/3178876.3186151 (assessed: 18.04.2023)

They must be transparent about their cyber-security practices and take responsibility for any breaches that occur. The broader ethical implications of digital technologies and personal data collection for cyber-security and privacy must also be considered, and steps taken to address these risks and challenges. Ultimately, balancing cyber-security and privacy requires a careful consideration of ethical principles and values, including fairness, transparency, accountability, and respect for individual rights, to ensure that personal data is protected while individuals' privacy rights are respected [Floridi L., Taddeo M., 2016: 19].

3.3. The Potential Trade-Offs between Cyber-security and Privacy

Some cyber-security measures: two-factor authentication, password managers, and encryption, require the collection and storage of personal data to be effective. This can include sensitive information like passwords, biometric data, and location data. The collection and analysis of this data can potentially violate individual privacy rights and raise concerns about surveillance.[60] Cyber-security measures, such as firewalls and intrusion detection systems, may monitor network traffic and user activity, raising concerns about the extent to which individuals' online activities are being monitored and tracked. Balancing the need for cyber-security with respect for privacy rights requires careful consideration of the potential trade-offs involved in implementing security measures [Lips M., Stupar A., 2021: 60–75].

Strict access controls and authentication protocols can enhance cyber-security by preventing unauthorized access to sensitive data. However, these measures may also require collecting and analyzing personal information like biometric data or device identifiers; it can be seen as an invasion of privacy. A monitoring network activity to detect potential cyber threats can be useful for identifying and mitigating security risks. Still, it may also involve collecting and analyzing data on individual users' online behavior, raising concerns about surveillance and infringement of privacy. Organizations must consider the potential trade-offs between cyber-security and privacy and strive to strike a balance that protects both individual privacy rights and organizational security needs [Latham J., Sassenberg U., 2021: 1–6].

[60] Giovanella F., Perri P. Privacy Risks of Cybersecurity Measures: An Overview. IEEE Access, no. 9, pp. 93098-93115. Available at: https://doi.org/10.1109/ACCESS.2021.3096631 (assessed: 18.04.2023)

Machine learning and artificial intelligence (AI) can be powerful tools for identifying potential cyber threats and strengthening cyber-security measures. However, these technologies may also involve analyzing large amounts of personal data, which can raise ethical concerns about privacy and discrimination. For example, if algorithms are trained on biased datasets or if certain groups are underrepresented in the data, the resulting cyber-security measures may discriminate against those groups. The use of machine learning and AI may result in the creation of new types of personal data, such as behavioral biometrics, that individuals may not even be aware are being collected and analyzed. This highlights the need for transparency and accountability in cyber-security practices to ensure that individuals' privacy rights are respected [Eubanks V., 2021: 22–25]. When organizations prioritize security over convenience, they may require users to follow strict protocols to access their data, such as entering long and complex passwords or using multi-factor authentication. While these measures can enhance security, they can also be time-consuming and frustrating for users, which may affect their productivity and overall experience. Balancing security and convenience requires finding a middle ground that minimizes the impact on user experience while still ensuring adequate security measures are in place. This can involve implementing technologies such as biometric authentication or single sign-on to streamline access to data while still ensuring its security [Rizvi S., Alhadreti O., 2021: 36 -39].

Balancing cyber-security and privacy involves a trade-off between protecting sensitive data from cyber threats and respecting individuals' privacy rights. Strict security measures may require collecting and analyzing personal data; it can raise ethical concerns about surveillance and discrimination. A stringent security measures can make it difficult for individuals to access their data easily and quickly, impacting user experience and productivity. The right balance is necessary to ensure that individuals' privacy rights are respected while sensitive data is protected from cyber threats. It requires careful consideration of ethical principles and values like fairness, transparency, and accountability, and ongoing monitoring and evaluation of security measures to minimize potential trade-offs [Sharma R., Jindal A., 2022: 1–22].

3.4. Suggest Ways in Cyber-security and Privacy Concerns can be Reconciled

Reconciling cyber-security and privacy concerns requires a balanced approach that respects both individual privacy rights and the need for ro-

bust cyber-security. Implementing data minimization is a strategy for reconciling cyber-security and privacy concerns by limiting the amount of personal data an organization collects, processes, and stores. By collecting only the minimum amount of personal data necessary for a specific purpose, organizations can reduce the risk of data breaches and cyber threats while respecting individuals' privacy rights [Ikram N., Burnett E., 2022: 97–108]. For example, an organization can limit the collection of biometric data to only those employees who require access to secure areas, rather than collecting it from all employees. Implementing data minimization can also help organizations comply with data protection regulations like the General Data Protection Regulation and the California Consumer Privacy Act requiring organizations to collect and process personal data only for specific purposes and with individuals' consent.

Encryption is a security measure that involves transforming plaintext data into cipher text to prevent unauthorized access. By using encryption, organizations can protect sensitive data both in transit and at rest. Encryption can be used to protect data stored on servers, as well as data transmitted over networks. In this way, encryption can help reconcile cyber-security and privacy concerns by providing a high level of security while also respecting individuals' privacy rights. However, encryption is not a panacea and can be circumvented by determined attackers. Therefore, it should be used in conjunction with other security measures to provide a layered defense [Sundararajan M., 2022: 002].

Fostering a culture of privacy is an essential way to reconcile cyber-security and privacy concerns. By promoting privacy as a core value and training employees on privacy best practices, organizations can create a culture that values privacy and respects individuals' rights. Policies such as privacy impact assessments, privacy notices, and data protection policies can also help demonstrate a commitment to privacy. The organizations can appoint a data protection officer to oversee privacy compliance and facilitate communication between employees, customers, and other stakeholders. By prioritizing privacy in their operations, organizations can build trust with customers and stakeholders and demonstrate a commitment to protecting personal data [Rosenberg Y., 2021: 36–42].

A privacy impact assessment (PIA) is a tool that organizations can use to assess the potential impact of new cyber-security measures on individuals' privacy rights. The PIA process involves identifying the personal data that will be collected, processed, and stored, as well as the potential privacy risks

associated with these activities. Bodies can use this information to identify ways to mitigate privacy risks and ensure that cyber-security measures are in line with ethical principles and values. By conducting PIAs, organizations can proactively address privacy concerns and demonstrate a commitment to protecting individuals' privacy rights [Hernández-García Á., Kudenko D., 2022: 30]. Implementing transparency and accountability is an essential step for reconciling cyber-security and privacy concerns. Organizations can be transparent about their cyber-security practices by clearly communicating their data collection and processing practices to their customers. This includes providing clear and concise privacy policies, informing customers about data breaches, and providing mechanisms for individuals to access, correct, or delete their personal data. The organizations can take responsibility for any breaches that occur by implementing incident response plans and promptly notifying affected individuals. This can help build trust with customers and demonstrate a commitment to protecting personal data, which is crucial for reconciling cyber-security and privacy concerns [Liao Q., 2022: 1072].

Balancing under study requires organizations to adopt a holistic approach that takes into account both security and privacy concerns. This involves implementing strategies like data minimization, encryption, and privacy impact assessments, while fostering a culture of privacy and transparency. By doing so, organizations are able to protect sensitive information from cyber threats and data breaches, while respecting individuals' privacy rights. A comprehensive and balanced approach that incorporates ethical principles and values, such as fairness, transparency, and accountability, is key to reconciling cyber-security and privacy concerns [Rajić M., Filipović S., 2021: 1–16].

Conclusion

The article highlights importance of balancing cyber-security and privacy and valuable insights into the legal and ethical considerations involved. For sure, there are still several questions that require more research to enhance understanding of this topic. One possible avenue for future research is to investigate the impact of emerging technologies, such as artificial intelligence and block-chain, on cyber-security and privacy. Another important area of research is to explore the potential benefits and drawbacks of data sharing and data protection mechanisms, and how they can be opti-

mized to strike a balance between cyber-security and privacy. Hence, more research is needed to examine the ethical considerations involved in the use of cyber-security measures, such as the use of surveillance technologies and their impact on individual privacy rights. These research directions can help policymakers and industry leaders to make informed decisions and develop appropriate regulations that balance the competing interests of cyber-security and privacy. In the digital age maintaining cyber-security and protecting sensitive information are crucial, but must be balanced against the fundamental right to privacy. This challenge requires a comprehensive and rationale approach that respects both privacy rights and the need for robust cyber-security. Bodies can implement various measures like data minimization, encryption, privacy impact assessments to protect personal data from cyber threats while respecting individual privacy rights. Moreover, bodies must take responsibility for any breaches occur and be transparent about their cyber-security practices to build trust with customers and demonstrate a commitment to protecting personal data.

Ethical and legal considerations must be taken into account in the development of digital technologies and their regulation to ensure that personal data is protected while also allowing for cyber-security measures.

To achieve the balance it is necessary for policymakers, business and individuals to collaborate and develop comprehensive solutions protecting sensitive information without infringing on individual privacy rights. This will require continuous education and awareness-raising initiatives to foster a culture of privacy and cyber-security. It will also require the development of legal frameworks that strike a balance between these two values. Prioritizing ethical and legal considerations in the development of digital technologies and their regulation will ensure that everyone can benefit from the digital age while also safeguarding individual privacy rights. Achieving this balance requires ongoing collaboration and dialogue between stakeholders to ensure all perspectives are considered and that the solutions implemented are sustainable and respectful of individual privacy rights.

On one hand, cyber-security is essential for protecting sensitive information and ensuring the proper functioning of digital systems. On the other hand, privacy is a fundamental human right that must be respected in any technological context.

A careful balance between these two values can be achieved through a combination of legal and technical measures, such as encryption, access

controls, and data minimization. It also emphasizes importance of international cooperation and coordination in addressing cyber-security and privacy concerns, as these issues are global in nature and require a collective response.

Cyber-security and privacy are two fundamental human rights that are often in conflict with each other. With increasing threat of cyber-attacks and data breaches, the need to maintain cyber-security and protect sensitive information has become more important than ever. However, in the process of implementing cyber-security measures, there is a risk of infringing on the right to privacy. The problem statement is that the current legal framework for cyber-security and privacy in various jurisdictions is inadequate in addressing the challenges of maintaining cyber-security while respecting privacy rights. The article emphasizes the need for a careful balance between cyber-security and privacy and suggests ways in which cyber-security and privacy concerns can be reconciled in a general context. By doing so, it aims to raise awareness of the need for ethical and legal considerations in the development of digital technologies and their regulation.

References

1. Abdul-Kareem A. (2021) Judicial Review of Electronic Evidence in the UAE: Challenges and Solutions. *Computer Law & Security Review,* vol. 41, p. 105488. Available at: https://doi.org/10.1016/j.clsr.2021.105488

2. Acquisti A., Grossklags J. (2013) Economics and Privacy. *Journal* of *Economic Literature*, vol. 51, no. 2, pp. 1–32.

3. Al-Fadhli N. (2021) UAE Cybercrime Law: Vague and Broad? *Journal of Information Privacy and Security,* vol. 17, no. 1, pp. 18–25. Available at: https://doi.org/10.1080/15536548.2021.1878225

4. Axelsson A.-S., Söderberg J. (2022) Cybersecurity and Privacy: The Interplay between Individual Rights and Organisational Responsibilities. *Computer Law Security Review,* vol. 43, p. 105639. Available at: https://doi.org/10.1016/j.clsr.2022.105639

5. Bamberger K., Mulligan D. (2019) *Privacy on the Books and on the Ground.* Cambridge University Press.

6. Barnes D., Liang X. (2022) Privacy, Security, and Ethics in Information Systems. *Information and Management*, vol. 59, no. 1, p. 103598. Available at: https://doi.org/10.1016/j.im.2021.103598

7. Bergmann M., Grohmann B. (2022) Cyber-security, Discrimination, and Fairness: A Systematic Literature Review. *Journal* of *Business Re-*

search, no. 143, pp. 197–207. Available at: https://doi.org/10.1016/j.jbusres.2021.08.010

8. Brennan-Marquez K., Hoffman S. (2022) Fragmentation and the Future of Privacy Law. *Columbia Law Review*, vol. 122, no. 1, pp. 9–55. Available at: https://doi.org/10.2139/ssrn.3883466

9. Chakraborty R. (2021) Data Security and Privacy: The Need for a Comprehensive Cyber-Security Strategy. *Journal of Public Affairs,* p. 2727. Available at: https://doi.org/10.1002/pa.2727

10. Chia P., Teo T. (2021) Cyber-security and Privacy in Australia. *Computers & Security,* no. 105, p. 102307. Available at: https://doi.org/10.1016/j.cose.2021.102307

11. Choo K.-K., Tan H. (2021) Privacy and Security Challenges in a Connected World. In: K.-K. Choo (ed.). Cyber Security and Privacy. Cham: Springer, pp. 3–17. Available at: https://doi.org/10.1007/978-981-15-9029-9_1

12. Eubanks V. (2021) When Artificial Intelligence Systems Perpetuate Bias. *Communications* of *the ACM*, no. 2, pp. 22–25. doi: 10.1145/3442037

13. Fisher D. (2021) Cyber-security and Privacy Law: The Evolving Intersection. *Boston College Law Review*, vol. 62, no. 6, pp. 2129–2149. Available at: https://doi.org/10.2139/ssrn.3832595

14. Floridi L. (2021) The Ethics of Cyber-security, Privacy and Artificial Intelligence. *Philosophical Transactions of the Royal Society*, no. 379, p. 2020242. Available at: https://doi.org/10.1098/rsta.2020.0242

15. Floridi L., Taddeo M. (2016) What is Data Ethics? *Philosophical Transactions of the Royal Society,* no. 374, pp. 1-19. Available at: https://doi.org/10.1098/rsta.2016.0360

16. Ghosh D., Scott M. (2022) Data Protection and Cyber-security: Walking the Tightrope between Privacy and Security. *Computer Law & Security Review,* vol. 43, p. 105666. doi: Available at: https://doi.org/10.1016/j.clsr.2022.105666

17. Greenwald G. (2019) *Permanent Record*. N. Y.: Penguin.

18. Greenwald G. (2021) The National Security Agency in the Age of Cyber Surveillance. *Foreign Policy*, no. 237, pp. 78–86. Available at: https://doi.org/10.2307/26947126

19. Gross A., Acquisti A. (2021) Transparency and Control of Personal Data: Balancing Privacy and Security. *Computers & Security*, no. 105, p. 102260. Available at: https://doi.org/10.1016/j.cose.2021.102260

20. Gürses S., Troncoso C. (2022) Privacy and Security: Tensions and Synergies. *IEEE Security and Privacy*, vol. 20, no. 1, pp. 78–84. Available at: https://doi.org/10.1109/MSEC.2021.3104862

21. Hawkins D. (2022) Experts Weigh In: Can Security and Convenience Coexist in a Post-Pandemic World? Available at: https://www.security-

magazine.com/articles/96037-experts-weigh-in-can-security-and-convenience-coexist-in-a-post-pandemic-world

22. Hernández-García Á., Kudenko D. (2022) Security, Privacy and Ethics of Autonomous Systems: A Review. *Electronics*, vol. 11, no. 1, p. 30. Available at: https://doi.org/10.3390/electronics11010030

23. Hickman L., Martin C. (2022) The FTC's Unfulfilled Promise: Revisiting the Effectiveness of the FTC's Data Security Enforcement Program. *Ohio State Law Journal,* vol. 83, no.1, pp. 73–132. Available at: https://doi.org/10.2139/ssrn.3839553

24. Hirila-Rus A., Borza A. (2022) The Need for a Unified European Cyber-security Strategy. In: 2022 International Conference on Cyber-security and Privacy Engineering, pp. 1–6. Available at: https://doi.org/10.1109/CySEng.2022.00008

25. Hu M. (2021) The Need for Comprehensive Federal Privacy Legislation. *Harvard Journal of Law & Technology,* vol. 34, no. 2, pp. 501–534. Available at: https://doi.org/10.2139/ssrn.3537656

26. Ikram N., Burnett E. (2022) Data Minimization: a Key Tool in Managing Data Protection and Cybersecurity Risks. *Journal of Data Protection & Privacy,* vol. 6, no. 2, pp. 97–108. Available at: https://doi.org/10.1108/JDPP-01-2022-0003

27. Izumi K. (2021) Strengthening Japan's Data Protection Framework: An Analysis of Recent Developments. *Asian Journal of Law and Society,* vol. 8, no. 1, pp. 1–23. Available at: https://doi.org/10.1017/als.2020.29

28. Joo S. (2022) The Challenges of Data Privacy and Cyber-security in South Korea. *Business Law Today*, vol. 32, no. 3, pp. 23–27.

29. Kim M., Kim Y. (2021) A Study on Privacy Regulation in South Korea: Focusing on Personal Information Protection Act and Related Statutes. *Information Japan*, vol. 24, no. 5, pp. 2675–2692. Available at: https://doi.org/10.3390/info24050154

30. Kharraz A., Robertson W. et al. (2021) Cyber-security Investments: A Prioritization Framework. *IEEE Security & Privacy*, vol. 19, no. 3, pp. 13–23. Available at: https://doi.org/10.1109/MSEC.2021.3058652

31. Koops B., Newell B. et al. (2021) The EU General Data Protection Regulation: Implications for International Cyber-security. *Journal of Cyber-security*, vol. 7, pp. 1–19. doi:10.1093/cybsec/tyaa013

32. Koops B., Newell B. et al. (2021) Ethical Governance of Cyber-security Surveillance. *Ethics and Information Technology*, no. 2, pp. 93–109. Available at: https://doi.org/10.1007/s10676-021-09578-1

33. Kshetri N. (2021) Block-chain's Roles in Meeting Key Supply Chain Management Objectives. *International Journal of Information Management,* p. 102178.

34. Kshetri N. (2021) A Global Analysis of Data Breaches: Focus on Sensitive Data Theft. *Journal of Business Research,* no. 133, pp. 326–334. doi: 10.1016/j.jbusres.2021.01.032

35. Latham J., Sassenberg U. (2021) Managing Balance between Cyber-security and Privacy: A Review of Relevant Empirical Research. *Current Opinion in Psychology,* vol. 36, pp. 1–6. Available at: https://doi.org/10.1016/j.copsyc.2020.06.004

36. Leong K. (2021) The Cyber-security Act and the Personal Data Protection Act. *Computer Law & Security Review,* vol. 41, p. 105484. Available at: https://doi.org/10.1016/j.clsr.2021.105484

37. Liao Q. (2022) Translating the GDPR's Accountability Principle into Corporate Practice. *International Journal of Environmental Research and Public Heal*, vol. 4, p. 1072. Available at: https://doi.org/10.3390/ijerph19031072

38. Lips M., Stupar A. (2021). Cyber-security, Surveillance and Privacy: Ethical Issues in the COVID-19 Pandemic. *Journal of Information, Communication and Ethics in Society*, vol. 19, no. 1, pp. 60–75. Available at: https://doi.org/10.1108/JICES-10-2020-0122

39. Liu X. (2017) The Cybersecurity Law of the People's Republic of China: A Content Analysis. *International Journal of Cyber Criminology,* vol. 11, no. 1, pp. 1–20. Available at: https://doi.org/10.5281/zenodo.573584

40. López-Pozuelo J. et al. (2022) Machine Learning Bias in Cyber-security: A Systematic Review. *Future Generation Computer Systems,* no. 128, pp. 1146–1162. Available at: https://doi.org/10.1016/j.future.2022.09.019

41. Luiijf E., Douma A. (2019) Cyber Security and Resilience: What Are We Talking about? In: Cyber Security: From Technology to Society. Cham: Springer, pp. 3–14.

