ISSN 2713-2749

Legal Issues in the DIGITAL AGE

Вопросы права в цифровую эпоху

1/2020

Legal Issues in the **DIGITAL AGE**

Вопросы права в цифровую эпоху

1/2020

ISSUED QUARTERLY

Articles

Comment

Publisher
National Research
University Higher School
of Economics

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

Cryptocurrency in Russian law: Surrogates, "Other Assets" and Digital Currency

Roman Yankovsky

Associate professor, Law Faculty, National Research University Higher School of Economics, Candidate of Juridical Sciences. Address: 20 Myasnitskaya Str., Moscow 101000, Russian Federation. E-mail: ryankovskiy@hse.ru

Abstract

For the last five years there has been a global boom of interest in cryptocurrencies, followed by the fall of their rates; at the same time, there was a wave of enthusiasm regarding the public offering of tokens (ICO) and disillusionment in them (due partly to the active counteraction by American and other influential regulators). Disputes on doctrine moved from suggestions of a new object of property rights to prohibitive initiatives. As these eventful years have shown, the global financial system is sufficiently stable to digest even such a decentralized phenomenon as cryptocurrency. In my opinion, it is now time to recall the tribulations of former discussions and draw a conclusion concerning their interim (one hopes) normative results.

Keywords

cryptocurrencies, money, digital currencies, virtual currencies, virtual assets, virtual assets, financial surrogates

For citation: Yankovsky R.M. (2020) Cryptocurrency in Russian Law: surrogates, "other assets" and digital currency. *Legal Issues in the Digital Era,* no 1, pp. 3–31.

Prerequisites for Regulation in Russia

From the very beginning it must be stipulated that the present article shall examine cryptocurrencies in their "classical" meaning — units of payment, possessing an exclusively settlement function and not authenticating any additional rights of demand toward the emitter. Recent years have seen the emergence of numerous forms of cryptocurrencies of various kinds: stablecoins, national cryptocurrencies, etc. The present article deals only with "classical" cryptocurrencies such as the widespread Bitcoin and Ethereum.

Initially, discussions concerning the legal regime for cryptocurrencies in Russia centered around the private and public law aspects. Within the sphere of private law, there were questions about the legal nature of cryptocurrencies: the character of rights to cryptocurrency, its place in the system of property rights, the qualification of cryptocurrency transactions and their validity, as well as possible means of legal protection of rights to cryptocurrency. Alongside this discussion (partially on the basis of arguments emerging in it) amendments were introduced into the Civil Code in 2019, including a clause on "digital rights"[1].

The polemics around public law concerned, first and foremost, observance of the anti money-laundering recommendations of the Financial Action Task Force (FATF) concerning cryptocurrencies (including the procedure and criteria for monitoring transactions involving cryptocurrencies), the correlation between cryptocurrencies and financial surrogates, permitted and proscribed operations with cryptocurrencies and potential sanctions regarding their performance. Prospectively, this discussion should result in the regulation of cryptocurrencies with a separate law "On digital financial assets"[2].

These questions are interlinked but were discussed within the context of various branches of the law by various public bodies and such discussions bore different results. For this reason, the present article shall examine both groups of questions consecutively: firstly, the private law issues, then — questions of "convergence" *inter alia* the legal qualification of transactions with surrogates, and then the purely public law issues.

1. Cryptocurrency in Private Law. Qualification of Cryptocurrencies

1.1. Qualification of "Intangible Goods" in Russian Law

In the field of private law, lawyers faced the impossibility of qualifying cryptocurrencies as an object of property rights. The point at issue is that

[1] Federal Law dated 18.03.2019 № 34-FZ "Amending parts 1—2, second clause of Article 1124 of the Civil Code of the Russian Federation."

[2] Draft Law № 419059-7 "On digital financial assets." Available at: URL: https://sozd.duma.gov.ru/bill/419059-7 (accessed: 12.07.2020). There was a subsequent suggestion to extrapolate regulation of cryptocurrencies into a separate law "On digital currency." This initiative is under discussion.

right for cryptocurrency has an obvious absolute character. Rights of that kind are typical for exclusive rights, personal non-property rights and property rights, and are not typical of contractual rights. Exclusive rights and personal non-property rights do not coincide with the economic content of cryptocurrency. It would appear reasonable to extend the regime of property rights to cryptocurrency — however the possibility of property rights to intangible objects does not correspond to the Continental legal doctrine that only acknowledges material objects of property (*rem,* things). The concept of the materiality of an object of property rights is reflected in German law[3], and later in the doctrines of many European countries, including Russia. [Scriabin S.V., 2004: 34]. This evoked recurrent difficulties with new objects of absolute rights: intellectual property, or, in recent history, uncertificated securities or electric power. Difficulties arose and continue to exist in qualifying virtual objects — for example, virtual gold and items gold and in online games, domain names, etc[4].

Moneys in cash, having a material form in Roman law and the subsequent Continental legal doctrine, have always been accepted as moveable generic divisible and unusable goods. Certain problems arose in qualifying cashless (bank) money: unlike cash money, such moneys are not deemed to be objects of property rights, they are determined as objects of contractual rights (of contract between bank and account holder) [Lunts L.A., 2004 (1927): 20]. This point of view was supported by doctrine and despite objections [Efimova L.G., 2001: 204–234], was established in the formulations of the Civil Code. *Inter alia* Article 128, determining the objects of title, divides cash money belonging to an owner on grounds of property rights to cashless money to which one has property rights of demand: ""Objects of civil rights" mean things, including, inter alia, money in cash and paper securities, other assets, for instance money in a cashless form, paperless securities…)[5]. An identical regime concerning cashless money was established in Germany, France, Great Britain [Sazhenov A.V., 2018b: 115].

The regulation of so-called "electronic money" (e-money) did not influence the qualification of cashless money in that "electronic money" only

[3] Materiality of things is established in §90 Bürgerliches Gesetzbuch. In Russian legislation there is no such requirement, but it is common in legal doctrine.

[4] Rozhkova M.A.On property rights to non-material objects in the system of absolute rights. 2020. Available at: URL: https://zakon.ru/rozhkova-ma/blogs (accessed: 30.05.2020)

[5] Art. 128 of the Civil Code.

fixes a certain balance of the rights of the participants in the payment system, but does not constitute a separate element of property rights. As the law "On the national payment system" stated, electronic money are one and the same financial monetary means that are moved within the framework of the form of cashless settlements accepted by the participants[6]. Thus, Russian legislation attributes "electronic money" to contractual rights, that may be directed towards not just banks, but also other participants in the system of cashless settlement.

1.2. Cryptocurrency as an Object of Rights *Sui Generis*

Thus, in the existing system of objects of civil rights, money is regarded as either material object (cash money) or as the right of demand to banks or other participants of the financial system (cashless money, "electronic money"). However, cryptocurrency in pure form does not fit in with either of these concepts. As I have already said, the nature of rights to cryptocurrency clearly tends toward the absolute, rather than the relative. Scholars have repeatedly tried to explain relative (contractual) nature of rights to cryptocurrency[7]. However, the attempt to find an obligated party within the blockchain only lead to further discrepancies. For example, some scholars endow the holders of cryptocurrency with rights of demand against the owners of blockchain nodes — you might as well say that when you buy a car, you are endowed with the rights of demand regarding all petrol stations.

In my view, cryptocurrency is an absolute right of a particular kind (*sui generis*). This position is sufficiently widely held [Tolkachev A.Yu., Zhuzhzhalov M.B., 2018: 114–116]; [Efimova L.G., 2019: 17–25]. Yet acknowledgement of the absolute nature of rights to cryptocurrency require a direct indication in law by virtue of the principle of *numerus clausus* — the list of absolute rights must be exhaustive and established in the law. Therefore, the regulation of rights to cryptocurrency as an absolute right, needs the establishment of the new object of civil rights — similar to that of uncertified securities. Of course, the introduction of such substantial amendments to legislation requires lengthy discussion — due to this, no decision satisfying

[6] Art. 3 of Federal Law dated 27.06.2011 № 161-FZ "On the national payment system".

[7] Uspensky M. Legitimate bitcoin. Available at: URL: https://zakon.ru/blog/2017/12/13/legitimnyj_bitkoin (accessed: 30.05.2020). See also: [Novoselova L.O. 2017: 11].

all parties has been formed to date. Lacking a concrete civil law regulation, in practice Russian courts find various reasons to evade not just qualifying cryptocurrency, but also to evade protecting rights to it.

Thus in 2017 a court in the Tyumen district[8] did not support the seller of bitcoins in a dispute versus an internet exchange: the court ruled that the interest of the claimant is not subject to court support since the subject of the transaction did not conform to the determination of electronic monetary means, is not a foreign currency and is not named in the Civil Code. As a result, the court decided that "all operations with the transfer of bitcoins are conducted by their holders at their own risk" and dismissed the case.

Such a qualifications can be explained only by the court's reluctance to rule on the matter in substance. The list of objects of rights established in Article 128 of the Civil Code is not closed; the lack of some object in it does not mean that rights to that object are not subject to judicial protection. The principle of *numerus clausus* does not allow the court to determine a new object of civil rights, but the formulation of Article 128 leaves a loophole: the court can relate to cryptocurrency as a "assets", not specifying its legal nature. This has become the mainstream policy in qualifying cryptocurrency among Russian courts for the next few years.

1.3. Cryptocurrency as an Asset

The collective category of "assets" in Russian law, although often limited to property [Sukhanov E.A., 2017: 44], comprises a wide list of rights, including both property rights and contractual rights. The category of assets is applied to different types of "masses": the bankruptcy estate ("the entire assets of the debtor"[9]), mass of the succession ("things, other assets, including property rights and obligations"[10]), marital assets of spouses ("assets acquired by spouses during marriage"[11]) et al. Disclosing the enterprise as an asset complex, the legislator includes ("blocks of land, buildings. constructions, equipment, fittings, raw materials, products, rights of demand, debts[12]).

[8] Ruling of the Ryazhsky regional court, Ryazan district, 26.04.2017 on case № 2-160/2017 (M-129/2017).

[9] Art. 131 of Federal Law of 26.10.2002 № 127-FZ "On insolvency (bankruptcy)"

[10] Art. 1112 of Civil Code.

[11] Art. 34 of Family Code.

[12] Art. 132 of Civil Code.

I repeat that the qualification of any substance as "asset" does not elucidate its legal nature, as "asset" is a collective concept. Therefore, qualifying cryptocurrency as "asset" does not help to establish its legal nature but does allow legally commercialize it. Strictly speaking, this is already sufficient for the protection of rights to cryptocurrency in contractual and tort disputes (by virtue of the principle of general rights protection established by Article 1064 of Civil Code) [Fedorov D.V., 2018: 54].

In this respect, the "Tsarkov Case" is indicative, in which the court examined the question of inclusion of cryptocurrency of a bankrupt (Tsarkov I.I.) into his assets for distribution. As I have mentioned above, the law clearly indicates the inclusion of such a mass — "the entire assets of the debtor" — with the exception of licenses and objects excluded by law (cryptocurrency is not that kind). Therefore, pursuant to the direct order of the law, the insolvency administrator is obligated to include the cryptocurrency to the assets for distribution.

The below court supported the bankrupt, having established that Tsarkov is under no obligation to transfer bitcoins. However the Appeals Court cancelled that decision and granted the claim of the insolvency administrator[13]. This decision was based on the following grounds:

In general, norms of Civil Code are discretionary, and therefore the list of objects of civil rights in Article 128 of Civil Code is non-exhaustive[14];

Although Civil Code does not disclose the concept of "other assets", allowing for contemporary realities and levels of technology this concept may be interpreted with maximum scope, *inter alia,* by including cryptocurrency in the composition of property;

Under the Law "On insolvency (bankruptcy)", any property of the bankrupt that is of economic value to creditors, may not be excluded from distribution;

The debtor's ownership of cryptocurrency may be proven by scrutinizing web pages and also by the circumstance that the debtor has access to his wallet.

[13] Resolution of Arbitration court of Appeal № 9 dated 15.05.2018 on case № A40-124668/2017.

[14] One may argue with the court about this: is the principle of disparity established by art. 1 CC ("citizens…are free to establish their rights and obligations on the basis of the contract…") applicable to the list of objects of civil rights?

Consequently, despite the fact that courts in the "Tsarkov Case" did not consider comprehensively the legal nature of cryptocurrency, a conceptually correct approach was formulated: cryptocurrency may be an object of property rights even without a stipulation of such in the law.

1.4. Do Cryptocurrency Relations Belong to the Field of Law?

Determination of the nature of the right to cryptocurrency is complicated by the technological specifics of the blockchain. The ability of the participant to enter information into the block — *inter alia,* to perform all cryptocurrency transactions — is determined by access to a specific address, Such access, irrespective of its form (login and password, certificate of electronic signature, etc.) is certain information held by the participant of the blockchain. Without this information, i.e. without access, it is impossible to perform actions within the blockchain. As neither the court nor the creditor can obtain the information required for access, it becomes impossible to encroach on the cryptocurrency without the consent of its owner. The same limitation complicates legal defence: it is impossible to enforce the fulfilment of a contract with transfer of cryptocurrency.

This raises the question of the nature of relations of cryptocurrency ownership. As doctrine says, in absolute legal relations — including property relations — the owner is confronted by an indefinite circle of obligated subjects. Can it be said that the participants of a blockchain are obligated to the "owner" of cryptocurrency — as after all, they are physically unable to hinder its "owner"? If the answer is "no, they are not obligated", the possibility of a very absolute right to cryptocurrency can be questioned. If it is accepted that "ownership means a factual relationship to an object that has no limits apart from coercion by third parties wishing to encroach on that object" [Sklovsky K.I., Kostko V.S., 2018: 131], ownership of cryptocurrency cannot be acknowledged as ownership: as enforced encroachment on cryptocurrency is impossible. In such a situation, we shall have to speak about relations within the blockchain not as a legal relations but of factual relations of some form — possibly a new type of social relations regarding which law is inapplicable [Savelyev A.I., 2016: 54]. This corresponds with the position of some German specialists in civil law who regard cryptocurrency transactions not as a legal relationship, but a certain "real act" [Fedorov D.V., 2018: 30].

It is possible to dispute this viewpoint. Encroachment on an object can occur in ways other than physical enforcement — it may be accomplished as a result of a faulty expression of will by the owner (deceit, threats, etc.) There are objects of property law the ownership of which also does not presume the possibilities of encroachment by third parties (for example, spacecrafts[15]). There are also objects of absolute rights *sui generis* (for example, the intellectual property), infringement of which has its own specifics.

The described particularities of blockchain technology also do not enable owners do defend their rights. For example, it is technically impossible to enforce a demand for it in either judicial or extrajudicial order[16]. Does such a limitation affect the substance of an obligation involving cryptocurrency?

In fact, the right to protection was considered an intrinsic element of an obligation for a long time; this viewpoint has changed only in contemporary literature under the influence of the theory of protective legal relations [Mertvishchev A.V., 2012: 12], pursuant to which even moral obligations, lacking protection, are considered as judicial relations. Contrary to moral obligations, obligations relating to cryptocurrency are not denied judicial protection in whole; such protection is simply hampered by the pseudonymity of abundant blockchains and the impossibility of performing a transaction without the consent of the debtor (these two factors should be distinguished from one another).

Nevertheless, cryptocurrencies are not a unique occurrence of an object of obligation that affects the application of means of judicial protection. Thus, it's impossible to force performance concerning personal obligations of the debtor (for example, an obligation to perform a musical composi-

[15] Regarding spacecraft, the doctrine acknowledges the regime on real estate even though this is not affirmed by legislation. Reference to spacecraft as objects were made in currently invalid laws "On pledge" (p.1 Art. 35) and "On state registration of real estate and transactions with it" (Art. 4). The law "On state registration of rights to spacecrafts" has been under discussion for several years but has not been submitted to the State Duma at this time.

[16] A.I. Savelyev [Saveliev A.I., 2018: 36—52] states that as the inapplicability of vindication claims against cryptocurrency does not allow considering rights to it as strictly absolute. It would appear that the error in this reasoning lies in that not all absolute rights are protected by a vindication claim. Moreover, it is inarguable that absolute and property right represent, as A.A. Ivanov puts it, "shades of grey" (A.A. Ivanov. Many shades of grey; absolute and relative rights (digital practice and a little bit of theory. Available at: URL: https://zakon.ru/blog/2018/08/31/mnogo_ottenkov_serogo_absolyutnye_i_otnositelnye_pravacifrovaya_praktika_i_nemnogo_teorii (accessed: 30.05.2020). These "shades" are determined, *inter alia,* in the application of proprietary-legal means of protection.

tion) [Gromov A.A., 2018: 10—15]. In Russian law it is not possible to force company stockholders to vote in a specific way, even if such an obligation is established by a shareholders agreement. In such and other cases the object of an obligation influences the possibility of the application of one or another means of judicial protection but does not abolish the obligation at whole. In the matter of cryptocurrency, interests that cannot be protected through enforcement of the performance of a contract, may be protected by payment of compensation for losses in monetary form. Protection from theft of cryptocurrencies shall be either of tort nature (a claim for inflicting damage to property), or of a conditional nature (*indebitatus assumpsit*) [Savelyev A.I., 2017: 149]; [Sazhenov A.V., 2018b: 117–118].

1.5. Judicial Protection of Rights to Cryptocurrency

In practice, difficulties in protection of rights to cryptocurrency arise most often due to their pseudonymity, and not the impossibility of performance against the will of the debtor. One of the first cases to be examined regarding protection for a transaction with cryptocurrencies was examined by the Arbitration Court of the Khabarovsk Territory in 2016[17]. With no adequate comprehension of the technical side of the matter, the court demanded that the claimant provide evidence regarding the transfer of cryptocurrencies to Russian jurisdiction, and without receiving that, dismissed the claim. In the opinion of the court, the lack of evidence regarding the appearance of cryptocurrency in Russian jurisdiction meant the impossibility of its use in a transaction, the performance of which the claimant attempted to prove, — a transaction aimed at the exchange of real estate for cryptocurrency.

In the "Totem" case the court also demanded evidence regarding the transfer of cryptocurrency to the claimants from the respondent[18]. The claimants asserted that they sent him 600 thousand roubles to acquire "Totem" cryptocurrency, after which he refused to respond to them. The respondent asserted that he had opened accounts for the claimants on the "Totem" website, as was agreed, and transferred cryptocurrency to these accounts. The below court ruled in favour of the claimants, but the court

[17] See: court acts on cases № A73-7423/2015 and № A73-6112/2015. Subsequently, the matter went as far as the Supreme Court, and at all levels the decision of the regional court was upheld

[18] Decision, Leninsky regional court, city of Ulyanovsk, 13.04.2018 on case № 1444/2018; appeal ruling of the Ulyanovsk regional court, 31.07.2018 on case № 33-3142/2018.

of appeal reversed that ruling. In fact, the dispute was reduced to the issue whether it was feasible to accept the balance of an anonymous internet wallet as affirmation of the transfer of cryptocurrency and which party has the burden of proof on. The appeals level placed the burden of proof on the claimants, and the respondent won the case.

In a similar case in the Tyumen Region, the question also hinged on the confirmation of a transfer of cryptocurrencies between the parties[19]. According to the materials of the case, the claimant transferred means to the credit card of the respondent, expecting a consideration (cryptocurrency). However, this did not occur, and he filed a *indebitatus assumpsit* claim. As evidence, the respondent provided the results of a notarial examination of the account on the platform of private exchange of cryptocurrencies, but the court did not deem this to be sufficient proof of the exchange of cryptocurrency. As a result, the transferred amount was deemed to be unjust enrichment by the respondent.

In the cited decisions, the courts did not question the validity of transactions with an object not named in the Civil Code and did not question the provision of judicial protection to actions occurring in the blockchain. In all three cases the decisive role was played by the pseudonymity of addresses in the blockchain, which prohibits proving the fact of the ownership of cryptocurrency by a concrete entity. The actual decisions of courts in such cases depend on whom the court encumbers with the burden of proving the transfer (or failure to do so) of cryptocurrency. If, for instance, a cryptocurrency contract states the addresses of wallets and rules of transfer, the parties' rights will more than likely be protected in case of court action.

I would note that although quite a number of court decisions have been made in the sphere of civil disputes connected with cryptocurrency, in my opinion one may not speak of the formulation of a consecutive court practice. Many decisions in such cases contain practically no rational reasonings. For example, in the "Cripton" case, the Moscow City Arbitration Court traditionally dismissed the claim by virtue of the unproven fact of unjustified enrichment. However, at the appellate level the court unexpectedly and comprehensively augmented the arguments of the below level court, *inter alia*: "Legislation of the Russian Federation does not contain such a method

[19] Decision. Zavodoukovsky regional court, Tyumen district, 11.10.2017 on case № 2-776/2017 (M-723/2017). The decision was appealed in the Tyumen regional court, the appeal ruling 24.01.2018 dismissed the appeal (case № 33-245/2018).

of protecting rights as obligation to return cryptocurrency… The indicated method of protection of rights is not established in article 12 of the Civil Code of the Russian Federation, and is thus not a lawful means of protecting rights and may not be applied, that is in the given concrete case the claimant is denied the right to judicial protection of its violated rights"[20].

2. Attempt to Introduce Cryptocurrency into the Civil Code

2.1. "Digital Currency" in the First Draft of Amendments to the Civil Code

From 2018, acting against the background of ongoing theoretical disputes, the legislator began to make efforts to regulate cryptocurrency. A draft law "On the introduction of amendments to parts one, two and four of the Civil Code of the Russian Federation" was presented to the State Duma[21], presuming augmentation of the Code with the categories "digital rights" and "digital money", in fact meaning the token and cryptocurrency.

The draft law proposed introducing a new type of property rights into the Civil Code — "digital rights". In substance, these rights signify a "digital code" that "validates the right" and exist "within the information system, answering to… the signs of a decentralized information system." A mandatory condition for the existence of digital rights is the ability to "provide an entity possessing a unique access to this digital code…the possibility of becoming acquainted with the description of the relevant object… at any time." The holder of a digital right is acknowledged to be "an entity possessing unique access to…the digital code…facilitating the execution of actions relating to disposal of digital rights".

This ambiguous determination, to put it simply, positions "digital rights" as access to a specific address in the blockchain. In turn, "objects of rights" may be tied to this address. If the user has access, he also has the right: if access disappears — digital right disappears with it. Such an approach is an

[20] Resolution of Arbitration court of Appeal № 9 dated 4 February 2020 on case № A40-164942/19.

[21] Draft law № 424632-7 On introduction of amendments to the first and second parts of Article 112 third part of the Civil Code of the Russian Federation (on digital rights). Available at: URL: http://sozd.duma.gov.ru/bill/424632-7 (accessed: 12.07.2020)

original resolution to the problem of protection of rights to digital assets: no access to digital assets means no rights to them.

As the digital rights envisaged by the draft law extended to any crypto asset, including blockchain tokens, a separate article — "Digital currency" — was envisaged to determine cryptocurrency as a more limited phenomenon. This currency was connected to the digital code that existed reciprocally with digital rights within the distributed system but, unlike them 1) it did "not authenticate rights to any object of civil rights" and 2) was used "for execution of payments". It was indicated separately that digital currency could be used as a means of payment "in the instances and under the conditions established by law" — In this instance, the norms of digital rights were to apply by analogy. Inevitably, the question arose regarding the capacity of digital currency in other situations — as property, as digital rights or as an object limited in turnover?

Clearly, digital currencies were described from the contrary: just as money can be described as a bearer security which does not authenticate any deriving rights (historically, this is similar to the characterization of the first banknotes), digital moneys were described as digital rights, not as granting any rights. Such a determination, expressed with a certain paradoxical elegance, has several shortcomings. Firstly, the very fact of determinations proceeding from the contrary often show that that the author was unable to grasp the substance of one or another phenomenon[22]. Secondly, it enables ascribing any tokens without the presumption of an understandable right of demand to cryptocurrency — for example, tokens granting the right to receive cryptocurrency at a future date are also cryptocurrency receipt if used for indefinite activity in "execution of payments". At the same time, characterization of digital currency does not include, for instance, secured cryptocurrencies insofar as they endow their holders with certain rights (although somewhat conditional ones).

2.2. "Digital Rights". Final Edition of the Law Omitting Cryptocurrencies

I shall not dwell on the numerous shortcomings of the interim version of the draft law but proceed directly to the approved version. It excluded

[22] One cannot but recall Plato's characterization of Man as a two-legged creature without feathers, which was brilliantly countered by Diogenes' observation regarding a plucked rooster [Diogenes Laertes, 1986: 226].

norms concerning "digital money" as in various other provisions. The article on "digital rights" was retained, but in an amended form. In the approved version digital rights are described as "named in this capacity in the law as obligatory and other rights, the content and conditions of performing which are determined in accordance of the rules of the information system that conforms to signs established by law." At the same time "the holder of a digital right is recognized as an entity that, in accordance with the rules of the information system, has the ability to dispose of that right"[23].

Clearly, the formulation has altered by comparison with the first version. After lengthy fruitless debates regarding the "digital code", "digital designation" and other technological definitions, the legislator chose to transfer to the closed list of digital rights that should be established in special laws. Two references regarding future legislation in one sentence ("named in this capacity by the law… conforming to signs established by the law") point to the indecision of the legislator that divested itself of the responsibility for specific signs of digital rights and demands thereto. To the erroneous benefit of misunderstood technological neutrality, the distributed register also disappeared; all that remained was the initial concept of "digital rights — denotes access", removing partially certain questions regarding protection of digital rights.

Amendments were also made to the approved draft law in Article 128 concerning objects of rights. The new formulation "Assets, including proprietorial rights (including cashless monetary means, undocumented securities, digital rights) allows the conclusion that digital rights are related to property rights in the composition of assets, but do not extend to objects. In such case, digital rights may also authenticate obligatory, corporate and even exclusive rights, depending on what shall be established by special legislation.

The final version of the draft law also failed to disclose the nature of rights to crypto assets (digital rights): are they absolute or relative? Is it possible to distinguish the right to crypto asset (access) from the right arising from a crypto asset (right of demand), or the rights to crypto asset is not a new object of civil rights but merely a form of their attachment to rights of demand from a crypto asset?[24] Therefore the questions raised in p. 2.2–2.3 of the

[23] Art 141.1 of Civil Code.

[24] See: Expert opinion regarding the draft of federal law №424632-7 "On the introduction of amendments in the first, second and third parts of the Civil Code of the Russian Federation. Approved at the meeting of the Council for Codification and Perfection of Civil Legislation under the President of the RF 17.01.2019, №183-1/2019. P. 3.

present article remain unresolved, and the substance of rights to cryptocurrency (as well as the legal nature of digital rights) has not been established by legislation.

With the exclusion of norms concerning "digital currency" from the draft it was announced that cryptocurrency shall be determined in a separate draft law "On digital financial assets" providing a more specific regulation of separate types of crypto assets and rules for their turnover. However, the legal regime of cryptocurrency, passed as a relay stick from the developers of the Civil Code, became an obstacle for the working group, and its activity became stuck at this point. Apart from the civil-legal qualification of cryptocurrency, difficulties arose with permission to use cryptocurrency as a method of payment in the absence of understandable mechanisms to counter money laundering and financing of terrorism (AML/CFT). The Central Bank finally proposed the complete exclusion of cryptocurrency from legislation; but FATF, in developing financial methods for countering money laundering, reacted to this proposal immediately by demanding the reinstatement of cryptocurrency in legislation[25].

In May 2020 the Committee of the State Duma on the Financial Market was presented with a new draft law — "On digital currency and the introduction of amendments into certain legislative acts of the Russian Federation", accompanied by amendments to the Code of Administrative Offences (CoAO) and the Criminal Code (CC). Consultations on this draft law are in progress.

3. Money, Monetary Surrogates and Cryptocurrencies

3.1. Money and Monetary Obligations

The unique nature of money is determined by its role as a general equivalent of value. Money measures the value of all other things, just as responsibility for violation of civil-legal obligations. This characteristic arises for both economic and political reasons — the state grants certain things the force of a means of payment, calling them money; related obligations become monetary ones. These days money is issued by the state itself, although historically there were many forms of money emitted by private entities and

[25] Aksakov: adoption of the law on digital financial assets is "suspended" due to the demands of the FATF, 21.05.2019. Available at: URL: https://tass.ru/ekonomika/6452798 (accessed: 12.07.2020)

recognized by the state — for example, bank receipts in the epoch of free banking [Dowd K., 2002: 7].

There are several theories on which signs distinguish money from other things, at which moment money acquires value, and can non-governmental units (private money) be perceived as money [Gleeson S., 2018: 29], yet I do not wish to address this problem in depth in the present article and will employ the terminology established by legislation.

Pursuant to Art. 140 of the Civil Code and the law "On currency regulation and currency control"[26], the money category includes cash and cashless monetary means. Money may be both in Russian roubles (the legal tender of the Russian Federation), and in foreign currency. The use of foreign currency as a method of settlement on the territory of the Russian Federation is permissible only on the basis of law. Foreign currency is emitted by foreign states or their groups (including international units of account); regional and private money, just as monetary signs of unacknowledged states[27] are not regarded as foreign currency. Accordingly, cryptocurrency does not relate either to money, or to means of payment.

The substance of the category of lawful means of payment appears in private law relations. Under obligations envisaging the transfer of money (i.e. under monetary obligations) the creditor is obligated to accept a lawful means of payment as settlement. Thus a lawful means of payment, as distinct from other payment means, may settle any monetary obligation without a supplementary expression of will by the creditor, and specifically the use of a lawful means of payment renders a financial obligation to be a monetary one. Similarly, irrespective of the substance of the obligation, it is the lawful means of payment that serve as an instrument for calculation of losses, subject to compensation in the event of failure to fulfil the obligation. A lawful means of payment is also a financial collection of lawful and contractual interests as well as forfeit in any circumstances[28].

[26] Federal Law "On currency regulation and currency control" dated 10.12.2003 № 173-FZ.

[27] List of signs of foreign currency recognized by the Russian Federation, formally established by the All-Russian Classifier of Currencies (OK (MK (ISO 4217) 003-97) 014-2000. Affirmed by the Resolution of the Gosstandart of Russia 25.12.2000 № 405-st.

[28] S. 9 of Information letter of the Chair of the Higher Arbitration Court of the Russian Federation of 04.11.2002 № 70 "On the application of articles 140 and 317 of the Civil Code of the Russian Federation by arbitration courts."

The parties to a contract have the right to exercise their own discretion (p. 4 of Art. 421 of Civil Code). However, the use of foreign currency as a means of settlement is permissible only on the basis of law. If the condition regarding means of payment violates this prohibition, the court may declare it void, but this does not mean invalidation of the contract as a whole (Art. 180 of Civil Code); the amount to be paid is subject to conversion into roubles on the due day of payment; it is calculated in accordance with the official exchange rate, unless another rate is established by law or the contact (Art. 317).

What happens if an obligation is expressed not in roubles, but in cryptocurrency or regional or private money? There may be various viewpoints on this issue depending on the interpretation of the correspondence of the norms of public law with the Civil Code: *inter alia* depending on how to evaluate the active prohibition on the turnover of monetary surrogates.

3.2. Cryptocurrencies — Monetary Surrogates?

The prohibition on emitting monetary surrogates was inherited by Russian legislation from the Soviet Union, and that — from the Russian Empire. This prohibition appeared in legislation for the first time in 1870, when the 1845 Code of Criminal and Correctional Sentences was augmented by Art. 1150, prohibiting private entities to "emit nameless monetary signs in the form of stamps, receipts, labels and other signs, or obligations promising the bearer a definite sum of money, goods or other objects". The appearance of this norm was caused by the widespread distribution of private money, which competed with state issue [Nersesov N.O., 2000 (1889): 238–241].

The next arising of the surrogate problem was in the 1920s, when against the background of post-war destruction various forms of cooperative money came into broad circulation. As a result, the turnover of surrogates was proscribed; acts of that time qualified surrogates as "securities which by the nature of their convertibility could acquire the significance of monetary signs" — *inter alia,* certain bearer documents regarding distribution of goods [Lunts L.A., 2004 (1927): 67–68].

Current legislation limits the emitting of monetary surrogates by the Constitution and the law "On the Central Bank of the Russian Federation." Article 75 of the Constitution prohibits "the introduction or emitting" of

"other money" on the territory of the Russian Federation except the Russian rouble. Article 27 of the Federal Law "On the Central Bank of the Russian Federation" proscribes the introduction of "other monetary units" and "monetary surrogates." Formally, not one of these norms prohibits the turnover of monetary surrogates and provides no definitions of them [Sazhenov A.V., 2018a: 57–60]: in fact this means that the definition of one or another unit of payment as a monetary surrogate is left to the mercy of the Central Bank [Bashkatov M.L., 2018: 81]. Despite the prohibition in force since 1994, the latter has never concretized it[29] — even in response to the issue of regional currencies in the 1990s (Ural francs, Khakass roubles et al). Nevertheless, I shall not interpret this norm religiously as a direct prohibition on the use of monetary surrogates in turnover.

In the absence of a definition of a monetary surrogate, it is not unreasonable to ask: into what groups does public law, in the form of the Constitution and the law "On the Central Bank" divide means of payment that are in turnover: apart from "money" and "monetary surrogates", is there some other, third group of means of payment?

If one is to adhere to the strict dichotomy "everything that is not money (roubles and foreign currency) is a monetary surrogate", then cryptocurrencies must be relegated invariably to the latter. In this instance the prohibition must be interpreted as the exclusion of monetary surrogates from turnover by the norms of public law, and Art. 189 of the Civil Code regarding a void transaction should apply to a hypothetical transaction involving cryptocurrency: just such are transactions aimed at the alienation of objects, limited or excluded from turnover[30]. Theoretically, as the case in point concerns violation of the law, can it be possible to invoke means of responsibility established by administrative or criminal legislation while sanctions for the introduction and turnover of surrogates do not figure currently in the CoAO or the CC?[31].

[29] In 2014 the Information message of the Central Bank cited the norm concerning the prohibition of surrogates, which shall be discussed further.

[30] P. 85 Resolution of the Plenum of the Supreme Court of Russia of 23.06.2015 № 25 "On the application of certain provisions of section 1 first part of the Civil Code of the Russian Federation by the courts".

[31] The Code of administrative provisions includes a prohibition on the "unlawful emitting of documents authenticating monetary obligations" but firstly this prohibition is difficult to apply to surrogates — for they are not money and relations involving relations with their use are not monetary, and secondly this norm is inapplicable to physical entities.

In practice, prior to its extension to transactions with cryptocurrencies, prohibition on the emitting of monetary surrogates figured in contemporary law enforcement practice only once — within the framework of the so-called "Case on colions"[32], that involved private currency ("colions"), printed typographically by M.Yu. Shlyapnikov, Moscow Region resident. The claim was filed by the public prosecutor of the city of Egoryevsk, Moscow Region, and on 6 July 2015 the Egoryevsk City Court, satisfied the prosecutor's claim in full; subsequently, the Moscow District Court dismissed Shalyapnikov's appeal, and the Supreme Court refused to examine it by way of supervision.

In January 2014 the site of Central Bank carried a press release "On the use of "virtual currencies" in executing transactions, including the Bitcoin"[33]. *Inter alia*, the document cited Article 27 of the law "On the Central Bank" prohibiting the introduction of monetary surrogates. Thus, cryptocurrency was relegated obliquely to surrogates. This was followed almost immediately by appearances of representatives of fiscal and law enforcement agencies in the same key. This started a futile struggle with cryptocurrency that lasted until 2018.

The attempt to stop the spread of cryptocurrencies by administrative efforts led to the adoption of the Resolution of the President dated 25.03.2014 № Pr-604 regarding the establishment of responsibility for the use of monetary surrogates and prohibition on the circulation of cryptocurrencies. Already in the summer of 2014 the Ministry of Finance had drawn up two draft laws regarding prohibition of cryptocurrencies: amendments to the CoAO including the emitting of monetary surrogates, the distribution of software designated for mining and similar actions[34], also amendments to the Criminal Procedure Code[35] introducing criminal liability for participation in the turnover of a monetary surrogate. The draft laws received posi-

[32] Decision of the Egoryevsk City Court on case № 2-1125/2015 (M-666/2015) 01.07.2015; Appellate determination of the Moscow District Court 28.09.2015 on case № 33-23296/2015.

[33] Information of the Bank of Russia "On the use of "virtual currencies" in transactionsн including the Bitcoin" dated 27.01.2014.Available at: https://www.cbr.ru/press/pr/?file=27012014_1825052.htm (accessed: 12.07.2020)

[34] Draft law "On the introduction of amendments to separate legislative acts of the Russian Federation" Available at: URL:https://regulation.gov.ru/projects#npa=18934 (accessed: 12.07.2020)

[35] Draft law "On the introduction of amendments to the Criminal Code of the Russian Federation and the Criminal Procedure Code of the Russian Federation"Available at: https://regulation.gov.ru/projects#npa=46853 (accessed: 12.07.2020)

tive conclusions and went through public discussion but were never passed to the Government for examination and, consequently, were not submitted to the State Duma.

Further work on the draft laws and related documents was suspended and mention of surrogates was excised from Central Bank documents. The final version of the Resolution of the Plenum of the Supreme Court of Russia "On the judicial practice in matters of legalization (laundering) of monetary means"…[36] was worded in the same style; its text allows an oblique conclusion that cryptocurrencies in Russia are not excluded from turnover. Why, in the first place, did the Supreme Court, having added[37] cryptocurrency to the matter of legalization of criminal income in 2019 under Articles 174 and 174.1 of the Criminal Code, not include them in p.2 of the Resolution devoted to laundering criminal income by the acquisition of assets excluded from legal turnover (narcotics, weapons etc.)? This is highly significant in qualification, as transactions with proscribed objects do not fall under the composition of laundering. Secondly, the Preamble to the Resolution of the Plenum in the new version contains a reference to FATF Recommendation 15, pursuant to which cryptocurrency is to be interpreted as "property" or "asset" but not as "surrogates"[38]. The bodies of executive power also confirmed the development of a legal mechanism for the confiscation of cryptocurrency[39] — as it is well known that confiscation of assets is not implemented regarding assets proscribed for turnover or removed from turnover[40].

---

[36] Resolution of the Plenum of the Supreme Court of the Russian Federation 7 July 2015 № 32 (in the version of 2019) "On judicial practice in the matter of legalization (laundering) of monetary means or other property acquired by unlawful means, and acquisition or disposal of other property consciously acquired by criminal means."

[37] Resolution of the Plenum of the Supreme Court of Russia 26 February 2019 № 1 "On the introduction of amendments into the Resolution pf the Plenum of the Supreme Court of the Russian Federation 7 July 2015 № 32 "On judicial practice in the matter of legalization of monetary means or other property acquired by unlawful means and acquisition or disposal od property acquired by criminal means.!

[38] FATF Guidance for a risk-based approach. Virtual assets and virtual asset service providers. 2019. Available at: URL: https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf (accessed: 12.07.2020); Clarifying note to Recommendation №15: The FATF Recommendations. P. 15, 70–71.

[39] MIA confirmed development of a mechanism for the arrest and confiscation of cryptocurrencies. Available at: URL: https://1prime.ru/finance/20191204/830642774.html (accessed: 12.07.2020)

[40] P. 14 Resolution of the Plenum of the Supreme Court RF dated 14.06.2018 № 17 "On certain questions regarding implementation of confiscation of property and criminal judicial procedure."

Thus at present apart from money and surrogates there is a certain third group of quasi-monetary substances to which cryptocurrency belongs. Consequently. transactions with it have legal force. The question is whether a contract executed with cryptocurrency implies a monetary obligation, can cryptocurrency be considered as payment for a contract? In examining the regime by M.B. Zhuzhalov and A.Yu. Tolkachev of "ordinary money" (things commonly accepted as forms of payment),suggest considering such transactions an exchange if both provisions are things[41], or an atypical transaction if one of the provisions is not material. If the parties agree to an alternative execution in money or cryptocurrency, the obligation will have a "flickering causation" dependent on the final counter-offer [Zhuzhalov M.B., Tolkachev A.Yu., 2018: 106]. A.I. Savelyev notes that if the debtor offers to settle the existing monetary obligation with an unlawful means of payment (*inter alia* with cryptocurrency) then with the consent of the creditor there can be a novation instead of settlement of the obligation, which ceases to be monetary [Saveliev A.I., 2017: 139–141].

4. "Combating Money Laundering" (AML CFT)

4.1. Cryptocurrency in the Russian Financial System

The architecture of the global financial system, formulated *inter alia* on the basis of international standards regarding the combating the laundering criminally acquired income and the financing of terrorism envisages that electronic payments should be accompanied by information concerning the sender and recipient of payment (the so-called "forwarding rule" or "travel rule"). Moreover, an intermediary organization must have the power to freeze suspicious electronic payments[42]. However these demands regarding cryptocurrencies cannot be implemented fully, firstly because information about senders and recipients of the relevant payments is pseudonymized and secondly because the participants of direct cryptocurrency transactions

[41] Under Russian law such a transaction will be considered an exchange if both provisions under the contract are goods (Art. 567 of CC; p. 3 Information Letter off the Presidium of the HAC RF 24.09.2002 № 69). "Review of the practice of resolving cases concerned with exchange agreements".

[42] Recommendation № 16 from "40 recommendations of FATF" The FATF Recommendations: International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. FATF/OECD, 2012-2019. Available at: URL: http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf (accessed: 12.07.2020)

are not financial institutions or other entities[43], conducting monitoring of clients.

Having realized this situation, Central Bank and Federal Financial Monitoring Service (Rosfinmonitoring) issued official prohibitive positions in 2014 regarding the cryptocurrency regime. Both documents charged supervisory financial organizations to treat cryptocurrencies with extreme caution, however firstly they offered no specific measures for the legalization of cryptocurrency transactions, and secondly there were questionable press releases issued with no definite legal force.

The first "cryptocurrency" press release of Central Bank in January 2014 stated that:

> *Granting legal entities services on the exchange of digital currency into roubles and foreign currency, also to goods (works, services) shall be regarded as a potential participation in the execution of questionable operations in the light of legislation aimed at combating the legalization (laundering) of income acquired by unlawful mean and the financing of terrorism.*

Although this position had no legal power, in the eyes of the public it became the first precedent for the state to affirm its stance concerning the regulation of cryptocurrencies. One month later, Rosmonitoring, the body responsible for combating legalization of unlawful income. issued a similar message regarding its position:

> *The aforesaid circumstances, and in the first place the anonymity of the payment, led to the active use of cryptocurrencies in the trafficking of drugs, arms, counterfeit documents and other criminal activity. The given facts, and also the possibility of uncontrolled trans-border transfer of monetary means and their subsequent cashing serve as grounds for a high risk of potential introduction of cryptocurrencies into schemes aimed at legalizing (laundering) income derived by unlawful means and financing terrorism…*[44]

[43] Such monitoring is also performed by representatives of "established non-financial enterprises and professions" — e.g. independent accounting companies or dealers in precious metals (recommendation 22).

[44] Information message from Rosfinmonitoring "On the use of cryptocurrencies". 06.02.2014. Available at: URL: http://www.fedsfm.ru/news/957 (accessed: 12.07.2020)

In 2015, 2018 and 2019 the Group developing financial means of combating money laundering issued recommendations concerning cryptocurrencies. These recommendations cannot be applied directly in the member-states of the FATF but must be implemented through national legislation.

In 2015 states of the FATF were apprised of the need to regulate the activity of organizations changing cryptocurrencies into fiat money (i.e. the activity of money exchangers and cryptocurrency exchanges with the ability of withdrawal and input of generally accepted money). It was indicated that if the use of cryptocurrency is prohibited in a country, it is necessary to bear in mind the risk of underground turnover of cryptocurrencies[45].

Amendments concerning virtual assets were introduced into the FATF Recommendations in 2018. *Inter alia* a determination of a virtual asset was established, and the qualification of crypto assets as assets was recommended.

In 2019 FATF published a number of documents[46], establishing additional requirements regarding cryptocurrencies ("virtual assets") and for providers of services in the relevant sphere, including crypto exchanges and online wallets (custodians): among other things, the latter were endowed with the "right of transfer", that had applied previously only to traditional financial transactions[47]. Presumably, member-states of the FATF shall introduce new rules within 12 months. This has already occurred in several jurisdictions — for example, analogous demands are contained in the Fifth "antilaundering directive" of the EU[48].

Clarifications by the FATF concerning cryptocurrency were not practically incorporated into Russian legislation. In 2017 there was an updating of the Information of Central Bank "On the use of private "virtual curren

[45] FATF Guidance for a risk-based approach. Virtual currencies. 2015. Available at: URL: http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf (accessed: 12.07.2020)

[46] FATF Guidance for a risk-based approach. Virtual assets and virtual asset service providers. 2019. Available at: URL: https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf (accessed: 12.07.2020); Clarifying note to Recommendation №15: The FATF Recommendations. P. 70—71.

[47] Ibid. P. 111—119.

[48] Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU. Available at: URL: https://ec.europa.eu/info/law/anti-money-laundering-aml-directive-eu-2018-843_en (accessed: 12.07.2020)

cies"(cryptocurrencies)"[49]: the new edition excluded the reference to monetary surrogates, and the need to develop an approach to determination and regulation of cryptocurrencies was noted. Also in 2019 the Supreme Court executed the FATF recommendation in the part of recognizing cryptocurrencies as a tool for committing crimes: they were named directly in the Resolution of the Plenum "On judicial practice in matters concerning the legalization (laundering) of monetary means…"

It should be understood that the FATF Recommendations allow a full prohibition on cryptocurrencies on the territory of member-states (which is being watched by Russian legislators[50]). However, within the framework of the risk-oriented approach adopted by the FATF, it is impossible to prohibit cryptocurrencies without a definition of their substance and regulation of their turnover in other operations of natural entities). Consequently, the Russian legislator cannot evade defining cryptocurrencies in legislation; on the other hand, defining their legal status is not obligatory.

4.2. The Activity of Law Enforcement Agencies Regarding Cryptocurrencies

At present, a paradoxical position has emerged: the state does not voice its position regarding the cryptocurrency market, taking unofficial measures against their use in entrepreneurial activity. This results in the impossibility of scaling activity connected with cryptocurrency, as at a certain stage the risks with compliance become too high.

The cause of the situation is that the "acts" of the Central Bank and Rosfinmonitoring at this time regarding the "suspicious nature" of operations with cryptocurrency, can be relegated even theoretically to controlled financial organizations and certain other participants of the financial system. If operations with cryptocurrencies are performed, for example, by natural entities, neither the Central Bank, nor Rosfinmonitoring, nor the General Prosecutor's Office (as an office performing general supervision over the observation of legislation) have any actual leverage to influence them. Ac-

[49] Central Bank of Russia. On the use of private "virtual currencies" (cryptocurrencies). 04.09.2017. Available at: URL: https://www.cbr.ru/press/pr/?file=04092017_183512if2017-09-04T18_31_05.htm (accessed: 12.07.2020).

[50] Director, Legal Department of Central Bank. We oppose institutions for the organization of emitting cryptocurrency in Russia. Available at: URL: https://www.interfax.ru/interview/699260 (accessed: 12.07.2020)

tivity in the cryptocurrency sphere is neither a criminal nor an administrative beach of the law, and natural and legal entities as such are not obligated to check their contracting parties under AML/CFT.

In fact, with regard to judicial and official persons, the General Prosecutor's Office has implemented various measures of influence:

Official warning regarding the unacceptability of breaching the law[51];

Summons to appear at the local law enforcement offices "for a discussion" within the framework of verifying observance of legislation[52];

Conducting a verification of observance of legislation including extraction of documents and confiscation of equipment presumably destined for use in breaching the law[53];

Filing of a claim for the blocking of a website on the grounds that it contains information forbidden by law or calling for a breach of legislation.

Although all measures are employed in practice, only blocking of a website is performed in a judicial procedure which leaves a sufficiently broad trail to enable evaluation of the statistics concerning site blockings and to reach conclusions, therefore I shall address this issue in greater detail.

The blocking of a site *per se* is permitted by Article 15.1 of the Federal law "On information…"[54], pursuant to which, if the court finds the information on the site to be "information, the dissemination of which is proscribed in the Russian Federation", the Federal Service for Supervision of Communications, Roskomnadzor, enters the site into a special register that is sent to the providers for blocking. At the same time, the legislation contains no prohibition on the dissemination of information regarding cryptocurrencies. The closest formulation (usually cited in such cases by an administrative claimant is contained in p.6 of Art. 10 of the Law "On information…": "Dissemination of information is forbidden…dissemination of which

[51] See e.g. The Prosecutor's Office issued a warning to the director of a car salesroom, who posted an Internet ad regarding the sale of a car for 55 "bitcoins". Prosecutor's Office of the Krasnoyarsk Region, 13.12.2017. Available at: URL: http://www.krasproc.ru/news/krsk/16647-prokuratura-oby-avila-predosterezhenie-direktoru-avtosalona-kotoryi-razmestil-v~ (accessed: 01.06.2020)

[52] Available at: URL: https://www.kommersant.ru/doc/3380400 (accessed: 12.07.2020)

[53] Available at: URL: https://www.rbc.ru/technology_and_media/01/09/2018/5b890f069a794729ceaa4791 (accessed: 12.07.2020)

[54] Federal Law of 27 July 2006 no 149-FZ «On information, information technologies and protection of information».

carries criminal or administrative liability." It is clear that no criminal or administrative liability is envisaged for the dissemination of information concerning cryptocurrency or any other activity related to it. However, this does not deter the Prosecutor's Office, which files claims for blockings — apart from cryptocurrency, sites on dozens of subjects are blocked[55]. Rulings are almost always in favour of the Prosecutor's Office.

An analysis of the sudact.ru site shows that as of 2016, the Prosecutor's Office lodged demands for the blocking of no less than one hundred sites that published information about the sale of crypto assets[56]. One of the significant cases of this type that reached the Supreme Court was the case of the "Bitcoinoinfo" site[57], blocked on 12 January 2017 at the request of the Prosecutor's Office of the Vyborg District Court of Saint Petersburg. The court justified its decision on the circumstance that the site disseminates information about a monetary surrogate — the "bitcoin" cryptocurrency, that is decentralized from virtual means of settlement and accumulation that is not supported by real value. In the "Bitcoininfo" case the holders of the site were able to have the decision reversed, having proved that interested parties (administrator of the domain name) were not included in the case, but there was no discussion concerning information on cryptocurrency as being unlawful.

Reversal of a court ruling in similar cases is an exception rather than the rule. Although in the period of active discussion about legislation concerning cryptocurrencies in 2018–2019 there was a certain degree of decline in the number of site blockings, and even the Prosecutor's declining rate of claims[58], sites carrying information about cryptocurrency continue to be blocked[59].

---

[55] See e.g.A user of Zakon.ru wrote how builders circumvent the law and the Procuracy fails to react. He was blocked by Roskomnadzor. Available at: URL: https://zakon.ru/discussion/2019/08/13/polzovatel_zakonru_napisal_o_tom_kak_zastrojschiki_obhodyat_zakon_i_prokuratura_ne_reagiruet_ego_zab (accessed: 12.07.2020)

[56] The reader can repeat my experience be accessing: https://bit.ly/3cTJsE8

[57] The ruling of the Vyborg District Court, 18.07.2016 on case № 2-10119/2016 (M-9635/2016). Appeal decision of the Saint Petersburg City Court 13.02.2017 on case № 33a-2537/2017.

[58] See e.g. ruling of the Kuybyshev District Court, City of Omsk, 24 July 2018 on case № 2a-2861/2018; application by the Omsk Procuracy 07.05.2019 №8-03-2019/6769.

[59] See e.g. ruling of the Nandomsk District Court, Arkhangelsk Region, 4 February 2020 on case № 2a-125/2020; Decision of the Anapa City Court, Krasnodar Region, 28 February 2020 on case № 2a-637/2020.

5. Conclusions

Cryptocurrencies have come a long way in the minds of Russian jurists over the past four years. Against a background of furious arguments between theoreticians and practitioners, the Russian lawmaker was force-marched through all the stages of attitudes to crypto assets on the well-known model of Elisabeth Kuebler-Ross: from rejection to depression (in the case of different types of tokens it even reached acceptance). However, as far as we are concerned, it is important to determine what food for thought these new phenomena brought to specialists; it is also important to look at how the state, that is — the lawmaker — has shown itself in practice.

The Regulator and other agencies (firstly, the Ministry of Finance) predictably agreed on a prohibiting policy, that was supported by the Government and the State Duma. There were significantly more prohibitive draft laws drawn up concerning cryptocurrencies than liberal ones, and it may be presumed that in one version or another, the prohibition will be implemented. This position is entrenched in the accepted regulatory policy regarding new information and financial technologies: they are either ignored (in the case of cryptocurrencies the scope of new technology did not allow this), or normatively limited. At the same time, this limitation of cryptocurrencies in Russia corresponds on the whole with the policy of the "hermetic sealing" of the global financial system being conducted by FATF.

As a prohibitive consensus has been reached by bodies of state power toward cryptocurrency, there was no comprehensive political-legal analysis during the development and discussion of the relevant normative acts, and the market (existing and potential) was not evaluated, alternative versions were not studied officially. What aims from the viewpoint of legal policy shall be served by a total prohibition on an entire group of economic relations? Shall this prohibition protect the rights citizens, investors, entrepreneurs? How shall it help to protect creditors' rights, ensure execution of contracts including transborder ones?

The legislator has proved to be exceedingly unwieldy when the matter came to actual law-making — consolidation of dissimilar groups of interests and development of a compromise position, evolvement of hypotheses and their verification on the basis of empirical data. Supra-actual changes in the CC (eventually taking up three pages) were developed and passed over about a year (development at the beginning of 2018, first publication

in March, adoption in March 2019); a more detailed law "On digital financial assets" is under development for almost three years (Resolution of the President Pr-2132 — October 2017, first publication — December 2017, is still under discussion but not passed). As a result, the nascent market of cryptocurrencies and crypto assets was lawfully adopted at first by offshore jurisdictions, then by some countries such a Switzerland, Great Britain and Estonia. By comparison the Duchy of Liechtenstein has worked out an exemplary law on the blockchain (the overall volume of which, with accompanying materials, approaches 200 pages) in less than two years (November 2016 — August 2018); the law was passed by parliament and came into force[60]. It stands to reason that while the law was being developed the risks relating to the new market (swindling, committing of crimes with the use of cryptocurrencies, legalization of unlawful income) did not disappear and citizens who had invested money in the time of the cryptocurrency boom suffered losses.

The judicial community also proved to be conservative. In the storm of "digital" debates over these years, no consolidated (and constructive) position emerged regarding crypto assets. Despite the circumstance that the first attempts to introduce "digital rights" into the Civil Code seemed to unite lawyers against a "common enemy", subsequently all planned normative acts were adopted without any influence by the community. The impression is that the law-making process involves only lawyers working out positions regarding separate clients: as a result, legislation concerning cryptocurrencies looks increasingly like a patchwork blanket from diverse norms "affirmed" by references to subordinate legal acts.

With rare exceptions (the Tsarkov and the Bitcoiminfo cases) have played no active role in clarifying the legal nature of cryptocurrencies and allied questions. Alongside the inaction of theoreticians this has resulted in no resolution of principles in doctrine — what is the legal nature of virtual property in the context of Art. 128 of the Civil Code, what constitutes a monetary surrogate, etc.

The listed problems are not typically Russian. As much as can be judged from a distance, the same path was followed by other states. Unfortunately, the general unpreparedness for principled regulation of new institutions only confirms the arguments of the "crypto anarchists" that the state, facing

[60] Available at: https://impuls-liechtenstein.li/en/blockchain-act-liechtenstein/ (accessed: 12.07.2020)

the realities of globalization and digitalization of the world's markets — is no "night watchman" but a "settled bandit" that is not prepared to surrender seized powers — including the power to regulate financial relations, international payments, financial markets and information networks. I mean that in these matters the state has shown itself to be an ineffective regulator, but has no intention of giving up attempts as it knows no other means of influencing social relations apart from those based on submission to force. In future, as I see it, the tendency toward "nationalization" of information networks, establishment of sovereignty over citizens' data, mandatory collection of information and so forth shall only increase. In this sense, the situation with the regulation of cryptocurrencies has offered us a good example from which those willing can learn lessons.

References

Bashkatov M.L. (2018) The modern money theory in terms of German dogma: genesis and challenges. *Grazhdanskoe pravo: sovremennye problemy.* Moscow: Statut, pp. 42–81 (in Russian)

Diogenis Laertius (1986) *Lives and opinions of eminent philosophers.* Moscow: Mysl', 572 p. (in Russian)

Dowd K. (ed.) (2002) *The Experience of Free Banking*. London: Routledge, 288 p.

Gleeson S. (2018) *Legal concept of money*. Oxford: University Press, 230 p.

Gromov A.A. (2018) Coercion to creating an audio and visual work, or the limits of real awarding. Comments to opinion of Supreme Court collegium on economic disputes. *Vestnik ekonomicheskogo pravosudiya*, no 4, pp. 10–15 (in Russian)

Efimova L.G. (2001) *Bank transactions: law and practice.* Moscow: NIMP, 654 p. (in Russian)

Efimova L.G. (2019) Crypto currencies as an object of civil law. *Khozyaystvo I pravo*, no 4, pp. 17–25 (in Russian)

Fyodorov D.V. (2018) Tokens, crypto currency and smart contracts in Russian bills in the international context. *Vestnik grazhdanskogo prava*, no 2, pp. 30–74 (in Russian)

Lunts L.A. (2004) *Money and monetary obligations in civil law.* Moscow: Statut, 350 p. (in Russian)

Mertvischev A.V. (2012) Natural obligations in Russian civil law. Candidate of Juridical Sciences Summary. Ekaterinburg, 29 p. (in Russian)

Nersesov N.O. (2000) On bearer papers in civil law. Moscow: Statut, 286 p. (in Russian)

Novosyolova L.A. (2017) On the legal nature of bitcoin. *Khozyaystvo i pravo*, no 9, pp. 3–16 (in Russian)

Savelyev A.I. (2017) Crypto currencies in civil rights. *Zakon*, no 8, pp. 136–153 (in Russian)

Savelyev A.I. (2018) Risks of tokens and blockchain activity in civil law. *Zakon*, no 2, pp. 36–52 (in Russian)

Savelyev A.I. (2016) Contract law 2.0: smart contracts as the end of classical contract law. *Vestnik grazhdanskogo prava*, no 3, pp. 32–59 (in Russian)

Sazhenov A.V. (2018a) Crypto currencies and quasi-money. *Predprinimatel'skoe pravo*, no 1, pp. 57–60 (in Russian)

Sazhenov A.V. (2018b) Crypto currencies and dematerialization in civil law. *Zakon*, no 9, pp. 106–121 (in Russian)

Sklovskiy K.I., Kostko V.S. (2018) The concept of thing. Money. Real estate. *Vestnik ekonomicheskogo pravosudiya*, no 7, pp. 115–143 (in Russian)

Skryabin S.V. (2004) A thing as an object of civil rights. *Yurist*, no 6, pp. 34–39 (in Russian)

Sukhanov E.A. (2017) *Property law*. Moscow: Statut, 560 p. (in Russian)

Tolkachyov A.Yu., Zhuzhalov M.B. (2018) Crypto currency as property: analysis of current status. *Vestnik ekonomicheskogo pravosudiya*, no 9, pp. 91–135 (in Russian)

Zhuzhalov M.B. (2019) Blockchain and international law activity in cyberspace. *Pravovedenie*, no 1, pp. 62–96 (in Russian)

The Challenges of Blockchain Technology to Competition Law

Christophe S. Hutchinson

Senior lecturer, Department of Legal Regulation of Economic Activities, Financial University under the Government of the Russian Federation. Address: 49 Leningradsky Prospekt, Moscow 125993, Russia. E-mail: sam_hutch2004@yahoo.fr; KSYUchinson@fa.ru

Abstract

Blockchain is a catch-all term for a combination of three technologies: distributed ledger, cryptology and network protocols. The first enables storing the same info in different places, the second allows secure transactions to be recorded and then encrypted on the distributed ledger. The third element governs the network and verifies transactions across the network automatically and independently. Considered by many as "the biggest technological innovation since the Internet"[1], blockchain is a decentralized, more secure and transparent model for transactions that operates on an encrypted peer-to-peer basis. This model makes trust between parties superfluous by instead placing trust in the underlying technological platform. This would effectively remove the need for intermediaries whose business has been to make up for the lack of trust; these include banks, brokers, governments, internet platforms, law firms etc.[2] While reducing the costs of contract enforcement and thus facilitating trade, blockchain technology may have significant implications for antitrust law. As decentralized organizations such as blockchain are not recognized as legal persons, this raises questions about whether anticompetitive practices and their perpetrators can be identified. For example, can a non-entity hold a dominant position? Can blockchain create a "monopoly without a monopolist"? Finally, if a blockchain is dominant, which users and/or entities hold that dominant position? This article intends to highlight the challenges that blockchain presents to the analyses of unilateral anticompetitive practices[3].

Keywords

distributed ledger, cryptology, network protocol, immutability, antitrust, public and private blockchain, dominant position on the relevant market, abuse of dominance, exclusionary abuse, exploitative abuse, discriminatory abuse.

[1] *Medcraft G.* Blockchain or distributed ledger technology: The biggest technological revolution since the Internet. 2018. Available at: https://podtail.com/en/podcast/oecd-on-the-level-podcast/the-blockchain-revolution-the-power-of-positive-di/ (accessed: 26.05.2020)

[2] *Penz-Sharp A.* Blockchain for Business: Ready or Not, Here it Comes, *CMS Wire*, 4 December 2017. Available at: https://www.cmswire.com/information-management/blockchain-for-business-ready-or-not-here-it-comes (accessed: 01.07.2019)

[3] Cartels are excluded from this study in order to keep this article to a reasonable length. Many of the points made in this article can nonetheless be applied to cartels.

For citation: Hutchinson C.S. (2020) The Challenges of Blockchain Technology to Competition Law. *Legal Issues in the Digital Age,* no 1, pp. 32–53.

Introduction

Blockchain is a general-purpose technology that threatens to disrupt markets and institutions across the world. While Internet enabled the publishing and digital transfer of information, blockchain by ensuring the trust necessary to undertake transactions and reducing uncertainties (through its use of dependable self-executing code) makes it possible to identify the ownership of assets, make them unique and traceable, and facilitate digital transfers that then enable exchanges of assets.

The World Economic Forum predicts that 10% of global gross domestic product will be stored on blockchain by 2027[4]. Blockchain's attractiveness lies in its ability to drastically reduce the transactional costs[5] required to create trust between parties through recourse to intermediaries such as banks, brokers, governments, internet platforms, law firms, legal procedures, etc.[6] It can indeed facilitate making contracts and mitigate widespread contractual inadequacies[7] by creating a world in which "computers... fill the gaps of contracts" [Schrepel T., 2018: 15].

Although it facilitates trade, blockchain also presents numerous legal challenges with substantial implications for antitrust law. One of these challenges is suggested by the word "antitrust" itself. On the one hand, a large part of competition law is referred to as *anti*-trust, using the American terminology that emerged as a reaction to the misuse of the trust instrument [Ernst D., 1990: 879]. On the other hand, blockchain technology eliminates

[4] World Economic Forum. Technology tipping points and societal impact, survey report 24. 2015. Available at: https://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf (accessed: 23.03.2019)

[5] *Roberts R., Epstein J.* On bitcoin, the blockchain, and freedom in Latin America. *ECON TALK*.13 February 2017. Available at: http://www.econtalk.org/jim-epstein-on-bitcoin-the-blockchain-and-freedom-in-latin-america/ (accessed: 13.05.2019)

[6] *Penz-Sharp* A. Blockchain for business…

[7] *Cong L., He Z.* Blockchain disruption and smart contracts. 27 December 2018, p. 4. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2985764 (accessed: 26.05.2019). "[B]lockchains, via decentralized consensus, enable agents to contract on delivery outcomes and automate contingent transfers. Hence, the authentic entrant is now able to signal her authenticity fully. This eliminates information asymmetry as a barrier for entry and greater competition, enhancing welfare and consumer surplus in this blockchain world."

the need for a fiduciary, that is, a person who creates trust, because it works automatically without any physical or artificial person[8]. What happens when antitrust law confronts a technology that works without a trusted counterparty? Is it time to leave behind both the regulatory apparatus of antitrust? From a legal point of view, are the current rules well suited to analyzing blockchain and its processes?