42. Mangla S. (2021) Cyber-security and Privacy: Balancing the Scales. *Journal of Cyber-security and Information Management,* no. 2, pp. 49–62. Available at: https://doi.org/10.21632/irjbs.12.1.1-16

43. Mendes R., Bonneau J. (2022) Balancing Privacy and Security: A Review of Technologies and Techniques. *IEEE Security & Privacy,* vol. 20, no. 2, pp. 78–89. doi: 10.1109/MSEC.2022.3125795

44. O' Harrow R. (2017) Privacy vs. Security: A False Dichotomy. *Journal of National Security Law & Policy,* vol. 9, no. 1, pp. 95–113.

45. Pavlou P., Lewis K. (2020) The Cambridge Handbook of Consumer Privacy. Cambridge: University Press.

46. Patterson M. (2021) The Weakening of Privacy Protection in Australia: A Critique of Recent Developments. *Melbourne University Law Review,* vol. 44, no. 3, pp. 825–857. Available at: https://doi.org/10.2139/ssrn.3759518

47. Purcell R. (2021) The GDPR: Success or Failure? *Journal of Data Protection & Privacy,* vol. 5, no. 2, pp. 135–148. doi: 10.1108/JDPP-12-2020-0053

48. Rajić M., Filipović S. (2021). Balancing Cyber-security and Privacy: An Ethical Perspective. *International Journal of Cyber-Security and Digital Forensics,* vol. 10, no. 1, pp. 1–16. Available at: https://doi.org/10.17781/P002959

49. Rass S. et al. (2021) Dealing with the Technical Complexity of Cyber-security and Privacy in the Digital Age. *Journal of Cyber-security*, no. 7, tyaa017. Available at: https://doi.org/10.1093/cybsec/tyaa017

50. Rosenzweig P. (2015) Balancing Privacy and Security: The Ethical Dimension. In: J. Quigley, D. Molnar (eds.) Routledge Handbook of Science, Technology, and Society. L: Routledge, pp. 318 –329.

51. Rideout V. (2022) Privacy in a Digital World: Canada's Laws Fall Short. *Canadian Journal of Law and Society,* vol. 37, no. 1, pp. 83–85. doi: 10.3138/cjls.37.1.83

52. Rizvi S., Alhadreti O. (2021) Investigating the Impact of Cyber-security Measures on User Experience. In: Proceedings of the 2021 3rd International Conference on Computing, Electronics and Communications Engineering, pp. 36–39. Available at: https://doi.org/10.1109/ICCECE52537.2021.9478139

53. Rosenberg Y. (2021) Creating a Culture of Privacy: Tips for Leaders. *Security Management*, no. 3, pp. 36–42. Available at: https://doi.org/10.1080/09540962.2021.1901422

54. Schaerer E. (2022) Cyber-security and Data Protection in Latin America: Regulatory Trends and Challenges. *Journal of Cyber Policy*, vol. 7, no.1, pp. 111–125. doi: 10.1080/23738871.2022.2040862

55. Singer N., Tufekci Z. (2021) The Ethics of Digital Contact Tracing. *Science*, no. 368, pp. 951–954. Available at: https://doi.org/10.1126/science.abb9414

56. Singer P., Tushman M. (2021) *Understanding Cyber-security and the Implications for National Security.* N. Y.: Columbia University Press.

57. Sharma R., Jindal A. (2022) Balancing Cyber-security and Privacy: A Review of the Literature. *Journal of Cyber-security*, vol. 8, no. 1, pp. 1–22. doi: 10.1093/cybsec/tyab006

58. Stevens A. (2022) Balancing Privacy and Cyber-security: A Delicate Dance. *Duke Law & Technology Review,* vol. 21, pp. 45–77.

59. Sun R., Xu Q. (2021) Innovate or Comply? Technology Adoption under the Chinese Regulatory Environment. *Information & Management*, vol. 58, no. 1, p. 103341. doi: 10.1016/j.im.2020.103341

60. Sundararajan M. (2022) Balancing Privacy and Cyber-security Using Encryption. *Journal of* Cyber-*security*, no. 81, tyac002. Available at: https://doi.org/10.1093/cybsec/tyac002

61.Taddeo M., Floridi L. (2021) The Challenges of Cyber-security and Privacy: A Review. *Science*, no. 371, pp. 53–54. doi: 10.1126/science.abf1424

62. Talbot D. (2021) The Cyber-Security-Privacy Paradox: Impact on Consumers, Businesses, and Governments. Available at: https://securityintelligence.com/posts/the-cybersecurity-privacy-paradox-impact-on-consumers-businesses-and-governments/

63. Thomas M. (2021) Data Protection: The UK's New Regime. *Computer Fraud & Security,* no. 3, pp. 6–9.

64. Van Eecke P., Oberschelp de Meneses A. (2021) The EU Cybersecurity Regime: GDPR and the NIS Directive Compared. *Journal of International Data Privacy Law,* vol. 11, no. 4, pp. 293–307. Available at: https://doi.org/10.1093/idpl/ipab015

65. Vadlamudi P. (2022) Balancing Cyber-security and Privacy: A Comprehensive Overview of Regulations, Challenges, and Solutions. *Journal of Information Privacy and Security,* vol. 18, no. 1, pp. 1–18. Available at: https://doi.org/10.1080/15536548.2022.2002224

66. Villeneuve E. (2022) The Privacy-Security Paradox: Navigating Ethical Tensions in the Age of Cyber-security. *Journal of Business Ethics,* vol. 183, no. 3, pp. 495–511. doi: 10.1007/s10551-019-04322-5

67. Warren M., Brandeis L. (1890) The Right to Privacy. *Harvard Law Review*, vol. 4, pp. 193–220. Available at: https://doi.org/10.2307/1321160

68. Wessel M., van der Sloot B. (2021) The US Needs Federal Privacy Legislation. *Journal of Cyber Policy,* vol. 6, no. 2, pp. 167–183. Available at: https://doi.org/10.1080/23738871.2021.1892145

69. White L. (2021) What Does Brexit Mean for GDPR? *Computer Fraud & Security,* no. 3, pp. 8–10. doi: 10.1016/S1361-3723(21)00043-5

70. Xu H., Zhang, R. (2021) Balancing Cyber-security and Privacy Protection. *IEEE Security and Privacy*, vol. 19, no. 2, pp. 9–12. Available at: https://doi.org/10.1109/MSP.2021.3055223

71. Yoo C. (2015) Cyber-security and Freedom on the Internet. *Harvard Journal of Law & Public Policy,* vol. 38, no. 1, pp. 129–137.

72. Zhang Y. (2021) The Legal Framework of China's Cyber-security: a Critical Review. *Journal of Cyber Policy*, vol. 6, no. 4, pp. 519–540. Available at: https://doi.org/10.1080/23738871.2021.1906843

73. Zheng Y. (2021) China's Cyber-security Law and its Implementation. *Telecommunications Policy*, no. 4, p. 102156. doi: 10.1016/j.telpol.2020.102156

Information about the author:

Naeem Allahrakha — LLM, Lecturer.

The paper was submitted to editorial office 11.06.2023; approved after reviewing 23.06.2023; accepted for publication 23.06.2023.

Legal Issues in the Digital Age. 2023. Vol. 4. No. 2.
Вопросы права в цифровую эпоху. 2023. Том 4. № 2.

Research article
УДК: 342
DOI:10.17323/2713-2749.2023.2.122.141

Children and Internet: Cyber Threats Sorts and Ways of Protection

Rina Venerovna Khisamova

National Research State Civil Engineering University, 26 Yaroslavskoye Shosse, Moscow 129337, Russia,
rina_khisamova@list.ru

Abstract

Digital transformation of contemporary reality encompasses practically all spheres of human life including children. In the article the author studies the risks that digitalization creates for children, identifies the main types of cyber threats posing a risk to children's normal development, and looks at the legal remedies available today to protect against such risks. The article begins with a study of the specific features of a child's legal personality, the landmarks in the history of recognizing the child as a self-standing legal subject, and the child's legal status characteristics. In particular, the article points to the principle of 'evolving capacities of the child' as the key feature of the child's legal status that implies gradual expansion of the child's legal capacity commensurate with the child's coming of age. The author notes that since this principle has been adopted in other branches of law, it must be likewise implemented in the information law because the Internet space has an enormous influence on children's development that must not remain unaddressed by the legislator or stay outside the regulatory environment. Applying general and special research methods, including the formal logic and the comparative analysis methods, the author gives a brief overview of current government, non-government and private means and methods of protecting children's rights on the Internet, and notes that combination of all the available methods provides the best results. To ensure functioning of the mechanism for the protection of children's rights in the Internet, the author suggests to take into consideration the special aspect of the child's legal status: the child's legal capacity gradually evolves, and the child receives legal capacity to independently exercise rights in the digital environment. The author recommends to seek ways and means to ensure a balance between the public and the private to protect children in conditions of a rapid growth of information and communication technologies.

Keywords

digitalization; children's rights; Internet; protection; cyber threats; information society; risks content; contact risks; digital self-protection; knowledge society.

For citation: Khisamova R.V. (2023) Children and Internet: Cyber Threats Sorts and Ways of Protection. *Legal Issues in the Digital Age,* vol. 4, no. 2, pp. 122–141. DOI:10.17323/2713-2749.2023.2.122.141

Introduction

Today's international law and, consequently, Russian law recognise the child to be a legal subject with a full set of rights [Abramov V.I., 2007: 21] and proceed from the principle that in all actions concerning children, the best interests of the child must be a primary consideration [Korshunova O.N. et al., 2021].

The years 2018 to 2027 have been declared the Decade for Childhood[1] in the Russian Federation. The key objectives of this Decade are to protect every child's rights and to create an efficient system for preventing offences against children — and those committed by children as well [Pavlova L.V., 2022: 19–22].

On the other hand, the strategy for the development of an information society, approved by a Decree of the President of the Russian Federation[2] for 2017–2030, a period similar to the Decade for Childhood, envisages gradual formation of a knowledge society in Russia, one that prioritises the receipt, preservation, production and dissemination of information as key conditions for the development of the citizens, economy, and State.

In the light of the above, it becomes an especially relevant task to protect children's rights in information space, for the formation of any society, including an information society,[3] starts precisely with the promotion of

[1] Presidential Decree No. 240 'On the Institution of a Decade for Childhood in the Russian Federation' 29.05.2017. Available at: URL: //http://static.kremlin.ru/media/acts/files/0001201705290022.pdf (accessed: 20.06.2022)

[2] Presidential Decree No. 203 'On Strategy for Development of Information Society in the Russian Federation for 2017–2030' 09.05.2017 // Consolidated legislation of the Russian Federation, 2017, No. 20, P. 2901.

[3] An information society is henceforth understood to mean one in which information and the levels of its use and availability have a drastic effect on individuals' economic and socio-cultural living conditions. This definition of an information society is suggested in

child development, while children, their undeveloped critical thinking, are especially vulnerable in the times when people's living conditions change.

In response to the challenges of computerisation and digitalisation, modern legal science is now in search for legal ways and methods to protect the rights of children who go online. This is reflected in some legal studies on children's safety in the Internet [Rybakov O.Yu., Rybakova O.S., 2018: 27–31]; [Kobzeva S.V., 2017: 33–39], and on interaction among the actors working to protect children's rights [Pavlova L.V., 2022: 19–22].

The review of this issue is quite relevant scientifically and high on the legal regulation agenda, which reflects most accurately the set of practical tasks faced by the legislator. Just a month ago the Government of the Russian Federation approved a new concept note on children's information security,[4] which stipulates that, among Russia's current total population of 146.4 million, 30.2 million (20.6 %) are minors, and 27 million (89.4 %) of these are active Internet users.

The article is a fruit of author's attempts to study the threats that Internet poses to children and to outline the legal mechanisms that could protect them.

1. Children as Legal Subjects

The legal subject category is a key concept of the theory of law, for it is 'the principal component (subsystem) and also the centre, or the core, of a legal system [Alexeyev S.S., 2005: 446].

And the essence of this concept may be understood in various ways. Let us agree with S. Ye. Channov's opinion that, conceptually, all the existing interpretations of the 'legal subject' can be divided into three basic approaches: a legal-formal (positivist) approach, an anthropocentric one, and a jus naturalistic one.

The first approach is generally based on the premise that it is a person possessing legal personality under the law that is considered a legal sub-

Para. 4 (r) of the Strategy for the Development of Information Society in the Russian Federation for 2017–2030, approved by Presidential Decree No.203 .

[4] Executive Order No. 1105-p of the Government of the Russian Federation of 28.04.2023 'On Approving the Concept of the Information Security of Children in the Russian Federation, and on Declaring the Executive Order No. 2471-p of the RF Government of 02.12. 2015 Invalid' // Consolidated legislation of the Russian Federation, 2023, No. 19, P. 3481.

ject [Mitskevich A.V., 1962: 5]. 'Legal subjects are persons or organisations whom the law grants a special legal property (quality) of legal personality that enables them to enter into various legal relations with other persons and organisations' [A.I. Abramova A. I., Bogolyubov S.A. et al., 2003: 544]. Proponents of the positivist approach identify only two attributes of a legal subject: legal personality and legal capacity [Ivansky V.P., 2016: 50].

The anthropocentric approach to defining the essence of the legal subject recognises a human being (natural person) to be a legal subject; in addition, legal personality may be attributed to certain groups of people [Channov S. Ye., 2022: 94, 109]. S.Ye. Channov cites the position of S.I. Arkhipov, who regarded the human being as a legal phenomenon that is a common ground for the emergence of all the existing legal subjects and, consequently, suggested that a legal subject should be understood as a set of human legal qualities encased in a special legal form (that of a legal entity or natural person). Within this approach, he identified individual and collective (legal entities, nations and peoples), intra-organisational and complex/composite legal subjects [Arkhipov S.I., 2004: 8–9].

And, thirdly, the jus naturalistic approach consists in identifying special attributes of a legal subject, among which the following are most frequently mentioned: organisational unity, ability to possess rights and bear duties and to enjoy/fulfil them on one's own; ability to take legally significant decisions; ability to bear legal responsibility for one's wrongdoings; being separate (organisationally and legally); possibility of legal individualisation; and possession of one's own will, purposes and interests, etc. [Ponomaryova Ye.V., 2019: 60–83]; [Dolinskaya V.V., 2012: 6–17].

Given that legal personality is not the key topic of the study, the author shall henceforth follow the positivist approach to legal subject and understand one as a natural person only, which is more relevant to the issue of the protection of human rights, including the rights of the child.

On the other hand, though the child's rights are an inalienable, integral and indivisible part of universal human rights [Zhavzandolgor B., 2004: 3], it is necessary to note children were not always recognised as self-standing legal subjects.

As V.I. Abramov points out, international legal thought realised before the Russian one the importance of the children's rights issue, and international law was also the first to provide for special protection of the most vulnerable groups, all those deprived of equal opportunities to defend their

own rights. In the aftermath of World War One, the League of Nations founded an International Child Care Association, and a Geneva Declaration of the Rights of the Child was approved in 1924. After World War Two in 1945 the United Nations General Assembly established the UN Children's Fund (UNICEF), and on 20 November 1959 a Declaration on the Rights of the Child (so referred to hereinafter) was proclaimed. And while the 1924 Geneva Declaration of the Rights of the Child regarded children as objects of protection only, in 1959 there was already a trend towards the recognition of the child as a legal subject [Abramov V.I., 2007: 3, 4], which was actually codified as a 'general rule' only in the Convention on the Rights of the Child (hereinafter Convention) adopted by the UN General Assembly on 20 November 1989. According to provisions of the Convention, the child is a full-fledged person with a full set of rights, an independent legal subject, not a 'mini adult with mini rights' [Trigubovich N.V. et al., 2022: 28–38].

International rule-makers thus took more than sixty years to codify, at the first attempt, the contemporary model of treating children as equal law subjects; in so doing, they took the lead and promoted a change in the child's position in the family and society at the level of each individual State, including Russia.

On the other hand, after recognising the child as an independent legal subject, international and then domestic legal regulation came to require states to provide the child with the protection required for his/her well-being. Such dualism, i.e. the recognition of the child as a full-fledged person with a full set of rights, on the one hand, and recognition of the State's duty to protect the child's rights, on the other, is what determines the special nature of children's legal personality, that must be taken into account as we study the legal specifics of the protection of children amid the formation of an information society.

2. Specifics of the Child's Legal Personality

The child's legal personality is closely related to his/her legal status, for legal status is actually the content of legal personality. We henceforth understand legal status to mean a set of rights and duties vested in a specific person—though, to be more precise, we should agree that the child's general legal status is a system of subjective legal rights, freedoms and interests and also the duties and responsibility of a special legal subject, namely the child,

as expressed in the values of natural law and rules of positive law and guaranteed by the society and State [Protsevskyi V.A., Golikova S.V., 2020: 29–31].

As was outlined above, legal theory recognises the child to be a special legal subject who possesses all the inalienable rights of human and citizen but is presumed to be immature and thus unable to exercise them in full on their own until they reach an age established by law. The Convention stipulates that every child by reason of his/her physical and mental immaturity needs special safeguards and care, including appropriate legal protection, before as well as after birth [Kolobayeva N.Ye., Nesmeyanova S.E., 2020: 14–21]. It has a sense to see how this protection is provided in some areas governed by various branches of law.

According to Article 60 of the Russian Federation Constitution, a citizen may exercise his or her rights and duties in full since the age of 18. In civil law, a child's status is determined by his/her legal capacity that is acquired or, more precisely, expands as the child grows up. For example, Article 28 of the Civil Code of the Russian Federation (hereinafter CCRF) defines the scope of the rights of minors, i.e. persons below the age of 14. According to Para 1 of that Article, deals on behalf of minors who have not reached the age of 14 years may only be effected by their parents, adopters or guardians, with the exception of the deals pointed out in Para 2 of that Article. The property responsibility for minor's deals, including those effected by them on their own, shall be borne, as a general rule, by their parents unless they prove that the obligation was not breached through their fault; they are also held responsible for any damage caused by minors.[5]

In turn, minors aged 14 to 18 may effect deals with their parents' written consent (or if they subsequently approve the deals in writing), except the deals they may effect on their own. Minors in the said age group bear property responsibility for the deals they enter into (independently or with their lawful representatives' consent) on their own and are also liable for any damage they may cause (CCRF Article 26. 1-3).

Thus it is admissible to conclude that in the field of civil law, the category of 'children' comprises two main groups: young minors (younger than 14) and minors (aged 14 to 18), either possessing its own scope of civil rights and civil duties.

[5] Consolidated legislation of the Russian Federation, 1994, No. 32, P. 3301; Para 17 of Resolution No. 25 of the Russian Supreme Court Plenum of 23.06. 2015 // Rossiyskaya Gazeta, 2015, No. 140.