This article intends to highlight the challenges that blockchain presents for analyzing unilateral anticompetitive practices. It is divided into two parts, the first of which describes how blockchain functions. The paper then argues that, because blockchains are anonymous, immutable and decentralized, questions arise about whether anticompetitive practices and their perpetrators can be detected.

1. How Blockchain Functions

This section focuses only on the fundamentals of blockchain's operations, highlighting those that are particularly relevant for antitrust analysis. In addition, this part deals with the distinction between public and private blockchains, which is important because of the implications of this distinction with respect to competition law. Finally, it explores the differences between Blockchain 1.0, 2.0, and 3.0 to show how blockchain is used today and what direction it may take in future.

1.1. General Aspects

Blockchain is a catch-all term for a combination of technologies which have come together to create networks that are capable of securing trust[9] between people that have no antecedent reason to trust one another. Blockchain combines the following three technologies: distributed ledger [Raval S., 2016: 21] cryptology and network protocol. Distributed ledger allows the storing of the same information in different places [Posner E., Weyl G., 2018: 368]. Although the cryptology that was created during World War II is

[8] *Murck P*. Who Controls the Blockchain? *Harvard Business Review*.19 April 2017. Available at: https://hbr.org/2017/04/who-controls-the-blockchain (accessed: 13.05. 2019)

[9] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system.2008. Available at: https://bitcoin.org/bitcoin.pdf (accessed: 12.05.2019). In the words of Nakamoto, blockchain is based on "cryptographic proof instead of trust."

nothing new[10], it enables encryption of transactions or data on a distributed ledger. By combining distributed ledgers and encryption, parties can trust one another. The third element, which is a new one, is network protocol [Dannen C., 2017: 3]. It governs the network and verifies transactions or data transfers across a network independently and automatically. By loading a protocol onto a computer, a person becomes a node in the network. The network protocol thus allows verification of what is in the network. A transaction or a transfer over the network is carried out when one party sends data, such as a digital coin or a piece of data, to another party over the network. Every time there is a change in the ownership of an asset due to this transaction a new block is added to the already existing blocks. All these blocks are linked cryptographically forming a chain through which it is possible to trace an entire transaction of any particular asset.

Blockchain has several advantages: first, it is *decentralized*. The network exists across a series of nodes formed by the computers that store the blockchain information and also contribute to verifying the transactions. When a transaction takes place, parties on both sides of the transaction interact with each other through peer-to-peer transmission, with communication being done directly between them and not through a central point. The nodes are like a "bunch of people sitting around saying: yes, yes, thumbs up, we all agree"[11] to the transaction being carried out on the network. The decentralization means that *no single participant controls the information* on the blockchain.

A second advantage of blockchain is that it is in principle *visible to all,* which means that all users on a blockchain can see all the transactions regarding an asset being traded on the blockchain and who holds an asset at any particular time[12.]

Third, it is *anonymous* [Champagne P., 2014: 136] as no user has to provide a name, an e-mail address, or any other personal data in order to download and use the network software [Tapscott D., Tapscott A., 2016: 282].

Lastly, blockchain data is also *immutable* [Walch A., 2017: 713]. Once information is stored on a block, it cannot be tampered with by individual participants unless the whole network agrees to such a change.

[10] Medcraft G. Op. cit.

[11] Ibid.

[12] Most of the data put on the blockchain is encrypted so that only people with the right keys can decrypt it. However, the "visible effect" remains the rule and the protocol design is visible by all.

1.2. Public vs. Private Blockchain

There are different types of blockchains. The difference comes down to whether the information stored on the blockchain is public or private and whether potential nodes and users on the network need permission to join or not. There is a taxonomy on public/private and permissioned/non-permissioned blockchain.

Public blockchains[13] such as Bitcoin and Ethereum are open to all. To become a node on those networks, each participant needs to set up their computer by implementing the governing protocol. They can remain pseudonymous behind a unique user identifier within the network. The ledger tracks each participant by their identifier. The ledger is transaction-based, and it notes the prior transaction history. This information can be used to assess whether the participant has sufficient funds, capacity, inventory, etc. to complete the requested transaction based on the prior transactions that either have credited or debited the account.

Anyone can propose blocks of transactions to be added to public blockchains. There is no central validation system that oversees the blockchain to determine which blocks of transactions get added or to determine which are valid when discrepancies occur. Instead, blockchains use present rules, a "consensus mechanism", to decide which record should prevail.

For example, the party on the Bitcoin blockchain that is the first to correctly solve a computational puzzle gets to propose the next block to the network. This is called "mining". The nodes on the network signal their acceptance of the proposed block by adding it to their copies of the blockchain after validating that the computational puzzle was solved directly, that the transactions in the block are valid, and that the bitcoin in each transaction was not previously spent. If there is a conflict between different versions of the blockchain, the chain that has the largest amount of computational work is considered to have the accurate record under a "proof of work" protocol. Under this system, there is no practical likelihood that one participant can be strategically prioritized or given an unfair advantage over another. To the extent disputes arise between participants, there are no default rules to resolve them[14].

[13] Public blockchains are also called "permission-less" or "open" blockchains.

[14] Thomas R. Blockchains and antitrust: New technology, same old risks . Available at: https://www.jonesday.com/blockchains-and-antitrust-new-technology-same-old-risks-08-02-2018/ (accessed: 16.05.2019)

A public permissioned blockchain is a system in which the information is public but entering new information or verifying a new transaction requires permission from a central authority. Such is the case, for instance, with a blockchain used for land registry. Any potential buyer can consult it and check the identity of the owner of a particular piece of land, but in order to make an entry in the registry the buyer must have the right permission. This type of blockchain is public because everyone can see who owns the land and it is permissioned to the extent that changes of property require permission from the state. The practical implications of this type of blockchain are huge. The Swedish government, for instance, is currently looking at a public permission blockchain as a way to collect land tax more efficiently because it is up-dated all the time and it permits linking the land registry blockchain to GPS coordinates[15].

A private blockchain, also called a permissioned blockchain, is a blockchain that restricts reading permissions to certain participants. In such a system, nodes are authorized by a central authority and the information can be used only by the members of the network because it is private. The central authority need not be a single entity. A group of entities is often a feature of a private blockchain. For example, this kind of permissioned blockchain has been used by the banking system for interbank transactions, clearing or settlement, or transferring accounts between insurance providers. In this type of blockchain, there are "full" nodes that actually own an entire copy of the ledgers and "light" nodes that have elements of the ledger, as is often the case in a private blockchain. For instance, a stock exchange owns all the ledgers that are in that system and an operator, in its capacity as owner of an equity or security, will have access only to their particular part of the chain, which is their account in it.

Private blockchains are subdivided into two different categories. The first is called a single entity blockchain. As its name suggests, a single entity will set up the protocol and run the blockchain, while reading permission may be public or restricted to certain participants. The second category is called a consortium blockchain. The consensus process in these is controlled by a pre-selected set of nodes. For example, the consensus mechanism could be made up of five companies, each of which operates a node, with three of them required to sign in order to validate a block. Regardless of the techni-

[15] Medcraft G. Op. cit.

cal particulars, all consortium blockchains operate under the leadership of a group instead of a single entity. In addition to private and public blockchains, there are also semiprivate blockchains. Those blockchains are run by a single company that grants access to any qualified user.

1.3. Consensus and Governance

Blockchains can be classified by the way they achieve consensus. The consensus mechanism is the general agreement, unanimous by nature, under which the blockchain works. The integrity of the blockchain relies on the chosen consensus to clear transactions.

Several major public blockchains (e.g., Bitcoin and Ethereum) currently use a form of consensus based on proof of work, in which certain users who are referred to as miners in these systems compete in solving a cryptographic puzzle in order to be chosen to verify the integrity of transactions [Vigna P., Casey J., 2018: 39]. The first to solve the puzzle is rewarded with a transaction fee. Many public blockchains are currently working on developing a "proof of stake"[16] consensus derived from cryptoeconomics and game theory [Kreps D., Wilson R., 1982: 253].

With private blockchains, however, there is generally no mining, no proof of work, and no remuneration. The benefits of a private blockchain come from its applicability to value. Uses of private blockchains include: (1) serving as a way to transfer value (currency, securities, votes, industrial patents, the Internet of Things (IoT), stocks, and bonds)[17]; (2) serving as a register to verify the exchange of products and assets[18]; and (3) serving as a smart contract by enabling an automatic program to insert terms and conditions [Cuccuru P., 2017 :179].

[16] *Zamfir V.* Introducing Casper "the Friendly Ghost", *Ethereum Blog*. 1 August 2015. Available at: https://blog.ethereum.org/2015/08/01/introducing-casper-friendly-ghost (accessed: 10.05.2019). "In it, the algorithm attempts to solve these problems by removing the mining concept entirely and replacing it with another mechanism. With the proof of stake, the same participant invests $1,000 by directly purchasing the cryptocurrency of the blockchain then deposits these cryptocurrencies using the proof of stake mechanism, which will then (pseudo-) randomly assign that participant the right to produce blocks and receive a reward." In short, the so-called "Casper Protocol" is set to transfer Ethereum from a proof-of-work to proof-of-stake model in the coming months.

[17] *Guegan D*. Public blockchain versus private blockchain. Documents de travail du Centre d'Economie de la Sorbonne.18 March 2017. Available at: https://halshs.archives-ouvertes.fr/halshs-01524440/document (accessed: 09.05.2019)

[18] Ibid.

Whoever controls the consensus — also known as the consensus mechanism — controls the governance of the blockchain [Huberman G., 2017: 3]. The consensus operates and communicates between network nodes. For instance, Dash[19], a crypto-currency, uses a governance system that allows its users to vote if they hold tokens. Decred, also a crypto-currency, has a more centralized governance system according to which some of its users, called the Masternode, have more power within the community. A blockchain's ability to implement anticompetitive strategies will vary depending on its governance system.

1.4. From Blockchain 1.0 to Blockchain 3.0

Antitrust concerns about blockchain platforms and the software operating on them pertain to different types of anticompetitive practices: those that are committed via the blockchain itself as a platform; and those that are committed via the applications running on the blockchain.

Not all blockchains allow software (called "layer 2") to run on top of their root blockchain ("layer 1") but most do. Ethereum, for example, is a root blockchain that allows any type of software layer. In fact, Ethereum was designed specifically to allow users to create "smart contracts" [Dannen C., 2017: 3] or agreements between accounts to automatically transfer tokens when certain conditions are met. Anyone can upload a program onto this platform and leave it to self-execute securely [Tapscott D., Tapscott A., 2016: 221].

These blockchain applications fall into three generations. The first, Blockchain 1.0, is similar to a currency and includes "cash, such as currency transfer, remittance, and digital payment systems" [Swan M., 2015: 23—34]. The second, Blockchain 2.0, is a contract, including "stocks, bonds, futures, loans, mortgages, titles, smart property, and smart contracts". This category includes all blockchains allowing applications that enable these financial activities. Finally, Blockchain 3.0 includes all "applications beyond currency, finance, and markets — particularly in the areas of government, health, science, literacy, culture, and art" [Swan M., 2015: 51].

These three types of applications (Blockchain 1.0, 2.0 and 3.0) can be developed freely on most blockchains.

[19] Available at: https://www.dash.org (accessed: 04.05.2019)

2. Challenges to Competition

Blockchain sets two main types of competition challenges: it complicates both the characterization of dominant market positions and the attribution of liability for anticompetitive practices. This is particularly concerning because anticompetitive practices are expected on blockchain, as demonstrated below by analyzing how and why monopolization practices might be implemented on it.

2.1. Characterization of a Dominant Position on the Relevant Market

The definition of a relevant market is a tool to set the boundaries of competition between firms by taking into account their material and geographical dimensions. Setting the boundaries of the relevant market can be challenging.

Blockchain raises important questions about what exactly a dominant position is. And because decentralized organizations like blockchain are not recognized as legal entities [De Filippi P., Wright A: 2018: 209], many issues arise. Can a non-entity hold a dominant position? Can blockchain create a "monopoly without a monopolist?" [Huberman G., 2017: 2]. Finally, if a blockchain is dominant in a market, which users and/or entities hold that dominant position?

Unless an entity holding a dominant position is deemed fully liable for all the practices implemented within it, liability will be attributed in different ways that depend on how a dominant position is characterized. The same is true for blockchains: the way in which the dominant position is characterized will determine the scope of liability.

A number of characterizations of dominance could be applied to blockchains. As far as the material dimension of relevant markets is concerned, different theories of liability are conceivable.

The first theory of liability would be to consider that each blockchain — as a general ledger on which transactions are registered — would hold a dominant position in and of themselves. If this were the case, all users of the blockchain would be considered co-holders of this dominant position. In practice, however, it would be illogical to consider all blockchain platforms as having a dominant position while attempting to prevent the implementa-

tion of anticompetitive practices by a fraction of their users. Applying this definition of a market would very significantly reduce the incentive to use blockchains because unwitting users could be held liable for practices performed by third parties unknown to them. Therefore, this first way of defining dominant positions should be rejected.

A second theory would assess market power based on the type of applications (products and services) that run on the blockchain as layer 2[20]. The type of blockchain (1.0, 2.0 or 3.0), which are different strata of smart contracts [Raskin M., 2017: 305], would then be at the center of a market definition that takes into account the two—sided nature [Rochet J.-C., Tirole J., 2003: 990] of the market by analyzing the functioning of applications. In particular, a layer 1 blockchain as a platform would be part of a different market because it does not compete with a layer 2 application.According to this approach, a blockchain's market power would be assessed in comparison with other digital products or services and potentially with non-digital alternatives. As a result, blockchain power would be evaluated the same way online sales can be integrated into the general sales market (including physical sales).

Such a characterization of a dominant position would make it possible to impute liability only to users who offer, run, or use a dominant application that has implemented an anticompetitive practice. This would then allow antitrust authorities to make a distinction between three key players on the blockchain: developers, users, and miners, depending on who commits the anticompetitive practice.

However, this fails to answer the question of which elements to take into account in order to evaluate the relative market power of different blockchains running the same type of applications: the number of users, the number of transactions recorded, the number of blocks, or the revenues, etc. In its Google decision, the court noted that the European Commission used market shares by volume as a proxy for several reasons. "First, market shares by value cannot be computed because general search services are provided free of charge to the user. Second, despite its best efforts, the Commission has been unable to obtain precise and verifiable values regarding the Rev-

[20] A further distinction would be made on whether the blockchain allows the realization of a service taking place outside of the technology, or whether it provides a service within the blockchain. In the first case, it will have to be determined whether the blockchain can be integrated into a wider market — as is the case, for example, with online sales that can be integrated into the general sales market (including physical sales). In the second case, only competition between blockchains would have to be evaluated.

enue Per Search ("RPS") of the main general search services. Third, advertisers look at usage shares when deciding where to place their search advertisements" [Schrepel T., 2019: 275].

In assessing the geographical reach of the relevant market, it should be emphasized that, although the language used on a blockchain is universal, some applications may be focused on a local market while others may compete at an international level. Only a case-by-case analysis is possible here.

In short, evaluating the market power of a blockchain network creates new challenges, one of which is the lack of a central power needed to urge the majority of blockchain users to adopt changes, a characteristic which greatly mitigates the idea of "power"[21].

2.2. Abuse of Dominance

This section focuses on the different types of unilateral practices (exploitation, exclusion, and discrimination) which may occur with blockchains. Before analyzing these unilateral practices in greater detail, two common trends are worth highlighting.

All information and transactions recorded on public blockchains are, to some extent, visible by all[22]. With regard to private blockchains, the transactions are visible only to their users if they are designed that way[23]. As a result, the number of anti-competitive practices may be lower on public blockchains than in other tech markets, precisely because public blockchains create greater transparency between users.

[21] This is seen, for instance, with Ethereum, which has to convince its own users to adopt upgrades to the software. See: *Kim C.* Ethereum upgrades as hard forks activate on blockchain, *coindesk*. 28 February 2019. Available at: https://www.coindesk.com/ethereumupgrades-as-hard-forks-constantinople-and-st-petersburg-activate-on-blockchain (accessed: 24.05.2019). Note that when a blockchain is changing its functioning rule, such as the protocol consensus, all blocks validated according to the new rules are seen by the blockchain software as being invalid. For that reason, all nodes need to upgrade their software to the new rules.

[22] Most of the data put in the blockchain is encrypted so that only people with the right keys can decrypt it. However, the "visible effect" remains the rule and the protocol design is visible by all. Therefore, when anticompetitive practices are set up in the blockchain, that information is visible. Only the manifestation of that practice may be encrypted.

[23] Privacy-oriented blockchain-based cryptocurrencies widely use «zero knowledge proof,» which provides trust. Trust in the system is also ensured by the fact that transactions are visible by all users. The more there are, the more trust there is in the blockchain and the higher its utility. It is therefore uncertain whether private blockchains will, in the future, make transactions non-visible.

Accordingly, it is to be expected that, because transactions can be viewed by all users on the blockchain, this inherent transparency tends to prevent anti-competitive practices and reduce their occurrence. But vigilance is required because unilateral practices will not entirely disappear due to a second pattern in blockchain known as the "opacity effect." On a blockchain, all transactions are encrypted [Werbach K., 2018: 45], and the identity of blockchain users is protected by pseudonyms. As a result, a transaction may be visible, but the nature and purpose of the transaction are unknown to outsiders, and this makes the interaction between users more opaque. This "opacity effect" is even stronger on private blockchains where the content of the blockchain is kept hidden from outsiders.

To demonstrate which unilateral practices could be implemented on blockchain, suppose that company Y is operating in a digital market. Y decides to diversify its activities and creates a private blockchain to do so. Y designs the blockchain so that Y can choose which users may access the blockchain, which operations the users can perform on it, and which protocol will govern the blockchain. Y has the power to change these settings at any time. To generate revenue, Y has developed a new professional social network called BlockJobs that operates as a layer 2 on its blockchain. BlockJobs enables users to post job offers and/or to apply for them. At each stage of the recruitment process — from the first interview to the acceptance or refusal of an offer — a smart contract is recorded on the blockchain. Everything is conveniently automated, but the registration of each of these transactions has a cost that its users looking for candidates pay with tokens. After a while, this application attains great success, and Y realizes that some of its competitors are using BlockJobs to recruit candidates that will enable them to better compete with Y. In response, Y implements an anticompetitive strategy and might adopt such practices as refusal to deal, tie-in-sales, predatory pricing, margin squeeze or exclusive dealing and rebates.

2.2.1. Exclusionary Abuse Practices

2.2.1.1 Refusal to Deal

Article 102 of the Treaty on the Functioning of the European Union (TFEU), which prohibits the abuse of dominant position, can be triggered when a monopolist refuses to deal with a competitor. Although a company

generally has no duty to deal with its rivals, the European Court of Justice has found antitrust liability when a monopolist refuses to sell a product to a competitor although it made that product available to others.

Refusal to deal is a common practice outside of blockchains, but it should be rarer in them, at least when it comes to public blockchains. A refusal to grant access to a blockchain would have to be implemented in its governance design, although by definition a public blockchain is coded to allow public access. No deliberate or exclusive selection of users is possible. As a result, the refusal to deal can be made possible only by modifying the access rules themselves. Exclusionary strategies are therefore incompatible with the inherent nature of public blockchains, and the blockchains that implement them would no longer be considered public ones.

In contrast, the refusal to grant general access is an essential characteristic of private blockchains[24]. Within such permissioned blockchains, the gatekeeping mechanism may take various forms (e.g. preventing a competitor from accessing blockchain information, proposing or registering new transactions, validating the blocks, etc.) and can be managed by different types of actors depending on the governance choices. For instance, a "[r] refusal to access the blockchain might be used to exclude maverick firms or new entrants" and, in general, to "exclude or raise the costs of rivals outside of the consortium"[25]. In order to illustrate a situation of refusal to deal (not allowing an entity to join a blockchain community), imagine that a blockchain exists among European banks for interbank payments. There may exist another way — the old way — of clearing interbank payments that is valid but slow and costly in comparison. If a new bank wanted to set up business in Europe, being a member of the blockchain may be necessary if it intends to become a competitive force. If the new bank is refused access or membership without justifiable grounds or on a cost basis that is not objective and reasonable, this might constitute an abuse[26] within the meaning of Article 102 of the TFUE.

[24] See note 5.

[25] OECD. Blockchain technology and competition policy (2018). Paper by the Secretariat. Available at: https://one.oecd.org/document/DAF/COMP/WD(2018)47/en/pdf (accessed: 03.05.2019)

[26] *Desal K*. Blockchain and competition law, Ernest&Young Law Alert, EU competition law April 2018. Available at: https://www.ey.com/Publication/vwLUAssets/ey-blockchain-and-competition-law/$FILE/ey-blockchain-and-competition-law.pdf (accessed: 3.05.2019)

If a permissioned blockchain attains the status of essential infrastructure and if refusal to give access to it is not properly justified, the exclusionary efforts of the gatekeepers also risk violating Art. 102 of the TFEU[27].

2.2.1.2. Tying/Bundling

Tying or bundling is the practice of making the sale of a product (or service) conditional on additional sales or obligations[28]. Tying may also entail subjecting a contract to the acceptance of supplementary obligations that have no connection with the original subject of the contract.

Tying or bundling is unlikely to occur in public blockchains because by definition they can be freely accessed or used. Making conditional its use to the purchase of a product is therefore unlikely.

On the other hand, private blockchains may that are created by for-profit companies have an interest in imposing tying or similar practices. Bundling may occur if an undertaking links the use of a blockchain (specializing, for instance, in mining a particular cryptocurrency's tokens) to ancillary services (e.g. a digital wallet or exchange service) which are offered outside the blockchain and in which the undertaking holds a dominant position. Tied sales are to be expected on private blockchains.

2.2.1.3. Predatory Pricing

Attempting to drive a smaller competitor out of a market by systematically undercutting its prices is another anticompetitive practice[29]. Pricing

[27] *Ristaniemi M.* & *Maicher K.* Blockchains in competition law-friend or fore? Kluwer Competition Law Blog, July 21, 2018. Available at: http://competitionlawblog.kluwercompetitionlaw.com/2018/07/21/blockchains-competition-law-friend-foe/?print=pdf [accessed: 19.04.2019]

[28] For an overview of tying, see Case 3/37.792, *Microsoft Corp*., Comm'n Decision (Apr. 21, 2004). For American cases, see *Jefferson Parish Hosp. District No. 2* v. *Hyde*, 466 U.S. 2, 1 (1984); *United States* v. *Microsoft Corp*., 253 F.3d 34 (D.C. Cir. 2001). Though the U.S. seemed to adopt the rule of reason after Illinois *Tool Works Inc.* v. *Independent Ink*, *Inc.*, 547 U.S. 28 (2006), "the general per se rule for tying arrangements when market power is present very likely still survives," per Hovenkamp H. The Rule of Reason, *Florida Law Review,* vol. 70, pp. 81, 96. For more on bundling, see *Economides N., Lianos I.* Elusive Antitrust Standard on Bundling in Europe and in the United States in the Aftermath of the Microsoft Cases. *Antitrust Law Journal,* vol. 76, p. 483.

[29] In the European Union predatory pricing is considered abusive if the prices charged by the dominant undertaking are below average variable costs or if the prices charged by the dominant undertaking are below average total costs and they are set as part of a plan for eliminating a

for blockchains typically takes the form of costly transaction fees when a user is submitting a transaction to be registered in the chain. Predatory pricing is very unlikely on public blockchains because it would be possible only if enough users could be persuaded to change the governance structure to accommodate such a change.

The situation could be quite different for private blockchains. For example, a large block validator or a mining pool might set transaction fees below cost in order to eliminate a rival cryptocurrency, or it might cross-subsidize certain key merchants and suppliers in order to prevent a competing cryptocurrency from reaching an efficient scale and generating enough profit to enter the market. These practices may be successful as they will not usually require the dominant undertaking to sacrifice profits. The predatory pricing test according to which if the prices charged by the dominant undertaking are below average variable costs and are set as part of a plan for eliminating competitors, would then apply.

2.2.1.4. Margin Squeeze

Another related practice occurs when a vertically integrated dominant company operates on upstream and downstream markets and sets the upstream price high enough so that companies are unable to sustainably compete in the downstream market[30].

In contrast to private blockchains, public blockchains are by definition horizontal. It is therefore very unlikely for a margin squeeze to be imple-

competitor. See Case C-202/07 P, *France Télécom* v. *Comm'n*, 2009 E.C.R. I-2369. In the United States, in order to establish predatory pricing, the plaintiff must show below-cost pricing and a dangerous probability of recoupment by the monopolist once the rival has been driven from the market. See *Brooke Group Ltd. v. Brown & Williamson Tobacco Corp*., 509 U.S. 209, 223—24 (1993).

[30] Commission of the European Communities. Guidance on the Commission's enforcement priorities in applying Article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings. 3 December 2008. Available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52009XC0224%2801%29 (accessed: 4.05. 2019). This states that margin squeeze occurs when a dominant undertaking may charge a price for the product on the upstream market which, compared to the price it charges on the downstream market, does not allow even an equally efficient competitor to trade profitably in the downstream market on a lasting basis.

See also: Case C-52/09, *Konkurrensverket* v. *TeliaSonera Sverige AB* 2011 E.C.R. I-527; Case C280/08 P, *Deutsche Telekom AG* v. *Comm'n* 2010 E.C.R. I-9555; and Case C-295/12, *Telefónica* and *Telefónica de España* v. Comm'n 2013 E.C.R. 619. In the United States, a margin squeeze does not constitute an independent cause of action under Section 2 of the Sherman Act. See: *Pac. Bell Tel. Co.* v. LinkLine Commc'ns, Inc., 555 U.S. 438 (2009).

mented on public blockchains. The case is different, however, for private blockchains. Because they allow income-generating applications while maintaining a financial interest in the platform layer, one can imagine that a strategy of margin squeezing could be implemented. Doing so would require that the dominant company — here the blockchain gatekeeper — changes the price it charges in the upstream market (i.e. the blockchain platform). In the development phase of a blockchain, such a strategy seems unlikely, but the potential for it means that it will have to be closely monitored in the years to come.

2.2.1.5. Exclusive Dealing

Another practice which falls under the prohibition in Article 102 of the TFEU consists in the requirement that a supplier with monopoly power over its customers not make abandoning a competitor's blockchain a condition for use of its blockchain to complete transactions[31].

Terms to that effect could be included in the user agreement to be signed before using the blockchain[32]. It seems unlikely that such exclusive dealing will be imposed on a public blockchain because it would entail incorporating exclusionary terms from the start. Moreover, once a transaction is registered on a blockchain, users have little interest in registering the transaction on another blockchain because doing so is costly. The technology itself reduces the incentive to use several blockchains for the same transaction.

The situation is quite different for private blockchains. Foreclosing competitors is an efficient way to increase the overall blockchain price to users and developers. Moreover, private blockchains have an interest in increasing their level of attractiveness by obtaining data that they alone can provide. In the BlockJobs illustration, Y may want to be the only company listing a certain type of job offer. BlockJobs therefore might want to impose exclusive

[31] For an overview of exclusive dealing, see: Case T-155/06, *Tomra Sys. ASA & Others* v. *Commission* 2010 E.C.R. II-4361, and Case C-413/14 P, *Intel Corp.* v. Commission, 2017 E.C.R. 632. In the United States, exclusive dealing may constitute a violation of Section 2 of the Sherman Act if it forecloses competitors from accessing the market. The D.C. Circuit held that "a monopolist's use of exclusive contracts, in certain circumstances, may give rise to a § 2 violation even though the contracts foreclose less than the roughly forty percent or fifty percent share usually required in order to establish a § 1 violation." *United States* v. *Microsoft Corp*., 253 F.3d 34, 70 (2001).

[32] For an example, see: Ethereum Foundation. Legal Agreement on the Ethereum.org website. Available at: https://www.ethereum.org/ (accessed: 18.05.2019)

dealing at the entry point of its blockchain. For this reason, it is very likely that exclusive dealing practices will be implemented on private blockchains.

2.2.1.6. Rebates

Yet another related practice is to grant retroactive rebates or rebates that are contingent on a customer obtaining all or most of its goods or services from the dominant actor[33]. Because all practices are recorded and visible on public blockchains, one user's discount will be visible to all and granting loyalty rebates or discounts could lead to pushback from users who do not benefit from such a discount. This is more likely to occur if such benefits are perceived as unjustified by other users. Public blockchains push for equal treatment of all users when there is no reason to differentiate among them.

Private blockchains do not necessarily benefit from this "visibility effect" because they can determine what information is visible to each user. They may also have a greater commercial incentive to attract reputable users by offering discounts. In the BlockJobs example, Y may want to give a discount on transaction registration fees to some big users. Rebates are, therefore, expected to be employed on private blockchains.

2.3. Exploitative Abuses

Exploitative abuses could be implemented on a blockchain by directly or indirectly imposing unfair conditions on existing customers or suppliers[34]. An exploitative abuse could occur when blockchain creators provide

[33] For an overview of loyalty rebates, see: Case C-413/14 P, *Intel Corp.* v. *Comm'n*, 2017 E.C.R. 632; Case 85/76, *Hoffmann-La Roche and Co. AG* v. *Comm'n*, 1979 E.C.R. 461; Case T-228/97, *Irish Sugar* v. *Comm'n*, 1999 E.C.R. II-2975; and Case T-219/99 *British Airways* v. *Comm'n*, 2003 E.C.R. II-5925. In the United States, discount and rebate scheme programs can violate Section 2 of the Sherman Act. See *LePage's Inc.* v. *3M*, 324 F.3d 141, 157 (3d Cir. 2003); *Cascade Health Sols.* v. *PeaceHealth*, 502 F.3d 895, 905 (9th Cir. 2007); *Eisai Inc.* v. *Sanofi-Aventis U.S.*, Civil Action No. 08-4168, 2014 WL 1343254 (D.N.J. Mar. 28, 2014).

[34] Article 102(a) of the Treaty on the Functioning of the European Union (TFEU) refers to the imposition of unfair purchase or selling prices as well as other unfair trading conditions. Consolidated Version of the Treaty on the Functioning of the European Union art. 102(a), 2008 O.J. C. 115/47. See Case COMP/38.636, Rambus Inc., 2010 O.J. C 30 (the Commission had to deal with potentially abusive royalties for the use of patents).

Such abuses could be created by the creation of a dual blockchain environment, one for those who pay the most and one for those who pay less and whose transactions may lag behind as a result.

services in exchange for preferential treatment[35] or when one blockchain imposes unfavorable measures on another blockchain. In the BlockJobs example, users who are unwilling to pay to gain visibility will face unfair conditions such as preventing them reading information on the blockchain, forbidding them from proposing news transactions on the blockchain or keeping them from validating blocks. However, because blockchain is still evolving rapidly, there is little use in focusing too much attention on exploitative abuses. The dynamism of the blockchain environment will likely correct these abuses themselves. This type of abuse is nonetheless possible and will undoubtedly be litigated.

2.4. Discriminatory Abuses

Discriminatory abuses occur when parties apply "dissimilar conditions to equivalent transactions with other trading parties, thereby placing them at a competitive disadvantage" [O'Donoghue R., Padilla J., 2013: 795][36]. These abuses are practiced in various ways, although price discrimination is the most common[37]. According to Judge Richard Posner, "price discrimination is a term that economists use to describe the practice of selling the same product to different customers at different prices even though the cost of sales is the same to each of them. More precisely, it is selling at a price or prices such that the ratio of price to marginal costs is different in different sales" [Posner R., 2001: 79–80].

[35] Østbye P. The adequacy of competition policy for cryptocurrency markets. Aug. 24, 2017. Available at: https://www.google.com/search?ei=aRn9XJ7QLoKwrgTI1KPgCw&q=%C3%98stbye+P.+The+Adequacy+of+Competition+Policy+for+Cryptocurrency+Markets+%28Aug.+24%2C+2017%29%2C&oq=%C3%98stbye+P.+The+Adequacy+of+Competition+Policy+for+Cryptocurrency+Markets+%28Aug.+24%2C+2017%29%2C&gs_l=psy-ab.3...42761.43832..44723...1.0..0.86.86.1.....0....1j2..gws-wiz.....6..35i39.021KJ8SPffc (accessed: 17.05.2019)

[36] See TFEU Art. 102(c) and 2008 O.J. C. 115/47.

[37] In European judicial history, there are few cases in which price discrimination alone was found abusive. See Case T-301/04, *Clearstream Banking AG* v. Comm'n, 2009 E.C.R. 317 (referring to anticompetitive foreclosure when an 'as efficient competitor' cannot compete effectively with the price of the dominant undertaking); see also C209/10, *Post Danmark A/S* v. *Konkurrenceråd-det*, 2012 E.C.R. 172, (ECJ clarifying that where prices are below average total costs while being above average incremental costs, a finding of abuse requires a demonstration of actual or likely exclusionary effects). In the United States, price discrimination by a monopolist violates Section 2 of the Sherman Act only to the extent that it is predatory or otherwise excludes competitors from the relevant market. See *Blue Cross & Blue Shield United of Wis*. v. *Marshfield Clinic*, 65 F.3d 1406, 1413 (7th Cir. 1995). Price discrimination may also violate the Robinson-Putman Act. See *Brooke Group Ltd*. v. *Brown & Williamson Tobacco Corp*., 509 U.S. 209, 220 (1993).

Because price discrimination involves favoring certain customers over others, it generally occurs in two ways: charging different customers different prices for the same product, or charging only some customers the same price for different products.

Because of the "visible effect"[38] of public blockchains, occurrences of price discrimination will be limited. However, within private blockchains users may encounter discriminatory terms because the application of different terms to different users is an effective way to urge users to join and use a blockchain. Discriminatory pricing can incentivize some users to stay active on the blockchain by offering lower prices, thus creating a potential discrimination claim for others. Accordingly, discriminatory abuses are more likely to happen on private blockchains. In the BlockJobs example, Y may initiate discriminatory terms to thank a user for a commercial advantage granted in another market. Once again, private blockchains will be at the center of focus.

Conclusion

This paper has outlined several anticompetitive practices. Most of the usual antitrust instruments will be ineffective against public blockchains[39] because antitrust law does not provide complete answers to three questions: how are anticompetitive practices committed on public "permission-less" blockchains to be detected; how is the economic operator responsible for these practices to be identified; and, finally, how are they to be remedied in the future. While the perpetrator of an anticompetitive practice on a blockchain can sometimes be identified, the effectiveness of sanctions and remedies may be hindered by the immutability of the blockchain[40].

The situation is different for private permissioned blockchains. On this type of blockchain, antitrust issues such as refusal to deal, margin squeezing or predatory pricing most often when an interested competitor is refused access. Although there may be legitimate business justifications to exclude a rival, adhering to several best practices will minimize antitrust risk. The reasons for membership criteria should be well documented and well defined,

[38] See note 24.

[39] *May T.* The Crypto Anarchist Manifesto. Available at: https://www.activism.net/cypherpunk/crypto-anarchy.html (accessed: 17.05.2019)

[40] Guegan *D.* Op. cit.

and they should point to procompetitive justifications. Criteria should also not be so narrowly defined that they could be construed as purposely excluding a certain competitor or set of competitors. When applying membership criteria, owners of the blockchain should not treat similarly situated competitors differently. Reasons for expulsion should be defined and known to all members. Finally, reasons for the removal of any member should be well documented and fall within the established criteria for expulsion outlined at the formation of the blockchain.

Another competition concern linked to the use of a private blockchain pertains to the type of consensus mechanism it opts for. An owner, operator or its designee that serves as the membership "gatekeeper" may have the ability to control how data disputes are resolved. It also may restrict which participants have the right to read, edit or fix discrepancies. These procedural rules potentially allow exclusionary practices to occur within the blockchain. The owner, along with the designated participants, may agree to disadvantage certain competitors.

By resolving discrepancies using a pre-set, objective consensus mechanism, such as proof of work, no single participant can control how a discrepancy is resolved. This reduces the likelihood that discrepancies will raise competitive issues, for example, based on favoritism or as a result of collusion among rival members. If a different system must be deployed, discrete parameters should be established explaining how the designated participants must resolve the discrepancy. Such a system could include, for example, having discrepancies or disputes resolved by a rotating, random set of participants[41].

Another challenge to overseeing competition in the use of blockchain lies in the enforcement by centralized regulators, such as the US Department of Justice, the US Federal Trade Commission or the European Commission, of the vertically designed rules and concepts of antitrust law to a technology built around the desire for decentralization [Werbach K., 2018: 487]. Hence, the need to find new ways of decentralizing antitrust law and antitrust authorities [Freedman M., 1962: 202], through the design [Cuccuru P., 2017: 179] and the implementation of new governance models using blockchain [Abramowicz M.,: 2016: 359,420].

[41] Thomas R. Op. cit., p.13.

References

Abramowicz M. (2016) Cryptocurrency-Based Law. *Arizona Law Review*, no 2, pp. 359, 420.

Bork R. (1978) *The Antitrust Paradox: A Policy at War with Itself*. New York: Basic Books, p. 462.

Bradley R., Summers L. (1990) On The Origins of the Sherman Act. *The Cato Journal*, no 3, pp. 737, 740.

Champagne P. (2014) *The book of Satoshi: The collected writings of Bitcoin creator Satoshi Nakamoto*. Plano: Publishing LLC, p. 136.

Cuccuru P. (2017) Beyond Bitcoin: An Early Overview on Smart Contracts. *International Journal of Law & Information Technology*, 2017, no 3, p. 179.

Dannen C. (2017) *Introducing Ethereum and Solidity: Foundations of Cryptocurrency and Blockchain Programming for Beginners*. New York: Apress, p. 185.

De Filippi P., Wright A. (2018) *Blockchain and the Law: the Rule of Code.* Boston: Harvard University Press, p. 209.

Devlin A. & Jacobs M. (2012) Anticompetitive Innovation and the Quality of Invention. *Berkeley Technology Law Journal,* no 1, pp. 1–53.

Economides N., Lianos I. (2010) Elusive Antitrust Standard on Bundling in Europe and in the United States in the Aftermath of the Microsoft Cases. *Antitrust Law Journal*, vol. 76, p. 483.

Ernst D. (1990) The New Antitrust History. *New York Law School Law Review*, no 35, p. 879.

Freedman M. (1962) *Capitalism and Freedom*. Chicago: University of Chicago Press, p. 202.

Hawk B (2018) English Competition Law before 1900, *The Antitrust Bulletin,* no 1, p. 19.

Huberman G. (2017) Monopoly Without a Monopolist: An Economic Analysis of the Bitcoin Payment System, *Columbia Business School Research Paper*, no 17–92, p. 2.

Kaiser H. (2011) Are “Closed Systems” an Antitrust Problem? *Competition Policy International,* no 7, pp. 91, 102–103.

Kreps D., Wilson R. (1982) Reputation and imperfect information. *Journal of Economic Theory*, no 2, p. 253–279.

Markovits R. (2014) Economics and the Interpretation and Application of U.S. and E.U. Antitrust. *The Antitrust Bulletin*, no 59, pp. 3, 19.

O’Donoghue R., Padilla J. (2013) *The Law and Economics of Article 102 TFEU*. Oxford: Hart, p. 795.

Popper N. (2016) Digital. *Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money.* New York: Harper, p. 412.

Posner R. (2001) *Antitrust Law*. Chicago: University of Chicago Press. p. 304.

Posner E., Weyl G. (2018) *Radical Markets: Uprooting Capitalism and Democracy for a Just Society.* Princeton: Princeton University Press, p. 368.

Raskin M. (2017) The Law and Legality of Smart Contracts. *Georgetown Law Technology Review,* no 1, p. 305.

Raval S. (2016) *Decentralized Applications: Harnessing Bitcoin's Blockchain Technology.* Sebastopol (Cal.): O'Reilly Media, p. 106.

Rochet J.-C., Tirole J. (2003) Platform Competition in Two-Sided Markets*. Journal of the European Economic Association,* no 4, p. 990.

Schrepel T. (2018) Predatory Innovation: The Definite Need for Legal Recognition. *Science & Technology Law Review,* no 21, p. 22.

Schrepel T. (2018) Antitrust conversations with Nobel laureates. *Concurrentialiste Review,* no 1, p. 15.

Schrepel T. (2019) Collusion by Blockchain and Smart Contracts. *Harvard Journal of Law & Technology,* no 1, p. 118.

Swan M. (2015) *Blockchain: Blueprint for a New Economy.* Sebastopol (Cal.): O'Reilly Media, p. 131.

Tapscott D., Tapscott A. (2016) *A Blockchain Revolution: How the Technology behind Bitcoin is Changing Money, Business and the World.* New York: Random House, p. 358.

Tsu S. (2017) *The Art of War*. London: Macmillan, p. 152.

Vigna P., Casey J. (2018) *The Truth Machine: the Blockchain and the Future of Everything*. New York: St. Martin's Press, p. 302.

Walch A. (2017) The Path of the Blockchain Lexicon (and the Law). *Review of Banking & Financial Law*, no 36, p. 713.

Werbach K. (2018) *The Blockchain and the New Architecture of Trust.* Cambridge (Mass.): MIT Press, p. 344.

Werbach K. (2018) Trust, but Verify: Why the Blockchain Needs the Law. *Berkeley Technology Law Journal,* no 33, p. 487.

Digital State, Digital Citizen: Making Fair and Effective Rules for a Digital World

Nikolay Dmitrik

Laboratory for legal informatics and cybernetics, Law Faculty, Lomonosov Moscow State University, Candidate of Juridical Sciences. Address: 1–13 Leninskie Gory, Moscow 119991, Russia. E-mail: dmitric@mail.ru

Abstract

The world is connected — governments, business and people are increasingly living and working in a globally connected digital space. People no longer identify themselves as belonging to spatial communities (neighborhood, town, city or country) but by subscribing to digital ecosystems like Apple or Android, Facebook or VKontakte, etc. Governments use digital platforms at the local, regional and national levels to administer certain powers and procedures (even electoral campaigns) and to get feedback from their citizens. As citizens become digital citizens — connected to a wide range of internet resources including electronic government, banking, local management systems, as well as to social media and global internet companies such as Google and Yandex — they simultaneously become subject to rights, rules, laws, and regulations locally and globally. But what are those rights and rules and what do they entail? Who has the responsibility of ensuring that all citizens have equal access to them and are protected from exploitation? What governs the way that global and local digital businesses operate? The article discusses the exercise and protection of rights in online and offline ecosystems in Russia with special attention given to enabling participation by citizens and to multiple stakeholders online and offline. The recommendations and conclusions here may be applicable to all countries experiencing digital transformation.

Keywords

Digital inequality; digital ecosystem; human rights online; privacy; private lawmaking; sovereignty.

For citation: Dmitrik N. (2020) Digital State, Digital Citizen: Making Fair and Effective Rules for a Digital World. *Legal Issues in the Digital Age,* no 1, pp. 54–78.

Introduction

The world is going through the Middle Ages again. Barbarian tribes have invaded the cosy world of our industrial *poleis* and brought along their own

rules and values. The digital Middle Ages have weakened states, led to the creation of guilds, and countered science with fakery. Fortunately, we know that these Middle Ages will be followed by an Enlightenment. There is only one thing that cannot be predicted. When the Middle Ages are over, will we be subjects or citizens? The answer to this question depends on the strategy that we, the people, choose now. For Russia, which is the principal focus of this article, the main factor in this choice is the interests of various actors. If their interests are or will be merged, i.e. efficiently restrict each other, we have a chance at citizenship. If not, then the main actors can act at will, and we will probably be ruled by a digital monarchy.

In order to analyze the current system of interests and possible ways of transforming it, of managing the transition from the digital Dark Ages to the Enlightenment, three main elements must be taken into account:

1) technological, social, and economic factors and risks of transformation;

2) transformation of states and state-made laws;

3) multinational corporations and their role in shaping social rules.

The analysis of these three elements will allow us to choose the tools and forms of democratic participation by the people — as digital citizens of digital states — in the development of fair and efficient rules for the new digital world.

1. Digital transformation and the risks it brings

Digital transformation has been analyzed in many scientific papers. For the purposes of this article, it is important to identify the main elements and factors of digital transformation and how they influence each other. Special attention is also given to the impact of digital transformation on the two main subjects of current citizenship relations: the state and the individual. For this purpose, digital transformation can be visualized as a pyramid (fig. 1) based on changes in the technologies whose use is transforming society. Those changes affect each layer above in turn until all of them affect us directly.

Technology is the first layer. Transformation is not pre-determined by technologies, and there is an important question about who will be pushing for transformation and who will be pulled along in its wake. To understand this, we should identify whose interests are fulfilled through the implementation of new technologies.

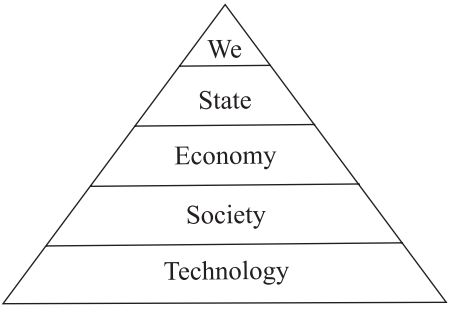

Fig. 1. Layers of the transformation pyramid

The present transformation was made possible by the synergistic effect of four technologies: cloud computing, mobile technologies, social networks, and big data [Prokhorov A., Konik L., 2019]. Users of the growing number of mobile devices produce more and more content that can be stored conveniently and cheaply in cloud services. Cloud services facilitate content sharing between users of different mobile platforms regardless of national boundaries. The growth in the volume of content makes new mobile devices and platforms attractive and requires additional cloud storage. The accumulated data "lands" on social networks, making it possible to analyze information from those networks and manage it using big data technologies. The accumulated data is used in turn for advertising and increasing the user value of new mobile services and platforms.

At the societal level, the virtual realm becomes a new kind of spatial one because these two competing environments — online and offline — provide the space for transformation. The virtual world is a new territory, and actual physical territory is the only thing it lacks. People become more a part of virtual communities than of what were formerly the "real" ones: our home communities, neighborhoods, cities or countries. The fate of Hollywood actors engrosses Russians more than the fate of their neighbors. The opinion of a friend on Facebook, wherever they may be, is more important than the opinion of a classmate. People easily entrust their lives to a Gett driver and distrust a prescription written by a doctor at a local clinic.

One after another, borders that separate different countries and cultures from each other are crumbling. Airplanes have made visiting anywhere in the world possible within a day or two. The internet has made any information available within seconds. Online education allows people in one place

to develop the competencies that are in demand in another. The last barrier — language — is going to fall: people are beginning to understand each other regardless of the languages they speak. State borders are only in our minds and not exist in reality. No one now cares about the boundaries of the Empire of Timur or the Roman Empire; they died out together with those who remembered them.

The virtual world has become the main source of trust in Russian society. Russian people do not trust the police, their neighbors or the government; but they do entrust the most valuable things — their social lives, opinions and money — to the social networks, the cloud and online financial services respectively[1]. What was spatial in the past has definitely become virtual now — identity, mobility, trust. Throughout the 20th century, the source of these things was the City. Neighborhood, factory, school, Institute, clothing style, favorite restaurants formed an identity. Metro lines and city avenues created mobility. Belonging to a team — a school class, an apartment building, or employees of the same organization — was a source of trust. All the same things since the beginning of the 21st century has been born by the virtual world[2], the Russian-language internet (Runet but in a completely different proportion. The change in the proportion between identity, mobility and trust in the transition from spatial to virtual communities is best seen in legal institutions such as privacy and personal freedoms (freedom of movement, freedom of economic and other activities), as well as in the management tools used to achieve both of them (fig. 2).

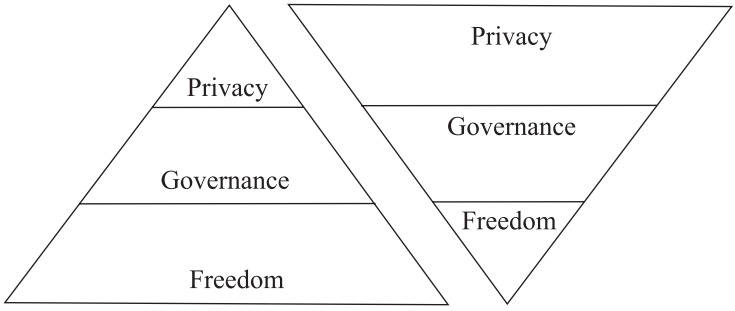

Fig. 2. Competing environments (online and offline)

[1] The Russian state is much worse than its people. Available at: URL: https://meduza.io/feature/2016/02/19/v-rossii-gosudarstvo-namnogo-huzhe-naseleniya (accessed: 05.01.2020)

[2] How the City will connect virtual and spatial. Available at: URL: https://www.kommersant.ru/doc/4094543 (accessed: 05.12.2019)

Big cities gave birth to privacy in the late nineteenth century [Warren S., Brandeis L., 1890: 193–220], but privacy is regarded as a dead issue for Internet [Holtzman D., 2006]; [Froomkin M., 2000: 1461]. There is very little freedom left in the urban environment with all its traffic rules, facial recognition cameras and neighbors in condominiums. The city is a normative environment that dictates how people live, what they wear, where they go at night, and what metro line to choose. The internet is by nature a realm of freedom, and that fact has been recognized even by the Russian government[3]. It is widely believed that the internet is difficult to regulate (there is still no specific law governing the internet in any of the post-Soviet countries). Russian cities, however, are strictly governed not only by appointing (not electing) mayors and city managers, but also through "smart" urban environments and infrastructure. The city and Runet substitute perfectly for one another. The better the internet is, the less people need to live in cities. The "smart" city is no city at all and could just as well be countryside. But a better urban environment is the key to shortening time spent online.

The world economy is experiencing the third wave of globalization [Straw W., Glennie A., 2012]. The second half of humanity — the poor for whom no technological innovations were available previously — has entered the world economy. Consumers of goods and services in the new economy are no longer limited to the middle class because they do not have to pay with money. As the world's population doubled over the past 50 years, the attention of consumers has become the main object of economic competition. Attention is a limited resource for consumers: an individual cannot use five phones and nine social networks while paying with twenty credit cards. Usually, one or two services in a particular field are used, which means that only few companies can become successful in each market. That is why harmful concentration in many sectors of the economy is the biggest risk for the so-called "attention economy" and why it has been identified by the World Bank as among the three main risks of the digital economy as a whole[4].

[3] Putin has proclaimed the importance of maintaining a free Internet. Available at: URL: https://iz.ru/865385/2019-04-08/putin-zaiavil-o-vazhnosti-sokhraneniia-svobodnogo-interneta (accessed: 05.12.2019)

[4] World Bank. World development report 2016: digital dividends overview (English). Available at: http://documents.worldbank.org/curated/en/961621467994698644/World-development-report-2016-digital-dividends-overview (accessed: 05.12.2019)

Money has stopped serving as a measure of value (almost everything is free in the digital world), and it is often no longer a source of motivation. The main value in this new world belongs to content provided by users for free. Nobody pays Wikipedia authors, free software developers (like Linux), bloggers, or even most online course lecturers. Judging by the amount of web content, Russian has been the second language of the internet for many years[5]. Within Russia, there are many websites in the traditional languages of the former Soviet republics (Tatar, Bashkir, Chuvash languages, etc.). Russians of all ethnicities have come together to create all of this because they felt that they were part of the new digital world and wanted to make it better.

Digital ecosystems (such as Google or Facebook) have become digital states with all the elements that were previously found only in a conventional nation state, although the ecosystems have them in a digital form. The digital state has the equivalent of laws (rules of a service or the digital platform's policies); a population (its users) that exceeds the population of any of the traditional states; and courts and law enforcement bodies (moderators). Soon digital ecosystems will have their own (digital) currencies like Libra and Gram.

With the advent of online ecosystems, even citizenship is no longer merely a relationship between two parties in which one (the citizen) has rights and the other (the state) has duties. In the Soviet Union, for example, the right to vote was exercised by a citizen directly to the state; the state created the conditions for the exercise of this right: it provided information, places and times for meetings with voters, as well as places for voting. Now the interaction of the citizen and the state at elections is accomplished through digital ecosystems, social networks, systems for identification and so on. Instances of fake news, election manipulation, and various internet petitions for certain changes or simply for the resignation of some officials show that the impact of the ecosystem on the state is much greater than the impact of the state on the ecosystem. Sometimes it can be said even that governance in Russia is carried out through these ecosystems rather than that the ecosystems are being governed by the state.

At the same time, it is increasingly difficult for the Russian state to position itself as necessary for the society. Electoral procedures are often re-

[5] Historical trends in the usage of content languages for websites. Available at: https://w3techs.com/technologies/history_overview/content_language (accessed: 05.12.2019)

placed by online surveys[6]. The Central Bank of Russia is working on an e-money project that will not require any supervision[7]. Blockchain and smart contracts can replace governmental registrars. There are more and more opportunities for decentralized governance in Russian society, but again only by resorting to digital ecosystems.

At the end of this brief description of digital transformation in Russia, it is necessary to focus on the risks associated with it. First, there are problems that Russia and other post-Soviet states must solve but cannot because these problems are global in nature. They are such problems as ecological degradation and diseases (epidemics like HIV, tuberculosis, malaria and polio as well as pandemics like COVID-19). The Russian state will have to recognize that it cannot address these issues alone and that it must begin to do so together with Russian society and other countries using new technologies and ecosystems.

Second, the digital transformation process is becoming a kind a digital rivalry for Russian people. It is still unclear whether Russians will be pushed into digital transformation or whether they can pull Russian government and business into it; whether Russian citizens will become the objects or the subjects of digitalization, or take part as consumers or stakeholders of digital ecosystems. Russians are at present almost entirely excluded from any discussions about their personal data (both in the courts[8] and in communities of experts who are developing new laws[9]), about access to the information on the internet, and about the rights and rules of digital ecosystems.

Finally, Russians are exposed to the same risks in digital transformation as people anywhere the world. These risks include:

uneven distribution of technologies (first of all, in medicine and education), many of which are inaccessible to poor people and small states;

[6] Active Citizen service in Moscow. Available at: URL: https://ag.mos.ru/home (accessed: 05.12.2019)

[7] Rapid Payments System. Available at: URL: https://sbp.nspk.ru (accessed: 05.12.2019)

[8] The courts have refused to recognize users as a third party in a lawsuit concerning the illegal use of data by Vkontakte, the largest Russian language social network. Available at: URL: https://roskomsvoboda.org/49260/ (accessed: 05.12.2019)

[9] Changes in Russia's Law "On personal data" are discussed among governmental bodies and businesses but without any participation by civil society. Available at: URL: http://sk.ru/foundation/legal/m/sklegal03/22237/download.aspx and http://sk.ru/foundation/legal/m/sklegal03/22236.aspx (accessed: 05.12.2019)

manipulation instead of personal autonomy whereby citizens are being manipulated by data, and the data employed to make decisions has been collected without regard for ethics, privacy and other rights;

vulnerability of Russian culture and the cultures of its national republics to other cultures, often more successful (like European model) or more aggressive ones (like radical Islam);

concentration of economic power in multinational companies, which are almost impossible to compete with and to regulate.

ecological and public health issues, which are in fact a cost incurred by the third globalization but which the state is trying to shift exclusively to its citizens.

These risks affect trust, which is the ultimate goal of digital transformation in Russia. The new virtual world that Russian people trust so much and so much want to trust[10] must not deceive them. It belongs to millions of Runet users, not to hundreds of thousands of hackers, not to thousands of officials and not to a bunch of mega-corporations. Russians have no other digital world; neither do our states and digital ecosystems. The value of the digital world is precisely that it is the same for all, and no one can go out and create their own. The only thing we can do is to work together to make it better.

No matter how the transformation takes place, its results must be reflected in the law. Law functions as a kind of DNA for society by reflecting accumulated changes and cutting away everything unnecessary and outdated. However, the main mechanism for creating law — the state — is itself undergoing a digital transformation. Therefore, in the next two sections of this article, we will consider the problems that states face in creating law and examine creation of law by multinational companies as one alternative.

2. States and law-making

The reality of the modern world involves a competition among legal systems because the subjects of law can to some degree choose where to live and conduct their business. There are two strategies for surviving competi-

[10] Paneyakh E. The death of state: Russian society between postmodern and archaic. Available at: URL: https://www.inliberty.ru/magazine/issue10/ (accessed: 05.12.2019)

tion. The first is to increase competitiveness, that is, to reduce costs (in the case of law we are, of course, talking about transaction costs) while increasing the utility of the product (we will assume that for law, utility is expressed in the protection of absolute rights, such as property rights and copyright). The second is monopolization, which permits higher costs and lower utility provided that subjects are not free to choose and —this is especially important for law — that they cannot leave the market.

Since the middle of the seventeenth century, states have enjoyed a monopoly on law-making [Backer L., 2007: 6]. This allowed law to disregard its own effectiveness, to raise transaction costs (for example, by allowing judicial proceedings to drag on for several years[11]) and assign a low priority to how useful it is. The main goal of legislation remains erecting barriers. There are external barriers such as national boundaries and the concept of sovereignty. External barriers protect an incumbent state from other competing states as well as from unwanted intrusions by international law. An example of an internal barrier would be the principle of legitimacy, which does not permit competing forms of law-making to exist within a single country (although there is an important qualification concerning federal and regional law-making powers).

In our era of globalization and the information society, monopoly leads both to localization (primarily of data) and balkanization as well as to extraterritorial application of laws. Attempts at localization are being made all over the world, including in the post-Soviet countries[12]. A total of 80 countries have legislation which contains localization requirements[13]. The prevalence of various restrictions on the location of data storage in the EU

[11] In 2014 the time to reach disposition for first instance civil and commercial suits ranged from 97 days in Lithuania to 532 in Italy, with an overall EU average of 250 days. Costs (comprising both lawyer billings and court fees) can sometimes be greater than the value of the claim. See: Fast-Tracking the resolution of minor disputes: Experience from EU member states. Available at: http://documents.worldbank.org/curated/en/670181487131729316/pdf/Fast-tracking-the-resolution-of-minor-disputes-experience-from-EU-Member-States.pdf (accessed: 05.12.2019)

[12] Decree of the President of the Republic of Belarus No. 60 1 February 2010 «On measures to improve the use of the national segment of Internet; Article 12 of the Law of the Republic of Kazakhstan 21 May 2013 No. 94-V «On personal data and their protection»; Part 5 of Article 18 of Russian Federal Law No. 152-FZ dated 27 July 2006 "On personal data". Numerous territorial restrictions on data storage are also contained in Russian Federal Law No. 149-FZ of 27.07.2006 "On information, information technologies and information protection".

[13] "InCountry tackles data localization laws with Data-Residency-as-a-Service platform". Available online at: https://diginomica.com/incountry-tackles-data-localization-laws-data-residency-service-platform (accessed: 05.12.2019)

has led it to reduce the number of territorial restrictions on data that is not personal because they were considered an obstacle to economic growth[14]. Balkanization is a term coined at the beginning of the twentieth century to refer to the collapse of a large state, its fragmentation and the formation of many hostile communities in its place [Todorova M.N., 1997: 33]. In digital terms, balkanization means dividing a global cyberspace which operates according to common rules into a collection of regional networks, each of which has its own standards and norms. States are the main force behind balkanization. But private companies also contribute to balkanization when they create incompatible ecosystems (such as Google and Amazon) and prevent people from using them together.

If localization and balkanization are brought to their logical conclusion, they will end in a digital serfdom in which each user will be tied to a place of production and consumption. Since the internet is the backbone of the modern economy, the entire economy will be localized and balkanized. A state that localizes its citizens will shore up its monopoly position by forcing their subordinate populations to follow its own rules, no matter how inconvenient (or ineffective) they may be. The good news, however, is that enslavement is not possible because of pre-existing competition, the need to reduce costs associated with it, and the effects of scale. In the balkanized Eurasian Economic Union, for example, a company will need to meet five different localization requirements and meet five different sets of standards and norms, while its market will not increase by more than a quarter compared to the Russian one. There are similar factors aligned against balkanization on a global scale. It would not make sense for an Asian company already operating in China, India and Indonesia to comply with EU anti-balkanization requirements because it will increase its market by no more than 10% accompanied by a possible doubling of costs. Localization and fragmentation are incompatible with economies of scale, which require openness and expansion. Thus, localization and balkanization cannot be used without negative economic consequences by states to avoid competition between legal systems.

Another aspect of the competition between legal systems is extraterritorial application of laws. Until recently, laws were connected with a territory — this was clear to everyone. However, the advent of the digital age and

[14] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union. Article 4.

attempts by states to maintain their monopoly on making the rules have led to interesting consequences.

The first step toward extraterritorial application of law was the New Public Management (NPM) concept that refers to a series of novel approaches to public administration and management that emerged in a number of OECD countries in the 1980s. The NPM model arose in reaction to the limitations of the old public administration in adjusting to the demands of a competitive market economy. The key elements of NPM were receptiveness to lessons from private-sector management and a focus upon entrepreneurial leadership within public service organizations [Osborne S., 2006: 377–388]. The related concept of the service state took multinational companies as a model from which to copy practices and technologies for governmental management, and it was spurred along by the competition between legal systems that was increasing in the context of the economic downturn. It was an Uber, so to speak, in the public administration market of the 1980s.

The more business management and public administration have converged, however, the more clear it becomes that companies do not have sovereignty the way states do. In other words, companies are not related to a territory in any way. "Citizenship" for companies always implies a contract (for supplies or employment or with customers). As a result, the territory that has always been useful to the state and been considered its main feature along with its population began to hinder it, to limit the sphere in which the state could become a monopoly, and to prevent its regulators from controlling multinational companies. States responded with an aggressive extraterritorial application of their laws.

The United States used many methods before the 1980s to expand its sphere of influence and to instill its values in other nations. By granting military and financial aid "with strings attached" the United States has attempted to influence other states' policies in the East-West struggle over human rights and in the development of nuclear weapons. Moreover, the United States has used its financial support of international organizations to further its policies including recognition of Israel and denial of aid to Vietnam and Kampuchea [Editors, 1984: 355]. Those actions were in line with the basic principle of international law that all states are equal as sovereigns and may not be coerced or controlled by foreign states[15]. Those actions remain wholly

[15] UN Charter. Art. 2, para. 1 and 4.

within that principle because they involve neither coercion nor control of other nations, but rather present those nations with a choice. If a state chooses to accept American aid, it must also accept American political values to some extent. If it chooses to reject those values, it may not enjoy the benefits of United States economic or military assistance [Editors, 1984: 358].

The classic 1979 American textbook on international law stood by traditional standards: state sovereignty is coextensive with state territory and within that territory is exclusive [Brounlie I., 1979: 53]. However, that same year in the *Mannington Mills, Inc.* v. *Congoleum Corp.* (595 F. 2d 1287, 1292–1293, 3d Cir. 1979) decision, the court recognized American jurisdiction in antitrust disputes even against foreign nationals operating within the territory of other states and thereby made American competition laws extraterritorial. A little earlier, US law pertaining to securities had been made extraterritorial in effect[16], and in the following year protection of human rights around the world was also proclaimed[17]. US laws passed in the 1980s, such as the Foreign Corrupt Practices Act of 1982 and the Foreign Assets Control Regulations of 1983, explicitly provided for their extraterritorial effect.

Extraterritorial application of EU law was confirmed (in relation to antitrust law) as early as 1972 in *ICI and others* v. *Commission* (1972 ECR 619) and subsequently expanded. Extraterritoriality was laid down in the Council of Europe conventions, first in a negative way as additional obligations imposed on relations with "inadequate" countries (Article 12, paragraph 3(b), of the 1981 ETS No. 108 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data); but then in a positive way as the right to access data regardless of their location (Article 32(b) of the 2001 ETS No. 185 Convention on Cybercrime) and eventually even as the right to regulate data flows regardless of where they are actually carried out (this is already part of Article 3 of the EU's General Data Protection Regulation).

The United States, the EU and other large countries very quickly adopted the principle of extraterritoriality, which severed the link between law and territory. Because these countries wanted to regulate certain relations abroad, states have sacrificed the exclusivity they once had in regulating relations within their own borders. Since the 1980s, a law created by a state is no longer immanently linked to the territory of that state. It may still be

[16] Leasco Data Processing Equip. Corp. v. Maxwell, 468 F.2d 1326 (2d Cir. 1972).

[17] Filartiga v. Pena-Irala, 630 F.2d 876, 880 (2d Cir. 1980).

considered the rule of "first choice" because it is likely that the courts of that state will apply it rather than any other rule. But it can be no more than that. Hoping to extend their monopoly on law-making by invoking extraterritoriality, states have outwitted themselves and undermined their monopoly.