In judicial proceedings, e.g. civil ones, children also have a special legal status whose basic provisions are set out in Article 37 of the Civil Procedure Code of the Russian Federation (CPC). Under the general rule in Para 1 of that Article, the capacity to exercise procedural rights, perform procedural duties and to entrust the conduct of legal proceedings to an attorney (civil procedure legal capacity) belongs in full to citizens who have reached the age of 18, and to organisations. By virtue of Para 3 and 5 of that Article, the rights, freedoms and lawful interests of minors, either above or below the age of 14, are protected by their lawful representatives, with the difference that the court will bring the former group of minors (aged 14 to 18) into the proceedings on a mandatory basis, and the latter (children under 14), at the court's own discretion. Pursuant to CPC Article 37.2, a minor may personally exercise his/her procedural rights and perform procedural duties in court after marrying or being recognised fully capable (emancipation); a minor may apply to court for emancipation since the age of 16. Besides, in cases provided for by federal law, in proceedings arising from civil, family, labour, and other legal relations, minors aged 14 to 18 may also personally defend their rights, freedoms, and lawful interests in court (Article 37.4).

Procedural law thus also differentiates a child's status depending on his/her age, taking into account some special legal institutions, such as emancipation.

According to the Russian administrative law, emancipation applies to a person who has reached the age of 16 by the time he/she commits an administrative offence (Article 2.3 of the Code of the Russian Federation on Administrative Offences, hereinafter CoAO). Pursuant to CoAO Article 2.3.2, taking into account the merits of the case and the available information about an offender aged 16 to 18, a Commission for Minors and Protection of their Rights may exempt such a person from administrative liability and prescribe measures provided for by the legislation on the protection of minors' rights.

We can thus observe some peculiarities of the child's legal status (e.g. clemency towards minors) in branches of public law as well.

Given that the above examples contain mentions of not only 'child (ren)' but also 'minors', with the latter term including different age groups of children in different branches of law, we find it necessary to draw a distinction between those concepts at the outset.

Although today's legal science contains some examples of no distinction between the categories of 'children' and 'minors' [Kapitonova Ye. A., 2010:

26], the term 'child' seems to be broader in content than the term 'minor'. The latter is a legal category that is generally branch-specific and related to a certain age to be reached [Amirova D.K., 2022: 40–46], which fully agrees with the positivist approach to understanding the essence of the legal subject and with the focus on natural persons' legal personality. So it is possible to agree with D.K. Amirova and henceforth consider the concept of 'child (ren)' as a single and universal one, and use narrower concepts of '(young) minor', etc., to define separate (branch-specific) forms of legal status.

Having sorted out this intricate terminology, is useful to return to the specifics of the child's legal status.

All the above-cited examples of the child's participation in various legal relations permit the conclusion that the child's legal status is based on the principle of 'the older, the more', that has actually been embraced by all the branches of law in the light of the specific social relations they govern. In doctrine this is termed the principle of 'evolving capacities of the child' with reference to Article 5 of the Convention on the Rights of the Child [Trigubovich N.V. et al., 2022: 38]. And the UN Committee on the Rights of the Child defines evolving capacities as a 'law-forming principle that envisages the process of growing up and learning, whereby children gradually acquire professional knowledge and insights and feel increasingly able to assume responsibilities and exercise rights'.

It seems that information law is not and cannot be an exception here, and the child's legal status as regards information technology should also be defined through the lens of this principle: with age, a child acquires greater freedom of action and greater discretion in the digital field, and it cannot be otherwise.

3. Digitalisation and Children: The Main Risks

Digitalisation, or digital society development, is the process of organising the performance of functions and activities (business processes), previously conducted by persons and organisations without using digital products, in a digital environment. Digitalisation implies the introduction of information technology into each individual aspect of any activity.[6]

[6] Order No. 428 of the Ministry of Communications and Mass Media of 01.08.2018 'On Approving Explanations (Methodological Recommendations) on the Development of Regional Projects under the Federal Projects of the 'Digital Economy of the Russian Federation' National Programme // SPS Consultant Plus.

Global and universal digitalisation certainly aims to create additional benefits for society and has a positive effect on people's lives and activities: we can now easily communicate from and to anywhere on the globe, promptly receive a state service, buy goods and services, visit a medical doctor, get additional education and pass our leisure time online.

On the other hand, as rightly noted by some scholars, digitalisation of social relations at the current state of the development of state and society cannot be presented as a new round of development that essentially reproduces something pre-existing at some new level. Virtualisation of legal relations is not similar to the transition from horse-drawn vehicles to motor cars or from oil lamps to electric lighting. The transformation processes in the digital environment are so profound that we should consider serious revision of the existing concept of protecting citizens' rights and freedoms and the means and ways of protecting social relations.

Indeed, the development of modern technology and its adoption in public and social practice are not yet supported by a virtual space infrastructure that might provide legal remedies. Such infrastructure is still existent in the real world only, and the virtual environment lacks the elements of legal protection that we are used to. The state is not equipped to interfere in data processing without the digital community's voluntary consent, for the new relations ecosystem excludes the usual agents to whom the authorities may address their prescriptions; nor can monies be refunded or 'restored' if lost due a technical error; a transaction aborted, a judgement enforced, etc.

The means of rights protection in the virtual world are embryonic now, so an individual is essentially unable to safeguard him/herself against the risks that come with the new technology [Kucherov I.I., Sinitsyn S.A. et al., 2022: 9, 10]. Children are certainly the most vulnerable group in this situation.

As noted by S.V. Kobzeva, Russian children start going online at an average age of six or seven. According to the Internet Development Foundation, children's Internet audience reached its top strength in the last six years: in 2010, 82% of adolescents would use the Net every day, and in 2016, 92%, with some 80% spending an average of three hours a day online, and every seventh, eight hours or more [Kobzeva S.V., 2017: 33].

Of course, children may use the Internet for their own benefit, but we should not be naïve enough to suppose that it is exclusively a benefit that carries no inherent threat to the child's well-being.

4. Types of Internet Threats to Children

Today it is possible to identify the following Internet-based risks that are full-scale threats to all users, including children:

content risks — illicit (pornographic, racist, gambling) and harmful (aggressive, hate speech) content, including harmful advice (suicide) and unwanted advertising;

contact risks — dangerous contacts with persons, including cyber-grooming (drawing a child into actions of a sexual nature), online harassment, cyber-bullying (humiliation or mobbing via mobile phones and other electronic devices), and cyber-stalking (online hounding or persecution);

virtual transaction risks — making unwanted (erroneous or accidental) transactions (purchases, remitting and receiving money, etc.), including online fraud;

Internet privacy and security risks — leaks of children's data and their uncontrolled use by third parties.

The above classification follows the proposals by S.V. Kobzeva, based, in turn, on studies by the Organisation for Economic Co-operation and Development (OECD) [Kobzeva S.V., 2017: 39]; importantly, it is non-exhaustive.

It should note that the same classification, with some variations, is also used by executive authorities as they perform their duties. For example, the website of the Ministry of Digital Development, Digital Policy and Mass Communications of the Chuvash Republic (Central Russia) mentions content, communications, electronic and consumer risks as the Internet risks faced by children,[7] which is similar in scope to the classification that we suggested above. So, the types of Internet risks have now been identified and cause no controversy; however, it is necessary to remember that, since digitalisation and virtualisation are ongoing processes, Internet threats may emerge and disappear, which necessitates further theoretical research. After the threats have been studied in theory, they are easier to eliminate in practice.

Now it is necessary to consider the legal mechanisms in place to protect Russian children's rights and interests from the above threats, given that the

[7] Available at: URL: https://digital.cap.ru/action/activity/telecom/internet-safety/zaschita-detej-ot-negativnoj-informacii/internet-riski (accessed: 30.05.2023)

Constitutional Court of Russia in a recent resolution pointed to the need to create and provide guarantees of the implementation of children's rights to special care and assistance and to prioritise their interests and well-being in all parts of life.[8]

5. Legal Protection of Children against Content Risks

As for current federal legislation, the content risks posed by some popular sources of information, including Internet, to children of all age groups seem to have been minimised as much as possible. Perhaps this results from the established worldwide approach to the protection of children from negative information and unconditional recognition of the need to provide such protection and, on the other hand, from a relatively straightforward approach that essentially consists in legislative restrictions on access to certain information.

The Russian legislator is now using the concept of 'children's information security' legally rooted in Article 14 of the Law on the Rights of the Child[9] and in the Law on the Protection of Children from Harmful Information[10] adopted pursuant to that Article.

According to Article 2 of that Law, information security of children means the children's state of being protected that eliminates the risk of any harm that information may inflict on their health and/or physical, mental, spiritual and/or moral development.

Children's information security is ensured irrespective of the information distribution channel in question, by introducing a legislatively established classification of information products (Chapter 2 of the Law on the Protection of Children from Harmful Information), establishing requirements on their circulation (Chapter 3), a procedure for expert testing of information products in certain cases (Chapter 4), and for state and public

[8] Resolution No. 7-П of the Russian Constitutional Court of 02.03.2023 'On the Case Concerning the Constitutionality of Article 17, Para 2 of the Civil Code of the Russian Federation in Connection with a Complaint by Citizen M.V. Grigoryeva'. Available at: http://doc.ksrf.ru/decision/KSRFDecision667150.pdf (accessed: 30.04.2023)

[9] Federal Law No. 124-FZ 'On the Main Guarantees of the Rights of the Child' of 24.07.1998 // Consolidated legislation of the Russian Federation, 1998, No. 31, P. 3802.

[10] Federal Law No. 436-FZ 'On the Protection of Children from Information that Harms their Health and Development' of 29.12.2010 // Consolidated legislation of the Russian Federation, 2011, No. 1, P. 48.

control and responsibility measures (Articles 5 and 22 of the Law on the Protection of Children from Harmful Information).

In implementing such measures the legislator proceeds from the children's age (under six, six, twelve, sixteen or older) to actually divide information, according to its content, into illicit information and restricted access information (Article 5.2 and 5.3). For comparison: the only restriction on adult citizens' access to open information that does not fall under the special legal regimes of secrecy is a prohibition contained in Article 10 of the Law on Information.[11]

On the other hand, the information security of children in the Internet is not very well implemented in practice: many websites containing information that must be of limited access for children under the law, particularly based on their age group, contain no special marking (the only 'happy' exception being online liquor shops that deny access to persons under 18 years of age). Content circulators often fail to differentiate content or to adapt it for various categories of persons, which is the direct cause why undesirable and even harmful information still reaches children on the Internet.

Access to prohibited information is much better regulated. Pursuant to Resolution No. 1101 of the Government of the Russian Federation,[12] the Federal Service for Supervision of Communications, Information Technology, and Mass Media (Roskomnadzor) now keeps a Unified Register of Domains and Websites with Illicit Content.[13] The procedure for including information in that register is sufficiently regulated by Articles 15.1-1–15.9 of the Law on Information, and the parties to those legal relations are well defined, as are their the rights and duties in respect of one another and State authorities, so we can say that the mechanism for restricting access to prohibited information is actually working.

---

[11] Federal Law No. 149-FZ 'On Information, Information Technology and Protection of Information' of 27.07. 2006 // Consolidated legislation of the Russian Federation, 2006, No. 31. P. 3448.

[12] Resolution No. 1101 of the Government of 26.10.2012 (version of 29.04. 2023) 'On the Unified Register of Domain Names and Site Page Locators in the Internet Information and Telecommunication Network, and of Network Addresses that Permit Site Identification in the Internet Information and Telecommunication Network, that Contain Information Whose Dissemination is Prohibited Unified Automated Information System' // Consolidated legislation of the Russian Federation, 2012, No. 44, P. 6044.

[13] Available at: URL: https://eais.rkn.gov.ru/ (accessed: 26.12.2022)

It has a sense thus to agree with S.V. Kobzeva's finding that the system for protecting minors from aggressive Internet content is functioning in Russia, but needs improvements [Kobzeva S.V., 2017: 39]. We particularly believe that S.V. Kobzeva is quite right and well-advised as she suggests legislative changes that will obligate Internet providers to: monitor and block the dissemination of illegal Internet content at public Internet outlets; provide new subscribers with the optimal level of filtration and protection from aggressive information, depending on the age and number of minor users; and include the installation and set-up of content filtration software in the list of their services.

6. Legal Protection of Children against Contact Risks

The information security provided for by current Russian law does not exclude or diminish other threats children may face as they go online.

A second category of risks faced by children on the Internet is contact risks, i.e. those arising from improper (dangerous) communication.

The main types of dangerous communications identified by today's legal science include:

cyber-aggression, same as cyber-bullying or trolling–humiliation or mobbing via mobile phones and other electronic devices;

cyber-grooming–drawing a child into actions of a sexual nature;

cyber-stalking–online persecution (shadowing).

Clear-cut legal mechanisms of protection against such threats are virtually non-existent now, but some of those actions on the Internet may be classified as criminal offences.

For example, under some circumstances acts of cyber-aggression may be found to fall under Article 110 of the Criminal Code of the Russian Federation 'Causing a Suicide' (Article 110.2 (d), Article 110.1 'Aiding and Abetting Suicide', or Article 110.2 'Organisation of Activities Aiming to Incite Suicide'. The elements of a crime covered by Article 111 'Wilful Infliction of a Grave Injury to Health that Entailed a Mental Disorder' are more difficult to prove practically, but that is still possible. Notably, commission of such crimes in respect of minors entails stricter penalties than in the ordinary case (where the victim is an adult).

Cyber-grooming is covered by the provisions of Article 133 'Compulsion to Commit Actions of a Sexual Nature' and Article 135 'Sexual Misconduct'.

Cyber-stalking is not prosecuted under the current criminal legislation.

A.I. Bastrykin, Chairman of the Investigation Committee of the Russian Federation, has repeatedly referred to the difficulties of investigating such crimes involving the use of the Internet: in his opinion, the virtualisation of society, especially its younger generation, has a number of serious negative consequences that include the emergence and development of information and telecommunication technology crimes [Bastrykin A.I., 2022].

We cannot but agree that protection of the information society's security is a most pressing issue that arises as the Russian state implements its digital economy policy, for digital crimes become more numerous with every passing year [Shevchenko O.A., Agadzhanyan M.A., 2021: 27–33].

On the other hand, it is important to understand and remember that the mere existence of criminal law mechanisms for protection against crimes committed in respect of children cannot redress the harm inflicted on the child. Given the priority nature of children's interests and facilitating their development, we find it objectively necessary to develop preventive legal measures that might contain the Internet crime.

7. Legal Protection of Children against Virtual Transaction Risks

Virtual transactions and the risks they pose can be seen from two perspectives: those of the child's property and non-property interests.

The former case is where a child makes undesirable online purchases and transactions not approved by his/her parents, The latter case is where a child buys harmful paid information products (fund-raising subscriptions, lectures, or courses) that are often not adapted to the child's or adolescent's age.

The property interests of children and their parents raising minors under Article 80 of the Family Code of the Russian Federation may be protected by invoking general provisions of civil law. For instance, parents may return or refuse an unsuitable item if the online seller provides this feature, or sue for the cancellation of the contract.

However, protection of children's non-property interests is outside legal regulation. The current law provides for no quick responses to, or safe-

guards against objectionable information products offered online, particularly by online fraudsters and info gypsies.

8. Legal Protection of Children's Privacy and Personal Data

Children's more vulnerable position online than adults' results, in particular, from minors' specific behaviour characteristics (like impulsiveness and emotional volatility) but also from the data owners being informed of the processing of their personal information in language that children cannot understand due to their age, and in some cases, from the fact that children (especially younger ones) cannot even realise that their personal data will be processed, and the resultant threats [Krylova M.S., 2019: 194–199].

Examples of such threats include:

doxing–unauthorised collection of information, particularly in digital file form;

deanon–public dissemination of personal data / other personal information;

faking–dissemination of false information; manipulation of public opinion [Bogatyryov K.M., 2022: 136–142].

No legal safeguards against the above threats have been established, for the legal regulation of children's and adults' personal data is not differentiated. And, while an adult person aware of his/her risks may take the necessary precautions, e.g. ban the use of cookie files, a child will hardly ever do that. The latter is what enables us to discuss, as part of legal discourse, the peculiarities of children's legal status that deserve due attention during the formation of a digital society.

9. Government and Non-Government Initiatives to Protect Children's Rights in the Internet

According to Article 4 of the Law on Children's Rights, the goal of government policy on children is to protect children from things that negatively affect their physical, intellectual, mental, spiritual, and moral development.

Experience of the most developed countries of the world, including Russia, shows that effective measures at the level of the state (i.e., undertaken on its initiative and with its support) are:

Impose a legal ban and restriction on dissemination of information that may be harmful to children;

Introduce a regulatory classification of web-sites;

Raise awareness of children, parents, and teachers on cyber threats and ways to tackle them.

At the same time, legislation *per se*, without an well-functioning enforcement mechanism, is insufficient; only where these elements are combined can one speak of real rather than nominal protection of children's rights.

In the section on content risks we described the mechanism used in the Russian media space to restrict access to prohibited information and, as a result, to effectively block a particular web-site with such information. Today, this is one of the key measures to protect children's rights on the Internet.

Introduction of ombudsperson for children's rights in the Russian Federation, both under the President and at the level of the constituent entities, is another strict measure. According to Article 2 of the Law on ombudspersons for children's rights,[14] the ombudsperson's work complements the existing means of protecting children's rights and legitimate interests, does not override the authority of government agencies to protect and restore children's violated rights and legitimate interests, and does not entail any review of such authority.

Main goals and objectives of ombudsperson are to ensure protection of children's rights and legitimate interests; support formation and effective functioning of a government system for implementation, compliance and protection of children's rights and legitimate interests by government authorities, bodies of local self-government, and government officials; monitor and analyse the performance of the mechanisms for implementation, compliance and protection of children's rights and legitimate interests etc. The areas where the ombudsperson is to solve the aforementioned tasks include children's safety on the Internet.

Furthermore, various special information web-portals and web-sites are established and operated with financial support from federal authorities, e.g., the web-portal *Don't Let It Happen!* [15] created with support from the Ministry of Digital Development, Communications and Mass Media to counter cyberthreats, modern slavery and dangers to children, and the Centre for the Safe Internet in Russia, an online news outlet on safe world-

[14] Consolidated legislation of the Russian Federation, 2018, No. 53 (Part I), P. 8427.

[15] Available at: URL: https://nedopusti.ru/site/ (accessed: 30.05.2023)

wide-web surfing[16] operating with support from the Federal Agency for Press and Mass Communications.

State remedies are more effective when combined with support for public initiatives because it is society, its sentiments, interests and goals that determine the meaning of state activity and state bodies. Hence, NGOs are now widely encouraged to work towards protecting children's rights on the Internet.

Cyber volunteering, a relatively new phenomenon of social online reality, is a type of volunteering that is done remotely via Internet technologies.

With regard to protecting children's rights against online threats, cyber volunteers can act as a "quick-response protector" to assist a child or young person in resolving a difficult case in the world-wide web.

The Ministry of Science and Higher Education has summarised the working experience of cyber volunteer movements and developed Methodological Recommendations for Educational Institutions of Higher Education on the Formation of Media and Cyber-volunteer Units in the field of countering illegal content. The Recommendations, circulated in Letter of the Ministry of Science and Education No. MN-6/115[17], are intended in particular for the employees of higher education institutions that are in charge of developing volunteer movements, as well as for staff members engaged in implementing the state youth policy on countering terrorist ideology and preventing extremism; however, the Recommendations can be used by any interested persons.