Once the state has lost its monopoly on making law, its monopoly on coercion cannot help. Laws are usually implemented voluntarily rather than under threat of coercion. Coercive state enforcement constitutes a net loss to society by incurring the cost of courts, bailiffs and prisons. A rule that is perceived as effective and fair, and therefore can be implemented without coercion, will be more useful for society (and for the state) than an ineffective or unfair law that requires huge resources to enforce it.

At this point, unfortunately, it is necessary to express a reservation about the monopoly on law-making in the state. Any state is a complex and extremely heterogeneous public entity in which the rules are in fact created only by a certain subgroup of people. The size and level of representation of the rule-making group in a state varies from country to country. It follows that legislative rules emanating from the state are not based on the interests of all the residents of a particular country but instead on the interests of those who have access to rule-making. However, modern political science studies indicate that democratic states with so-called "inclusive" institutions — those with a model of law-making that takes into account the widest possible range of individuals — enjoy a relative advantage in the competition between countries (i.e., in the competition between different ways of establishing law and order). Countries with "extractive" institutions that exclude a great many people from creating rules end up by imposing rules that ignore the interests of the majority of society, those countries and are therefore less competitive [Acemoglu D., Robinson J., 2012]. The rules adopted by either kind of country are consecrated for both in the name of the state, after which the question of whether they are to be implemented voluntarily or under compulsion arises.

A rule is implemented voluntarily if it does not contradict the individual's concepts of fairness and effectiveness. Suppose that the law-making segment of society wants to know what is considered fair and appropriate in society. How could this be accomplished?

In democracies the interests of society are conveyed in an organic way to the participants in rule-making through elections. In other words, a person

must represent the interests of at least some part of society if they are to become engaged in drafting the law. Taken together, all those who are admitted to the rule-making process will represent a large part of society. In authoritarian states, this mechanism does not work, and other more or less artificial ways must be employed. The most common one would be to consult sociological surveys and other public opinion research (which is also used as a backup mechanism in democratic countries).

Opinion polls in Russia show that people do not consider state law something of their own. Over the past ten years the question, "Do you think that the interests of the government and society coincide in Russia now?" was answered "definitely yes" by only two to three percent of respondents[18]. Since November 2007 this proportion has fluctuated by no more than one percent. And this consistently high level of alienation from the law indicates that, although the interests of the people are known to those who make the rules, that knowledge does not affect the content of the rules and does not make them more "popular". The situation is similar with such quasi-democratic ways of "citizen participation in the management of state affairs" as the Russian public initiative[19]. At the time of writing, none of the initiatives that have gained the necessary support of citizens at the federal level have been implemented in the form of laws. Somewhat more effective are so-called "crowdsourcing" projects in which people act as experts, that is, carriers of special knowledge rather than interests. For example, the federal website regulation.gov.ru allows any registered citizen to comment on a draft regulatory act, and the state body concerned is obliged to consider those comments. The federal project "Regulation of the digital environment" provides for even greater involvement of citizen-experts so that anyone may become a member of the specialized working groups that develop draft regulations for the digital economy.

It is impossible to check the performance of the regulation.gov.ru feedback system because there are no publicly available statistics on whether comments are implemented or not. The relative ineffectiveness of this federal project for regulating the digital environment is indirectly indicated by the mere six acts adopted over the two years of its existence (on digital rights, on crowdfunding, on electronic employment records, on electronic

[18] Survey by the Yuri Levada Analytical Center. 28 November 2019. Available at: URL: https://www.levada.ru/2019/11/28/obshhestvo-i-gosudarstvo/ (accessed: 05.12.2019)

[19] Available at: URL: www.roi.ru (accessed: 05.12.2019)

notary services, on changes in the regulation of electronic signatures, and on VAT for electronic services), which is less than one percent of the total number of federal laws passed while the project has been ongoing. The texts of the adopted laws suggest that approving them has been difficult. This is shown by the blanket and cross-referenced norms. For example, according to Article 141.1 of the RF Civil Code, digital rights are to be identified as such in the laws pertaining to obligations and other rights; however, as long as there are no such laws, the rule concerning digital rights does not apply. There are also reservations about a potentially different regulation through special laws, and the lack of detail in the legal rules allows them to be applied directly without by-laws and other regulatory legal acts. Therefore, it is difficult to regard the results of these "crowdsourcing" legislative processes as making "people's" law. Nor are they rules that will be seen as fair and effective, and their poor quality will prevent them from becoming the "law of first choice" when people make decisions.

3. Law-making by multinational companies

Multinational enterprises barely exist under international law; some scholars have gone so far as to describe them as "invisible" [Jones F., 1994: 893–923]. However, a better metaphor would be the blind men and the elephant. None of the states see the whole elephant. Some states find a headquarters and financial center and think that the company is like an office. Other states find production facilities and think that the company is a factory. Others feel the cargo flows of multinational corporations on their roads and decide that the company is a logistics provider.

Each state sees only those legal entities that operate within their territory, but they fail to see the essence of the entire company because each state by default regulates only the activities that take place within its boundaries. No matter how much states try to extend their power beyond their territories, the extraterritorial effect of the law is the exception, not the rule. Multinational companies are entities that transcend national states and have acquired features such as power, authority and relative autonomy to a degree that would be extraordinary for any domestic entity. Taken as a whole, these features give multinational companies an internal legal system that resembles the comprehensive legal system of a national state. Like states, multinational companies create rules and ensure that they are generally

binding, both in a voluntary (legally persuasive) and in a compulsory (legally enforced) manner.

The first feature — power — is inherently relational, typically defined as the ability of A to get B to do something that B otherwise would not do. The political powers of multinational enterprises can be broken down into the following typology [Ruggie J., 2018: 317–333]:

instrumental power, the most traditional form of which is business lobbying;

structural power, which may include companies' choice of locations and the ability to transfer risks to suppliers;

discursive power, which refers to the ability of businesses and business associations to frame and define public interest issues in their favor — that is, to shape ideas that then come to be taken for granted as the way things should be done, even for non-business entities like governments.

The second feature — authority — is, in brief, the right to prescribe. The sources of authority for multinationals are the principles of private property rights (including intellectual property) and freedom of contract. These core elements of this traditional source of authority are enshrined in, elaborated by, and enforced through public and private law, including obligations under the WTO and international investment agreements[20].

The third feature — relative autonomy — may be understood through two possible answers to the question of who owns publicly traded firms: they own themselves, or no one does. In effect, these answers amount to the same thing. There appears to be only one answer to the question on whose behalf multinationals exercise their authority: on their own behalf.

Multinational corporate power is much more organic and portable than state power. It is not tied either to a particular territory or population, and therefore it is not bound by any obligation to make either-or choices when selecting its locations and employees. It is more organic in promoting values and ideas, and those values are simpler and much more aligned to the interests of the people than abstract socialism or liberalism. These factors have worked in favor of corporations before, but in the global information society they make the gap in effectiveness between corporations and states even greater.

[20] Ibid.

It is important to make a qualification here: it is extremely difficult, or perhaps impossible, to describe a multinational company as a single entity with a single mechanism for forming and expressing its purpose or to assign a single identity to it. A multinational company is an ecosystem with a relatively stable core and constantly changing peripheries. This weakens the certainty of the legal system that such a company generates.

The headquarters of a multinational company can determine strategic values, allocate resources, work to create a more favorable environment for the company, and establish the conditions for working with suppliers and employees — but the rules themselves are most likely not determined by the headquarters. They will consist of a set of agreements concluded within the company's ecosystem and compliance methods chosen by legal entities that are part of the company's ecosystem in different countries. Therefore, these corporations do not have a macro level of law equivalent to the legislation of states (at least not yet). But at the micro level, when choosing the rules for behavior here and now, the law of multinationals is in force because each person entering the ecosystem of the company has access to the entire set of rules that they are to be guided by in a particular situation. Despite the lack of a macro level legal system, there is an area in which these corporations have a kind of "sovereignty": their power over themselves. Self-empowerment is already an impressive feature, given the tens and hundreds of organizations, hundreds of thousands of employees, and billions of users bound together by these corporations. And from the point of view of legal certainty, their "law for us" is much better than the "law for them" created in non-democratic states as described above.

The "population" of multinational companies (which is their customers) does not participate in the management of those corporations. Just as there are no states without populations, there can be no multinational company without users. But unlike states, most of which are democratic or seek to be, most multinational companies are authoritarian. A product made by a particular company, whether it is fuel, a car, a phone or a social network, is standardized — the user can choose only to buy or not buy a particular item from the assortment.

The point, however, is that there are multiple users and companies, and together they all form a market. The product market is an environment in which the will of users can be expressed in relation to corporations, and therefore the market restricts the arbitrariness of corporations. The chain of relationships turns out to be long: users (as well as investors and other par-

ticipants in financial markets) focus on their own interests and on information collected and distributed by civil society organizations and professional communities and by the media. They then adjust their market behavior in relation to the corporations present in the market. But this chain is quite workable, and it corresponds exactly to electoral democracy: both have a certain number of candidates and a large number of users, while each user is limited to a choice between buying or not buying. In their totality — either in the market or in elections — users and voters choose the products and candidates that best suit the overall interests of a given society. The election process is both organic and motivates candidates to meet the interests of the people. The rules created by the selected candidates (corporations) should in theory also correspond to the interests of the voters. This creates a "consumer democracy", which is the key to digital citizenship.

4. Tools of Digital Citizenship

Citizenship is usually understood as a relationship between a citizen and the state [Mamasahlisi N.M., 2018: 37–47]. This relationship is assumed to be exclusive. However, there is no longer any exclusivity in a plurality of legal systems. Examples of multiple legal systems have been cited many times, but let us consider another one for our purposes: ordering airplane tickets from Russia to Europe. The consumer is located in Russia, which means that Russian legislation applies. But the platform for ordering tickets is American. And the airline is European, with EU law applicable both to transportation (taking into account the requirements of the UN's International Civil Aviation Organization, of course) and to the processing of passenger data. The payment system is from China. At the same time, the ticket ordering platform, the airline, and the payment system have their own rules, which they as global companies have brought into line with the legislation of all possible countries — which means that they do not fully comply with any of them. All these legal systems are applied together with each one claiming its own exclusivity and making no allowance for the others. But strangely enough, all these legal inconsistencies do not prevent the consumer from ordering a ticket, paying for it and flying. At all stages of the process, the participants will more or less understand what they need to do and how to go about it.

What conclusions can be drawn from this example? The main thing is that these legal systems, despite their multiplicity, are compatible with each

other. This is due, first of all, to the limits on legal regulation that are insurmountable for any legal system. But, in addition, it is because of the narrow windows of opportunity for creating a rule, no matter where it comes from (a state or a company). Such opportunities for negotiation, or what Lassalle called the actual relations of force, form the connected interests mentioned at the beginning of this article. The parties estimate their costs for establishing a relationship or finding an alternative one, for enforcing a rule or changing it. As a result, the list of possible conditions for a norm (law or contract) is short. It is important to note that this approach to standards is possible when they are created and applied on a mass scale. A single contract or law may not take into account the interests of the other party to the relationship. The legal system on the whole always reflects the actual relationship of power, that is, the sum of the interests and capabilities of all its actors.

There are several historical examples. The 1990s were period when copyright was triumphant. In 1995 the TRIPS Agreement — the "constitution" of copyright holders — came into force. It significantly reduced the number of fair use exceptions to copyright and tightened the enforcement of intellectual property laws. The WIPO Copyright Treaty was adopted by the member states of the World Intellectual Property Organization (WIPO) in 1996. In addition to many other restrictions, it prohibited circumventing the technological measures of protection of works (Article 11). The golden era of technological copyright protection began with regional codes on CDs and encrypted DVDs and scrutiny of private use. This Copyright Treaty was followed in 1998 by adoption of the Digital Millennium Copyright Act (DMCA) in the United States and by the European Union's Directive 2001/29/EC on the harmonization of certain aspects of copyright and related rights in the information society. When this trend finally reached Russia, it resulted in the amendments to the Federal Law "On copyright and related rights" that prohibited circumvention of technological measures of copyright protection. But 1995 was also the beginning of two decades during which recorded music revenues slumped by over a third[21].

Another example is online advertisement. Targeted advertising has been the main source of revenue on the internet since the early 2000s. In an attempt to make advertising even more targeted, online platforms collected all the data they could reach, and banners on sites took up all the available

[21] IFPI state of the industry overview 2016. Available at: https://www.ifpi.org/downloads/GMR2016.pdf (accessed: 05.12.2019)

space. Everything changed with the advent of the AdBlock program, which blocked all ads and not just the annoying ones. By siding with their customers, browsers have also blocked third-party cookies[22]. Taken together, these measures have made the entire industry of real time bidding for advertising pointless. Developing online advertising for two decades without considering the interests of users has made them hostile to it.

It is worth mentioning that other competing companies played an important role in both examples. AdBlock itself began to sell ads (more precisely, to trade in refraining from blocking ads). The hollow victory of copyright holders led to the emergence of Napster, and then iTunes and Spotify. But, in any case, the winners have learned a lesson: the new market situation developed because it is more in line with the interests of users.

These examples show also that the digital citizenship framework is quite complicated. Together with national states, there are at least four other principle actors [Backer J., 2007: 13–14]: (i) multinational corporations and other enterprises; (ii) elements of civil society, primarily the economic and human rights non-governmental organizations (NGOs); (iii) media; and (iv) consumers of the products of the corporations, the investment community and financial markets. These actors have fundamentally adverse interests, but are dependent on each other[23] and have connections among their interests. The individual's interests are implemented through a set of tools corresponding to the digital citizenship framework. We shall use the typology suggested by Ruggie [Ruggie J., 2018: 32] to classify potential tools for digital citizenship.

The instrumental and structural power tools of digital citizenship are based on network effects or, more precisely, on queuing network effects. Any system is designed for certain traffic levels, and cannot work properly at peak loads. If users' activity is in some way coordinated, it will cause a demand peak at certain points in the system, which results in blocking the activity or changing the structure of the system. The best example of such coordinated activity is DOS (denial of service) attacks, which cause targeted websites go out of service. Although any hacking into an information or telecommunication system is illegal, social hacking — advocacy — is legal and quite efficient.

[22] IAB Europe guide to the post third-party cookie era. Available at: https://designrr.s3.amazonaws.com/mardare_at_iabeurope.eu_80924/_3804.pdf (accessed: 05.12.2019)

[23] Ibid.

Even in Russia, there are enough tools for digital citizenship, provided that their use is coordinated in the interests of citizens. In addition to the websites roi.ru and regulation.gov.ru and also the federal project for regulating the digital environment, which were already mentioned, there are regional crowdsourcing portals (with names like "active citizen" and "good deed"), and online petition sites in addition to social networks. The actions of individuals using these tools in isolation are unlikely to be noticed, but mass actions are already having an impact on both the state and companies[24]. The use of all the digital citizenship tools of this kind will permit using a multi-stakeholder approach to developing rules of conduct at the level of legislation and corporate policies. A multi-stakeholder approach is not yet a democracy, but it is better than altogether excluding the population from law-making.

The disadvantage of depending on these instrumental techniques is that they are difficult to implement and the least effective of all the tools for digital citizenship. The tools now in use have been specifically designed to make it difficult for the public to influence the rules that the government or companies are making. Yes, this is feedback, but the decision is made by the addressee, not by the people submitting feedback. In addition, using this framework requires substantial resources to pay for the work of the participants that make it effective. Therefore, the multi-stakeholder initiatives are not for the poor.

The digital citizenship tools derived from structural power are more promising. People, like companies, can vote with their feet. For example, online cinemas cannot win the fight against pirate websites in Russia. The more severe the penalties for pirates are (up to a lifetime ban), the higher the number of users of pirate sites[25]. The same kind of deterrent was used to block the Telegram messaging service. The more efforts the authorities

[24] Digitally coordinated actions have prevented Yandex from treating Russian opposition leaders. Available at: URL: https://www.bbc.com/russian/news-52457393. and have changed the government's policy on both drugs (Available at: URL: https://www.coe.int/en/web/media-freedom/detail-alert?p_p_id=sojdashboard_WAR_coesojportlet&p_p_lifecycle=0&p_p_col_id=column-1&p_p_col_pos=1&p_p_col_count=2&_sojdashboard_WAR_coesojportlet_alertId=49031605.) and hate speech (Available at: URL: https://rg.ru/2019/10/10/mvd-raziasnilo-kogda-nuzhno-zavodit-delo-ob-oskorblenii-vlasti.html.) (accessed: 05.12.2019)

[25] The number of daily rutracker.org users is over 1 million. Available at: https://apparat.cc/world/rutracked/.) compared to an estimated 6 million users per year for legal online video services (Available at: URL: https://www.vedomosti.ru/technology/articles/2019/09/10/810965-bolshe-6-platyat) (accessed: 05.12.2019)

make to block it, the more users it has[26]. These structural tools are also effective because they are more organic. People are using them not only to express their opinions, but also to switch to using more effective services and thus supporting them. Attention is the main resource of the modern economy. By shifting attention, society rewards or punishes actors.

Discursive tools are even more effective, but also more dangerous. Combining online around certain values allows you to spread these values very quickly. This will lead to changes in the policies of individual companies and perhaps even of the state, but it will create a threat of discrimination for those who do not share those same values. Feminist or orthodox religious movements, support for or denial of the rights of minorities, promotion of certain approaches against domestic violence, stigmatization of certain social groups (for example, law enforcement officers) — all this is dangerous for Russia's multicultural and multiethnic society. However, within this framework, diverse values compete for the attention of the audience and so mutually restrict each other, and this will prevent the most odious of them from influencing the policies of the state and companies.

The tools of authority are almost never in the hands of the individual. A citizen is always the weaker party in relations with the state or a company. But ultimately the state or company is also people and no one but people. They have the most authority because they are united in a certain institution. All individuals have rights, such as the right to property (including intellectual property), the right to personal data, and the right to an image. By coordinating their actions to implement and protect their rights, individuals will be able to acquire significantly greater contractual power. The institution of collective lawsuits, which was adopted by Russia in 2019, should be quite helpful in this regard. Previously, rights could be defended only on an individual basis. In theory, collective management of personal data (similar to collective copyright management) is also possible. As societies of performers and artists changed the balance of power in the film and recording industry in the mid-twentieth century, collective management of personal data can change the balance of power in advertising and social media.

In conclusion, let us consider relative autonomy. The multiplicity of legal systems is a given. Both the legal systems of states (which are ranked by various

[26] Available at: URL: //www.rbc.ru/technology_and_media/13/04/2019/5cb19f339a794741a319f84d (accessed: 05.12.2019)

indexes, such as Doing Business) and the legal systems of multinational companies are locked in competition. The tendency is to increase competition, not decrease it. Inefficient localization requirements are being superseded by portability and compatibility requirements. The entire framework is much more complicated and includes also elements of civil society, media, consumers, the investment community and financial markets. Each of these actors is relatively autonomous from the others, but together they are all interconnected.

In analyzing the consequences of digital transformation, we have found that it generates ecosystems. With a bit of exaggeration, we could say that the world is being taken over by ecosystems, by both state-owned and company-owned ecosystems, either online or offline. None of these ecosystems owns us fully. Instead, each of us is a citizen of many ecosystems. Our digital world can be made better by influencing digital ecosystems with the instruments of digital citizenship. In a multi-ecosystem environment, it is always possible to find one that meets our interests and use it to change the legal systems of states and companies.

Ecosystems should be considered a common good, not the property of some person or group of people. Therefore, they must be managed as a common good based on the principle of participation of all stakeholders with consideration of the interests of all parties. In other words, the ecosystems should be built and function in a way that is convenient for us to belong to them as citizens. By making ecosystems better, people, businesses and states become better parts of those ecosystems.

Conclusions

Our world has become borderless with everyone connected to everyone. Neither states nor multinational companies can now enjoy any kind of exclusivity. They have to compete with each other for the scarcest resource in our modern economy: people's attention. As in any market, competition is imperfect, and market failure is possible. But the multiplicity of legal systems and the multiplicity of ecosystems for individuals give them the ability to overcome the failure of one ecosystem (for example, the monopoly of Facebook or Google) by using another ecosystem (for example, the ecosystem of digital resistance). In the digital world, nothing is exclusive.

The same individuals in certain areas of their life can be part of the state (voting in elections, being a member of a political party, participating in lo-

cal government, being a public servant or even a political figure), a participant in the ecosystem of a multinational company (being a business owner, a shareholder, an employee), and finally just a person (living somewhere, having a family and friends). In each of these areas, people create rules — this is what makes us a society, ensures the consistency of our actions, and gives us certainty. Rules themselves are created only by people and no one except people. The difference is only in the organizational mechanisms for the creation and application of rules.

Given the available tools of digital citizenship — such as instrumental, structural, and discursive power; property-based or contract-based authority; and the relative autonomy of existing digital ecosystems — individuals in the digital world now have a sufficient set of tools to become citizens of digital states rather than their subjects. The main requirement is that individuals be aware of their interests and coordinate their actions with other individuals by choosing an ecosystem from the available framework.

References

Acemoglu D. & Robinson J. (2012) *Why Nations Fail: The Origins of Power, Prosperity, and Poverty*. L.: Crown Business, 546 p.

Backer L. (2007) Economic Globalization and the Rise of Efficient Systems of Global Private Lawmaking: Wal-Mart as Global Legislator, *University of Connecticut Law Review*, no 4, pp. 1–41.

Brownlie I. (1979) *Principles of Public International Law*. Oxford: Clarendon Press, 732 p.

Editors (1984) Extraterritorial Application of United States Law: The Case of Export Controls. *University of Pennsylvania Law Review*, vol. 132, pp. 355–390.

Froomkin M. (2000) The Death of Privacy? *Stanford Law Review*, vol. 52, pp. 1461–1543.

Holtzman D. (2006) *Privacy Lost: How Technology is Endangering Your Privacy.* N.Y.: Jossey Bass, 352 p.

Johns F. (1994) The Invisibility of the Transnational Corporation: An Analysis of International Law and Legal Theory. *Melbourne University Law Review*, vol. 19, pp. 893–923.

Mamasahlisi N.M. (2018) Citizenship as an Element of the Constitutional Status of the Individual in Russia. *Candidate of Juridical Sciences Thesis.* Moscow, 214 p.

May C. (ed.) (2006) Global Corporate Power. New Delhi: Viva Books, pp. 1–20.

Osborne S. (2006) The New Public Governance? *Public Management Review*, no 3, pp. 377–388.

Prokhorov A., Konik L. (2019) *Digital transformation. Analysis, trends, world practices.* Moscow: Alyans Print, 368 p.

Ruggie J. (2018) Multinationals as global institution: Power, authority and relative autonomy. *Regulation & Governance*, vol. 12, pp. 317–333.

Straw W. & Glennie A. (2012) The third wave of globalization. Report of the IPPR review. Available at: https://www.ippr.org/files/images/media/files/publication/2012/01/third-wave-globalisation_Jan2012_8551.pdf.

Todorova M.N. (1997) *Imagining the Balkans*. Oxford University Press, 257 p.

Warren S. & Brandeis L. (1890) The Right to Privacy. *Harvard Law Review*, vol. 4, pp. 193–220.

World Bank (2016) World development report 2016: digital dividends overview. Washington: World bank, 105 p.

Reinventing “Magic Circle” in the Age of Internet Government Control: the Lessons of Videogame Law for Modern Practices of Legal Interpretation

Vladislav Arkhipov

Associate professor, Department of Theory and History of State and Law, Saint Petersburg State University, Candidate of Juridical Sciences. Address: 7-9 Universitetskaya Embankment, Saint Petersburg 199034, Russia. E-mail: v.arhipov@spbu.ru

Abstract

The restrictions for disseminating certain kinds of information that is considered publicly offensive and (or) dangerous has made topical a fundamental problem of the limits of reasonable interpretation and application of law to the contexts that could be characterized as virtual, playful or otherwise non-serious. From the standpoint of interdisciplinary approach including mostly philosophy of law and game studies, the underlying problem reflected in the representative examples above, has substantial similarities with the “magic circle” concept studied in the research direction that is conventionally called “videogame law”. However, existing theories of magic circle, both in game studies and law, are not satisfactory to resolve this problem. The article suggests that the solution can be found in theoretical sociology concept of “generalized symbolic media”. If an object of social relationship is an “external referent of value” of such media and has convertible “socio-currency value”, this means that such object is significant enough to be included into the scope of legal regulation. However, for the application of law to be appropriate without doubt, such an object should also share functional similarity with the core meaning of the relevant legal norm. Together, these two criteria, conventionally designated as “the criterion of seriousness” and “the criterion of reality”, are necessary and sufficient to assert that interpretation and application of law is not absurd, but reasonable in cases related to virtual reality that is characterized by possibility to include simulation that is out of scope of law.

Keywords

law; theoretical sociology; medial turn; virtual reality; magic circle; semantic limits of law.

For citation: Archipov V.V. (2020) Reinventing “Magic Circle” in the Age of Internet Government Control: The Lessons of Videogame Law for Modern Practices of Legal Interpretation. *Legal Issues in the Digital Age*, no 1, pp. 79–98.

Introduction

In the experience of the Russian Federation, a recent trend of states to seek "sovereignization" in the informational space finds one of its implications in establishing the rules restricting "information prohibited for dissemination [in the Internet]" [Efremov A.A., 2018: 202]. By the date this paper is finished, more than a few criteria for blocking of dissemination of such information in the Internet were established by the Federal Law of July 27, 2006 "On Information, Information Technologies and Protection of Information" (hereinafter the "Information Law"). Some of the criteria are explicitly mentioned in Part 5 of Article 15.1 and in Part 1 of Article 15.1.1 of the Information Law. Furthermore, the courts furthermore have the competence to recognize information as prohibited for dissemination in the Internet in "open" cases in view of Part 2 of Article 15.1 of the Information Law. In each case, however, such information has to be considered as publicly dangerous or offensive, by means of either legislative assumption, or court argumentation respectively.

There is already a plenty of cases where certain information disseminated in the Internet has been considered as "prohibited for dissemination" according to the abovementioned rules. From the standpoint of theory of law, constitutional law and information law, many of these cases do not pose any substantially novel kind of legal problems, except for the "classic" ones, such as, for instance, the problems of the limits of freedom of speech, balancing of constitutional values and general efficiency of website blocking in view of the legislative intention. However, there is a number of cases where, from common sense perspective, "things went wrong" for unusual reasons. For instance, mass media refer to one of the decisions of Zavodoukovsky District Court, Tyumen Region[1] by means of the following illustrative opinion of anonymous Roskomnadzor employee: "We once received a court order to block a site with information about making dynamite in Minecraft. The site said that if you mix sand and coal, you get dynamite. *And you think what to do with this court decision: you can't execute it and block Minecraft* (italics are mine. — *V.A.*). As a result, we talked to the lawyers and wrote to the prosecutor's office to ask them to review the decision" [Yakovlev A., 2018].

[1] Decision of the Zavodoukovsky District Court, Tyumen Region, of 12 July 2016, Case No. 2–662/2016. Available at: URL: https://zavodoukovsky––tum.sudrf.ru/modules.php? name=sud_delo&srv_num=1&name_op=doc&number=25808719&delo_id=1540005& new=0&text_number=1 (accessed: 02.10.2018)

There is also an earlier similar case: the Federal Drug Control Service once blocked one of the forums of the online game *Eve Online* due to the fact that the player discussed 'drugs', which were 'used' by videogame characters, on that forum [Likhachev N., 2012]. Each of these cases, as well as similar cases that eventually could be found in the materials of practice, may seem to be insignificant and ludicrous, but the point of this paper is to demonstrate that, instead, they help to reveal a fundamental problem of law that becomes relevant in modern times.

As can be seen, in each of the cases mentioned above, the question is implied that in some cases related to the digital game environment, the interpretation and application of law may be absurd. However, it is not easy to propose a universal criterion of absurdity there. The fact of realization of social relations in the virtual space of a computer game itself cannot be a universal explanation. As an illustration, in 2020 an in-game library with real extremist materials was created on one of the servers of the same *Minecraft* videogame[2]. But the very fact of using such materials, which are clearly subject to legal regulation of the "real world" cannot be the only opposite criterion either. Let us imagine that some videogame refers to fictional extremist materials, but such materials become prototypes for the real world. Or, referring to the second of the above examples, a game dedicated to fictional drugs suddenly becomes a tool for propaganda of the objects limited for economic exchange. This state of affairs tacitly suggests that there should be some other explanation, perhaps of general theoretic nature, that could explain why in some cases seemingly fictional, non-serious and/or game phenomena could be included into the scope of "real" law without violation of common sense, while in other cases they clearly should remain in distance from day-to-day social reality.

The ideas presented in this paper are based on the hypothesis that, from the standpoint of interdisciplinary approach including mostly philosophy of law and game studies, the underlying problem reflected in the representative examples above, has substantial similarities with the 'magic circle' concept studied in the research direction that is conventionally called 'videogame law'. In view of this, the contemplated problem can also be understood as

[2] Reporters sans frontières crée une faille pour vaincre la censure en construisant un refuge pour la liberté de la presse. Où ? À l'intérieur de l'un des jeux vidéo les plus populaires du monde, Minecraft. 2020. Available at: https://rsf.org/fr/actualites/rsf-inaugure-la-bibliotheque-libre-un-centre-numerique-de-la-liberte-de-la-presse-au-sein-dun-jeu (accessed: 19.03.2020)

the problem of the limits of reasonable interpretation of the legal texts that excludes something that is "inside" such magic circle from the scope of application of "real" law. From methodological perspective, it is suggested that theoretic sociology would also be of great help in identifying what has "real" legal significance and hence can define what is indeed "publicly dangerous" and/or "offensive", and what should remain within the boundaries of playful virtual laws for the purpose of legal application. Lawrence Lessig once mentioned that studying the pervasive legal issues of cyberspace might help us to understand more some general principles of law [Lessig L., 1999: 502]. In a similar way, reinventing of the magic circle along the lines suggested in this paper may help to separate legally significant cases from the legally insignificant ones both for practical and theoretical purposes.

1. The Concept of the Magic Circle and its Criticism

The term 'magic circle' is widely used in cultural studies, sociology and interdisciplinary approach of game studies. Legal scholars later adopted it too. In this paper, it would make sense to have a general look at the discussion of the magic circle concept in game studies and then verify the relevance of various ways the lawyers adopt it. The reason is that it is tempting to use this concept, as it is known by this moment, in an attempt to find an easy solution to the contemplated problem.

From the beginning, this concept has meant an assumed conventional boundary between the space of a game and "real life". The history of the use of this metaphorical term goes back to the work of J. Huizinga, 'Homo Ludens. According to the Dutch thinker, "[f]ormally speaking, there is no distinction whatever between marking out a space for a sacred purpose and marking it out for purposes of sheer play. The turf, the tennis-court, the chessboard and pavement-hopscotch cannot formally be distinguished from the temple or the magic circle" [Huizinga J., 1938: 20]. He applied this term even to the law itself: "Every place from which justice is pronounced is a veritable *temenos*, a sacred spot cut off and hedged in from the 'ordinary' world. The old Flemish and Dutch word for it is *vierschaar*, literally a space divided off by four ropes or, according to another view, by four benches. But whether square or round it is still a magic circle, a play-ground where the customary differences of rank are temporarily abolished" [Huizinga J., 1938: 77]. The concept of magic circle has been widely discussed in game studies. However, recently it was subject to criticism.

According to M. Consalvo, when J. Huizinga wrote about magic circle, he based this idea on "a magic circle for play, which bounded a space and set it apart from normal life. Inside the magic circle, different rules apply, and it is a space where we can experience things not normally sanctioned or allowed in regular space or life"; "… [such a] conceptualization of the magic circle was developed in the 1930s, **long before the advent of digital games** (emphasis added — *V.A.*), by a theorist with particular views of what did and did not constitute play… our sense of space and place was radically different from what it is now. In suggesting a place "set apart" from everyday life, that space could be envisioned as geographic space fairly easily — the playground, the boxing ring, the hopscotch outline" [Consalvo M., 2009: 409]. In contrast, digital games are rather a dynamic activity. Such an activity disperses in the experience of day-to-day life. The dividing line between games and other aspects of life is not clear and stable — instead, people get into and out of games in an intermittent manner, so that the concepts of "frames" and "keys" of E. Hoffman and G. Fine are more appropriate [Consalvo M., 2009: 414]. V. Lehdonvirta presented another example of the criticism of the magic circle concept: fluid character of everyday life does not allow delineating virtual and real worlds clearly [Lehdonvirta V., 2010].