10. Digital Protection (Self-Protection) as a Special Measure

It is common knowledge that, in theory, the right to defence can be exercised either through specially authorised state bodies or through the independent actions of an authorised person. Accordingly, two types of defence are distinguished:

Non-jurisdictional, when the right to defence is implemented through independent actions of the authorised person (self-protection, use of swift enforcement measures, pre-trial dispute settlement, non-enforcement of rules in the implementation of a right);

Jurisdictional, when the right to defence is implemented through government bodies and other bodies authorised by the state to protect rights (arbitration courts, notaries) [Kurbatov A.Yu., 2013].

[16] Available at: URL: https://www.saferunet.ru/ (accessed: 30.05.2023)

[17] SPS Consultant Plus.

The Family Code of the Russian Federation entrusts primarily the parents or persons in *loco parentis* with the protection of children's rights, so the sphere of parental discretion or responsibility begins where the state legal protection of children's interests on the Internet ends.

Technically, Internet users get access to the world-wide-web by means of devices of various types and through communication services provided under a contract that minors are not entitled to enter into, so only the telecommunications service recipient that owns the device can provide such access to minors. Such recipients include parents, statutory representatives, educational and other organisations, and it is them that the legislator charges with the primary duty to filter content that a child can access.

At present, the main non-jurisdictional measure for protecting children's rights on the Internet is the so-called parental control or, in other words, content filtering on home computers and other electronic devices that children use to access the Internet. Parents can filter content on their own, 'in manual mode', or can purchase special software[18]. And, since this protective measure is effected through digital technologies, we believe it would be appropriate to talk of a new remedy, namely digital protection (self-protection). T. Sustina, lawyer at the Moscow Region Bar Association, notes that the issue of digital self-protection for children is now recognised by the world community as an international policy priority [Sustina T., 2022: 8–9].

Conclusion

The current Russian law certainly responds to the challenges of digitalisation and informatisation of modern society by providing specific legal measures to ensure the protection of children's rights on the Internet. As was found and outlined above, from a legal perspective, children's rights in Russia are best protected against content-related risks, much less protected against contact-related risks, and even less against virtual transaction risks and Internet privacy and security risks.

At the same time, the present norms and regulations are only isolated responses intended to protect children's rights that fail to constitute a holistic system. For such a system to form, it is necessary to continue developing legal aspects of children's activities in the information space and virtual interaction on the Internet. In course of this development, regulation of the

[18] Available at: https://lifehacker.ru/roditelskij-kontrol-na-telefone/ (accessed: 10.05.2023)

information law and the need for a harmony between the public and the private in state protection, non-governmental protection, and self-protection of children's rights must be taken into account.

References

1. Abramov V.I. (2007) The Rights of the Child and Their Protection in Russia: Theoretical Analysis. Doctor of Juridical Sciences Thesis. Saratov, 55 p. (in Russ.)

2. Alexeyev S.S. (2005) Theory of State and Law. Textbook. Moscow: Norma, 283 p. (in Russ.)

3. Amirova D.K. (2022) The concept of 'Child' in Criminal Law Regulation Terminology: Legislative Regulation and Improvement. *Vestnik Kazanskogo juridicheskogo instituta MVD*=Bulletin of Kazan Law Institute of Internal Ministry, no. 4, pp. 40–46 (in Russ.)

4. Arkhipov S.I. (2004) *Subjects of Law: A Theoretical Study.* Saint Petersburg: Centre-Press, 466 p. (in Russ.)

5. Bastrykin A.I. (2022) Development of the Digital Infrastructure for the Educational Process in the System of the Investigation Committee: Global Virtualisation Risks for the Young Generation. *Rassledovanie prestupleniy*= Investigation, no. 1, pp. 9–13 (in Russ.)

6. Bogatyryov K.M. (2022) Threats to Media Security in a Digital Environment: Systematisation and Analysis. *Aktualnye problemy rossiyskogo prava*=Issues of Russian Law, no. 7, pp. 136–142 (in Russ.)

7. Channov S.Ye. (2022) Artificial Intelligence System as a Legal Subject/ Quasi Subject. *Aktualnye problemy rossiyskogo prava*=Issues of Russian Law, no. 12, pp. 94–109 (in Russ.)

8. Dolinskaya V.V. (2012) Legal Status and Legal Personality. *Zakony Rossii*=Russian Laws, no. 2, pp. 6–17 (in Russ.)

9. Ivansky V.P. (2016) To Define Man as a 21st Century Law Subject through the Lens of the Quantum Information. Concept of Law. *Administrativnoe pravo i process*=Administrative Law and Process, no. 1, pp. 70–75 (in Russ.)

10. Kapitonova Ye.A. (2010) The Child's Constitutional Duties in the Russian Federation. Candidate of Juridical Sciences Summary. Penza, 25 p. (in Russ.)

11. Kobzeva S.V. (2017) Protection of Minors' Rights from Threats on the Internet *Informatcionnoe pravo*=Information Law, no. 2, pp. 33–39 (in Russ.)

12. Korshunova O.N. et al. (2021) Protection of Minors' Rights by the Public Prosecutor: A Guide. Moscow: Yustitia, 588 p. (in Russ.)

13. Krylova M.S. (2019) Legal Protection of Minors' Personal Data in Electronic Communication in the European Union. *Aktualnye problemy rossiyskogo prava*=Issues of Russian Law, no. 3, pp. 194–199 (in Russ.)

15. Kucherov I.I., S.A. Sinitsyn S.A. et al. (2022) Digital Economy: Lines of Legal Regulation. A Guide. Moscow: Norma, 376 p. (in Russ.)

14. Kurbatov A.Ya. (2013) *Protection of Rights and Lawful Interests.* Moscow: Justitcinform, 172 p. (in Russ.)

15. Mitskevich A.V. (1962) *Subjects of Soviet Law.* Moscow: Yurizdat, 212 p. (in Russ.)

16. Pavlova L.V. (2022) On Improvement of Co-ordination and Interaction Among Actors in Protecting the Rights of the Child. *Administrativnoe pravo i protcess*= Administrative Law and Process, no. 7, pp. 19–22 (in Russ.)

17. Ponomaryova Ye. V. (2019) Subjects and Quasi Subjects of Law: Theoretical and Legal Aspects of Distinguishing. Candidate of Juridical Sciences Summary. Ekaterinburg, 32 p. (in Russ.)

18. Protsevsky V.A., Golikova S.V. (2020) Child's Constitutional Law Status in the Russian Federation. *Semeinoe i zhilishnoe pravo*=Family and Shelter Law, no. 6, pp. 29–31 (in Russ.)

19. Rybakov O Yu., Rybakova O.S. (2018) The Child and Internet Space: Legal Safeguards of Security. *Informatcionnoye pravo*=Information Law, no. 1, pp. 27–31 (in Russ.)

20. Sitdikova L.B. (2011) Civil Justice and Implementation of a Minor's Right to Protection. *Arbitraznyi igrazhdanskyi process*=Arbitration and Civil Process, no. 2, pp. 8–10 (in Russ.)

21. Shevchenko O.A., Agadzhanyan M.A. (2021) Cyber Hooliganism as a Consequence of Development of Digital Rights in Information Society. *Bezopasnost biznesa*=Security of Business, no. 5, pp. 27–33 (in Russ.)

22. Sustina T. (2022) Internet Security of Children. *Advokatskaya gazeta*= Advocates Gazette, no. 5 (in Russ.)

23. Theory of State and Law (2003) Textbook. A.S. Pigolkin (ed.). Moscow: Gorodetz, 544 pp. (in Russ.)

24. Trigubovich N.V. et al. (2022) Concept of the Improvement of Legislation Regulating the Relations between Children and Parents. *Zakon*=Law, no. 1, pp. 28 –38 (in Russ.)

25. Zhavzandolgor B. (2004) International Legal Protection of Children's Rights. Candidate of Juridical Sciences Summary. Moscow, 25 p. (in Russ.)

Information about the author:

R.V. Khisamova — specialist.

The article was submitted to editorial office 03.04.2023; approved after reviewing 18.05.2023; accepted for publication 18.05.2023.

Legal Issues in the Digital Age. 2023. Vol. 4. No. 2.
Вопросы права в цифровую эпоху. 2023. Том 4. № 2.

Comment

Review
УДК: 347
DOI:10.17323/2713-2749.2023.2.142.157

Key Issues in the Intellectual Property Court Presidium Rulings

M.A. Kolzdorf[1], N.I. Kapyrina[2]

[1] Intellectual Property Court, 5/2 Ogorodnyy Proyezd, Moscow 127254, Russia

[2] MGIMO University, 76 Prospekt Vernadskogo, Moscow 119454, Russia

[1] mkolzdorf@hse.ru, ORCID: 0000-0003-3227-3348, Researcher ID: AAI-1625-2019,

[2] n.kapyrina@my.mgimo.ru, ORCID: 0000-0003-1276-1600, Researcher ID: AAQ-3784-2021,

Abstract

The comment reviews key positions in the rulings of the Presidium of the Russian Intellectual Property Court (IPC) issued between July and September 2022. The Chamber hears cassation appeals against the decisions of the IPC first instance and deals primarily, but not only, with matters of registration and validity of industrial property rights. Therefore, the review predominantly covers substantive requirements for patent and trademark protection, as well as procedural issues both in the administrative adjudicating mechanism at the Patent office (Rospatent) and at the IPC itself. The current review encompasses a variety of topics related to trademark Law, patent law and various procedural matters.

Keywords

bankruptcy; trademarks; appellations of origin; Paris Convention; descriptive sign; patent term extension; novelty; originality; industrial design; co-ownership of trademark; termination of protection; evaluation of evidence.

For citation: Kolzdorf M.A., Kapyrina N.I. (2023) Key Issues in the Intellectual Property Court Presidium Rulings. *Legal Issues in the Digital Age,* vol. 4, no. 2, pp. 142–175. DOI:10.17323/2713-2749.2023.2.142.157

I. Trademarks

1. Opposition Based on a Trademark whose Protection has been Terminated

IPC Presidium Resolution of 15 September 2022 in Case No. IPC-584/2021

When assessing signs for compliance with Para 6, Art. 1483 of the RF Civil Code, it is necessary to take into account also those trademarks whose term of protection has expired, but whose protection can be reinstated in accordance with the procedure provided for by Para 2, Art. 1491 of the Civil Code.

Rospatent refused to register a trademark in respect of part of the services filed in the application on the basis of Para 6, Art. 1483, the Russian Federation Civil Code because of the existence of an earlier trademark of a third party.

The applicant filed an opposition with Rospatent, in which it referred to the fact that the term of legal protection of the earlier trademark had expired.

Rospatent rejected this reasoning and dismissed the opposition.

Rospatent offered the following arguments: according to Para 2, Art. 1491, the Civil Code, the term of the exclusive right to a trademark may be extended for ten years at the request of the right holder submitted during the last year of validity of such a right. The validity term of the exclusive right to a trademark may be extended an unlimited number of times. At the request of the right holder, the latter may be granted six months after the expiry of the exclusive right to the trademark to file the said application for term extension. The right holder of the earlier trademark submitted to Rospatent a request to benefit from the six-month period for filing an application for extension of the validity of the trademark with additional materials (the proceedings on these materials have not yet been completed).

The first instance court concluded that Rospatent had lawfully compared the disputed sign to the earlier trademark, but cancelled Rospatent's decision due to the fact that the term of legal protection of the earlier trade-

mark had expired by the time of consideration of the case without the possibility of extending such protection.

The IPC Presidium upheld the first-instance court's ruling while stating the following.

At the time of Rospatent's contested decision it was possible to restore the legal protection of the earlier trademark in accordance with the procedure in Para 2, Art. 1491 of the Civil Code. This fact proved that Rospatent was obliged to take into account the trademark in question when checking the compliance of the applicant's sign with the legal requirements under Subpara 2, Para 6 of Art. 1483 of the Civil Code (i.e., Rospatent made a legit comparison.)

However, at the time the first instance court considered the case, this was no longer possible, which allowed the court to adopt the appropriate decision in connection with the loss of the possibility to restore legal protection of the earlier trademark.

2. Possibility of Misleading where there is no Risk of Confusion

IPC Presidium Resolution of 29 August 2022 in Case No. IPC-295/2021

Subpara 1, Para 3 and Subpara 2 Para 6, Art. 1483 of the RF Civil Code are independent grounds for refusal of state registration of a trademark or invalidation of the legal protection granted to a registered trademark.

The provisions of Subpara 1, Para 3, Art. 1483 shall apply, among other cases, if one person has widely used a sign for a long period of time and it has been proven that the sign in the consumer's mind persistently associates with the person who used it, and another person has acquired the exclusive right to such a sign through its registration as a trademark.

Disputed trademark (unprotected elements: the shape of the package, the words "PELMENI", "PREMIUM QUALITY PRODUCT")

Two companies jointly engaged in the production of "pelmeni" (meat dumplings) filed an objection with Rospatent against the registration of the disputed trademark, also registered in respect of "pelmeni". Rospatent invalidated the this trademark due to its non-compliance with the requirements of Subpara 1, Para 3, Art. 1483. The first instance court upheld this administrative decision, and the IPC Presidium upheld the court's decision.

The court agreed with Rospatent's decision that the disputed trademark itself does not carry any direct information that could mislead the consumer as to the manufacturer of the goods.

At the same time, the invalidity applicants have succeeded in proving that, due to their joint long and intensive production and sale of "pelmeni" in a tied black-coloured bag, this sign has become widely known among consumers. Due to such popularity, specific associations have risen in the minds of consumers before the priority date of the disputed trademark; hence, the disputed sign can be misleading for the consumer.

The first instance court rejected the rightholder's argument that the presence of other elements in the disputed trademark, such as the applicant's company name, which, in its opinion, occupies a dominant position, ensures compliance with the requirements of Subpara 1 Para 3, Art. 1483.

The IPC Presidium found these conclusions justified, emphasising that the comparison was made between the disputed trademark, on the one hand, and a long-standing and widely used sign, on the other, that, *inter alia*, had been established by a number of judicial acts that had entered into legal force and a decision of the antimonopoly authority.

In the course of the judicial review one question was particularly discussed: the possibility of recognising the disputed trademark as misleading in relation to a well-known sign when no likelihood of confusion under Subpara 2, Para 6, Art. 1483 of the Civil Code was found between the disputed trademark and the same well-known sign registered as a trademark. According to the case materials, the packaging shape used by the invalidity applicants had been registered as a trademark before the disputed trademark's priority date, and during the examination of the disputed trade mark Rospatent did not find any likelihood of confusion of the 'junior' trademark with the previously registered 'senior' trademark. Therefore that registration gave rise to a presumption of validity, as the absence of the likelihood of confusion between the two signs compared was now presumed.

In the course of cassation appeal, the IPC Presidium used its right to send enquiries to the scholars in accordance with the procedure provided

for by Part 1.1, Art. 16 of the RF Commercial Procedural Code, in order to obtain clarifications on the relationship between Subpara 1, Para 3, and Para 6, Art. 1483 of the Civil Code, specifically on the value of the presumption validity based on the absence of likelihood of confusion.

As a result, the IPC Presidium concluded that Subpara 1, Para 3 and Subpara 2, Para 6, Art. 1483 of the Civil Code are independent grounds for refusing to register a trademark and independent grounds for invalidating the granting of legal protection to an already registered trademark.

The provisions of Subpara 1, Para 3, Art. 1483 of the Civil Code shall also apply, among other situations, if one person has been widely using a sign for a long time and it has been proved that this sign creates in the consumer's mind a persistent associative link with the person who used it, and another person has acquired the exclusive right to such a sign through its registration as a trademark.

The IPC Presidium pointed out that in this particular case, the aforementioned presumption of validity could simply not be overcome, since the misleading element of the disputed trademark had been disclaimed.

In such a case, the fact that the mentioned element of the disputed trademark misleads consumers by virtue of the provisions of Subpara 1, Para 3, Art. 1483 of the Civil Code, allows to consider the entire trademark as misleading, on the one hand (without analysing other elements included in the trademark), while the disclamation of this element does not allow challenging its registration under the rules of Subpara 2, Para 6, Art. 1483 of the Civil Code, on the other hand.

Thus, the IPC Presidium recognised that in this case it was legitimate to apply Subpara 1, Para 3, Art. 1483 as an independent ground for invalidating the granting of legal protection to the disputed trademark.

3. Evaluation of Evidence Found on the Internet

IPC Presidium Resolution of 05 August 2022 in Case No. IPC-17/2022

It cannot be argued that consumers have developed certain associative links with a sign merely on the basis that an unknown person has entered some information into a free content encyclopaedia, without analysing the duration of the placement of such information on the Internet, the number of its views and citations, etc.

Rospatent rejected the application for the sign "White Hand" in respect of a broad list of goods of ICGS Classes 5, 32, and services of ICGS Classes 35, 39, and then rejected the applicant's objection against this decision. The IPC recognised the last decision of Rospatent invalid due to its non-compliance with the requirements of Subpara 2, Para 3 of Art. 1483. The IPC Presidium upheld the first instance court's ruling.

When considering the objection, Rospatent pointed out that the experts, based on information from Wikipedia and one literary source, saw in the applied verbal sign a reference to the name of a number of terrorist organisations that were active in foreign countries (Serbia, Guatemala) at the beginning and in the second half of the 20th century. In doing so, Rospatent noted that the applicant had not provided any documents refuting that information and rejected the argument that there was no such banned terrorist organisation in the Russian Federation, pointing out that such a socio-political phenomenon as terrorism had no geographical boundaries or time frames.

The first instance court pointed out that this decision was unlawful because Rospatent had not analysed the associative links arising in the consumer's mind upon seeing the sign. The mere fact of mentioning the sign 'White Hand' as the name of a terrorist organisation is not a basis for applying the provisions of Subpara 2, Para 3, Art. 1483 of the Civil Code: to do so, the relevant associations arising in the consumer's mind and the nature of their perception of the sign must be assessed.

The IPC Presidium reminded that in order to assess the sign for its compliance with the norms of Subpara 2, Para 3, Art. 1483 of the Civil Code, it is necessary to take into account how consumers perceive this sign in each specific case, based on the sign's semantic meaning and taking into account all relevant factors on a case-by-case basis.

The IPC Presidium then supported the position of Rospatent that propaganda of terrorism and registration as a trademark of a sign reproducing the name of a terrorist organisation and perceived as such by the Russian consumer was unacceptable.

At the same time, the IPC Presidium noted that Rospatent's conclusion based only on information from an encyclopaedia such as Wikipedia, from other Internet sources referring to it, and from a literary publication of approximately the same year of publication as the application filing date, does not correspond to the expected level of legal motivation, especially

since Rospatent has broad powers to involve a wide range of sources and information at different stages of sign evaluation to motivate its decisions.

The IPC Presidium reminded that the activities and decisions of a public body should inspire the confidence of citizens, society and organisations.

4. Co-ownership of Trademarks under International Registration

IPC Presidium Resolution of 27 July 2022 in Case No. IPC-281/2021

In view of the provisions of Art. 6 quinquies (B) of the Paris Convention, the granting of legal protection in the Russian Federation to a trademark registered under international registration cannot be recognised invalid on the grounds of its inconsistency with the norms of Art. 1478, Civil Code (due to the fact two legal entities are the right holders of the trademark).

An individual entrepreneur applied to Rospatent with an objection against the granting of legal protection to a trademark under an international registration. Initially the registration was in the name of one foreign legal entity, but years later the international registry was amended, and two foreign legal entities became the right holders. Rospatent refused to grant the objection, following which the individual entrepreneur appealed to the IPC. The first instance court dismissed the claims, and the cassation court upheld this ruling.

In rejecting the claims, the first instance court drew attention to the admissibility of co-ownership of a trademark under an international registration in the case of its registration as such in the country of origin, which is directly evidenced by the rules of the Paris Convention.

The IPC Presidium also noted that under Art. 6.quinquies (B) of the Paris Convention, trademarks falling under this Article of the Convention may be refused registration or invalidated only in the following cases:

where the signs may infringe rights acquired by third parties in the country where protection is claimed;

if the signs have no distinctive character or consist exclusively of signs or indications which may serve, in trade, to indicate the kind, quality, quantity, intended purpose, value, place of origin of the goodsm or the time of production, or which have become customary in the current language or

in the bona fide and established commercial practices of the trade of the country where protection is claimed;

if the signs are contrary to morality or public policy and, in particular, of such a nature as to deceive the public.

Article 10.bis of the Paris Convention provides for the invalidation of the granting of legal protection to a trademark if its registration constitutes an act of unfair competition.

Under the Paris Convention, there are no other grounds for refusal to grant legal protection to trademarks under international registrations.

In accordance with the meaning of the above norms of international law, the granting of legal protection to a trademark under international registration in the Russian Federation may be refused only on the grounds expressly mentioned in the said legal norms.

Thus, the IPC Presidium agreed with the conclusion of the first instance court that the granting of legal protection in the Russian Federation to the contested internationally registered trademark cannot be invalidated on the grounds of its inconsistency with the norms of Art. 1478 of the Civil Code (due to the fact that the right holders of the trademark are two legal entities).

5. Methodology for Comparing a Trademark and an Appellation of Origin

IPC Presidium Resolution of 22 July 2022 in Case No. SIP-1042/2021

For the purposes of Para 7, Art. 1483 of the Civil Code, the trademark (the sign applied for registration) is to be subjected to comparison with account of its strong and weak elements and the appellation of origin taken as a whole,**.**

Rospatent refused to register the sign 'Palazzo di Parma' with respect to a broad list of ICGS Class 29 goods and to satisfy the applicant's objection, despite the voluntary reduction of the list of goods. The first instance court, on the contrary, recognised the designation as fancy and cancelled Rospatent's decision due to the violation of the provision of Subpara 1, Para 3, Art. 1483 of the Civil Code. The court also disagreed with Rospatent's conclusion that the sign does not comply with the provisions of Para 7, Art. 1483.

In particular, the first instance court did not agree with the conclusion that the applied-for sign and the earlier appellation of origin 'PROSCIUTTO DI PARMA' have a common strong element 'DI PARMA' / 'di Parma'. The Court stated that the subject of comparative analysis to establish similarity on the semantic criterion should be the verbal elements 'Palazzo' of the disputed designation and 'PROSCIUTTO' of the earlier appellation of origin, which have no phonetic and semantic similarity. Taking this into account, the court ordered Rospatent to register the contested sign.

The IPC Presidium, in its turn, decided to change the first instance court's decision and passed a new court order obliging Rospatent to reconsider the objection against the refusal to grant legal protection to the trademark, with account of the legal positions set out in the ruling.

Firstly, the IPC Presidium rejected Rospatent's claim that the court decision did not comply with the requirements of Subpara 1, Para 3, Art. 1483. The decision of Rospatent was rightly recognised invalid because the circumstances regarding the probable associative links with the sign applied for registration in relation to each product (group of products) had not been investigated in detail.

Secondly, the IPC Presidium noted that, in general, it is a methodological error to look for strong and weak elements in an appellation of origin, since such a means of individualisation is granted legal protection if the sign as a whole has become known in relation to specific goods.

Accordingly, the IPC Presidium clarified that for the purposes of Para 7, Art. 1483 of the Civil Code, a trademark (a sign applied for registration) is subject to comparison with account of its strong and weak elements and the appellation of origin as a whole.

6. Termination of Trademark Protection in case of Right Holder's Bankruptcy

IPC Presidium Resolution of 21 July 2022 in Case No. SIP-1172/2021

If the right holder has voluntarily terminated his/her activity as an individual entrepreneur, but at the time when a third party files an application for early termination of the legal protection of a trademark, bankruptcy proceedings have already been initiated against this right holder, the interests of such third party shall be satisfied not at Rospatent by considering the said application, but by purchasing the trademark at auction as part of bankruptcy proceedings.

A company filed an application with Rospatent for early termination of the legal protection of a trademark due to the termination of the right holder's activities as an individual entrepreneur.

Rospatent refused to satisfy the objection because at the time the application was filed, a debt restructuring procedure had been introduced against the right holder. Consequently, all the assets of this person constitute the bankruptcy estate, the disposal of which is carried out as part of the bankruptcy case.

The first instance court upheld Rospatent's decision.

The company has filed a cassation appeal. The company pointed out that it follows from the clarifications of Para 175 of the Resolution of the Plenum of the Supreme Court of the Russian Federation No. 10 of 23 April 2019 'On the Application of Part Four of the Civil Code of the Russian Federation', that the exclusive right to a trademark is included in the estate to be sold for the purposes of satisfying the property claims of creditors only when an individual entrepreneur ceases to operate against his/her will, i.e. in the event of a bankruptcy. In this case, according to the company's opinion, the right holder stopped their business activities at their own will; therefore, the legal protection of the disputed trademark should be terminated.

The company pointed to important violations of the application assessment procedure, arguing that it was the task of Rospatent to perform early termination of legal protection of trademarks, and that Rospatent failed to do so.

The IPC Presidium did not agree with the arguments for the following reasons.

According to Part 1, Art. 45 of the Russian Federation Constitution, everyone is guaranteed the protection of his or her rights. A company is not the only person to whom such protection is guaranteed; it is guaranteed to everyone, including those whose interests contradict those of the company.

In the context of early termination of the legal protection of a trademark, it is the not duty of Rospatent to automatically terminate such protection at the request of any person, but to consider the merits of the issue and terminate the legal protection only if there are grounds therefore (and there are no obstacles thereto).

Thus, the key question in this dispute is whether there were really no grounds for early termination of the legal protection of the disputed trade-

mark and whether Rospatent was able to establish this (which includes the actions which, in the company's opinion, violate the procedure).

As directly follows from the said Para 175 of Resolution No. 10, the Supreme Court considers only three of all possible cases involving individual entrepreneurs: 1) voluntary cessation of business activities without any operations with the trademark, 2) voluntary cessation of business activities with subsequent transfer of the trademark to a legal entity or individual entrepreneur (or where the right holder obtains a new status of an individual entrepreneur), and 3) forced termination of business activities (including bankruptcy).

The Supreme Court does not consider the case of a voluntary cessation of business operations followed by bankruptcy.

From this point of view, both the purpose of the legislative regulation and the substance of the Supreme Court's clarifications need to be clarified so as to determine whether they can apply by analogy to the situation in the present case.

The IPC Presidium drew attention to the legal position stated in the Supreme Court's ruling of 21 March 2018 No. 306-ES17-19720: in addition to the provisions of the Civil Code, which give legal grounds to strip the right holder of the exclusive right to a trademark, one should also take into account the special norms of the Bankruptcy Law, which are aimed at protecting the rights and legitimate interests of creditors of the bankrupt right holder. Therefore, to achieve a balance between the interests of the person wishing to use the trademark and the creditors interested in the fullest satisfaction of their claims at the expense of the debtor's property, the trademark must be purchased at an auction for a fair price.

The essence of the legislative regulation laid down in Subpara 4, Para 1, Art. 1514 of the Civil Code is that in order to secure the interest of a particular person who is not the holder of a trademark, protection for a sign that is no longer used in business operations must be discontinued (no justification of such interest is required).

According to the logic of the Supreme Court, this interest is to be protected unless an interest that is more important for the law and order is identified (the interest of the legally compliant right holder in the second case described by the Supreme Court or the interest of creditors in the third case).

The situation considered in this case is essentially a compilation of the second and third situations considered by the Supreme Court. Namely,

business operations were ceased on a voluntary basis, but at the time the application for early termination of the legal protection of the disputed trademark was filed, the arbitration court ruled that a procedure for restructuring the individual's debts should be introduced in respect of the right holder. The individual was later declared insolvent (bankrupt).

In that situation, both Rospatent and the first instance court focused on the legitimate interest of the creditors, seeking to satisfy their claims at the expense of the debtor's property.

The company's interest in the trademark in such a situation may be protected in different way, namely, by purchasing the trademark at an auction for a fair price.

7. Descriptive Nature of a Sign

IPC Presidium Resolution of 20 July 2022 in Case No. SIP-1044/2021

The characteristics of a goods that prevent registration of a sign on the basis of the provision of Subpara 3, Para 1, Art. 1483 of the Civil Code include the intended result of the use of goods for the purpose specified.

Disputed sign

Rospatent refused to register the disputed sign, citing, in particular, non-compliance with the requirements of Subpara 3, Para 1, Art. 1483 of the Civil Code, since the verbal elements 'Mouse Death' indicating the purpose (to cause death to rodents, i.e., mice) and properties (destroying rodents, i.e., mice) of the goods in question.

The first instance court overturned the decision of Rospatent, which rejected the applicant's objection, and concluded that the disputed verbal elements should be protected. In the opinion of the court, this element is fancy and not descriptive in respect of ICGS Class 5 goods, as it does not directly

indicate the property and purpose of the goods, nor does it indicate the type of goods, the name of raw materials or materials from which ICGS Class 5 goods are made, nor does it contain any definition of a animal poison.

In overturning the decision of the court of first instance, the IPC Presidium stated that the substantive law had been applied incorrectly: the court had unjustifiably narrowed the content of Subpara 3, Para 1, Art. 1483 of the Civil Code.

Pursuant to this norm, signs consisting only of elements characterising goods, including those indicating their type, quality, quantity, property, purpose, value, as well as the time, place and method of their production or sale, cannot be registered as trademarks.

The "properties of the goods" and "purpose of the goods" mentioned in this norm are only examples of possible characteristics of the goods. The wording "including", from the point of view of the Russian language, clearly means that the list of possible characteristics of the goods is not exhaustive.

Such characteristics may also include the intended result of using the product for the purpose specified (in the case under review, the cessation of activity of a rodent, in particular, a mouse).

(On re-examination, the intellectual property court dismissed the claims in its judgement of 18 October 2022).

II. Patents

8. Extension of Patent Term for a Divisional Application

IPC Presidium Resolution of 29 August 2022 in Case No. SIP-1141/2021

In case a patent granted on the basis of a divisional application is extended, the filing date of the divisional application should be considered to be **the initial application filing date.**

Rospatent issued supplementary patent at the request of the right holder on the basis of Para 2, Art. 1363 of the Civil Code.

The company believed that Rospatent extended the term of the disputed patent validity in violation of Para 2, Art. 1363 of the Civil Code and filed a petition to the IPC to recognise the actions of Rospatent as unlawful. The Company pointed out that the statutory requirement of at least five years between the filing date of the claim for an invention and the date of the first

authorisation for the use of its protected product had not been met in the case at hand.

The authorisation to use the medicinal product related to the disputed patent was received in 2014, while the divisional application that served as the basis to grant the disputed patent was not filed until 2020.

The IPC disagreed with this argument of the company, noting the following.

Taking into account Paras 1 and 2, Art. 1363 of the Civil Code, two legal events are relevant for establishing if the validity term of a patent for an invention relating to a medicinal product based may be extended:

1) date of patent application filing from which the term of validity of the patent shall be calculated;

2) date of the first authorisation to use the medicinal product (registration certificate). A patent for an invention relating to a medicinal product shall be renewed if more than five years have elapsed between dates (1) and (2).

For the purposes of Para 2, Art. 1363 of the Civil Code, the application filing date shall be determined by the date from which the patent term is calculated. Since the beginning dates of the calculation of patent validity term for a patent granted on the basis of a divisional application and for a patent granted on the basis of an initial application coincide and are determined by the initial application's filing date, the filing date of the divisional application (for the purposes of this norm) should be considered to be the filing date of the initial application.

9. Invention Novelty and Science Fiction

IPC Presidium Resolution of 29 July 2022 in Case No. SIP-649/2021

Mere suggestions about possible future technical solutions do not vitiate the novelty of the invention. Otherwise, when analysing novelty, the prior art should have included science fiction literature, among other things.

Rospatent received an objection and, upon considering it, invalidated the patent for the invention 'S1P Receptor Modulators for the Treatment of Multiple Sclerosis' on the grounds of the lack of novelty. The patent holder appealed to the IPC, which granted its application and recognised the decision invalid due to its failure to comply with the requirements of Paras 1 and 2, Art. 1350 of the Civil Code, ordering Rospatent to reconsider the ob-

jection to the granting of the patent. The IP Presidium upheld the decision of the first instance court, dismissing the cassation appeals of Rospatent and the invalidity applicant.

In granting the claim for invalidation of Rospatent's decision, the IPC examined not only the information sources presented in the case materials, but also took into account the answers of scholars and research institutions to the court enquiries made by the court pursuant to the procedure provided for by Part 1.1, Art. 16 of the Commercial Procedural Code, as well as the answers by expert R. Y. Yakovlev to the questions asked by the court and representatives of the parties.

The first instance court concluded that the technical solution was not presented in the prior art because the opposing source only made a theoretical assumption, and a survey was planned to verify this assumption.

The IPC Presidium upheld the decision, noting the validity of the approach that merely announcing a trial of a drug in the required dose does not provide a basis for recognising the known use of the drug in that dose.

10. Assessing Originality of an Industrial Design

IPC Presidium Resolution of 28 July 2022 in Case No. SIP-1251/2021

When an industrial design is assessed for its compliance with the condition of patentability 'originality', the disputed object must be evaluated and its essential, dominant features have to be singled out in the first place. Such features are determined irrespective of the analogue design chosen: they are inherent in the industrial design and characterise it as such.

Rospatent granted a patent for the industrial design 'Furniture module-transformer with storage system, sofa and folding bed' and rejected an invalidity application against it.

The first instance court decision, upheld by the ruling of the IPC Presidium, invalidated Rospatent's decision due to non-compliance with the requirements of Para 3, Art. 1352 of the Civil Code (assessment of originality).

In rejecting the cassation appeal, the IPC Presidium reminded that when checking the originality of an industrial design, first of all, its appearance is examined and its essential, dominant features are identified. The Presidium recalled the definitions of such features and their differences from mere nuancing features.

In the next step, the appearance of the product is compared with the appearance features of an opposing product selected from the range of analogues. This comparison makes it possible to determine whether the set of distinctive essential features of the disputed industrial design creates a different visual impression from the item in question.

When comparing the visual impressions of two items, information about known solutions that determine the appearance of products of this purpose and similar purposes (about the range of analogues) is taken into account, and the limitations of designers' abilities to develop a solution for the appearance of the product of the given purpose, associated, in particular, with the functional features of the product are considered (consideration of the designer's degree of freedom).

In the present case, however, as the first instance court found, instead of determining the essential features inherent in the disputed industrial design, then examining the closest analogue to determine whether these essential features are inherent in it, and identifying the essential features of the disputed industrial design which are distinctive from the closest analogue, thus determining the materiality of the contribution of such distinctive features to the appearance of the disputed industrial design, Rospatent began by comparing the disputed and opposed appearances of the products, and selected only the most material distinctive features of the disputed industrial design.

The IPC Presidium CIP emphasised that the essential, dominant features of the disputed appearance of a product are determined irrespective of the analogue chosen: they are inherent in the industrial design and characterise it as such.

Information about the authors:

M.A.Kolzdorf —LLM, Senior Lecturer.

N.I. Kapyrina — Candidate of Sciences (Law), Assistant Professor.

Contribution of the authors:

M.A. Kolzdorf — para 1, 6, 8.

N.I. Kapyrina — para 2, 3, 4, 5, 7, 9, 10.

The article was submitted to the editorial office 11.06.2023; approved after reviewing 23.06.2023; accepted for publication 23.06.2023.

Legal Issues in the Digital Age. 2023. Vol. 4. No. 2.
Вопросы права в цифровую эпоху. 2023. Том 4. № 2.

Review

Review
УДК: 342
DOI:10.17323/2713-2749.2023.2.158.175

New Information Technologies and Data Security

Ludmila Konstantinovna Tereschenko[1], Olesya Evgenievna Starodubova[2], Nikita Alekseevich Nazarov [3]

[1, 2, 3] Institute of Foreign Legislation and Comparative Law under the Government of the Russian Federation,

[1] Adm2@izak.ru

[2] olesyastarodubova@gmail.ru

[3] naznikitaal@gmail.com

Abstract

The paper provides a review of the research workshop "New Information Technologies and Data Security" took place on 23 May 2023 at the Institute of Foreign Legislation and Comparative Law (ILCL). The authors reflect the keynotes of the reports made by representatives of the Institute of Legislation and Comparative Law, Kutafin Moscow State Law University, National Research University–Higher School of Economics (NRU-HSE), Moscow State Lomonosov University (MGU), Plekhanov State University of Economics, Moscow State City Pedagogical University, etc. The paper provides an insight into the legal issues under discussion: concept and meaning of data security in the current environment; development vectors of the data security institution in the context of digitization; limits of sovereignty in the information domain; international legal regulators of data security; sustainable security mechanisms in the face of contemporary challenges and threats; impact of advanced information technologies such as artificial intelligence, big data, machine-sensible right to data security; personal data security; state control and liability for violation of information law, etc.

Keywords

data security; meta verse; digital avatar; personal data; biometric personal data; cross-cutting digital technologies; Big Data; artificial intelligence; information sovereignty; technological sovereignty.

For citation: Tereschenko L.K., Starodubova O.E., Nazarov N.A. (2023) New Information Technologies and Data Security. A review. *Legal Issues in the Digital Age,* vol. 4, no. 2, pp. 158–175. DOI:10.17323/2713-2749.2023.2.158.175

On May 23, 2023 the Institute of Foreign Legislation and Comparative Law hosted the research workshop "New Information Technologies and Data Security".

In opening the session, moderator **L.K. Tereschenko**, Chief Researcher, ILCL, Doctor of Juridical Sciences, Honored Lawyer of Russia, Russian Academy of Sciences expert, pointed out that the process of digitization has marked a new stage for data security as new issues and challenges resulting from new technologies and new opportunities called for a review of previous decisions, and there was a change of priorities and requirements to data security, only to solicit an adequate regulatory response.

Information technologies themselves are not something to be rebuffed. They are neutral and they open up new opportunities which can be used for a variety of purposes. This changes both the amount and content of data security. Moreover, data security of one group of subjects may not exactly coincide with that of another group in terms of meaning.

Information technologies are increasingly used to interfere in internal affairs of other countries, undermine their sovereignty and violate territorial integrity. This is destructive not only for information and public psychology but also directly impacts infrastructure facilities, banking sector and national data systems through hacker attacks, dissemination of fake information, intentionally false statements, calls for mass riots, extremist action, etc.