In contrast, J. Stenros defends the concept of magic circle for the purposes of game studies. According to him, it still is relevant to describe (1) a "psychological bubble", i.e. "a protective frame" surrounding the player who is in psychological state corresponding to the game process, (2) a metaphor for a social contract that constitutes a game activity, and (3) a kind of arena for gameplay that is "temporal or spatial 'site". The latter might be the most relevant for the present study, since such kind of 'site' "…is culturally recognized as a structure for playful action, or an inert ludic product. As the social negotiation of a magic circle becomes culturally established and the border physically represented, arenas emerge as residue of the playing (the tennis court, April Fool's Day, **game products** (emphasis added. — *V.A.*). These sites are recognized as structures that foster play even when empty (and they can be constructed in ways that seek to foster playfulness), but require use to be activated as the border of the magic circle remains social. As socially recognized they have severed the need to be engaged in with a playful mindset" [Stenros J., 2012: 14–15].

However, such discussion of magic circle belongs to the context of game studies, and not of jurisprudence. The approaches criticizing the contem-

plated concept without substantial reservations are not helpful for law. It is acceptable for game studies to assert that virtual world and real world are intertwined, but in law that would undermine legal certainty. At the same time, the approaches that insist on keeping the magic circle concept are also not particularly informative and specific. Returning to the initial examples of the paper, on the opposite, what we need are quite specific principles on how to discern where it would be acceptable to apply law in respect of certain kind of social relationships focused on information exchange. Even if it is not a general 'magic circle' so that the metaphor works to its fullest (i.e. directly referring to 'circle' as a figure that is round and plain), it can be a different figure, not necessarily round, but there should be a principle of how we draw it.

Certain lawyers have perceived this idea in application to massive multiplayer online games, and there are at least two more or less established adaptations of the magic circle metaphor in law. B. Duranske suggested a 'magic circle test' that has to be applied to social relationships in multiplayer online games: "An activity that occurs in a virtual world is subject to real-world law if the user undertaking the activity reasonably understood, or should have reasonably understood, at the time of acting, that the act would have real-world implications" [Duranske B., 2008: 75]. We should pay tribute to pioneer enthusiasm of the author. However, such a test actually implies the question of whether an individual may be subject to legal liability (intent and negligence are tacitly referred to in the test), but does not shed much light on the core question of whether real law *generally* can invade a virtual world. Liability is not the only matter here — the core question may concern any other kinds of impact of law. Furthermore, by now the concept of "committing actions in the virtual world" seems not particularly clear, especially in view of the previously mentioned criticism of the game studies' concept of the magic circle. In other words, this approach is very good for its time, but it inherits the weak points of the general theory of magic circle, that is lack of clarity on demarcation between what is virtual and what is real. Even with J. Stenros' defence of magic circle, the arguments of M. Consalvo and V. Lehdonvirta on the intermittent nature of games and mutual dispersion of virtual and real, respectively, remain undisputed and have the same significance in jurisprudence as they do in game studies.

Elaborating the discourse further, J. Fairfield suggested an approach that conventionally can be called a 'consensual theory of magic circle'. According

to him, "[u]nder the old conception of the magic circle, such a result [differentiated attitude to virtual property depending on the subjective composition of the legal relationship participants] makes no sense: either virtual property is "virtual," and interests in it are utterly unprotected by law, or it is "real" and fully protected against all comers. Under the new conception articulated by this Article, players in virtual worlds are real, the actions are real, and even the digital objects of their actions are real. The critical question is not whether the property is real or not, or whether a theft of property is real or virtual, but whether a given act as relates to the property is inside or outside the scope of consent of the parties (emphasis added. — V.A.). As between the game god and the player, the EULA may clearly indicate that the god may alter or delete a given digital object at will. But as between players, one player's theft of another's property may well exceed the scope of consent and thus be actionable in fraud or conversion" [Fairfield J., 2009: 834–835].

Without doubt, J. Fairfield's adaptation of the magic circle concept into the jurisprudence is good, but not universal enough. His theory of consent allows resolving of legal conflicts or collisions limited to private interests, but can be debatable in application public interests. Of course, we can introduce high-level fictions of consent made by sovereign people in a constitution and subordinate laws, but this will not save us in all situations. Imagine a legal text, drafted already under such a fiction. Question of whether we can extend the meaning of certain word in such a text to some phenomena of virtual reality may arise again, and we will have to return to the starting point. In view of this, we need to rephrase the core question and switch from the initial idea to find delineation between virtual and real to something else.

2. Qualification of the Problem from the Standpoint of Legal Theory

The principal position developed in this study is that the problem of the relationship between "virtual" and "real" in law, as discussed in this article, is not a narrowly specialized problem, such as of civil or information law. On the contrary, the problem is universal. We can present the original formulation of the problem as follows: in what cases can real law regulate relations in the virtual world? However, as we see from various criticism to the concept of magic circle, the difference between the virtual world and the real is uncertain or absent. Nevertheless, one of the ways to re-conceptualize the question in

other form would be speaking about conditional limits of the law in the mediaspace, defined by socially significant meanings and sometimes difficult to discern due to the deceptive conditions of the ludic turn[3] ('deceptive' because of various simulacra) that is inherent to the medial turn[4] in general.

The high purpose of law is to give certainty to an uncertain social reality. The problem we are considering from the perspective of legal theory can be interpreted as a problem of application of law and a problem of effect of legal norms. However, the central part of the problem, in which all its aspects converge, is interpretation of law as a constitutive component of legal theory and practice. Is it possible to interpret a legal text as a basis for a legal norm that applies to certain social relations mediated by a mediaspace, sometimes characterized by simulation? If we change the perspective of the analysis of the magic circle in this way, its viable interpretation in jurisprudence relates to the limits of the reasonable interpretation of law, or even certain kind of limits of law in general. At the same time, such limits are defined in relation to the mediaspace, i.e. the space of meanings, and in relation to the scope of possible meanings of this or that legal text, whether they include certain relations mediated by media reality. Hence, it is possible to designate the problem under study as a problem of defining the *semantic* limits of law.

In the history of legal thought, Lon Fuller had already tacitly touched this, although this part of his ideas has not find proper elaboration until now. In "Anatomy of the Law", he wrote the following passage: «Within any society there are contentions which run *so counter to generally shared assumptions that they would be rejected out of hand by any judge of sound mind*

[3] The concept of ludic turn (or 'game turn') has been described in detail by J. Raessens who noted, in particular, that "[t]o start with the first element, media use may initially look like harmless, disinterested fun. Think of all the creative adaptations of Star Wars on YouTube. It can also, however, become involved in political ends. Think of the Turkish court recently blocking access to YouTube because it allegedly hosted videos that attacked Atatürk, the founder of the Republic of Turkey; the element of make believe refers to the dual nature of media" [Raessens J., 2010: 14].

[4] As the Russian mediaphilosopher V.V. Savchuk noted, "«[a]fter a series of major for the twentieth and early twenty-first century turns, more and more insistently voices are heard to recognize the summing and, at the same time, fundamental medial turn»; «...media is both a method of communication, and an instrument of production, and **a sophisticated method of simulation** (emphasis added. — *V.A.*), and an instrument of political struggle». The following observation is also important: «[a]fter the linguistic one, a medial turn comes — an ontological evidence of a change in reality — that being and media-reality are identified and interchanged, dissolving into each other. The stages of its formation are as follows: reality is mediated by thinking, thinking by language, language by sign, and sign by media. Being built on top of each other, "being" in modern conditions is given only through the media» [Savchuk V.V., 2014: 24].

(emphasis added. — *V.A.*). A man kills his father; in answer to a charge of murder he pleads that his father was a virtuous man with a firm belief in heaven; the taking of his life, therefore, dispatched him into an infinity of happiness such as he could never enjoy on earth; one who confers such a boon should be rewarded, not punished. An official embezzles a large sum from the state; he answers the charge against him by citing a preamble of the Constitution declaring that the state exists to promote the greatest happiness of the greatest number; the money he took made the defendant very happy; the resulting infinitesimal diminution in the wealth of every other citizen could not possibly produce a perceptible decrease in *his* happiness. (If these illustrations seem out of place in a serious context like the present, it may be remarked that St. Thomas Aquinas dealt at some length with the problem of the first; Jeremy Bentham gave earnest attention to the issues presented by the second.)… Contentions like those just suggested are not ruled out of order by any statute, judicial decision, or custom. Their rejection does not depend on law; on the contrary, it may be said that the law depends on their rejection in the forum of ordinary lay opinion. Some extralegal consensus on what is clearly out of bounds is essential to shrink the periphery of explicit law to workable dimensions" [Fuller L., 1968: 113].

Thus, we took special legal problems of multiplayer computer games as a starting point. In the end, we have come to a rather universal problem, typical for any case of simulation, imitation or mimesis — in the broadest sense, this all can be conventionally characterized by the term 'virtual' and its derivatives. The possibility of such universalization defines the problem under consideration as a problem of legal theory and philosophy. One of the specific theoretical and legal manifestations of this problem is the search for reasonable limits of interpretation and, as a consequence, the application of law to relations involving the simulation, imitation or mimesis in question. In our case, the "generally shared provisions" which Fuller referred to, predetermine implicit rules of common sense, through which we can avoid absurd interpretations of legal norms related — specifically in the case of the problem in question — to the virtual context. If we were to restate Fuller's examples in the realities of today, we could come to an example where a court charges a videogame player who "killed" another character with a crime under Article 105 of the Criminal Code of the Russian Federation ("Murder"). This would rather be absurd. However, what could be the way to define such implicit rules?

3. Criticism of the Existing Approaches to Magic Circle

Returning to the initial example, the question can be rephrased as a question of finding that exact element (or elements) in the facts the constitute and (or) surround certain media phenomenon that should be assessed from the standpoint of law with the effect that such assessment would tell us whether law can be applied to the corresponding social relationships.

As we have noted, J. Huizinga suggested considering qualities of *space* as something that would allow differentiating between several contexts that are regulated by different sets of rules. It is tempting to stop constructing a bridge to legal philosophy here by saying that the space of a game is exactly the factor that could serve as the criterion for separating situations[5] where one set of rules (e.g. rules of game) shall be applied instead of other (e.g. rules of law). It may be tempting to use this approach in discussion of virtual property though, but even in that case, it would not be clear enough. The fact that virtual goods are subject to sale and purchase for real money breaks the logic of the criterion of space, since real money do not belong to virtual space of a game. This deficiency is the same as M. Consalvo speaks of — modern games are not similar to games of the past that required certain detached space to exist.

Besides space, there can be two more potential alternatives based on the previously mentioned discussion of magic circle. The first idea of the recent magic circle supporter, J. Stenros, related to "psychological bubble" ("protective frame") is not applicable in this context because it refers to individual state of mind, and not to any intersubjective communicative phenomenon. This idea, however, correlates with the "magic circle test" suggested by B. Duranske, and shares the same criticism. If some user acted being protected by such a "psychological bubble", but it could be reasonably expected from her to do so, this can be used in legal argumentation on whether or not there has been intent e.g. to inflict harm, or negligence. Apparently, the second idea of J. Stenros related to *social contract* that constitutes a game activity, sounds more relevant and correlates with the magic circle adaptation by J. Fairfield. Applicability of this theory is also limited for the following reasons. First, not every case of interaction "inside" a virtual world that is significant for

[5] A common language word "situation" is used here with intent. In the course of present discussion we do not yet know which specific term exactly to use. It would be too early to say "space", "relationship" or anything else.

real law, is based on consent of the parties. Even if we extend the scope of the parties in such a way, that it would include videogame provider and state (so that we can say that by means of certain law, as a legislative act of representative authority, the parties expressed their consent), this would not eliminate the problem at its core. It would not tell us what to do in a situation, where the legal texts that constitute the expression of such consent are not particularly clear and still require some common sense principle to interpret it.

Just as a kind reminder, we are trying to answer the question of what is that exact element (or elements) in the facts the constitute and (or) surround certain media phenomenon that should be assessed from the standpoint of law with the effect that such assessment would tell us whether law can be applied to the corresponding social relationships. So far, we have dismissed *space*, *state of mind* and a kind of social contract (consent). Identifying something as a special space for game or other similar "non-serious" activity will be of partial help, because if things go wrong, law can be applied even to a football game. For instance, if a player intentionally inflicts harm to health to other player. In a similar way, state of mind may be relevant to resolve the matter of real legal liability, but not of the absurdity of applying law in a given situation in principle. Finally, social contract (e.g. in a form of a consent that is potentially binding from the standpoint of law) is also quite situational.

Let us consider the social contract criticism in more detail. Imagine a realistic videogame that contains actual explosive recipes. Players and the videogame company express their "consent" and "say" that it is acceptable. Apparently, if we consider the example of the Russian law related to government control over the Internet, or any other similar approach, the state is in position to request that this information is removed from the videogame. Based on J. Fairfield's theory, we can say that the state is also a party to this complex social relationship, and there is no state's consent to this. However, this works only in case when we are sure that there is an expression of state's consent or dissent. If there is doubt, since in our case the state makes such an expression by means of normative legal acts that usually contain general concept-words, we need to base our conclusion on consent or dissent on something, and here we actually come back to the initial question that still remains open. Furthermore, there can be different details that will make things more complicated in one sense, and simpler in other. For instance, the explosives' recipe may pertain to ancient times, and no one can create it

now because it is not possible to find proper materials. In this modification of the case, it may be natural to exclude this case from the scope of the state's "consent". What we are trying to find is the underlying general principle, if we follow the assumption that there is one.

4. Virtual Property, Money and Generalized Symbolic Media

There can be a hint as to how to solve this riddle. It may lie in the area pertaining to virtual worlds that already received detail account in legal research. For some special reason, there is little doubt that real law, in principle, can interfere with any kind of relationship that seemingly takes place in a virtual world as long as real money is involved. For long period already the idea to consider virtual property, initially existing as a part of an imaginary, albeit shared, virtual world, as some kind of object of civil rights or even property [Saveliev A.I., 2014] causes no surprise. As it was mentioned more than 15 years ago, introducing real money trading into virtual world practices "breaks the illusion that it is all a game", the illusion that characterized most games of the past and some games of the present that do not allow infusion of real money into the process [Castronova E., 2004: 195]. Hence, the connection of game practices to real money, and those relationships where such money is an immediate object of interaction, are a clear case where intervention of real law into virtual interaction is justified. The task implied in this paper is to find a general principle of such an intervention. Therefore, general understanding of what money is, and what the objects similar to money are, allows finding the answer.

According to modern theoretical sociology, money is a kind of *generalized symbolic media*. Conventionally, Talcott Parsons was the first to suggest this concept, as we know it by now, even though its premises could be related to prior authors [Abrutyn S., 2015]. This concept can be compared with Pierre Bourdieu's ideas of the symbolic economy [Bourdieu P., 2019]. However, while the French sociologist was more concerned with studying symbolic "macroeconomics", the concept of generalized symbolic media focuses on the nature of "social currency" and the mechanisms of its conversion. According to Parsons, the social system consists of four subsystems: political, economic, legal and cultural. Each of these social systems has its own "symbolic medium", which can be considered as some kind of con-

vertible "social currency". For example, power, understood as a right (and monopoly) to coercion, is the "symbolic medium" for the political system. Power, directly or indirectly, legitimately or not, can be acquired through money, while money is the "symbolic medium" of the economic system. This, according to Parsons, is an example of the conversion of "social currency". It is important to note that what has such an "exchange value", and not just a certain significance within the social system, has value within a social system.

S. Abrutyn emphasizes that the concept of generalized symbolic media is not just alive but also has significant methodological potential. Although this concept was popularized by Talcott Parsons and Niklas Luhmann, and later by Jurgen Habermas, its origins can be seen in Karl Marx's "Capital" and Max Weber's economic sociology and, moreover, in G. Simmel's phenomenology. Parsons proceeded from the fact that the exchange takes place between systems, while S. Abrutyn stresses that the exchange mediated by generalized symbolic media takes place between people and groups, and hence they are more relevant for micro-level of analysis [Abrutyn S., 2015: 446, 450]. S. Abrutyn suggests complementing the concept with the notion of an "external referent of value" — a specific object that is used to communicate the value of a generalized symbolic medium. A banknote, an attribute of power, a symbol of religious affiliation could all serve as examples. In total, he identifies ten institutional areas, each of which corresponds to a generalized symbolic medium and external referent of value, between which institutional and individual exchange is possible. In addition to economics and politics, he singles out, for example, the institutional area of *kinship*, to which the medium of "loyalty" corresponds with genuine external referents of value [Abrutyn S., 2015: 454]. In the context of digital economy, it should be noted popular word "token", which denotes, among other things, a unit of economic value in cryptocurrencies, is an obvious example of an external referent of value.

It is likely now that the following would be true, if we apply this theory to law. In general, if the object of social relationships, interpreted as an external referent of value, has a convertible "social-currency value" — and we are talking about such generalized symbolic media as money, political power, influence and others that are constitutive to social reality — then the application of law to social relationships with such object is within the framework of common sense. If not, then the application of law to such

relationships will be absurd and, as a result, unacceptable. The distinction between "virtual" and "real" is based on the idea that the object of social relationships has a convertible social and currency value that determines the very possibility of interpreting and applying the law in a given case. In other words, magic circle is possible as a strong and illustrative metaphor, but such a circle surrounds not individuals, their relationships, spaces where they act or anything else, but specific objects implied in the interaction. Virtual property that is traded for real money, as opposed to genuine in-game money, such as gold a player can obtain through questing in a single-player role-playing game, is within the scope of law. It is an external referent of value of real money, and hence property laws that naturally relate to money worth themselves can be applied to it. However, money is not a single generalized symbolic medium. Other good example is power that can be found, for instance, in those communities of virtual worlds that are able to drive people to do something outside the game. Furthermore, these and other generalized symbolic media could be "converted" into each other, and such "convertibility" by itself is a test that allows to recognize something significant enough for legal regulation.

5. The Criteria of "Reality" and "Seriousness"

Let us summarize the previous reasoning and refine the criteria implied in it. In the case of each legal collision emerging due to architectural peculiarities of mediareality (such as in the examples of *Minecraft* and *Eve Online* provided in this paper), it is necessary to verify two criteria that will make it possible to determine the applicability of the relevant legal norm to social relationships in discussion. (Since both criteria and the subsequent generalization have already been formulated by the author in his dissertation submitted for defence in the form that the author considers satisfactory, but have not yet been published, it would be most appropriate to provide them in the form of direct citations.)

The first criterion is "the lack of functional relevance (adequacy) of the object of social relationships to the central meaning of the concept-word used in the legal text (the "criterion of reality"). Interpretation of a legal text that implies the need to determine whether an object of social relationships that is mediated by the mediareality is within the scope of the possible meanings of the concept-word used in such text, as well as the subsequent

application of law, requires correspondence between such object and the concept-word. In current socio-cultural conditions, the facts of the media-reality are on the "periphery" of the meaning of legal texts. The definition of functional relevance is the establishment, in late Wittgenstein's language, of a "family resemblance" between meanings relating to easy cases of core meaning and peripheral facts of the media reality. That said, the functionality is the legally relevant criterion for such "family resemblance". Based on common sense, functionality itself is defined by how the object of social relationships can be used by actors (subjects of law) in a sense *significant* for the intersubjective social reality. With this approach, if, for example, a social institution for trading of virtual objects — the artifacts of the media reality — has emerged, then "family resemblance" between them and the core meaning of the legal concept-word "property" can be established. It should also be taken into account that new media are defined by such qualities as fractality, automation, variability, and transcoding [Manovich L., 2001], and this, in most cases, predetermines the impossibility of structural adequacy of the artifacts of new media and the core meaning of the concept-words of those legal texts which are oriented towards establishing of technologically neutral rules of behavior. In the context of this research, the notion of functional relevance is opposed to the "fantasy nature" of social relationships object in relation to the legal reality. It is necessary to emphasize that here we are not talking about the fantasy nature of an object as such (in virtual reality, all objects are to some extent of fantasy nature), but about the fantasy nature of representing the key functional properties of the object in virtual reality (i.e., what the objects "do" rather than "how they look")[6].

The lack of functional relevance, even though it is necessary criterion, is not sufficient to make proper conclusion in each particular case. Therefore, "the criterion of functional adequacy should be supplemented by the

[6] Furthermore, in fact, the criterion under consideration is designated as the "criterion of reality" because objective law is by definition not possible as a simulacrum. If there is something that has certain external features of law in a society, but it is a simulacrum, there is no law in such a society. The existence of generally accepted and obligatory rules of conduct (one of the main features of law), even if they are implicit or different from those formally declared, is an empirical social fact of the intersubjective social reality. A separate legal text or other legal phenomenon can exist as a simulacrum, but law as a whole cannot. Thus, law is not a simulacrum, and simulacra cannot be included in the legal reality, except for the cases where the simulacrum itself acts as a socially significant object of the relationship. In view of this circumstance, there is a need to define the second criterion of common sense in the application of law and the interpretation of legal texts in relation to the mediareality".

criterion of convertible socio-currency value, which can be justified on the basis of the concept of generalized symbolic media, developed in theoretical sociology (the "criterion of seriousness). Hence, if the object of social relationships, interpreted as an external referent of value, has convertible "socio-currency value" — and we are talking about such generalized symbolic media as money, political power, influence and other carriers of inter-subjective values, which are constitutive of social reality, — then the application of law to the relationship with such an object is within the limits of common sense. If not, then applying law to such relationships would be *potentially* absurd (depending on whether or not the "criterion of reality" is also met). Possible criticism of the name of the criterion on the basis that the word "seriousness" implies a subjective attitude rather than an intersubjective quality, whereas the term "significance" would be more appropriate, does not seem convincing. "Significance" can also be subjective. Importantly, the way in which the game is played, and seriousness in the context of simulation is recognized in game studies, which are an essential part of the methodology of the approach discussed in this paper.

To summarize, "the proposed approach can be conceptualized in the term *"semantic limits of law"*, which implies the specified criteria of reality and seriousness, and expresses the philosophical and dogmatic-legal concept of the relation of real law to the simulation, updated in the conditions of the medial turn. The use of this term can be legitimized in academic discourse by analogy with the effect of legal norms in "ordinary" space and through the concept of the mediaspace as a symbolic space in which both socially significant meanings and simulacra can be found, setting the direction of the problem of relations between the sign and the signified in jurisprudence. The philosophical legal significance of the concept of the semantic limits of law is expressed in the understanding and explanation of the problems of law in the conditions of the medial turn. The dogmatic significance of the concept of the semantic limits of law is expressed in the fact that it allows to apply the criteria of reality and seriousness for the definition and justification of the absurd, not corresponding to the common sense, cases of interpretation of legal texts and application of law, and therefore can be used in the academic-grounded analysis of legal texts and law enforcement decisions, as well as in the applied legal argumentation. In total, this approach can be considered as a kind of reinvented magic circle test.

6. Practical Application of the Reinvented Magic Circle Test

Let us consider how this works in relation to the initial example with *Minecraft* blocking. The intellectual operations that reflect application of the concept of semantic limits of law can be summarized and illustrated as the following sequence that is custom-tailored to a legal collision that already happened and has to be assessed (depending on the task at hand, some steps may change their position).

In the case of restricted information on blocking a website containing a description of a recipe of "explosive" in a videogame, there are intuitive notions about the absurdity of the result of the interpretation of the relevant legal text. Hence, the first step is to make a hypothesis about the absurdity of the result of interpretation of certain legal text or application of certain law.

By means of abstraction, a functional feature of the central meaning of the norms on counteraction to terrorist activity that relate to "explosives" is singled out. From the point of view of common sense, they are oriented to what can really explode. This is the process of analytical determination of the core meaning of the concept-words used in the legal text for further use as a "reference point" for checking the functional adequacy ("the criterion of reality") of the identified object of social relationships.

Then, it is necessary to single out the scope of those objects that generally can be subject to law, and determine from what angle they may be subject to law. Within any complex social relationships, from the legal point of view, there is a complex factual composition, including several objects, which may be in any combination of connections with generalized symbolic media. In the present case, this would be recipe of "dynamite".

Verification of the functional adequacy of the identified object of social relationships to the core meaning of the relevant concept-words of the legal text. If something in reality (or mediareality, but so that the effect takes place in reality) "behaves" as an object modeled in the results of the analysis of the core meaning of the legal norm, then this is "it".[7] However, this is not the

[7] By the way, this principle is perhaps even more obvious for the problems of virtual property: if something can be sold for real money, it is not absurd to consider, *a priori*, the possibility of applying property rules to this object. Here it becomes obvious that the meaning of building a special concept of the semantic limits of the law (i.e. reinvent the magic circle) could be questioned if functional adequacy was an objectively exhaustive criterion.

case. Still, even if the recipe of dynamite is fictitious, common sense suggests that game content could potentially be evaluated from another normative point of view — for example, if the game has become a tool for broadcasting terrorist "values" in social reality.

Assessment of the convertible socio-currency value of the object of social relationships from the point of view of theoretical and empirical sociology. The key method is mental experiment that ideally is performed on the basis of empirical data, on the convertibility of the value component of the object under study, based on the idea of external referents of value of generalized symbolic media.[8] For the purposes of this discussion, let us refrain from sociological studies now, but assume that this criterion is not satisfied.

Structuring of the legal argumentation by "translating" the key arguments of the analysis into the language of legal dogmatism. This is necessary so that the semantic content of an argument can be incorporated into a system of rational legal reasoning, which itself serves as an external referent of value ensuring the functioning of the legal system as a subsystem of general social system based on generalized symbolic media such as value commitments and, especially, influence.

The last stage is of particular importance from the standpoint of legal dogma. For example, following the tradition of legal reasoning and the well-established practice of using the word "absurd" in law enforcement acts, the conclusion that the result of a legal interpretation implies the extension of the legal norm to social relationships whose subject matter does not possess the qualities of "reality" and "seriousness" at the same time may be expressed in the phrase "absurd interpretation of the [legal text]". The notion of a legal relation, the subject of which has "socio-currency value", can be correlated with the dogmatic notion of "the most important social relationships" (commonly used to describe what normative legal acts are intended to regulate), the notion of "external referent of value" — with the notion of "special object of legal relation", etc. and *vice versa*.

[8] Leaving aside the main example from *Minecraft*, another good example clarifying this thesis is videogame *America's Army* that has become the subject of more than one academic study. This videogame was specially created by the US Army to promote military service and direct recruitment [Robertson A., 2017]. Besides this feature, it is an ordinary videogame. In other words, being a videogame normally used for entertainment, it simultaneously and apparently is an external referent of the value of such a generalized symbolic media as [political] power.

Conclusion

In the conditions of medial turn, legal conflicts related to the question of the limits of possible "interference" of law into the field of virtual in the broad sense of the word become quite relevant. This no longer concerns special legal collisions related to virtual property, but presupposes much broader context of the question how law should relate to mediareality that quite often contains various simulacra that should not be subject to law.

Interpretation of this problem for the purposes jurisprudence, from the technical (legal-dogmatic) point of view, involves the analysis of issues of legal interpretation and, specifically, the relationship between absurdity and common sense in the interpretation and application of law. At the same time, we are, first of all, interested in that very kind of absurdity, which is determined by going beyond the boundaries of the "area of meanings" of legal texts as a phenomenon aimed at the social reality of everyday life. The limits of law that define the boundaries between common sense and this kind of absurdity cannot be found in classical concepts of dogmatic jurisprudence or in currently familiar interdisciplinary research, nor the existing concepts of magic circle can be applied to formulate the relevant universal principle.

This paper suggests to reconstruct such boundaries using the concept of generalized symbolic media, where the external referents of value are the objects of social relationships, in connection with which the question of the fundamental possibility of applying law arises. Thus, the kind of magic circle necessary for law realize its functions as a conventional and formally defined model of social reality is determined by the constitutive elements of such social reality — the external referents of value of generalized symbolic media.

References

Abrutyn S. (2015) Money, Love, and Sacredness: Generalised Symbolic Media and the Production of Instrumental, Affectual, and Moral Reality. *Czech Sociological Review,* no 3, pp. 425–471.

Bourdieu P. (2019) *Economic Anthropology: Course of Lectures at College de France (1992–1993)*. Moscow: Delo, 408 p. (in Russian)

Castronova E. (2004) The Right to Play. *New York Law School Law Review,* no 1, pp. 185–210.

Consalvo M. (2009) There is No Magic Circle. *Games and Culture*, no 4, pp. 408–417.

Duranske B. (2008) V*irtual Law. Navigating the Legal Landscape of Virtual Worlds*. Chicago: ABA Publishing, 461 p.

Efremov A.A. (2017) Formation of the Concept of Information Sovereignty of the State. *Pravo. Zhurnal Vysshey shkoly ekonomiki*, no 1, pp. 201–215 (in Russian)

Fairfield J. (2009) The Magic Circle. *The Vanderbilt Journal of Entertainment and Technology Law*, no 4, pp. 823–840.

Fuller L. (1968) *Anatomy of the Law*. New York: Praeger, 355 p.

Huizinga J. (1949) *Homo Ludens. A Study of the Play-Element in Culture*. London: Routledge, 220 p.

Lehdonvirta V. (2010) Virtual Worlds Don't Exist: Questioning the Dichotomous Approach in MMO Studies. Available at: http://www.gamestudies.org/1001/articles/lehdonvirta/ (accessed: 24.05.2019)

Lessig L. (1999) The Law of the Horse: What Cyberlaw Might Teach. Available at: http://cyber.law.harvard.edu/works/lessig/finalhls.pdf. (accessed: 24.05.2019)

Likhachev N. (2012) Russian Eve Online portal has been blocked for guidance on drug use. Available at: URL: https://tjournal.ru/flood/46910-eve-space-block (accessed: 10.12.2018) (in Russian)

Manovich L. (2001) *The Language of New Media*. Cambridge: MIT Press, 202 p.

Raessens J. (2010) *The Ludic Turn in Media Theory*. Available at: https://dspace.library.uu.nl/handle/1874/255181 (accessed: 10.12.2018)

Robertson A. (2017) *America's Digital Army: Games at Work and War*. Lincoln: University of Nebraska Press, 228 p.

Savchuk V.V. (2014) *Mediaphilosophy — Rush of the Reality*. Saint Petersburg: RHGA Publishing, 109 p. (in Russian)

Saveliev A.I. (2014) The Legal Nature of Virtual Objects Purchased for Real Money in Multiplayer Games. *Vestnik grazhdanskogo prava*, no 1, pp. 127 –150 (in Russian)

Stenros J. (2012) In Defence of Magic Circle: The Social and Mental Boundaries of Play. Proceedings of DiGRA Nordic 2012 Conference: Local and Global Games in Culture and Society. Available at: http://www.digra.org/wp-content/uploads/digital-library/12168.43543.pdf. (accessed: 10.12.2018)

Yakovlev A. (2018) I work at Roskomnadzor. *The Village,* 26 Jun. 2018. Available at: URL: https://www.the-village.ru/village/people/howtobe/316129-zapreschalschik (accessed: 24.05.2019) (in Russian)

The Voice and Speech Processing within Language Technology Applications: Perspective of the Russian Data Protection Law

Ilya Ilin

PhD Student, School of Law, University of Tartu. Address: Näituse 20, 50409 Tartu, Estonia. E-mail: ilya.ilin@ut.ee

Abstract

Language technology (LT) in its broad sense comprises speech technology, computational linguistics, and natural language processing technology. These technologies are expected to have great economic potential and a considerable impact on the everyday life of society. The development of LT fosters applications for artificial intelligence (AI) and broadens the horizon for its advancement. LT deals not only with written forms of linguistic expression but also extends to voice and speech. Voice excluding speech or its contents is a combination of unique physical patterns, such as vocal qualities, volume, speed, and certain other biometric data. Voice can provide medically relevant information, e.g. about a person's mental state, stress level, etc., which is potentially sensitive medical data. Voice with inclusion of speech content can also include personal data (e.g. name, address, ID number, etc.). Consideration of voice and speech as personal data presents a range of legal vulnerabilities and challenges for developing and disseminating LT. This paper explores the extent to which the special regime used for personal data derived from voice and speech affects how it is processed and how it bears on the development and dissemination of LT. This investigation will identify legal vulnerabilities that arise in this connection, and its findings should be useful to both researchers and entrepreneurs in LT. The results of this study provide a basis for further research into LT and related legal issues concerning personal data in Russia.