The emergence of new types of harmful information (trash streams and fake news etc.) with a negative impact on data security drives the problem beyond the national borders, only to give it an international, cross-border dimension. Rather than targeting data integrity, availability and confidentiality, attacks seek to destroy parts of the technological infrastructure to make it dysfunctional. The good news is that both public and private sector actors increasingly address the issues of data security.

A.V. Minbaleev, Head, Information Law and Digital Technologies Chair, Kutafin Moscow State Law University, Doctor of Juridical Sciences, pointed out to the fundamental issue of personal data security in the digital environment.

The speaker identified the following key vectors of data security:

1) A need to protect personal data in the digital environment. Users leave a great number of digital footprints in terms of statistical information useful for an analysis of actions in the Web which finally provides data on human beings. In this regard, it would be reasonable to upgrade the personal data law to specify and broaden the concept of personal data.

2) Personal data processed in large amounts constitute Big Data. However, Big Data have no protection mechanism. There is a need to improve both the Big Data law regulation and processing requirements in the digital environment. Requirements to information systems for personal data are usually stationary, only to make them inapplicable to cloud-based processing of Big Data.

3) Personal data protection needs to be adjusted to the digital context.

4) Protection of biometric personal data including genetic information in the digital environment. Formation of a biometric data monopoly. The Federal Law "On Identification and/or Authentication of Natural Persons Using Biometric Data, Amending Specific Regulations of the Russian Federation and Voiding Specific Legal Provisions of the Russian Federation" (No. 572-FZ of 29 December 2022)[1] raises a number of issues of the measures to be taken and reveals risks of data leakage. The government is pursuing a set of policies to force individuals to provide their biometric personal data. There are many questions on verification of biometric personal data by banks and other subjects supposed to feed data into the system.

5) Data protection issue in light of reliability. Right of access to reliable information, right to sharing reliable information. Problem of fakes and deep fakes. Artificial intelligence is now used to discredit public officers and celebrities and to commit frauds. Apart from amending the law, the culture of sharing reliable data needs to be promoted in society.

6) Issue of digital doubles. What is a digital avatar? What is its nature? Multiple threats including cloning. Digital avatars could be deleted and amended. This segment requires an assessment and further study.

7) Use of particular digital technologies. In a number of cases we have to use information technologies or data systems that, on the contrary, may be unavailable because of sanctions. As a result, users may be deprived of possibility to exist in the digital environment. In this case, the rights of us-

[1] Collected Laws of Russia. 2023. No. 1 (part I), Article 19.

ers are significantly restricted in violation of the principles enshrined in Federal Law No. 149-FZ "On Information, Information Technologies and Data Protection" of 27 July 2006[2].

V.N. Lopatin, Head and Research Director, Republican Research Institute of Intellectual Property, Chairman, National and Multinational Technical Committees on Standardization "Intellectual Property", Chairman, Association of Russian Lawyers, Commission on Intellectual Property, Doctor of Juridical Sciences, Professor, has identified priorities for systemic improvement of data security. In his presentation, V.N. Lopatin underlined time has come to reinvent and redefine data security priorities in the context of wider use of modern information technologies.

The data security was first identified as a segment of the national security system in 1989 when it traditionally meant protection of information, state/official secrets, specific data resources and public information systems.

The following three main categories are normally indentified in the system of data security assets:

information and data resources;

data systems;

society, individual and state.

To focus the resources at necessary points, priorities need to be defined for each group of assets.

As regards information, these include above all personal data, Big Data of an enormous autonomy, intellectual property in the context of protecting proprietary interests. The use of information technologies for protecting information and data resources.

Critical infrastructure protection issues.

One of the priorities of mass media and online media is to protect persons, society and state from the impact of misleading, fake information including the one created through the use of artificial intelligence.

The national legal system of information security relies on the principles of priority of international law. Russia was among the first to propose a convention against information warfare to be adopted by the United Na-

[2] Collected Laws of Russia, 2006, No. 31 (part 1), Article 3448.

tions. The analysis of law enforcement practices suggests that these provisions are not duly followed.

There is a need to take an inventory of the country's international treaties from the perspective of national information sovereignty. Reinventing the system of international law at the regional regulatory level. In terms of data security, there is a need in strict regulation at the regional level (BRIRC, EAEU, etc.) for all three categories. Speaking at the 11th Petersburg International Legal Forum[3], D.A. Medvedev noted, on the one hand, the importance of international law and its institutions for Russia and, on the other hand, inefficient application of international law.

Giving up the practice of creating traditional institutions of international law and establishing new regional law enforcement centers.

The speaker also stressed the major role of standards across all information segments including for the law enforcement system. Russia boasts the world's first intellectual property standards system. A system of standards to apply information technologies to data security at the national, regional and international levels is critical for future national sovereignty in information.

T.A. Polyakova, Chief Researcher, Acting Head, Information law and international data security department, Institute of State and Law, Russian Academy of Sciences, Doctor of Juridical Sciences, Professor, discussed the vectors of modern legal studies in the area of data security.

As a much wider multidisciplinary concept for both research and regulation, data security is regarded as an institution. With the Russian Federation assuming the responsibility for new constitutional provisions and security of persons, society and state as applied to the use of information technologies and digital data sharing (amended Article 71 of the Constitution)[4], a serious basis for further legal support of data security has emerged. While data security ranks fourth among the strategic priorities of national security[5], the current geopolitical environment is driving it to the forefront.

---

[3] Available at: URL: https://legalforum.info/news/itogi-xi-peterburgskogo-mezhdunarodnogo-juridicheskogo-foruma/ (accessed: 24.01.2023)

[4] Constitution Amendment Law of the Russian Federation No. 1-FKZ «On Improving Regulation of Specific Issues of the Arrangement and Functioning of Public Authorities". 14 March 2020 // Collected Laws of Russia, 2020, No. 11, Article 1416.

[5] Presidential Decree No. 400 "On the National Security Strategy of the Russian Federation". 02 July 2021 // Collected Laws of Russia, 2021, No. 27 (part II), Article 5351.

The priorities for studies in the area of data security include:

specifying the concept of "data";

system of legal principles underlying the national data security;

analysis of current challenges and threats;

international experience of legal support of data security;

conceptual approaches to the development of a system of administrative and legal measures including issues of multinational cooperation;

international data law.

A.V. Morozov, Chair, Computer Law and Data Security, Higher School of Public Administration, Moscow State University, Doctor of Juridical Sciences, Candidate of Technical Sciences, Professor, discussed the issues of developing and introducing new domestic information technologies to ensure data security for Russia.

In his report "The development vectors of the data security institution in the context of digitization", **A.A. Efremov**, Leading Researcher, ILCL, Doctor of Juridical Sciences, Associate Professor, discussed the general regulatory model of data security including its elements such as strategic planning, international and domestic regulation. The strategic planning challenges for data security include multiplicity of documents, development gap between the IT, electronic engineering industry and technological development, a need to take into account the provisions of the new foreign policy vision of the Russian Federation[6].

The international regulation of data security is fraught with issues like protection of sovereignty, regulatory models imposed by unfriendly countries and international organizations (digital neo-colonialism), the data localization dilemma and cyber-space fragmentation or advanced development, export and regulation of domestic technologies, multiplicity of platforms for regulatory development (GEG, OEWG, ITU, SCO, EAEU), future participation of Russia and EAEU partners in the Council of Europe Convention on the protection of personal data, and prospects of standardization in the area of information technologies and data security.

Domestic regulation of data security raises the issues like impact of digital economy on legal regimes applicable to data including development of a legal

[6] Presidential Decree No. 229 "On Approving the Foreign Policy Vision of the Russian Federation" 31 March 2023 // Collected Laws of Russia, 2023, No. 14, Article 2406.

regime for data, transition from papers exchange to data exchange, maintaining data security in removing legal restrictions on data sharing and storage, establishment of a universal trusted digital environment, a need in trust building mechanisms to introduce digital technologies as part of legal regulation.

N.N. Kovaleva, Head, Department of Digital Technology Law and Bio-Law, National Research University–Higher School of Economics, Doctor of Juridical Sciences, Professor, discussed issues of ensuring data security in the metaverse.

The metaverse is a new development stage of the Internet and an enormous market that, on the one hand, is rich with new opportunities for manufacturing, services and entertainment while, on the other hand, is many times more prone to possible attacks, with the risk of known data security threats on the rise along with the emergence of new ones. Children are especially vulnerable among population groups. The metaverse is focused on the use of cryptocurrencies and NFT, only to make it more dependent on hardware. With biometric security built into augmented reality devices, the confidentiality of users comes under a threat.

While the metaverse is primarily about overseas servers and technologies, a Russian metaverse needs to be created. Rich with new opportunities, the metaverse technology can drive economic growth, but data security threats — especially those affecting persons — cannot be resisted without government action. It is necessary to reform the public regulation of these technologies and encourage firms to develop domestic software.

N.V. Putilo, Head, Social Legislation Department, ILCL, Candidate of Juridical Sciences, made a point that the studies of data security in the area of public health should take into account the multiple nature (from the perspective of underlying powers and implementation mechanisms) of the constitutional right of persons to health and presence of data as an element of information environment (thing at law) both in its content and implementation mechanism. At the constitutional level, this element is represented by the right to reliable data on the status of favorable environment (Article 42 of the Constitution), prohibition to collect, store, use and share private information without consent of the person in question (Article 24), and the right to freely search for, receive, transmit, produce and share information by any lawful means (Article 29).

These provisions are specified at the level of sectoral legislation, primarily within of three institutions: public sharing data important for health;

sharing health data in specific information systems set up by the government; digital profile of the patient as a complex of private data available to a limited range of persons as a new sophisticated institution emerging relatively recently.

According to Putilo, public health protection relationships understood as a legal link between "individuals, entities and government in connection with the disease prevention (including the activities to prevent consumption of poor quality products likely to damage public health), health and medication assistance, as well as incidental relationships (for example, donorship, rehabilitation)" may be divided into two segments where data security threats are at their maximum:

organization of health care;

provision of health services.

In the health sector, the integrated public information system incorporating as necessary components a set of subsystems including those responsible for data security (personal data anonymization, data protection subsystems) has become a major tool for introducing digital health services and improving organizational relationships within Russia's health care. The efforts to find more ways to protect all information in the integrated health database should become a major vector of regulation in the three areas:

data confidentiality (to avoid unauthorized access to, copying, provision or sharing);

data integrity (to avoid unauthorized deletion or modification);

data availability (to avoid unauthorized blocking or technical availability problems and to ensure timely access).

Issues in each of the three components will threaten public health that may be damaged through actions (or inaction) by both patients themselves or other parties as a result of shortcomings of information they possess.

In her report "Legal aspects of ensuring children's data security", **N.S. Volkova**, Deputy Head, Social Legislation Department, Acting Academic Secretary in ILCL, Candidate of Juridical Sciences, discussed aspects of protecting minors in the Internet.

As a background to her report, she has cited official statistics whereby 98 percent of Russian minors aged 15-18 will go online on a daily basis, an evidence confirming that children are active actors of the information en-

vironment. The web access is closely related to the ability to receive information and exercise the right to freedom of expression as a prerequisite of other digital rights to be exercised by children (in the digital environment). Moreover, the ever evolving and progressing technologies bring forth new challenges to data security in the Internet. Children's intensive familiarization with the cyberspace, vulnerability and exposure to outside influences and media trends as well as inadequate awareness of various risks in the web can harm their personal development by predetermining destructive behavior patterns in the future. Creating a safe digital environment is thus a core objective of public policies in respect of children and teenagers.

In analyzing the underlying regulatory framework, speaker observed that it is fairly extensive and includes, apart from regulations governing general issues of data sharing and protection, special provisions like Federal Law No. 436-FZ "On Protecting Children from Information Harmful for Their Health and Development" of 29 December 2010 and a number of bylaws. The recent years have witnesses a major reform of this legislation caused by a need to reflect new challenges in the information environment including for protecting rights of minors. One of the legislative trends was a focus on preservation of values typical of the Russian mentality and on ensuring comprehensive security for children. In this regard, a special responsibility should be assumed not only by the authorities and society but also families. It is the family that lays the brickwork of reference values and ensures moral and ethical development of children. It is for this reason that the Children Data Safety Concept updated in 2023 devotes so much attention to the attitudes regarding education, something that, in the speaker's opinion, is not quite in line with the document's purpose and the subject matter of the relations it covers.

Also N.S. Volkova noted that governments have been taking more steps in recent years to protect the physical, ethical, emotional and psychological state of children following interactions in the digital environment. Many states have legalized the concepts of cyber-bullying and cyber-grooming, put into effect the mechanisms to prevent these anti-social phenomena, and introduced tougher sanctions for negative effects on life and health of minors subject to web bullying. Russia has yet no legal definition of bullying and cyber-bullying reported in non-regulatory official documents as anti-social phenomena. It is clear, however, that the right pattern of behavior, readiness and ability to resist unprovoked aggression in social media are necessary communication skills in the cyberspace to become an integral part of education and upbringing. She reiterated the need for close coop-

eration between public authorities and civil society, education institutions and parents to ensure information safety, develop uniform approaches and effective mechanisms for protecting minors in cyberspace.

S.I. Konev, Deputy Dean, Legal Department, Oil and Gas Gubkin State University, has presented a report "Public control/supervision of compliance with the personal data law".

One would be hard pressed to deny a premise of Murphy's law that progress is a substitution of one inconvenience for another. In providing personal data to various information systems (both public and corporate) we gain in time or service quality at the cost of our privacy. Moreover, different forms of threats to personal data safety are ever growing. These may be risks of technical nature resulting from malfunctioning of information systems (through both intentional fraudulent actions and unintentional actions by operators) or uncontrolled personal data sharing (well manifested in respect of interpreted data) etc. The government represented by the relevant regulator cannot but respond to the threats by establishing a set of binding requirements to safe data processing addressed to all operators of personal data regardless of their status. Moreover, the mechanisms for enforcement of control and supervision assume a risk-oriented approach and preventive measures, with the latter to anticipate control. The law provides for the following preventive measures: summarizing enforcement practices, awareness raising, warning notice, consulting, preventing visit. These measures, whatever the essence and meaning of each might be, have a dual effect. On the one hand, the Roskomnadzor reports over the last few years suggest that the number of violations of binding requirements is declining. On the other hand, news portals will regularly report massive leakages of personal data at major operators such as Yandex or Sberbank. Meanwhile, it is noteworthy that the Roskomnadzor has disregarded two forms of preventive action, namely, self-assessment and encouraging fair behavior.

S.I. Konev believes these measures, in view of the dynamics of social relationships in question, to build trust between the regulator and the control subjects by allowing the latter to impact the possible risk category is in line with the risk-oriented approach as a whole. Surely, the fair behavior criteria and self-assessment methodologies will need to be developed. New forms of prevention, streamlining of control/supervision and other measures applied by the government are hoped to minimize violations of binding requirements to personal data processing in the future to guarantee privacy in the cyberspace.

I.V. Bashlakov-Nikolayev, Chair of State and Law, The Presidential Academy (RANEPA), Candidate of Economic Sciences, Senior Lecturer, has congratulated all those present with the anniversary of the ILCL and wished further centenary of fruitful activities. In his presentation "Legal aspects of data and technological security in the process of de-cartelization of the Russian economy" he observed that, according to the social regulator, the Russian economy is teeming with cartels and collusions, only to constrain competition. In addition, there is an issue of de-cartelization.

The speaker noted that the economy of the digital age makes a difference in terms of faster exchange, including that of goods, between businesses, with new contacts and partners easier to find and new transactions faster to consummate. One example is creation in Russia of five websites under the contract system for transactions in the digital form. Meanwhile, digitization of this process has brought about new threats. Did they affect cartelization?

Admittedly, they did. As reported by criminologists and anti-trust bodies, the cyberspace accounts for more than half of all crimes. Approximately 90 percent of cartels were revealed at e-auctions, as a rule at those under the contractual system, with auction participants connected with customers through various means. Here it is possible to manipulate bids and auctions and thus affect the price to be paid by the public budget for goods to be delivered. Moreover, digitization created another vulnerability — characterized by rapid exchange and manipulation of data — related to identification and comparison of bids, and pressures to abandon a bid. In addition, such vulnerabilities use technologies of artificial intelligence and big data.

Meanwhile, digitization is not only about the negative side. In fact, the early cartels which emerged outside the national borders were identifiable only with the help of human sources. Now a "digital" cartel leaves many traces which allow to identify it: for example, a big digital cat developed by the Federal Anti-Monopoly Service have already identified 90 cartels at e-auctions. The crimes of this sort are investigated by identifying digital footprints left by "digital" cartels, location of the message sender, algorithm in use, range of the parties involved, etc. These things, according to the speaker, make it easier to reveal cartels. Further improvements and upgrading of artificial intelligence and big data will facilitate de-cartelization even more. On the other hand, this creates an institutional problem of recognizing as cartels all persons regardless of their impact on competition.

As a matter of conclusion, the speaker underlined that while digitization creates more opportunities for de-cartelization than ever before, there is an institutional issue of how to interpret the definition of cartels.

Yu.V. Truntsevsky, Head, ILCL Department of Anti-Corruption Methodology, Doctor of Juridical Sciences, made a presentation "Information technologies and anti-corruption standards".

The speaker mentioned his involvement in 2000-2010 in a study targeting students in three states: Russia, Kazakhstan and the United States. One question asked as part of the study was how much liberty — including the right to privacy — they would give away for public security. It turned out that students in Russia were almost invariably prepared to sacrifice their rights for the sake of public security. He ventured to propose that if such study were conducted now, it would yield similar results. In addition, the ILCL staff conducted an empiric study of the extent of corruption in respect of digitization in general and data security in particular. The study was focused on the issues related to tax returns since this process embraces multiple data including personal data.

While in some states of the world the institution of tax return may envisage a liability extending to criminal sanctions, Finland, listed among non-corrupted states by the Transparency International, does not require any tax return since the procedure is voluntary. In Russia, the list of those to submit tax returns has become ever longer since 2008, only to require enormous time — up to several days — to complete, with whole offices employed by managers to do the job. However, it has failed to do away with corruption. On the other hand, this process could be automated and with good reason. Recently a software allowing public servants to use public resources to complete tax returns rather than do it themselves was developed jointly with a multifunctional center for public and municipal services. In fact, a person who has to file a tax return receives a pre-completed document that the speaker proposed to call a kind of "vehicle tax". The process is as follows: a person authenticates the document upon making sure the "horsepower" in question is his.

To combat corruption, the society would thus want to collect data on people. This assumes creating a digital profile to underlie tax reporting. The argument that such profile can enable data leakage with negative implications does not hold since our personal data are already available online this way or another. In the course of his report, the speaker gave an example of how he had to send his data via various communication networks, each time at the risk of being picked up and hacked.

In his presentation "Law enforcement constitutionalism as an ideological basis of data security in the context of digitalization", **O.A. Stepanov**, Chief

Researcher, ILCL's Judicial Law Center, Doctor of Juridical Sciences, Professor, discussed a number of aspects related to personal data and digital profiles.

O.A. Stepanov underlined that data security issues are relevant to each of us. An obvious example is leakage of personal data, something that causes fraudulent telephone calls, a trend exponentially on the rise. Moreover, as Yu. Truntsevsky said, there are fears of possible data leakage from the digital profile of an individual as a whole.

Privacy protection issues are normally dealt with at the level of criminal and administrative law. Meanwhile, penalties or sanctions envisaged by the legislation do not avert violations, only to further undermine data security. Once personal data get online, they remain there. One possible solution is to establish the institution of personal digital profile at the constitutional level. In this event, a personal digital profile will be treated as a relatively independent category, with individuals able to apply technological protection measures such as hiding their e-mails, domicile, etc.

In her presentation "Constitutional law substance of personal data security", **E.E. Nikitina**, Senior Researcher, Department of Constitutional Law, ILCL, Candidate of Juridical Sciences, observed that an analysis of all data security documents applicable to an individual rather than state and society reveal that these terms are not compatible by their nature. Overall, the category of personal security is almost never discussed in jurisprudence has failed to develop the relevant concept though it should be treated as and make up a part of constitutional law. The reason is technological: the farther we move online, the more of human rights (to health, education) follow suit, as though to become information rights. There should be a theoretically different approach to personal data security. It is not solely the right to information that makes up the substance of personal data security but equally a number of other constitutional rights available to individuals.

In his report "Requirements to software development process and quality", **V.A. Edlin**, ILCL Postgraduate Student, drew attention to legal issues of software quality. Despite of some requirements to software quality, all of them are related to personal data protection. Meanwhile, software is not something that hangs up in space. These products are currently used in accounts, integrators etc. The relevant examples can include a possibility to register at a service via another service, reciprocal authentication through the use of trusted systems (Yandex, Google etc.), as well as a possibility to receive cookies in accessing a website from a third-party application supposed to track and transmit data on user actions to a third party.

Such close integration is vital for the product itself. Admittedly, the security of such a system is measured by the security of its most vulnerable component. If an element of pass-through authentication is not adequately protected, the whole system may be hacked. This requires to determine a consistent set of requirements to data systems. The software development is currently *on the loose*, with many applications being produced, sometimes to last a day. With time, such applications are supposed to match the quality of the product. Meanwhile, the practice shows that users are not concerned with quality: they want access to the content they need as soon as possible and without much ado.

In this context, regulation cannot be expected to be initiated by the private sector. Therefore, specific areas and requirements to software extending beyond personal data should be identified at the legislative level. The current trends show that there is an understanding that software is not just an outcome of intellectual activities but also a service. Thus, regulations applicable to service quality should presumably apply to the Law "On Protection of Consumer Rights". There are some examples, such as car sharing, when it happens.

In her presentation "Implementation issues of official secrecy regime in the context of digitization", **E.V. Leoshkovich,** Senior Lecturer, Saint Petersburg State University of Aerospace Instrumentation, ILCL Postgraduate Student, drew attention to the fact digitization has brought about a situation when it is no longer possible to identify a list of jobs with an access to information to be kept secret. In light of the discussed vocational standards, while a physician is under obligation to keep medical secrets, the junior staff is not. New jobs like a remote banking specialist are emerging with no obligation to keep banking secrets. He underlined the issues of personal data security should be carefully examined to develop a law on official secrets or impose an obligation on everyone to keep such information confidential.

In her report, **A.V. Kalmykova**, Senior Researcher, Administration Law and Process Department, ILCL, Candidate of Juridical Sciences, discussed issues of regulating critical data infrastructure.

In her presentation "The use of information technologies for legal regulation of culture and education", **E.A. Savchenko,** Researcher, ILCL Social Legislation Department, Candidate of Juridical Sciences, drew attention to the presentation by V.N. Lopatin who said that protecting interests of state and society is a major task of data security, with a safe digital education

environment and protection of traditional cultural and ethical values being among regulatory priorities. Culture as such is part and parcel of Russia's national security strategy[7]. Meanwhile, there is still a problem of public non-awareness of this wealth that requires advertising for social cause. Moreover, the speaker has noted that there is a need to legislatively define the concept of digital culture and digital education environment, as well as the criteria of quality content.

In his report "Security of personal data and their digital footprint", **M.M. Stepanov,** Senior Researcher, Department of Legal Theory and Multidisciplinary Studies, ILCL, Candidate of Juridical Sciences, observed that the protection of the right to privacy is critical for data security. Meanwhile, the regulation of digital footprint is sparse despite a satisfactory regulatory scope of the personal data law. In this regard, in the speaker opinion, it is necessary to regulate the relationships covering personal digital footprint for protection of information on network users and their right to privacy, and for security of such data as a whole.

In his report "Legal issues of personal data collection, processing and protection", **D.A. Basangov,** Senior Researcher, ILCL Laboratory of Legal Monitoring and Sociology of Law, Candidate of Juridical Sciences, discussed the impact of digital technologies on regulation of personal data sharing and details of personal data collection, processing and protection in achieving the public objective to form a personal digital profile. The speaker identified current issues with regard to the consent to processing of personal data, their confidentiality and protection. The problem is that there is no regulatory division between giving and withdrawing consent in respect of a part of personal data. Meanwhile, operators force the user to accept these rules in order to have access to a service. Moreover, it should be borne in mind data processing continues when the subject in question no longer uses the service, only to violate, in the speaker's view, human and civil rights and interests.

The presentation also focused on the issue of collection and processing of publicly available personal data, as well as on the impact of new technologies on personal data processing. As a matter of conclusion, speaker made proposals to have artificial intelligence more responsible for a harm caused by the violation of confidentiality of personal data.

[7] Presidential Decree No. 400 "On the National Security Strategy of the Russian Federation" dated 02 July 2021 // Collected Laws of Russia, 2021, No. 27 (part II), Article 5351.

In her report "Security of personal data in the platform economy", **T.A. Klepikova**, Lecturer, NRU-HSE, Senior Manager, Yandex Taxi, pointed out that technological development and progress have a major impact on relations between individuals, society and state across a variety of areas. IT penetration and a need for data security have affected many areas ranging from public administration to social protection. Moreover, new segments and institutions — like the platform economy — emerge in the digital economy to change the current social brickwork. In Russia, more than 15.5 million people are estimated to have some experience of employment in the platform economy[8]. Meanwhile, even more numerous are those who consume its products and services, only to require to take into account their rights and obligations, with personal data security issues in this area becoming a specific regulatory priority.

Russia's current statutory regulation follows a trajectory of protecting the integrity and sustainability of the national segment of the Internet, providing for universal identification rules, substituting for software/hardware imports, ensuring the digital sovereignty and security of critical data infrastructure. This is suggestive of a narrow and technology-oriented approach to data security.

Personal data security in the context of platform relationships will require a more general and comprehensive approach to include both organizational/technical security measures, guarantees of civil rights and liberties in the Internet, economic and public law aspects. Meanwhile it is not possible to describe the range of legal guarantees available to individuals on platforms for lack of a generally acceptable definition of the platform economy in either law or doctrine. The aspect obviously needs further examination. A complex nature of these relationships calls to apply the provisions of information, civil, administrative, constitutional, tax, labor, mass media legislation and probably some aspects of the law on protection of children from harmful content.

In his presentation "Legal uncertainties of data security in the context of automated binding decision-making in public administration", **N.A. Nazarov**, Senior Specialist, Laboratory of Regulating IT and Data Protection, ILCL, Postgraduate Student, discussed a currently urgent subject not adequately covered by the national doctrine. The sector of public administra-

[8] The Platform Employment in Russia: Scale, Motivation and Barriers to Participation: analytical report. O.V. Sinyavskaya, S.S. Biryukova et al. Moscow, 2022.

tion abounds with examples of automated binding decision-making that range from calculation of benefits, allowances and pensions to crime anticipation. Moreover, at the first glance these technologies exhibit a number of advantages for data security compared to human operator such as: artificial intelligence can avoid social engineering problems; and new systems can be developed to run automatic software tests for known cyber vulnerabilities.

Meanwhile, the use of these systems in their current shape is fraught with multiple potential risks, the first being a possibility to feed misleading information to artificial intelligence through other technologies. For example, one can clone the voice and video image of someone requesting a benefit or subsidy to be transferred to a bank account. Moreover, misleading information can be created in real time using the so-called *deep fake* technology. The second issue is possible leakage of data with serious implications for individuals, society and state. The data used in such systems is not a chaotic dataset but an already processed data array on each specific individual. The third issue is a possibility to manipulate input data. The knowledge of weights allows to manipulate data, that is, provide those documents that are more important for decision-making than others. There is also an issue of *trash* data input for machine learning. Finally, the fourth problem of automated binding decision-making in public administration is that of the impact on output data. Successful computer attacks on the systems themselves can change the whole decision-making process. Presumably, the point of change cannot be identified due to the *black box* specifics of artificial intelligence. As a possible option, speaker proposed to develop requirements to the technical, organizational and legal protection.

L.K. Tereschenko thanked all speakers for interesting reports and fruitful discussions.

The research workshop and discussions were also attended by leading experts in information law: **I. Yu. Bogdanovskaya**, Ordinary Professor, National Research University–Higher School of Economics, Editor-in Chief, *Legal Issues in the Digital Age* Journal, Doctor of Juridical Sciences; **P.P. Kabytov**, Head, Laboratory of legal regulation of information technologies and data security, ILCL, Candidate of Juridical Sciences; **A.A. Tedeev**, Professor, MSU and Shenzhen University, China; **E.K. Volchinskaya**, Chief Specialist, Legal Department, Federal Notary Chamber, Candidate of Economic Sciences; **M.S. Zhuravlev**, Lecturer, Department of Digital Technologies and Biolaw, Researcher, NRU-HSE Institute of Digital Environment Law, Candidate of Juridical Sciences; **V.A. Bozhenova**, Lecturer,

Department of Digital Technologies and Biolaw, NRU-HSE; **A.A. Antopolsky**, Senior Lecturer, Plekhanov Economic University, Candidate of Juridical Sciences; **M.D. Lvova**, Adviser, Alexeevsky Municipal District Administration, Moscow; **R.R. Mazitov**, State and Law Department, Senior Researcher, Far Eastern Institute of Legal Studies under the Ministry of Interior, Khabarovsk City; **I.A. Strakhov**, Head, Alexeevsky Municipal District Administration, and Postgraduate Student, Moscow City Pedagogical University; **A.A. Kashirkina**, Leading Researcher, ILCL Center of International Law and Comparative Legal Studies, Candidate of Juridical Sciences; **O.E. Starodubova**, Research Assistant, Administrative Law and Process Department, ILCL; **V.V. Shtukin**, Senior Researcher, Center for the Study of Territorial Governance and Self-Governance, Academy of Social Governance, Candidate of Juridical Sciences; **A.N. Morozov**, Leading Researcher, Center of International Law and Comparative Legal Studies, ILCL, Candidate of Juridical Sciences; **D.A. Pechegin**, Leading Researcher, Center for Criminal and Criminal Procedure Law and Legal Practice, ILCL, Candidate of Juridical Sciences.

Information about the editors:

L.K. Tereschenko — Doctor of Juridical Sciences, Chief Researcher, Honored Jurist of Russia.

O.E. Starodubova — Research Assistant.

N.A. Nazarov — Senior Specialist, Postgraduate Student.

The paper was submitted to editorial office 30.05.2023; approved after reviewing 11.06.2023; accepted for publication 11.06.2023.

Legal Issues in the **DIGITAL AGE**

AUTHORS GUIDELINES

The submitted articles should be original, not published before in other printed editions. The articles should be topical, contain novelty, have conclusions on research and follow the guidelines given below. If an article has an inappropriate layout, it is returned to the article for fine-tuning. Articles are submitted Word-processed to the address: lawjournal@hse.ru

Article Length
Articles should be between 60,000 and 80,000 characters. The size of reviews and the reviews of foreign legislation should not exceed 20,000 characters.

The text should be in Times New Roman 14 pt, 11 pt for footnotes, 1.5 spaced; numbering of footnotes is consecutive.

Article Title
The title should be concise and informative.

Author Details
The details about the authors include:

- Full name of each author
- Complete name of the organization — affiliation of each author and the complete postal address
- Position, rank, academic degree of each author
- E-mail address of each author

Abstract
The abstract of the size from 150 to 200 words is to be consistent (follow the logic to describe the results of the research), reflect the key features of the article (subject matter, aim, methods and conclusions).

The information contained in the title should not be duplicated in the abstract. Historical references unless they represent the body of the paper as well as the description of the works published before and the facts of common knowledge are not included into the abstract.

Keywords
Please provide keywords from 6 to 10 units. The keywords or phrases are separated with semicolons.

References
The references are arranged as follows: [Smith J., 2015: 65]. See for details http://law-journal.hse.ru.

A reference list should be attached to the article.

Footnotes
The footnotes include legal and jurisprudencial acts and are to be given paginaly.

The articles are peer-reviewed. The authors may study the content of the reviews. If the review is negative, the author is provided with a motivated rejection.

Вопросы права **В ЦИФРОВУЮ ЭПОХУ**

ЕЖЕКВАРТАЛЬНЫЙ НАУЧНО-АНАЛИТИЧЕСКИЙ ЖУРНАЛ

«Вопросы права в цифровую эпоху» — научный ежеквартальный электронный журнал, направленный на всесторонний анализ права в цифровую эпоху. Его главная цель заключается в рассмотрении вопросов, связанных с правовыми последствиями постоянно меняющихся информационных технологий.

Цифровая эпоха — это эпоха информационных и коммуникационных технологий, обусловливающих дальнейшее общественное развитие, в том числе с использованием цифровых данных. Но вместе с тем цифровое развитие выявляет пробелы в праве и потребность в новых правовых решениях.

“Вопросы права в цифровую эпоху” — журнал, который предоставляет возможность юристам — ученым и практикам — обмениваться мнениями. В том числе журнал поощряет междисциплинарные дискуссии по темам, находящимся на стыке права, технологий, экономики и политики в современном мире.

“Вопросы права в цифровую эпоху” — рецензируемый журнал. В нем применяется двойное “слепое” рецензирование присылаемых материалов.

Журнал приглашает авторов присылать статьи, отражающие результаты научных исследований регулирования цифровой среды. Редакция приветствует теоретические и компаративистские подходы, исследование перспектив правового развития в различных странах.

Журнал зарегистрирован Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций и включен в реестр зарегистрированных средств массовой информации серия серия Эл № ФС77-83367

ISSN 2713-2749

Адрес редакции
Россия, 109028 Москва, Б. Трехсвятительский пер, 3,
офис 113
Тел.: +7 (495) 220-99-87
http://law-journal.hse.ru
e-mail: lawjournal@hse.ru

Legal Issues in the **DIGITAL AGE**

Консультативный отдел

Вопросы права
В ЦИФРОВУЮ ЭПОХУ

Учредитель
Национальный исследовательский университет «Высшая школа экономики»

2/2023

ЕЖЕКВАРТАЛЬНЫЙ НАУЧНО-АНАЛИТИЧЕСКИЙ ЖУРНАЛ ТОМ 4

Статьи

Комментарии

Обзор

СТАТЬИ

Научная статья

УДК: 347.1
DOI:10.17323/2713-2749.2023.2.4.25

ЦИФРОВАЯ ВАЛЮТА В СОВРЕМЕННОЙ РОССИИ: ЮРИДИЧЕСКОЕ СОДЕРЖАНИЕ И МЕСТО В ОБОРОТЕ

Александр Иванович Гончаров[1], Андрей Николаевич Садков[2], Виталий Андреевич Садков[3], Давуд Ахмедович Давудов[4]

[1, 2, 4] Волгоградский государственный университет, Россия 400062, Волгоград, Университетский проспект, 100.
[3] Волгоградская академия МВД, Россия 400075, Волгоград, Историческая ул., 130.
[1] goncharov@volsu.ru, GAI-AlexanderGoncharov@yandex.ru.
[2] sadkov@volsu.ru.
[3] wrendek@mail.ru.
[4] davudov@volsu.ru.

Аннотация
Информационное общество нашего времени характеризуется широкомасштабным и интенсивным использованием компьютерных технологий в большинстве сфер экономических отношений. Очень многие процедуры взаимодействия личностей и хозяйствующих субъектов компьютеризированы и оцифрованы. Дистанционные технологии, применяемые в Интернете, позволяют коллективам, в частности, производить математические вычисления и получаемые данные использовать в интересах участников таких коллективных вычислений. Совокупность таких электронных данных в Российской Федерации легитимирована как цифровая валюта. Юридическое содержание и место цифровой валюты в имущественном обороте и системе его государственного регулирования является актуальным объектом научной разработки. В статье на основе исследования отечественного законодательства и научных публикаций обосновывается юридическое содержание цифровой валюты как зашифрованной информации и вида иного имущества; анализируются законодательные конструкции, предусматривающие функционирование цифровой валюты в качестве средства платежа и инвестиций; выявляются качественные признаки цифровой валюты, присущие объекту гражданских прав. Цифровая валюта исследована как совокупность электронных данных и информация, дано авторское определение цифровой валюты. Цифровая валюта в обороте раскрывается как зашифрованная информация, расчетно-обменный эквивалент и инвестиционный актив. Аргументирована ошибочность законодательного признания цифровой валюты средством платежа. Критически оценены правовые кон-

струкции о возможности использования цифровой валюты в качестве инвестиций. Исследованы особенности оборота и развитие нормативного регулирования цифровой валюты в российском правопорядке. Осуществлен правовой анализ парламентского законопроекта о «майнинге» цифровых валют. Обосновывается сущность и формулируется определение деятельности, направленной на получение цифровых валют путем математических вычислений на частных компьютерах. Цифровая валюта рассматривается как разновидность иного имущества, сделан вывод о возможности признания «монеты» цифровой валюты объектом гражданского права. Изучены современные доктринальные разработки преимущественно российских учёных, энциклопедические и нормативные источники. Вносятся предложения о совершенствовании правового регулирования общественных отношений в сфере имущественного оборота цифровой валюты.

Ключевые слова
цифровая валюта; информационные технологии; математические вычисления; информация в электронной форме; Интернет; законодательство; имущественный оборот; иное имущество.

Благодарности: Исследование выполнено во исполнение гранта Российского научного фонда (проект № 23-28-00475).

Статья опубликована в рамках проекта по поддержке публикаций авторов российских образовательных и научных организаций в научных изданиях НИУ ВШЭ.

Для цитирования: Гончаров А.И., Садков А.Н., Садков В.А., Давудов Д.А. Цифровая валюта в современной России: юридическое содержание и место в обороте // *Вопросы права в цифровую эпоху.* 2023. Том 4. № 2. С. 4–25 (на англ. яз.) DOI:10.17323/2713-2749.2023.2.4.25

Информация об авторах:

А.И. Гончаров–доктор юридических наук, доктор экономических наук, профессор.
А.Н. Садков — кандидат юридических наук, доцент.
В.А. Садков — кандидат юридических наук, преподаватель.
Д.А. Давудов — кандидат юридических наук, доцент.

Статья поступила в редакцию 22.02.2023; одобрена после рецензирования 09.03.2023; принята к опубликованию 28.04.2023.