Keywords

personal data, protection; biometric data; data-intensive product; language data; language technology.

For citation: Ilin I. (2020) The Voice and Speech Processing within Language Technology Application: Perspective of the Russian Data Protection Law. *Legal Issues in the Digital Age,* no 1, pp. 99–123.

Introduction

The rate of growth in language technology (LT) and its popularity indicate both that this field has great economic potential and that it will have a considerable impact on social development. LT in a broad sense comprises computational linguistics, speech technology, and natural language processing technology. The development of these technologies fosters artificial intelligence (AI) applications and broadens the horizon for its advancement. Examples of LT can be found in almost every aspect of our life. These applications vary from grammar checkers and text translators to applications that can control complex machines, synthesize voice, identify people, and communicate with them.

LT deals not only with the written forms of linguistic expression which generally refers to words, but also includes voice and speech as core elements of the communication process. Voice makes the communication process fast and facilitates inputs of data and interaction between computers and people (Holmes W., 2001: 1).

Voice and speech can be used as an element of language data (e.g. vocalized texts, audio records, broadcasts, etc.) for creation of models and datasets or as the input or output for LT products and applications.

The usage of voice and speech within LT requires legal compliance with the regulations that are applicable, and that to a large extent depends on the legal status of voice and speech. The human voice and speech are legally complex phenomena. Voice and speech can be simultaneously covered by copyright, related rights (mainly a performer's rights), rights of the data subject and personality rights. This study focuses on voice and speech from the perspective of Russian law pertaining to data protection by examining the development and dissemination of LT within the legal framework defined by the Russian model of data protection.

In most cases, voice and speech are analyzed together as one complex object. At the same time, one should note that there is a difference between the terms "voice" and "speech". Voice refers to a process that creates acoustic waves. refers to a process that creates phonemes. In other words, it is possible to consider voice as the vocal component of speech (Behrman A., 2017: 4).

Voice without speech and its contents refers to a combination of unique physical patterns such as vocal qualities, volume, speed and certain other

biometric data. Voice can provide medical information, e.g. person's mental state, stress level, etc. and can contain sensitive medical data. Voice in connection with speech content can also include personal data (e.g. name, address, ID number, etc.).

The difference between these two terms should be recognized. When it is essential for analysis, voice and speech may be studied separately from each other.

Consideration of voice and speech as personal data presents a range of legal vulnerabilities and challenges due mainly to the necessity of processing voice and speech for the purpose of developing and disseminating LT. This paper will explore to what extent the special regime for handling personal data affects the development and dissemination of LT, and it will identify and classify the related legal liabilities. The paper should be useful both to researchers and entrepreneurs in LT. The results of this study provide a basis for further research into LT and legal issues concerning personal data in Russia.

The paper is divided into three main sections and a conclusion that summarizes the findings. The first section focuses on the types of personal data with respect to the context of voice and speech processing within LT. The second section analyzes the data protection rules for voice and speech processing. Legal compliance with these rules affects LT development and dissemination. The third section aims to identify the limits of such compliance. The identification of limits is based on legal analysis provided in the previous sections and on the material, temporal and territorial scope of the data protection regulation.

1. Definition of Voice and Speech as They Relate to Data Protection

The right to personal data protection arises from developments in technology. (Hijmans H., 2016: 48) The development of the information and communication (ICT) sector, the increase in cross-border data flows, and the transition to a digital economy have led to problems caused by easy access to personal data (Hungerland F., et al., 2015: 33, 57). In this context, personal data requires a special regime of legal and technical protection. The special legal regime for personal data, on the one hand, ensures protection of the rights belonging to the subject about whom data has been collected. On the other hand, it places a legal restriction on its optimal usage by ICT products.

The first problem in personal data protection is to identify which data is personal. Obviously, such data as names, passport data and addresses are personal. However, determining what is personal may be more involved when it comes to more legally complicated things such as voice and speech. At the same time, consideration of voice and speech as personal data places them under a special legal regime and therefore affects their further processing and use.

There are two general approaches to the analysis of voice and speech with respect to personal data protection (see fig. 1)

According to the first approach, voice and speech are to be regarded as a general category of personal data. The main focus of this approach is on speech content (speech data).

The second approach considers voice without much emphasis on speech data and content. The main focus is on voice and its unique combination of physical patterns that is legally designated as belonging to special categories of personal data (e.g. health data, biometric data).

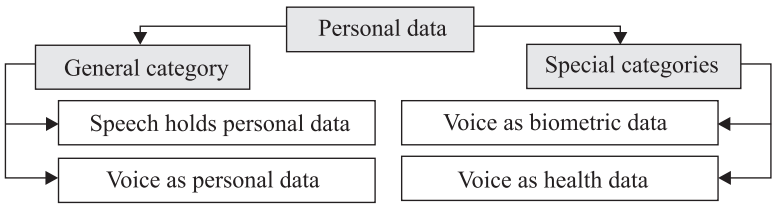

Fig. 1. Voice and speech as personal data

Russian data protection regulations apply to speech processing in the event that the speech data and its content include personal data. The Federal Law "On personal data[1]" defines personal data as any information that refers to an identified or identifiable natural person (data subject[2]). This definition is broad and covers practically any data about individuals. For instance, existing case law has found that the following kinds of data are personal: surname, name and patronymic; year, month, day and place of birth; address; family and social status; property status; education, profession and

[1] Federal Law "On personal data" No. 152-FZ dated 27 July2006, entry into force: 26 January2007. Available at: URL: https://pd.rkn.gov.ru/authority/p146/p164/ (accessed: 18.05.2020). All translations from Russian into English are by the author unless otherwise noted.

[2] Article 11 Federal Law "On personal data" No. 152-FZ.

income[3]; passport data[4], e-mail address[5], and information on crossing national borders[6].

This broad understanding of which data are personal implies that voice and speech should be regarded as personal data whenever they refer to an identified or identifiable data subject.

However, there is still the question of how to apply the data protection regulations when LT developers do not know the identity of the subject whose voice and speech data are being processed within LT. For example, there could be voice samples without any linked descriptions and information. The Federal law "On personal data" does not provide a definite answer to this question. At the same time, the European Court of Human Rights (ECHR), whose case law applies to Russia, does provide protection under those circumstances[7].

The Russian data protection regulations specify three main categories for personal data: general, special and biometric personal data. There is also a fourth category of personal data — publicly available personal data — which was established by Decree of the Government of the Russian Federation No. 1119 "On approval of the requirements for the protection of personal data when processing them in information systems of personal data[8]".

Russian data protection law defines publicly available personal data as data that has been included in publicly accessible sources (directories, ad-

[3] Case law: Presidium of the Russian Supreme Arbitration Court, Resolution in case No. A36-5713 / 2014, dated 29 April 2015, available at: URL: https://kad.arbitr.ru/Card/21af41bd-86ed-4551-b372-10bb6499cf3d (accessed: 18.05.2020)

[4] Case law: Appeal Determination of the Moscow City Court dated 22 May 2014, No. 33-14709, available at: https://mos-gorsud.ru/mgs/services/cases/appeal-civil/details/957f8cd4-63f9-4f26-bfc2-223eec1fb06c?caseNumber=33-14709 (accessed: 18.05.2020)

[5] Case law: Kalininsky District Court (St. Petersburg, Russia), Decision No. 12-253 / 2015 dated 26 May 2015, available at: URL: https://kln--spb.sudrf.ru/modules.php?name=sud_delo&name_op=sf&delo_id=1540005 (accessed: 18.05.2020)

[6] Case law: Moscow City Court, Appeal Determination dated 10.04.2014, No. 33-11688, available at: URL: https://mos-gorsud.ru/mgs/services/cases/appeal-civil/details/9b7aa84e-2dc9-4599-8f70-4edb1a9eb708?caseNumber=33-11688 (accessed: 18.05.2020)

[7] Case law: ECHR. *S. and Marper v. the United Kingdom*, Nos. 30562/04 and 30566/04 [GC], 4 December 2008, § 84. available at: https://rm.coe.int/168067d216 (accessed: 18.05.2020)

[8] Clause 5 of the Decree of the Government of the Russian Federation No. 1119 "On approval of the requirements for the protection of personal data when processing them in information systems of personal data".

dress books[9]) with the explicit consent[10] of the data's subject. The placement of personal data without explicit consent in public sources does not automatically make it publicly available[11]. Publicly available personal data is still considered personal data and should be processed in compliance with data protection regulations[12]. However, there are fewer requirements for processing it. For instance, those data may be processed without consent[13]. Publicly available biometric data, however, is an exception, and it may be processed only with the consent of data subject.

The publicly available category of personal data is excluded from the general tripartite division of the personal data analyzed here for two reasons. First, the Federal law "On personal data" does not classify it as an independent category; and second, it is reasonable to assume that the availability characteristic in general refers to the location and manner of data storage rather than to the characteristics of the data itself.

One special category of personal data is data that indicates political opinions, racial or ethnic origin, philosophical or religious beliefs, and health or sexual orientation[14]. Biometric data are those that refer to the biological and physiological characteristics that can be used to identify a person[15] (e.g. DNA, fingerprints, voiceprints, the image, eyes, body structure[16]).

The tripartite division of personal data into general, special and biometric is the initial prerequisite for data processing. For instance, biometric data can be processed only after the explicit consent of the data subject has been received[17]. Processing of the special category of personal data is generally

[9] Article 8 (1) Federal Law "On personal data" No. 152-FZ.

[10] The data subject has the right to withdraw consent (Article 8 (2) Federal Law "On personal data" No. 152-FZ).

[11] Case law: Decision of the Moscow District Arbitration Court of 09 November.2017 in case No. A40-5250/2017, available at: https://kad.arbitr.ru/Card/eb1907d9-be95-4b0e-85c7-0481aef89b31 (accessed: 18.05.2020)

[12] Article 6 (1) Federal Law "On personal data" No. 152-FZ.

[13] Article 6 (1) Federal Law "On personal data" No. 152-FZ.

[14] Ibid. Article 10.

[15] Ibid. Article 11.

[16] "Explanations of the issues in attributing photo, video, fingerprint data and other information to biometric personal data and the features of their processing" issued by Roskomnadzor on 30 August 2013, available at: URL: http://www.garant.ru/products/ipo/prime/doc/70342932/ (accessed: 18.05.2020)

[17] Article 11 Federal Law "On personal data" No. 152-FZ.

prohibited[18]. In addition, the different categories data require different levels of protection (Krivogin M., 2017: 82–83).

The main criteria used to classify data as personal is the identifiability of a natural person, which to a great extent depends on the context of processing data. Depending on the context, data may be identifiable for one person and not identifiable for others (Oostveen M., 2016: 306).

The context of voice and speech processing within LT is affected by the way it is used and by the technology applied. These factors define the number of activities that may be executed through voice and speech.

Voice and speech can be used in two ways. In the first, voice and speech are considered an input for an existing application (e.g. a voice command made to a voice-operated assistant). The second way is to use voice and speech as language resources (LR) for creating LT applications and to treat them as sources of the language data that they contain,

Creating an LT application largely depends on the existence and number of the LR available (Jents L. and Kelli A., 2014: 164–165). LR are a core element of an LT application and in a broad sense may be described as the range of datasets consisting of texts in oral and written form (language data) which are subsequently used in a machine-learning process (Kelli A. et al., 2018: 79). Creation of LR depends upon two consecutive processes: digitalizsation of language by collecting and transforming the language data into a machine-readable form; and mining texts by analyzing data with a machine-learning algorithm (Jents L. and Kelli A., 2014: 167–170).

These classifications are essential for determining the limits to legal compliance with data protection rules. Those limits are discussed in the third section of this paper.

The context for voice and speech processing within LT is also affected by the technology applied. It could be voice biometrics, speech analysis, speech recognition and speech synthesis. Each type of voice and speech processing focuses on a different kind of information included in voice and speech.

Voice biometrics takes the human voice as a unique personal characteristic that can be used to identify a person along with DNA and fingerprints (Jain A.K., et al., 2004: 4–7). Speech analysis deals with the information which can be obtained by voice, such as level of stress, emotional state,

[18] Ibid. Article 10.

mood and other data concerning a person's mental condition (Chang K., et al., 2011: 1–2). Speech recognition is used to convert speech into text through automatic transcription (Clark A., et al., 2013: 299), and the reverse process is speech synthesis which is used to vocalize a text by converting the text materials into speech (Dutoit T., 1997: 1). Speech synthesis technology does not produce a real human voice that can be recognized and then traced to a particular person. However, that technology is included in this analysis because it is built on neural networks. Neural networks are trained with real examples of human speech (e.g. voice recordings, radio broadcasts), and therefore personal data is still being used in developing of speech synthesis applications (Jents L. and Kelli A., 2014: 172–174). Moreover, personal data could be an output of this kind of technology.

It follows from this description of voice and speech processing by LT that voice and speech can be categorized into the following types of personal data (Table 1).

Table 1

Voice and speech processing and personal data categories

Type of processing	Way used / Information	Personal data category
Voice biometrics	**Input:** special physical characteristics	Biometric data
Speech analysis	**Input:** special physical characteristics	Special data category — Health data
Speech recognition	**Input:** speech content **LR:** Language data for LT creation	General data
Speech transcription	**LR:** Language data for LT creation	General data

Processing voice without a definite connection to speech data and its content should be classified as biometric data. The Russian data protection regulations differentiate biometric data from the other personal data categories. Biometric data reveal the physiological, physical, or behavioral characteristics of a natural person[19]. Voice processing as biometric data in LT has two main purposes: to verify the identity of a person (voice biometrics) or to gain a new piece of information about a person (voice and speech analysis) (Jobanputra N., et al., 2008: 6).

[19] Article 11 Federal Law "On personal data" No. 152-FZ.

Like fingerprints or facial recognition, voice biometrics uses voiceprints as a way to verify and identify a natural person. Biometric systems come in two modes: verification and identification. Verification mode means that a voiceprint is compared with the voiceprint that was originally used to set the identity being claimed. Identification mode means that the system scans the database of voiceprints to find a match, which establishes an identity (Jain A.K., et al., 2004: 1–3). Voiceprints are often used in combination with other categories of personal data. For instance, a bank's voice security system may also ask a client to provide their ID or telephone number. In this scenario, the system checks both the voiceprint and the personal data provided.

The Russian data protection law designates information as biometric data only if the operator uses physiological and biological characteristics for identification purposes[20]. The use of data processing for the purpose of identification is the main characteristic which indicates that a piece of biometric data is personal biometric data[21]. Hence, voice should not be regarded as personal biometric data unless it is used for identification purposes.

Speech analysis processes voice and speech (their characteristics) in order to gain a new piece of information about a person's state. For instance, voice and speech analysis are often used in medical applications. (Chang K., et al., 2011: 1–2) because they can provide data about emotional states, level of stress (Hafen R. and Henry M., 2012: 499–502) or other information concerning health.

At this point it would be natural to ask whether voice should always be considered health-related data or not. Russian data protection regulations do not specify what information is health-related. However, the regulations pertaining to preservation of health do establish the concept of a medical secret and stipulate that all information about requests for medical assistance, information about illnesses, or information obtained through medical treatment and examination should be considered medical secrets[22]. The disclosure and processing of such information are prohibited, although there are a

[20] Ibid.

[21] "Explanations of the issues in attributing photo, video, fingerprint data and other information to biometric personal data and the features of their processing", issued by Roskomnadzor on 30 August 2013, available at: URL: https://pd.rkn.gov.ru/press-service/subject1/news2729/ (accessed: 18.05.2020)

[22] Article 13 Federal law "On the fundamentals of protecting the health of citizens in the Russian Federation" No. 323-FZ, entry into force: 22 November 2011. Available at: URL: http://kremlin.ru/acts/bank/34333 (accessed: 18.05.2020)

few exceptions[23]. The analysis of secret medical data justifies classifying it as a subgroup of the special data category concerning health.

There is no reason to maintain that voice is always health-related data and therefore to provide special legal treatment for it. If there were such a reason, all broadcasting, radio, music and TV shows would have to be classified as processing special data (health data). Voice is properly regarded as health data only when it is intentionally used to obtain information about health.

The analysis of voice and speech as personal data indicates that practical approaches to defining personal data recognize that voice and speech are personal data. It should be noted that there was a case in which recorded voice was not regarded as personal data (Arkhipov V. and Naumov V., 2016: 879). Nevertheless, the common understanding of personal data does not leave much room to argue that voice and speech are not personal data. At the same time, there is still a question about classifying it into an appropriate category of personal data.

Proper definition of the personal data category for voice and speech has important consequences for processing them in LT. Each category has a different level of protection and therefore different regulatory rules for their processing. In the following section, these regulatory rules are analyzed in relation to each respective data protection category. Voice and speech may be classified as in the general personal data category which is covered by general rules of personal data processing and also as in special categories of personal data, such as health and biometric data which have special requirements for their processing.

2. Regulatory Rules for Voice and Speech Processing

Whenever voice and speech are designated as personal data, their processing by LT should be carried out in compliance with data protection rules. Russian data protection regulations define personal data processing so broadly that virtually all manipulations of personal data are included. The Federal law "On personal data" states that processing includes operations with data which are performed by non-automatic or automatic means and are connected with collecting, recording, structuring, storing, usage, transmission and so forth[24].

[23] Ibid. Article 13 (3).

[24] The complete list of the operations that are regarded as data processing is established by Article 3 (3) Federal Law "On personal data" No. 152-FZ.

There are usually several parties engaged in data processing. For instance, the voice identification made by bank security systems involves transfer of the collected voice samples to a voice database that could be in locations remote from the bank. Russian data protection regulations singles out only one entity which can perform data processing (the operator). The Federal law "On personal data" defines the operator as a special entity (a natural or legal person, government authorities) performing data processing and defining its scope, methods and purposes[25]. The operator is the key figure in personal data processing. The technical process of data processing can be arranged by an operator directly or an operator may delegate data processing to a third party[26].

The primary and fundamental principles for personal data processing have been determined by Article 5 of Convention No. 108[27] and are reflected in Article 5 of the Federal law "On personal data". In accordance with Article 5 of Convention No. 108, personal data is to be processed and collected lawfully[28] and fairly[29]; the data must be relevant[30]; processing must be limited to the purposes for which it was stored[31], accurate[32] and kept in a form which allows identification of the data subject no longer than required for

[25] Ibid. Article 3 (2).

[26] Ibid. Article 6 (3).

[27] Article 5 of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, reference ETS No.108, treaty open for signature by the member States of the Council of Europe and for accession by the European Union at Strasbourg 28 January 1981. Entry into force: 1 October 1985, available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108 (accessed: 18.05.2020)

[28] Article 5 (a), Article 5 (b) Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, reference ETS No.108. Case law: ECHR, *Taylor-Sabori v. the United Kingdom* No. 47114/99 22 October 2002, available at: http://hudoc.echr.coe.int/eng?i=001-60696 (accessed: 18.05.2020); ECHR, *Peck v. the United Kingdom* No.44647/98 28 January 2003, available at: http://hudoc.echr.coe.int/eng?i=001-60898 (accessed: 18.05.2020); ECHR, Khelili *v*. Sweden, No, 16188/07, available at: http://hudoc.echr.coe.int/eng?i=001-107033 (accessed: 18.05.2020)

[29] Article 5 (a) Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, reference ETS No.108. Case law: ECHR, *Haralambie v. Romania*, No 21737/03, 29 October 2009, available at: http://hudoc.echr.coe.int/eng?i=001-95397 (accessed: 18.05.2020); ECHR, *K.H. and others v. Slovakia*, No.32881/04 28 April 2009, available at: http://hudoc.echr.coe.int/eng?i=001-92418 (accessed: 18.05.2020)

[30] Article 5 (c) Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, reference ETS No. 108.

[31] Ibid. Article 5 (b).

[32] Ibid. Article 5 (d).

the purpose of storing the data[33]. These are the main principles of personal data processing for guaranteeing a minimum level of the protection for it. Additional rules for personal data processing are based on these fundamentals.

The data protection rules fall into three groups: rules concerning security of processing, the lawfulness of processing, and transparency of processing. Voice and speech may come under the special and biometric personal data category and therefore be classified as sensitive data; or they may be in the general personal data category and therefore be treated as non-sensitive data. The legal framework for processing of these two categories should be examined with this in mind.

The first group of rules stipulates security measures that should be applied in data processing. Under the Russian data protection regulations, these measures should be implemented by the operator engaged in personal data processing. There are two groups of security measures: technical and organizational[34]. The Federal law "On personal data" provides only general provisions for the security measures. In practice, the operator in personal data processing is to arrange for an audit of the information systems that are used for personal data processing and identify which of the four categories is applicable to the systems[35]. Proper identification of an information system's category is crucial for assigning the level of threat and determining security measures[36].

The second group of data processing rules is derived from the principle of lawfulness. This principle presumes that personal data processing must be executed in strict compliance with the law and be legally justified.

Russian data protection regulations allow the following grounds for non-sensitive personal data processing: consent of the data subject; contractual performance; compliance with a legal obligation; protection of vital interests; performance of a task carried out in the public interest; and processing

[33] Ibid. Article 5 (e).

[34] Article 19 Federal Law "On personal data" No. 152-FZ.

[35] According to the Order of the FSTEC of Russia, the Federal Security Service of Russia, and the Ministry of Information Technologies and Communications of Russia No. 55/86/20, 13 February 2008, four classes of information systems exist.

[36] Decree of the Government of the Russian Federation 1 November 2012 No.1119 "On the approval of the requirements for the protection of personal data when processing them in information systems of personal data", available at: URL: https://rg.ru/2012/11/07/pers-dannye-dok.html (accessed: 18.05.2020)

for legitimate interests[37]. Moreover, non-sensitive personal data can be processed for statistical reasons[38] or processing may be done in order to comply with an obligation to disclose information[39].

The rules for processing sensitive personal data vary depending on its data protection category. Hence, the rules are different for voice and speech processing when they are processed as either health or personal biometric data.

Processing of health data is in general prohibited[40]. However, there is no blanket restriction on biometric data processing, which may be performed with consent from the data subject[41].

An analysis of the existing justifications for lawful personal data processing yields the conclusion that the most pertinent legal grounds for voice and speech processing by LT are consent and the legitimate interest. However, if an LT has been developed by research units, the legal justification of performing a task in the public interest by conducting research is applicable as well.

The last group of rules for personal data processing concern transparency in data processing. The transparency of data processing is defined as the data subject's right to ascertain the existence of automated personal data processing, its main purposes, and the identity and habitual residence or place of business of the controller of data processing operations[42].

These principles and rules for personal data processing should be applicable to voice and speech processing by LT under the appropriate personal data category. Compliance with these rules establishes the scope of a data subject's legal rights concerning personal data protection.

However, there is still the question of the limits of this compliance. In other words, does the application of data protection rules extend to voice and speech processing? Furthermore, it should be acknowledged that a data subject's rights are not absolute and that they should be weighed together with other fundamental rights such as freedom of thought, expression and infor-

[37] Article 6 Federal Law "On personal data" No. 152-FZ.

[38] Ibid. Article 6 (1–9).

[39] Ibid. Article 6 (1–11).

[40] Article 10 (1) Federal Law "On personal data". A list of the exceptions to the general rule is provided in: ibid. Article 10 (2).

[41] Ibid. Article 11.

[42] Article 8 (a) Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, reference ETS No.108.

mation, and the right to linguistic and religious diversity (Docksey C., 2016: 197–199) In the next section, the limits on this compliance are investigated.

3. The limits of Compliance with Data Protection Rules

The processing of voice and speech by LT should be carried out in accordance with data protection rules. However, to what extent does data protection regulation apply to voice and speech processing? For instance, suppose that a language model for natural language processing has been created by using personal data. Does that mean that further use of the products based on that model should be subject to data protection regulations?

The limits of data protection regulations can be established by reference to the material, time and territorial scope of the data protection regulations concerning voice and speech processing by LT.

The material scope of data protection regulations pertaining to voice and speech processing can be identified with the various levels involved in LT product development. Those levels include collecting language data for datasets, compiling datasets, annotation of datasets, models, and creation of a product (Kelli A., et al., publication pending).

Collecting language data is one part of the process of creating LR. Voice and speech are used as raw material in the collection stage, and processing them involves only collection of data along with minor technical manipulations of it. Up to this point personal data cannot be anonymized to such an extent that a data subject cannot be identified.

The next level requires that the language data collected be systemized and organized according to specific conditions. However, the language data remains the same as before, and processing modifies only the systematization of the data. As regards data protection, there is not much difference in the legal status of voice and speech processing at the first and second processing levels. However, there is a technical difference in that it becomes difficult for a data subject to identify that their data has been included in the dataset because of the integrated character of the database (dataset).

The creation of the annotated datasets is the third process in collecting and organizing data. The legal status of voice and speech within datasets are the same as at the previous levels. It should be noted that data annotation occurs according to three scenarios for data analysis — automatic, semi-automatic, or physical — and this bears on issues concerning copyright and

identification of an author for such annotations. But the topic of the intellectual property protection for language data is outside the scope of this paper.

Data collection, systematization and annotation all regard voice and speech only as language data without any consideration of biometrics. The data used is not anonymized, and therefore the main concern is that speech will contain personal data. In this sense, the processing of voice and speech at these levels requires compliance with data protection regulations. This processing should be conducted with the legal justifications appropriate for the general data processing category.

The output of collecting, systematizing and annotating language data are various language datasets such as Open Subtitles[43], the Common Crawl dataset[44], the Universal Dependencies treebanks[45], etc. Some of these datasets are employed subsequently for creating language models that describe the rules for a given language and how that language works. In a broad sense, these examples of models may include pre-training language models (Devlin J. et al., 2018: 1–2), various word lists, n-gram lists, dictionaries, and pre-training word embeddings (Grave E. et al., 2018: 1–2, 5). LT relies heavily on models of this kind as the basis for most LT applications.

Considered as personal data, voice and speech in language models are used as general data, and there is no focus on their unique patterns. Therefore, they cannot usually be placed in the special or biometric data protection category, and this is because a language model incorporates only the general category of personal data (e.g. a voice sample concerning the data subject's name or e-mail). The legal liability in the use of such a model can be minimized by anonymizing the personal data Anonymized personal data as understood in Russian data protection regulations are personal data that do not require identification[46]. The processing of the anonymized personal data is subject to fewer requirements (Mavrinskaya T.V. et al., 2017). However, if the data were not non-personal from day one of its collection and were not anonymized throughout their processing, then the anonymization process is nevertheless classified as personal data processing[47].

[43] Available at: https://www.opensubtitles.org/ru (accessed: 18.05.2020)

[44] Available at: http://commoncrawl.org/ (accessed: 18.05.2020)

[45] Available at: https://universaldependencies.org/ (accessed: 18.05.2020)

[46] Article 3 (9) Federal Law "On personal data".

[47] Ibid. Article 3 (3) states that personal data processing is any action (operation) or a combination of actions (operations) performed both automatically and manually with personal data, includ-

The legal handling of language data does not always correspond to the legal handling of the language model that was built on that data. (Kelli A., et al., publication pending) A language model consists of language rules, and it is a very challenging technical task to extract personal data from the model. Even if a model has been built upon language data that contained personal data, the identifiability of data subjects in most cases is lost once the data has been processed.

However, a question remains about the appropriate use of datasets that contain personal data for creating language models. Because these datasets contain personal data, processing then should be undertaken on proper legal grounds[48]. Choosing the proper legal basis for data processing would depend on the way in which the model will be used. The kind of problem that may arise is illustrated by the following scenario. Suppose that a model has been designed for use in research; the personal data collected has therefore been processed as qualifying for the exemption from restrictions on personal data processing when that data is used for research or as having the appropriate consent. But then suppose that it has been disseminated or made available publicly. In that case, the data could be anonymized, or additional consent that covers commercial use and public access should be obtained. Resorting to these solutions may require substantial technical and procedural adjustments.

Creation of a language model can be considered as the stage after which language data is excluded from the end product (i.e. an LT application). For instance, personal data regulations will not cover a synthesized voice (an output of an LT application), although it has been created by using a language model that included personal data. The legal regulatory status of the used language data does not extend to the end product. Therefore, for the purpose of data protection, the language data regulations no longer apply to LT after a model has been created. However, the legal status of the inputs (e.g. voice commands) should still be ascertained by considering personal data protection.

The time limits for data protection are determined by the duration of data protection rights, and it is therefore crucial to establish when the data subject's rights expire. For instance, there was a case in which the Russian voice

ing collection, recording, arrangement, accumulation, storage, specification (updating, changing), extraction, use, distribution (including transfer), anonymizing, blocking and destruction of personal data.

[48] Ibid. Article 6.

company STC Group synthesized the voice of a dead Russian actor and then vocalized a novel with the synthesized voice[49]. Russian data protection regulations protect the personal data deceased persons[50], and the data processing must be carried out in compliance with data protection rules[51]. At the same time, Russian data protection regulations do not establish the duration of that protection. To fill in this gap, it would be reasonable to make the duration equal to that for protection of a person's private life (Vazhorova M.A., 2012: 57–59). That protection persists for at least 75 years after a person's death[52].

Another concern regarding the limits of data protection regulation is its territorial extent and the external effect of such rules. The problem is that LT products are not usually intended for only one country and are often distributed in different jurisdictions. For instance, the speech-to-text system developed by Google[53] supports more than 120 languages and can be integrated with other ICT products developed in various countries with different models of data protection. The limits for compliance with data protection would then also be determined within the national jurisdictions of the countries to which the LT products are distributed. Do LT developers therefore need to comply with the data protection rules applied where their products are distributed? The situation becomes even more complicated when the LT developers use cloud computing which depends upon trans-border data flows. For instance, the speech-to-text system developed by Yandex[54] is distributed as a cloud service. The Yandex cloud is certified as an information system that fully meets Russian data protection requirements[55]. However, in the

[49] An example of synthesised voice is available at: https://www.youtube.com/watch?v= hvaB1exK9rY (accessed: 18.05.2020)

[50] Case law: Decree of the Federal Arbitration Court of the Eastern Siberian District dated 1 July 2008 No. A33-14182/2007, available at: URL: https://kad.arbitr.ru/Card/c7241b92-6ff6-42ee-b233-b398a3080b4b (accessed: 18.05.2020)

[51] If a personal data subject has died, consent for processing their personal data is to be provided by the heirs of the personal data subject, unless the personal data subject gave such consent while still alive. Article 9 (7) Federal Law "On personal data".

[52] Article 152.2 (5) The Civil Code of the Russian Federation (Part I of IV) No. 51-FZ dated 30 November 1994, entry into force: 1 January 1995. Available at: URL: http://www.wipo.int/edocs/lexdocs/laws/en/ru/ru083en.pdf (accessed: 18.05.2020)

[53] Cloud Speech API, available at: https://cloud.google.com/speech-to-text (accessed: 18.05.2020)

[54] Yandex SpeechKit, available at: URL: https://cloud.yandex.ru/services/speechkit (accessed: 18.05.2020)

[55] Available at: URL: https://storage.yandexcloud.net/yc-compliance/conformance_ru_pdp.pdf (accessed: 18.05.2020)

event that this system is integrated into a European ICT product, the problem of complying with both sets of regulations arises as does the issue of the applicability of data protection laws from different jurisdictions.

Russian national data protection regulation as a general rule does not have an extraterritorial effect. Therefore, it does not apply to non-residents that are processing the personal data of Russian citizens abroad. This rule has two exceptions. The first one concerns the data localization requirement, and the second is a consequence of the anti-terrorism measures addressed in the "Yarovaya package[56]".

The localization rule for personal data of Russian citizens was stipulated for data protection regulation by Federal Law 242-FZ dated 27 April 2017[57]. This amendment created a new requirement that data processing operators store, collect and use personal data of Russian citizens only in databases located within Russian territory[58].

The economic impact of the Russian data localization rule has been studied by the European Centre for International Political Economy (ECIPE). According to the Centre's report, the rule mostly harms the economy and reduces the productivity of Russian companies because they must build their data centers in Russia, and they are not allowed to use similar services abroad (even if it were economically feasible). The ECIPE estimate that the resulting economic losses amount to around 0.27% of gross domestic product[59].