Научная статья

УДК: 336.221
DOI:10.17323/2713-2749.2023.2.26.45

ОСОБЕННОСТИ НАЛОГОВОГО РЕГУЛИРОВАНИЯ ИНДУСТРИИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В РОССИИ И В ГОСУДАРСТВАХ ЕВРОАЗИАТСКОГО ЭКОНОМИЧЕСКОГО СОЮЗА

Мария Александровна Перепелица[1],
Виктория Викторовна Мирончуковская[2]

[1, 2] Елецкий государственный университет имени И.А. Бунина, Россия
399770, Липецкая область, Елец, ул. Коммунаров, 28,
[1] perepelitsa.doc@gmail.com, https://orcid.org/0000-0003-4648-1789
[2] bosfor4878@mail.ru, https://orcid.org/0000-0001-7658-2375

Аннотация
В статье рассмотрены особенности применения Российской Федерацией и странами-участницами Евразийского экономического союза (ЕАЭС) — Беларусью, Казахстаном, Кыргызстаном механизмов налогового стимулирования IT-отрасли. Анализируются налоговые льготы, упрощённая система налогообложения и режим налогообложения на территориях особых экономических зон (ОЭЗ), специальных экономических зон (СЭЗ), парка высоких технологий (ПВТ). Внимание также уделено порядку доступа и аккредитации компаний для работы в ОЭЗ, СЭЗ или ПВТ с применением льготного режима налогообложения. Делается вывод, что государства применяют все механизмы налогового стимулирования: налоговые льготы, упрощённую систему налогообложения, ОЭЗ, СЭЗ, ПВТ, однако по-разному их используют, что влияет на уровень развития отрасли. Россия практикует избирательный и дифференцированный подход, из–за чего большая часть IT-компаний отсекается от льготного режима налогообложения. Страны ЕАЭС выработали в данном вопросе более положительный подход с упрощением регистрационных процедур, необходимых для вхождения отечественных и зарубежных компаний в льготные зоны и допуска в ПВТ и СЭЗ IT-специалистов. Предлагается воспользоваться опытом стран ЕАЭС и при регулировании доступа иностранных компаний из дружественных государств в качестве резидентов на территории ОЭЗ России. Это будет способствовать внедрению новых технологий и обмену опытом с отечественными компаниями. Также обоснован тезис, что для целостного и системного развития отечественной IT-отрасли нецелесообразно дифференцировать компании на Software Company (специализирующиеся на высоких технологиях) и компании, на таких технологиях не специализирующиеся. Обращено внимание на необходимость расширения перечня видов IT-деятельности, открывающих отечественным компаниям доступ к льготному налогообложению. Отмечается, что опыт налогового стимулирования данной отрасли в странах ЕАЭС показывает, что применяемый ими подход позволяет объединить большинство IT-компаний и специалистов–физических лиц на территории отдельной СЭЗ или ПВТ, что выгодно как самим компаниям и физическим лицам из–за льготного налогообложения, так и государству, которое ведёт учет им и производимой ими продукции и открытий. В России IT-компании, если они не входят в ОЭЗ, раздроблены и их труднее в этом смысле контролировать. Сделан вывод, что России целесообразно обеспечить единообразное применение механизмов налогового стимулирования отечественной IT-отрасли на всей территории страны, что будет способствовать её развитию и росту конкурентоспособности на международном рынке.

Ключевые слова
IT-отрасль; IT–компания; налогообложение; налоговые льготы; особые экономические зоны; парк высоких технологий.

Благодарности: работа выполнена в рамках проекта поддержки публикаций авторов российских образовательных и научных организаций в научных изданиях НИУ-ВШЭ.

Для цитирования: Перепелица М.А., Мирончуковская В.В. Особенности налогового регулирования индустрии информационных технологий в России и государствах Евроазиатского экономического союза // *Вопросы права в цифровую эпоху.* 2023. Том 4. № 2. С. 36–45 (на англ. яз.) DOI:10.17323/2713-2749.2023.2.26.45

Информация об авторах:
М.А. Перепелица — доктор юридических наук.
В.В. Мирончуковская –кандидат философских наук.

Статья поступила в редакцию 11.06.2023; одобрена после рецензирования 23.06.2023; принята к опубликованию 23.06.2023.

Научная статья

УДК: 347.1
DOI:10.17323/2713-2749.2023.2.46.77

ПРИОБРЕТЕНИЕ ТАЛАНТОВ И СОГЛАШЕНИЯ О НЕКОНКУРЕНЦИИ: ПРОБЛЕМЫ АНТИМОНОПОЛЬНОГО ЗАКОНОДАТЕЛЬСТВА

Алексей Юрьевич Иванов[1], Ольга Андреевна Николаенко[2]

[1, 2] Национальный исследовательский университет «Высшая школа экономики», Россия, Москва 101000, Мясницкая ул., 20,
[1] aivanov@hse.ru
[2] oagavrilova@hse.ru

Аннотация
В последние годы компании уделяют все больше внимания перспективным идеям и исследователям. В различных фармацевтических отраслях большая часть фирм покупает таланты, но не клиентскую базу и продукцию. Когда компания приобретает контрольный пакет акций небольшой фирмы, ориентированной на исследования и разработки, продавцом часто является ведущий научный сотрудник, и с ним заключаются договоры о неконкуренции, конфиденциальности и другие формы обязательств, которые заставят его работать исключительно на целевую компанию. Приобретения и стратегическое сотрудничество с далеко идущими эффектами «блокировки» страдают от недостаточного применения антимонопольного законодательства, и ни антимонопольные органы США, ни Комиссия Европейского союза, ни антимонопольные органы стран БРИКС не уделяют должного внимания инновационным проблемам, возникающим в связи с этим. Наше предложение, которое, как мы признаем, требует дальнейшего анализа и разработки, заключается в том, чтобы рассматривать исследователей и ключевых специалистов как инновационные активы — и признавать эти активы на рынках сырья или НИОКР, на которых они де-факто работают. Это позволит проанализировать, не захватывают ли крупные корпорации соот-

ветствующие рынки исследований и разработок, создавая мертвые зоны, лишенные инновационных решений.

Ключевые слова
поглощение; таланты; инновационный актив; защита конкуренции; антимонопольное правоприменение; исследования и разработки; соглашение о неконкуренции.

Для цитирования: Иванов А.Ю., Николаенко О.А. Приобретение талантов и соглашения о неконкуренции: проблемы антимонопольного законодательства // *Вопросы права в цифровую эпоху.* 2023. Том 4. № 2. С. 46–77 (на англ. яз.) DOI:10.17323/2713-2749.2023.2.46.77

Информация об авторах:
А.Ю. Иванов — кандидат юридических наук, директор.
О.А. Николаенко – кандидат юридических наук, научный сотрудник.

Статья поступила в редакцию 22.03.2023; одобрена после рецензирования 28.04.2023; принята к опубликованию 18.05.2023.

Научная статья

УДК: 347.1
DOI:10.17323/2713-2749.2023.2.78.121

БАЛАНС МЕЖДУ КИБЕРБЕЗОПАСНОСТЬЮ И КОНФИДЕНЦИАЛЬНОСТЬЮ: ПРАВОВЫЕ И ЭТИЧЕСКИЕ ВЗГЛЯДЫ В ЦИФРОВУЮ ЭПОХУ

Н. Аллахракха

Узбекистан, Ташкент 100047, Ташкентский государственный юридический университет,
Chaudharynaeem133@gmail.com, 0000-0003-3001-1571

Аннотация
В современном цифровом мире особую актуальность приобретают вопросы кибербезопасности и защиты конфиденциальной информации. Однако не менее важно соблюдать и другое неотъемлемое право человека — право на неприкосновенность частной жизни. Вниманию читателя предлагается анализ правовых и этических вопросов соблюдения баланса между кибербезопасностью и неприкосновенностью частной жизни в цифровую эпоху. В статье рассматриваются трудности, возникающие в ходе организации системы кибербезопасности при одновременном соблюдении права на тайну частной жизни; обсуждается нормативно-правовая база кибербезопасности и тайны частной жизни в разных юрисдикциях. Автор также анализирует возможные этические последствия балансирования между названными ценностями и предлагает пути к нахождению компромисса между ними в общих случаях. Подчёркивая важность тщательного соблюдения баланса между кибербезопасностью и тайной частной жизни, автор стремится привлечь внимание к теме важности этических и юридических аспектов развития и правового регулирования цифровых технологий.

Ключевые слова
кибербезопасность; тайна частной жизни; цифровая эпоха; правовые соображения; этические соображения.

Для цитирования: Аллахракха Н. Баланс между кибербезопасностью и конфиденциальностью: правовые и этические взгляды в цифровую эпоху // *Вопросы права в цифровую эпох*у. 2023. Том 4. № 2. С. 78–121 (на англ. яз.) DOI:10.17323/2713-2749.2023.2.78.121

Информация об авторе:
Н. Аллахракха — кандидат юридических наук, преподаватель.

Статья поступила в редакцию 21.02.2023; одобрена после рецензирования 09.03.2023; принята к опубликованию 28.04.2023.

Научная статья

УДК: 342
DOI:10.17323/2713-2749.2023.2.122.141

ДЕТИ В ИНТЕРНЕТЕ: ВИДЫ КИБЕРУГРОЗ И ПРАВОВЫЕ СПОСОБЫ ЗАЩИТЫ ОТ НИХ

Рина Венеровна Хисамова

Национальный исследовательский Московский государственный строительный университет, Россия, Москва 129337, Ярославское шоссе, 26,
rina_khisamova@ list.ru

Аннотация
Цифровая трансформация современной действительности, затрагивая практически все сферы жизнедеятельности человека, не обходит стороной и детей. В настоящей статье автор исследует риски цифровизации, возникающие в отношении детей, выделяя основные виды интернет-угроз, опасные развитию ребенка, и доступные на сегодня правовые способы защиты от них. Исследование начинается со специфики правосубъектности ребенка, которую подчеркивают вехи исторического пути признания ребенка самостоятельным субъектом права и выявления особенностей присущего ему правового статуса. В частности, в качестве ключевой особенности правового статуса ребенка выделяется принцип его «развивающихся способностей», который предполагает постепенное, релевантное взрослению ребенка расширение его юридических возможностей. Отмечается, что данный принцип, воспринятый другими отраслями права, должен быть имплементирован и в нормы информационного права, поскольку интернет-пространство оказывает на развитие детей колоссальное воздействие, что не может оставаться вне сферы внимания законодателя и за рамками правового регулирования. Используя общие и специальные научные методы, включая метод формальной логики и метод сравнительного анализа, автор приводит краткий обзор нынешних государственных, общественных и частых способов защиты прав детей в Интернете, отмечая, что наиболее действенным является гармоничнее сочетание всех имеющихся способов.

В целях действенности механизма защиты прав детей в Интернете предлагается принимать во внимание специфику правового статуса ребенка, которая заключается в постепенном расширении его правовой свободы и предоставлении правомочий для самостоятельного осуществления прав в цифровой среде, и стремиться к балансу публичного и частного начал при защите детей в условиях развития информационно-коммуникационных технологий.

Ключевые слова
цифровизация; права детей; Интернет; защита; киберугрозы; информационное общество; контент-риск; контактный риск; цифровая самозащита; общество знаний.

Для цитирования: Хисамова Р.В. Дети в Интернете: виды киберугроз и правовые способы защиты от них // *Вопросы права в цифровую эпоху.* 2023. Том 4. № 2. С. 122–141 (на англ. яз.) DOI:10.17323/2713-2749.2023.2.122.141

Информация об авторе:
Р.В. Хисамова — специалист.

Статья поступила в редакцию 03.04.2023; одобрена после рецензирования 18.05.2023; принята к опубликованию 18.05.2023.

КОММЕНТАРИИИ

Обзор

УДК: 347
DOI:10.17323/2713-2749.2023.2.142.157

ОБЗОР КЛЮЧЕВЫХ ПОЗИЦИЙ ПРЕЗИДИУМА СУДА ПО ИНТЕЛЛЕКТУАЛЬНЫМ ПРАВАМ

Мария Александровна Кольздорф[1], Наталья Игоревна Капырина[2]

[1] Суд по интеллектуальным правам, Россия, Москва 127254, Огородный проезд, 5/2
[2] МГИМО (У) МИД России, Россия, Москва 119454, проспект Вернадского, 76
[1] mkolzdorf@hse.ru, ORCID: 0000-0003-3227-3348, Researcher ID: AAI-1625-2019,
[2] n.kapyrina@my,mgimo .ru, ORCID: 0000-0003-1276-1600, Researcher ID: AAQ-3784-2021

Аннотация
В обзоре приведены ключевые позиции из постановлений Президиума Суда по интеллектуальным правам, принятых с июля по сентябрь 2022 года. Президиум Суда по интеллектуальным правам рассматривает кассационные жалобы на решения суда первой инстанции, в частности, по делам, связанным с регистрацией объектов интеллектуальных прав и с оспариванием правовой охраны. Соответственно данный Обзор преимущественно по-

священ вопросам охраноспособности объектов патентных прав и средств индивидуализации, а также отдельным процессуальным аспектам деятельности Роспатента и Суда по интеллектуальным правам. В новом Обзоре рассмотрены различные вопросы, связанные с товарными знаками, а также с патентами и различные процессуальные вопросы.

Ключевые слова
банкротство; товарные знаки; НМПТ; Парижская конвенция; описательное обозначение; продление патента; новизна; оригинальность; промышленный образец; соправообладание товарным знаком; прекращение охраны; оценка доказательств.

Для цитирования: Капырина Н.И., Кольздорф М.А. Обзор ключевых позиций Президиума Суда по интеллектуальным правам // Вопросы права в цифровую эпоху. 2023. Том 4. № 2. С. 142–157 (на англ. яз.). DOI:10.17323/2713-2749.2023.2.142.157

Информация об авторах:
М.А. Кольздорф — заместитель начальника Отдела обобщения судебной практики и статистики, магистр, старший преподаватель.
Н.И. Капырина — кандидат юридических наук, доцент.

Вклад авторов:
М.А. Кольздорф — части 1, 6, 8.
Н.И. Капырина — части 2, 3, 4, 5, 7, 9, 10.

Статья поступила в редакцию 11.06.2023; одобрена после рецензирования 23.06.2023; принята к публикации 23.06.2023.

ОБЗОР

Обзор

УДК: 342
DOI:10.17323/2713-2749.2023.2.158.175

СОВРЕМЕННЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ (ОБЗОР НАУЧНО-ПРАКТИЧЕСКОГО СЕМИНАРА)

Людмила Константиновна Терещенко[1], Олеся Евгеньевна Стародубова[2], Никита Алексеевич Назаров[3]

[1, 2, 3] Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации, Россия, Москва 117218, Большая Черемушкинская ул., 34,
[1] Adm2@izak.ru
[2] olesyastarodubova@gmail.com
[3] naznikitaal@gmail.com

Аннотация
В статье содержится обзор научно–практического семинара «Современные информационные технологии и информационная безопасность», состоявшегося 23 мая 2023 г. в Институте законодательства и сравнительного правоведения при Правительстве Российской Федерации. Приведены ключевые тезисы докладов участников семинара — исследователей из Института законодательства и сравнительного правоведения, Московского государственного юридического университета им. О.Е. Кутафина, Национального исследовательского университета «Высшая школа экономики», Московского государственного университета им. М.В. Ломоносова, Российского экономического университета им. Г.В. Плеханова, Московского городского педагогического университета и др. В обзоре освещены насущные правовые проблемы в том числе: понятие и содержание информационной безопасности в современных условиях; векторы развития института информационной безопасности в условиях цифровизации; границы суверенитета в информационной сфере; международно-правовые регуляторы информационной безопасности; механизмы устойчивого обеспечения безопасности в условиях новых вызовов и угроз; влияние новейших информационных технологий, таких как искусственный интеллект, большие данные, машиночитаемое право на информационную безопасность; информационная безопасность личности; государственный контроль и ответственность за правонарушения в информационной сфере.

Ключевые слова
информационная безопасность; метавселенная; цифровой аватар; персональные данные; биометрические персональные данные; сквозные цифровые технологии; большие данные; искусственный интеллект; информационный суверенитет; технологический суверенитет.

Для цитирования: Терещенко Л.К., Стародубова О.Е., Назаров Н.А. Современные информационные технологии и информационная безопасность (Обзор научно-практического семинара) // *Вопросы права в цифровую эпоху.* 2023. Том 4. № 2. С. 158–175 (на англ. яз.) DOI:10.17323/2713-2749.2023.2.158.175

Информация о составителях:
Л.К. Терещенко — доктор юридических наук, главный научный сотрудник, заслуженный юрист Российской Федерации.
О.Е. Стародубова — ассистент.
Н.А. Назаров — старший специалист, аспирант.

Статья поступила в редакцию 30.05.2023; одобрена после рецензирования 11.06.2023; принята к опубликованию 11.06.2023.

АВТОРАМ

Требования к оформлению текста статей

Представленные статьи должны быть оригинальными, не опубликованными ранее в других печатных изданиях. Статьи должны быть актуальными, обладать новизной, содержать выводы исследования, а также соответствовать указанным ниже правилам оформления. В случае ненадлежащего оформления статьи она направляется автору на доработку.

Статья представляется в электронном виде в формате Microsoft Word по адресу: lawjournal@hse.ru
Адрес редакции: 109028, Москва, Б. Трехсвятительский пер, 3, оф. 113
Рукописи не возвращаются.

Объем статьи
Объем статей до 1,5 усл. п.л., рецензий — до 0,5 усл. п.л.

При наборе текста необходимо использовать шрифт «Times New Roman». Размер шрифта для основного текста статей — 14, сносок — 11; нумерация сносок сплошная, постраничная. Текст печатается через 1,5 интервала.

Название статьи
Название статьи приводится на русском и английском языке. Заглавие должно быть кратким и информативным.

Сведения об авторах
Сведения об авторах приводятся на русском и английском языках:

- фамилия, имя, отчество всех авторов полностью
- полное название организации — места работы каждого автора в именительном падеже, ее полный почтовый адрес.
- должность, звание, ученая степень каждого автора
- адрес электронной почты для каждого автора

Аннотация
Аннотация предоставляется на русском и английском языках объемом 250–300 слов.
Аннотация к статье должна быть логичной (следовать логике описания результатов в статье), отражать основное содержание (предмет, цель, методологию, выводы исследования).

Сведения, содержащиеся в заглавии статьи, не должны повторяться в тексте аннотации. Следует избегать лишних вводных фраз (например, «автор статьи рассматривает…»).

Исторические справки, если они не составляют основное содержание документа, описание ранее опубликованных работ и общеизвестные положения, в аннотации не приводятся.

Ключевые слова
Ключевые слова приводятся на русском и английском языках. Необходимое количество ключевых слов (словосочетаний) — 6–10. Ключевые слова или словосочетания отделяются друг от друга точкой с запятой.

Сноски
Сноски постраничные.
Сноски оформляются согласно ГОСТ Р 7.0.5-2008 «Система стандартов по информации, библиотечному и издательскому делу. Библиографическая ссылка. Общие требования и правила составления», утвержденному Федеральным агентством по техническому регулированию и метрологии. Подробная информация на сайте http://law-journal.hse.ru.

Тематическая рубрика
Обязательно — код международной клас-сификации УДК.

Список литературы
В конце статьи приводится список литературы. Список следует оформлять по ГОСТ 7.0.5-2008.

Статьи рецензируются. Авторам предоставляется возможность ознакомиться с содержанием рецензий. При отрицательном отзыве рецензента автору предоставляется мотивированный отказ в опубликовании материала.

Плата с аспирантов за публикацию рукописей не взимается.

Выпускающий редактор *Р.С. Рааб*
Художник *А.М. Павлов*
Компьютерная верстка *Н.Е. Пузанова*