[56] Unofficial named after Irina Yarovaya, one of its authors, the package consists of two Federal Laws: (i) Federal law "On amendments to the Federal Law 'On counteracting terrorism' and certain legislative acts of the Russian Federation regarding the establishment of additional measures to counter terrorism and ensure public safety") No. 374-FZ dated 6 July 2016, entry into force: 20 July 2016. Available at: URL: http://kremlin.ru/acts/bank/41108 (accessed: 18.05.2020); (ii) Federal law "On Amendments to the Criminal Code of the Russian Federation and the Code of Criminal Procedure of the Russian Federation with regard to the establishment of additional measures to counter terrorism and ensure public safety" No. 375-FZ dated 6 July 2016, entry into force: 20 July 2016. Available at: URL: http://kremlin.ru/acts/bank/41113 (accessed: 18.05.2020)

[57] Federal Law "On amendments to certain legislative acts of the Russian Federation regarding the clarification of the procedure for processing personal data in information and telecommunication networks" No. 242-FZ dated 21 July 2014, entry into force1 September 2015. Available at: URL: http://www.consultant.ru/document/cons_doc_LAW_165838/ (accessed: 18.05.2020)

[58] Article 18 (5) Federal Law "On personal data".

[59] Available at: URL: http://ecipe.org/publications/data-localisation-russia-self-imposed-sanction/?chapter=5 (accessed: 18.05.2020)

There are four conditions to be met in order for the Russian data protection rule to apply. The first condition is that the information must contain personal data. Second, this personal data must have been collected (the operator must have obtained these data from third parties). Third, the data must have been processed in a way arranged by an operator. The last condition is that this data must be connected with Russian citizens (Savelyev A., 2016: 144–145).

That fourth condition leads to the problem of determining citizenship within ICT technologies. For example, how can the citizenship be identified for a person who gives a command through voice assistance, or how can the citizenship of a person whose voiceprint is processed be identified? Roskomnadzor (the Russian data protection authority) has issued an official opinion[60] that partly solves this problem. According to this opinion, the term "citizenship" is to be replaced with the territory in which processing takes place. If there are uncertainties about the data subject's citizenship, all information processed and collected within Russian territory must be localized at databases located in Russia[61]. However, it is still unclear how to identify and process personal data of Russian citizens that are collected outside Russian jurisdiction.

The localization rule is crucial for the companies that use cloud services localized in other jurisdictions as well for the companies that provide services in the Russian market, even if they do so without having any branches or representatives within Russian territory. For instance, the social network LinkedIn developed by LinkedIn Corporation has no representative offices, departments or other legal entities in Russia. However, because the company breached the localization rule by processing the personal data of Russian citizens outside of Russian jurisdiction, LinkedIn was banned in Russia[62].

In addition to the localization rule, there is one more exception to the territorial reach of Russian data protection. This exception is also connected with the Yarovaya package, although it is not directly concerned with data protection. It has a different material scope than the Federal law "On personal data" and mostly concerns the public sector (national and public secu-

[60] Letter by Roskomnadzor No. 08АП-3572 dated 19 January 2015.

[61] Letter by Roskomnadzor, p. 5.

[62] Case law: *LinkedIn Corporation v. Roskomnadzor* 02-3491/2016, decision of the Tagansky District Court (Moscow, Russia) dated 4 August.2016; appeals determination of the Moscow City Court dated 10 November 2016 case No. 33-38783 / 16. Available at: URL: https://www.mos-gorsud.ru (accessed: 18.05.2020)

rity). The Yarovaya package introduced special anti-terrorism measures that also created new obligations for data storage and data processing.

The measures it introduced require the organizers of information dissemination and telecommunication service providers to store internet traffic (voice and text messages, photos, videos, sounds, file metadata) for periods from six months to three years. The law also requires that, upon issuance of a special order, encryption keys for decrypting internet traffic be provdided in the event that the required data is stored or processed in encrypted form[63].

This package was adopted in 2016; however, some of the issues it raised are still surrounded by legal uncertainties. For instance, it refers to the concept of "organizer of information dissemination", and the law does provide a legal definition of that entity[64]. However, legal analysis of it shows that it is too broad and may cover every internet service and any webpage that somehow interacts with a user (e.g., placing cookies). The definition of the "organizer of information dissemination" is not limited to any national boundaries and therefore may refer to such internet giants as Google, Facebook as well as to other messenger and communication services, such as WhatsApp, Viber, Skype and Telegram and even to blog owners and blog hosting platforms such as Tumblr, Wix and Medium, to administrators for domain names, etc. This legal uncertainty exposes foreign companies to the legal vulnerability of being considered by government authorities as organizers of information dissemination, and that would make it necessary for these companies to comply with the rules described above.

Complying with those rules, however, can be difficult for companies because they would be forced to violate their own data protection rules (e.g. rules established by the General Data Protection Regulation [GDPR[65]]) or

[63] Article 10.1 Federal Law "on information, information technologies and protection of information" No. 149-FZ dated 27 July.2006, entry into force: 26 January 2007. Unofficial English translation available at: http://www.wipo.int/wipolex/ru/details.jsp?id=15688 (accessed: 18.05.2020); Article 46 (1), Article 64 Federal law "On communications" No. 126-FZ dated 7 July 2003, entry into force: 1 January 2004. Available at: http://www.wipo.int/wipolex/en/details.jsp?id=17111 (accessed: 18.05.2020)

[64] Article 10.1 Federal Law "On information, information technologies and protection of information" No. 149-FZ.

[65] 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), dated 27 April 2016, Entry into force: 25 May 2018, available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj (accessed: 18.05.2020)

their contractual obligations (e.g. confidentiality clauses). One of the most consequential examples of the impact of the Yarovaya law package on data protection regulation is the Telegram lawsuit[66] that resulted in Telegram being blocked in Russia[67].

The final problem with the territorial scope of the data protection regulations concerns trans-border data flows and cloud computing. For example, most voice assistants provide their services through cloud computing technology.

For that purpose, it is crucial to identify the country, where personal data was collected and compare its national data protection rules with the Russian ones. The possibility of working with trans-border data can be judged only after making those comparisons.

For instance, legally transferring personal data between Russia and European countries currently is complicated. Even though the Russian and European legislation accept similar international legal grounds for processing personal data and they follow the same data protection principles, their laws have not been harmonized, and their different models for data protection are being applied. Most of the concerns are about how the Russian localization requirement and the requirements of the Yarovaya package relate to the GDPR.

One should note that Roskomnadzor attempted to solve the problem with a localization rule regarding trans-border data flows and stated that the personal data of Russian citizens should be initially collected and stored in databases that are located in Russia. However, it can subsequently be copied and transferred to databases located in other countries[68]. However, the problem of harmonizing the rules in the Yarovaya package with data protection regulation has not been solved.

Conclusion

Voice and speech processing by LT in most cases is regarded as processing of personal data. There are not a great many concerns about the clas-

[66] Case law: Case 02-1779/2018. Tagansky District Court (Moscow, Russia), available at: https://mos-gorsud.ru/rs/taganskij/services/cases/civil/details/2cc72aea-39e7-4f8e-adc9-37d170966efa?caseNumber=02-1779/2018 (accessed: 18.05.2020)

[67] Available at: URL: https://www.nytimes.com/2018/04/13/world/europe/russia-telegram-encryption.html (accessed: 18.05.2020)

[68] Letter by Roskomnadzor.

sification of voice and speech as personal data. However, disputes may arise about which category of personal data covers voice and speech.

Depending on the context of their processing, voice and speech may belong to the general data protection category or to the special (health) or biometric personal data category.

Voice and speech are classified as in the general category when they identify a person (the data subject). This could occur when speech contains some personal data or when a voice sample is linked with information that may disclose a particular person's identity.

Voice and speech are classified as health data when the processing is intended to extract information about emotional state, level of stress or other information concerning health.

Voice and speech are classified as biometric data when they are used in biometric systems for personal verification or identification by analyzing unique vocal patterns.

Each category of personal data comes with different rules for voice and speech processing. Hence, the main risk and legal liability for voice and speech processing is brought about by incorrect determination of personal data categories.

There are two approaches to determining the category of personal data for voice and speech. The first approach presupposes that voice and speech are used as language data (a language resource) for creating a language model. In most cases, these models may include data from the general personal data category and only rarely use sensitive personal data. Because a language model does not use voice and speech for verification and identification, it can be assumed that the biometric personal data categories do not apply to language models nor to the data which was used for their creation.

The second approach presupposes that voice and speech are used as an input to LT end products. What kind of language data were used for creating a product is of no importance for this approach, and the emphasis is on which data category is used to make an LT application work. Depending on the technology used in an application and its functions, these data could be classified as either in the general or special categories of personal data.

Classification of voice and speech as personal data requires LT developers to comply with data protection rules, and any processing of voice and speech should be conducted in accordance with data protection regulations.

The limits to that compliance are defined by the material, time and territorial scope of the data protection regulations pertaining to voice and speech processing. The material scope of data protection regulation varies with the stages in the development of an LT product. The need for legal compliance with data regulations applicable to language data ends once the language model has been created. The processing of voice and speech within end products should be carried out in accordance with the data protection rules applicable to the particular category of personal data.

The time limits for compliance with the data protection regulations are governed by the duration of data protection rights. Russian data protection regulations protect the personal data of deceased persons; however, the duration of such protection is not clear. By analogy with the protection of a person's private life, the author concludes that the period of protection should be at least 75 years after a person's death.

The territorial limits of compliance depend on the applicable data protection regulation. There is no uncertainty about the need for voice and speech processing in applications developed and disseminated within Russian territory to comply with the national Russian data protection regulations. However, the situation becomes more intricate when these activities are performed by a foreign company. The existing legal uncertainty in Russian data protection regulation makes the compatibility of Russian data protection rules with different legal systems (e.g. the one) problematic. The existing regulations on data protection mean that foreign LT developers must comply with both their own national data protection rules and with the Russian ones. Hence, companies may find that they must choose which regulation they will breach. The comparison of Russian data protection regulation as it applies to LT with that of other jurisdictions is a matter for further investigation.

References

Arkhipov V. and Naumov V. (2016) The legal definition of personal data in the regulatory environment of the Russian Federation: Between formal certainty and technological development. *Computer Law & Security Review*, no 6, pp. 868–887.

Behrman A. (2017) *Speech and voice science*. San Diego: Plural publishing, p. 482.

Chang K. et al. (2011) AMMON: A speech analysis library for analyzing affect, stress, and mental health on mobile phones. *Proceedings of Phone Sense*. Available at: http://people.eecs.berkeley.edu/~jfc/papers/11/AMMON_phonesense.pdf (accessed: 18.05.2020)

Clark A., Fox C., and Lappin S. (2013) *The handbook of computational linguistics and natural language processing*. Oxford: Wiley, p. 650.

Devlin J. et al. (2018) BERT: Pre-training of deep bidirectional transformers for language understanding. Available at: https://arxiv.org/pdf/1810.04805.pdf?source=post_elevate_sequence_page (accessed: 18.05.2020)

Docksey C. (2016) Four fundamental rights: Finding the balance, *International Data Privacy Law*, no 3, pp. 195–209.

Dutoit T. (1997) *An introduction to text-to-speech synthesis*. Dordrecht: Springer Science & Business Media, p. 275.

Furey E. & Blue J. (2018) She Knows Too Much — Voice Command Devices and Privacy. *29th Irish Signals and Systems Conference (ISSC)*, The Institute of Electrical and Electronics Engineers (IEEE), pp. 1–6.

Grave E. et al (2018) Learning word vectors for 157 languages. Available at: https://arxiv.org/pdf/1802.06893 (accessed: 18.05.2020)

Hafen R. & Henry M. (2012) Speech information retrieval: A review. *Multimedia systems*, no 6, pp. 499–518.

Hijmans H. (2016) *The European Union as guardian of internet privacy*. Cham: Springer International, p. 564.

Holmes W. (2001) *Speech synthesis and recognition*. London: Taylor & Francis, p. 298.

Hungerland J. et al (2015) The digital economy.Strategy 2030 — Wealth and Life in the Next Generation. Berenberg Bank und Hamburgisches Welt WirtschaftsInstitut. Available at: http://hdl.handle.net/10419/121322 (accessed: 18.05.2020)

Jain A. et al (2004) An Introduction to Biometric Recognition. *The Institute of Electrical and Electronics Engineers (IEEE) Transactions on Circuits and Systems for Video Technology*, no1, pp. 4–20.

Jents L. & Kelli A. (2014) Legal aspects of processing personal data in development and use of digital language resources: the Estonian perspective. *Jurisprudencija*, no 1, pp. 164–184.

Jobanputra N. et al (2008) Emerging security technologies for mobile user accesses. *The electronic Journal on E-Commerce Tools and Applications*. Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.374.5082&rep=rep1&type=pdf (accessed: 18.05.2020)

Kelli A. et al (2018) Processing personal data without the consent of the data subject for the development and use of language resources. Selected papers from CLARIN Annual Conference, 2018. Linköping University Electronic Press. Available at: https://www.ep.liu.se/ecp/159/008/ecp18159008.pdf (accessed: 18.05.2020)

Kelli A. et al (2012) Copyright and Constitutional Aspects of Digital Language Resources. *Juridica International*, vol. 19, pp. 40–48.

Krivogin M. (2017) Peculiarities of Legal Regulating Biometric Personal Data. *Law. Journal of the Higher School of Economics*, no 2, pp. 80–89 (in Russian)

Mavrinskaya T.V. et al (2017) Anonymizing personal data and Big Data technology. *Interactivnaya nauka*, no 16, pp. 1–8 (in Russian)

Oostveen M. (2016) Identifiability and the applicability of data protection to big data. *International Data Privacy Law*, no 4, pp. 299–309.

Savelyev A. (2016) Russia's new personal data localization regulations: A step forward or a self-imposed sanction? *Computer Law & Security Review*, no 1, pp. 128–145.

Soldatova V.I. (2020) Protection of personal data in applying digital technology. *Lex Russica*, no 2, pp. 33–43 (in Russian)

Vazhorova M.A. (2012) The relationship between the concepts of "information about private life" and "personal data". *Bulletin of the Saratov State Law Academy*, no 4, pp. 55–59 (in Russian)

Commentary on the Legal Practice of Database Protection

Protection of Allied Rights to Database: V Kontakte Ltd. v. Dabl Ltd.

Maria Kolsdorf

Lecturer, Law Faculty, National Research University School of Economics. Address: 20 Myasnitskaya Str., Moscow 101000, Russian Federation. E-mail: kolsdorf@hse.ru

Abstract

Analysis of causes and outcome of recent judicial conflict between solid database companies.

Keywords

personal data, social network, exclusive, users, violation, expenditure, compensation, case, claimant, respondent, the Appeals Court, the Intellectual Property Court.

For citation: Kolsdorf M.A. (2020) Commentary on the Legal Practice of Database Protection. Protection of Allied Rights to Database: V Kontakte Ltd. v. Dabl. Ltd. *Legal Issues in the Digital Age*, no 1, pp.124–134.

Under Russian law, a database is deemed to be a collection of independent materials in objective form, systematized to enable such materials to be located and processed with the aid of computers (P.2 of Article 1260 of the Civil Code of the Russian Federation, hereinafter — CC RF).

Databases may be protected in two regimes — as an object of author's rights and/or as an object of allied rights.

For a database to receive protection by virtue of allied rights, the manufacturer of the database must bear substantial costs for its creation (P.1 of Art. 1334 of CC RF).

In the application of the given regulations of the law, practical questions have arisen whether a social network in which a user posts his personal data independently may be recognized as a database protected by allied rights, who holds rights to it, which investments are taken into consideration in assessing the database's protection feasibility, may it be an auxiliary product of the company's activity ("spin off"), and also within which parameters may third parties make use of the data of social network users.

The aforesaid questions were examined by courts in the matter of V Kontakte Ltd. v. Dabl Ltd. (case № A40-18827/2017[1]).

The "V Kontakte" company filed a claim against the "DABL" company and the joint-stock company "Natsionalnoye Byuro Kreditnykh Istoriy" [National Bureau of Credit Histories. — Trans.] for a ruling that the actions of the Respondents in extraction and subsequent use of information elements from the database of the "V Kontakte" social network's users constitute a violation of the Claimant's exclusive rights as the manufacturer of the database containing data of the users of the "V Kontakte" social network, and demanding a cease and desist order obligating the Respondents to terminate the breaching of the Claimant's exclusive rights and the payment of compensation for the said breach of exclusive rights to the amount of 1 rouble.

The "V Kontakte" company, considering itself to be the holder of exclusive allied rights to the database of users of the social network, elements (information units) that are cards of users, asserts that that the "DABL" company, acting for the purpose of manufacturing its own database, engages in automated extraction, copying and systematization of part of the information of the social network's database from all users' cards (*inter alia* from the following columns (fields): surname, given name, data on place of employment and education, place of birth and residence, profiles of the user's friends, photographic images of the user, data on frequency of visits to the network, the communication device through which the network is accessed) and uses this information in its commercial activity. *Inter alia*, the "V Kontakte" company has established that the companies "DABL" and "Natsionalnoye Byuro Kreditnykh Istoriy" have executed an agreement granting the latter the right to use the software support of the Respondent, which in the view of Claimant "V Kontakte" is engaging in extraction and use of a substantial part of its database.

[1] Available at: URL: https://kad.arbitr.ru/Card?number=A40-18827/2017 (accessed: 20.01.2020)

The "V Kontakte" company bases its claim to its exclusive allied rights to the database of its users on the grounds that it produced and continues to produce substantial material and organizational costs for the manufacture and support of the social network's infrastructure, with the exceptional application of which the users' database exists and is expanded, moreover as the expansion and composition of the users' database is the purpose of relevant investments. Furthermore, the "V Kontakte" company stresses that the manufacture of the database of social network users is a vital issue for the Claimant, as the existence of a social network without users (and a database of them) is impossible.

Assuming that the actions of the "DABL" company include the extraction and use of a substantial part of elements from the social database's users, which runs counter to normal social database use and is an unjustifiable infringement of the holder's rights, the "V Kontakte" took the matter to court.

Pursuant to an amicable resolution of the matter with "Narsionalnoye Byuro Kreditnykh Istoriy", the claim against the latter was terminated.

The court examined the claim filed by the Claimant against the "DABL" company. It was established by courts that the "V Konakte" company is the administrator of the "V Kontakte" social network, which forms a hardware-software complex comprising three parts (blocks): hardware, software and information. It ensues from the Claimant's position in the matter, that the information part of the social network is formed of several automated databases, each of which consists of independent elements (materials), systematized by a specific means allowing the location and processing of elements with the aid of an electronic computer. One such base is the database of users of social networks that contains an aggregate of independent elements (users' cards) with information concerning every user registered with the social network. The database is augmented by new independent elements with the aid of the given algorithm for collecting data upon the registration of a new user through the social network's site.

The courts have also established that the "DABL" company is the developer and proprietor of computer programs which, on the basis of its own technological methods and algorithms of search, storage and analysis of data from social networks, including the "V Kontakte" social network, gathers and automatically processes data concerning users of social networks for the purpose of estimating the creditworthiness of potential and existing borrowers. Holding rights to the indicated program, "DABL" offers its own

program products to third parties, facilitating work with social network data for the indicated purposes.

The Court of First Instance ruled against satisfying the claims against the "DABL" company[2]. The court act is motivated by the fact that the "V Kontakte" company was unable to prove that the creation of the database corresponding to the characteristics indicated in article 1260 of CC RF, or the fact of the arising of exclusive rights to the database in the sense of article 1334 of CC RF. *Inter alia*, the Court of First Instance considered unproven the circumstance that the "V Kontakte" company incurred substantial financial, material, organizational and other costs in the manufacture (including processing or presentation of relevant materials) of the database, directed specifically toward the creation of such a database. Clarifying its conclusion, the Court of First Instance cited the rules for use of the "V Kontakte" site, from the contents of which it emerges that the "V Kontakte" company, as the administrator of the social network, does not perform "filling" of the database, and all information entering the database is published by third parties (users of the social network).

The Court of First Instance established that the "V Kontakte" company provided no evidence confirming that the Respondent extracted any materials from the database of users of the social network. The actions of the Respondent were qualified by the Court of First Instance as search and processing of generally accessible information in the Internet, rights to which are the property of users of the social network, and not the "V Kontakte" company. Furthermore, the Court of First Instance indicated that the Claimant provided no evidence concerning the transfer of the entire contents of the database or a substantial portion of its stored materials on to another information medium with the use of any technical means and in any form.

The Court of First Instance also concluded, that as the "DABL" company is not the database administrator and received no special logins and passwords for access to the database, the said company has no technical means of accessing the database or extracting materials from it.

The Appeals Court revoked the decision of the Court of First Instance[3], indicating that the conclusion of the court regarding the absence of a users'

[2] Decision of the Moscow Arbitration Court 12.10.2017. Case № A40-18827/2017. Available at: URL: https://kad.arbitr.ru/Card?number=A40-18827/2017 (accessed: 20.01.2020)

[3] Resolution of the Ninth Arbitration Appeals Court 06.02.2018. Case № A40-18827/2017. Available at: URL: https://kad.arbitr.ru/Card?number=A40-18827/2017 (accessed: 10.12.2019)

database *per se* contradicts the evidence in the materials of the matter. The Appeals Court reached a conclusion regarding the existence of a database of users of the social network, with all the characteristics of a database in the sense of p. 2 of Article 1260 of the CC RF.

Furthermore, the Appeals Court disagreed with the conclusion of the Court of First Instance regarding the absence of substantial costs in the creation of the disputed database. Allowing for the circumstance that the formation of a social network (providing for the existence and filling of the users' database) by the "V Kontakte" company involved considerable financial, organizational and other costs, including costs for the creation and support of its infrastructure (technical equipment ensuring the functioning of servers), purchase of necessary equipment and servers, as well as expenditure on human resources, and the number of user's database elements (over 400 thousand users' profiles) greatly exceeds ten thousand independent information elements, the Appeals Court concluded that the "V Kontakte" company proved its exclusive allied rights to the database.

The Appeals Court indicated further that the materials of the matter overturn the decision of the Court of First Instance that the "DABL" company does not extract and use materials from the database.

The Appeals Court also established that the extraction and use of even a negligible part of the database in the present case is deemed to be a violation of an exclusive right by virtue of p. 3 article 1335 CC RF, as the actions of the "DABL" company contravene normal use of the database and constitute an unjustifiable infringement of the database manufacturer's lawful interests. The Appeals Court based this conclusion on the grounds that the "V Kontakte" company has obligations to all the users of its social network to provide protection for the users' personal data from illegal or accidental access, copying, dissemination, reproduction, collection, systematization, storage and transfer of information from the social network for commercial or non-commercial purposes, or its use wholly or in any part by any means without the user's consent.

Having established the fact of the Claimant's exclusive allied rights to the database and the fact of the Respondent'a violation of the said rights, the Appeals Court satisfied the Claimant's demands in part, obligating the Respondent to cease violation of the Claimant's exclusive rights.

The Intellectual Property Court revoked the abovementioned court acts and directed the case for a new examination[4], noting the following.

1. The database of users of a social network may be recognized as a database protected by an allied right.

The circle of circumstances to be proven upon the examination of a claim for protection of an exclusive right to a database, including responsibility for its breach, includes: the fact of the existence of an object of allied rights (database), the fact of the Claimant's possession of an exclusive right to the indicated object of allied right, and also the fact of the violation of the indicated right by the Respondent.

Establishment of the exclusive right of the manufacturer of the database requires the existence of the putative object of an exclusive right — a database answering to the characteristics contained in p. 2 of Article 1260 and p. 1 of Article 1334 of CC RF.

Acting on the basis of the aggregate evidence in the materials of the case, the Appeals Court established that the database of users of the "V Kontakte" company is a database in the sense of p. 2 of Article 1260 of CC RF, as it is presented in an objective form, contains an aggregate of independent materials concerning users of the social network and is systematized in a manner enabling their location and computer processing.

2. Recognition of an entity as manufacturer of a database does not necessarily require its independent filling of the database, the manufacturer may create conditions for the filling of the database by users.

The court dismissed the Respondent's argument that the Claimant has no exclusive right to the database as filling of the database is performed directly by users and that the "V Kontakte" company does not incur expenses in collection of database elements.

The court noted that it ensues from the provisions of articles 1333 and 1334 CC RF that the manufacturer of a database is an entity that organized the creation of the database and work on the collection, processing and presentation of its component materials. Moreover, the indicated norms do not set a mandatory condition requiring the independent filling of the database by its manufacturer: the creation by third parties of relevant conditions for

[4] Decision of the Intellectual Property Court 24.07.2018. Case № A40-18827/2017. Available at: URL: https://kad.arbitr.ru/Card?number=A40-18827/2017 (accessed: 20.01.2020)

filling the database and performance of subsequent processing and presentation of materials received from such parties also qualify by acting law as actions establishing the legal status of the manufacturer of the database.

3. Assessment of the materiality of expenditure on the manufacture of the database pursuant to article 1334 CC RF requires examination of not an entity's subjective intentions regarding direct investment into the database, but the objective need for substantial expenditure for its manufacture. It is essential to establish the materiality of expenditure for the manufacture of the database, and not the data *per se*.

The "DABL" company denied the existence of an exclusive right to the database, as in its opinion the database of users of the social network is a "subsidiary product" ("spin off") from the activity of the "V Kontakte" company in its administration of the social network.

The court rejected this argument, indicating the following.

P.1 of Article 1334 of CC RF contains a refutable presumption of the materiality of financial, material, organizational or other costs incurred for the purpose of manufacturing a database if such a database consists of at least ten thousand independent information elements (materials) making up the database's content.

Consequently if the manufacturer of the base proves that the database contains more than ten thousand independent elements, proving the immateriality of expenditure for the manufacture of that database, and also organization of work on the collection, processing and presentation of its component materials devolves on the Respondent as a party to the dispute that challenges the presumption established by law.

Russian legislation, specifically, the provision containing in Article 1334 of CC RF, indicates that the manufacturer of a database, the creation of which (including processing or presentation of the relevant materials) requires substantial financial, material, organizational or other costs, holds exclusive rights to extract materials from the database and realize their further use in any form and by any means (exclusive right of the manufacturer of the database). In the absence of evidence to the contrary by the database, the manufacture of which requires substantial costs, is deemed to be a database composed of at least ten thousand independent information elements (materials), comprising the content of the database (second paragraph of p.2 of Article 1260 of CC RF).

Thus, pursuant to the indicated norm, it is essential to examine not the subjective intention of an entity regarding direct investment into the database, but the objective necessity of substantial expenditure for the manufacture of the database. It is also essential to establish the materiality of expenses for manufacture of the database, and not the data *per se.* The assessment of the materiality of such expenditure is an object for examination by courts considering the matter in substance.

In the present case, the Respondent has not denied that the manufacture of the database of users of the social network (including, *inter alia,* the processing and presentation of the relevant materials justifying its existence) calls objectively for substantial expenditure as such a base, the volume of its elements determined by the Appeals Court as substantially exceeding ten thousand independent elements, serves as a fundamental information resource and a key instrument in the functioning of a social network — a site created and supported by the Claimant.

4. The law establishes two different components of violations of exclusive (allied) rights to a database in application of the substantial and insignificant component parts of the database, therefore the court must establish one of the indicated components in every instance.

Pursuant to the second paragraph of p.1 of Article 1334 of CC RF, the component part of the violation of the exclusive right of the manufacturer of a database includes the extraction of materials from the database and conducting their further use without the consent of the holder of rights, with the exception of cases envisaged by the CC RF.

At the same time, extraction of materials is deemed to be the transfer of the entire content of the database or a significant part of the materials contained therein on to another information medium with the use of any technical means and in any form.

P. 3 of Article 1335.1 of CC RF establishes the unacceptability of repeated extraction or use of materials comprising an insignificant part of a database if such actions contravene normal use of the database and prejudice the lawful interests of the manufacturer of the database.

Thus, in the first instance the violation lies in the aggregate of the following actions: extraction (transfer of the entire content of the database or a substantial part of the materials therein to another information medium

employing any technical means and in any form) and the subsequent use of the entire database or the substantial part of its component materials, committed without the consent of the holder of rights (p.1 of Article 1334 of CC RF).

In the second instance the violation lies in the repeated performance of one of the actions (extraction or use) in relation to the insignificant part of the database if it conflicts with normal use of the database and unjustifiably infringes the lawful interests of the manufacturer of the database (p. 3 of Article 1335.1 of CC RF).

The Appeals Court qualifies the actions of the Respondent as a violation of the exclusive right of the manufacturer of the database pursuant to p.1 of Article 1334 of CC RF, and p.3 of Article 1335.1 of CC RF, in view of which the court act on the appealed decision of the Appeals Court contains an internal contradiction.

In connection with this circumstance, the court directed the matter for a review, so that the Court of First Level considered which actions the Respondent actually performed.

5. The Claimant's determination of the amount of compensation sought below the limits envisaged by law does not impede the court from granting the amount demanded in the event of proof of the fact of violation.

The amount of compensation is determined by the court within the limits established by the CC RF, depending on the nature of the violation and other circumstances of the matter, allowing for the reasonableness and fairness of the demand.

P.1 of Article 1311 of CC RF establishes the following limits for compensation in the event of violation of an exclusive right to an object of allied rights: 1) in the amount of ten thousand roubles to five million roubles, determined at the discretion of the court on the basis of the nature of the violation; 2) twice the cost of counterfeit phonogram copies; 3) double the amount of the cost of the right to use the object of allied rights, determined on the basis of the price which, under comparable circumstances, is usually charged for the lawful use of such an object in the way used by the violator.

As noted in p. 43.3 of the Resolution of the Plenum of the Supreme Court of the Russian Federation and of the Plenum of the Higher Arbitration Court of the Russian Federation dated 26.03.2009 № 5/29 "On questions arising in connection with the entry into force of the fourth part of the Civil Code of

the Russian Federation" [5], in considering matters regarding requests for compensation in the amount from ten thousand to five million roubles, the court determines the amount of compensation within the limits envisaged by law at its own discretion, but not in excess of the demand requested by the Claimant.

P. 43.2 of the same Resolution indicates that compensation may be demanded upon proof of the fact of violation.

Therefore, the Claimant's determination of the amount of compensation *per se* being lower than the limits envisaged by law does not impede the court's satisfaction of the compensation demanded in the event that the fact of violation has been proven.

6. A claim for termination of a violation may be made against not only an entity making unlawful use of another party's database, but also against the software developer, facilitating performance of the said activities.

The "DABL" company has asserted that it does not itself extract or use materials from the database, insofar as interaction with sites in the Internet (including, *inter alia*, the "V Kontakte" company) is performed by users of software, the developer of which is the company.

In this connection the Intellectual Property Court instructed lower courts that should it be established that materials from the database are actually being extracted and used, not by the "DABL" company but through its software support, the demands of the "V Kontakte" company are subject to examination with allowance for the circumstance that by virtue of Article 1252 of CC RF, a demand for termination of actions violating a right or threatening its violation, may be filed not only against the entity committing such actions or performing necessary preparations for it, but also against other entities that could terminate such actions.

Conclusion

Thus, the Intellectual Property Court has pronounced the following significant legal positions pertaining to protection of databases.

A social network may be acknowledged to be a database protected by allied rights despite the circumstance that the database is filled by its users

[5] Available at: URL: https://www.wipo.int/edocs/lexdocs/laws/ru/ru/ru112ru.pdf (accessed: 20.01.2020)

themselves, it is unimportant for the acknowledgement of rights to the database as to who placed data directly, the importance lies in who organized the collection of data. Such an organizer holds exclusive rights to the database — the social network.

As Russian law acknowledges the presumption of the existence of substantial investments into the manufacture of a database if it contains at least 10 thousand independent elements, the recognition of an exclusive right to the database requires the Claimant to prove the existence of the indicated number of elements. In the present case the Respondent, disputing the existence of an allied right to the database must present refuting evidence. At the same time the court does not examine the subjective intentions of an entity regarding direct investment into the database, but the objective necessity of substantial expenditure for its manufacture, i.e. it may be a subsidiary product ("spin off") from the company's activity.

If the Respondent has developed a program facilitating the illicit extraction and use of materials from another entity's database, it may face a demand for termination of the violation. In order to establish the existence of the violation, it is necessary to examine the algorithms of the working of the said program for the purpose of determining whether there is an extraction and use of materials from the database, and in what volume.

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.

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.

Выпускающий редактор *В.С. Беззубцев*
Художник *А.М. Павлов*
Компьютерная верстка *Н.Е. Пузанова*

Подписано в печать 15.07.2020. Формат 70×100/16
Усл. печ. л. 8,5.