ISSN 2713-2749

Legal Issues in the DIGITAL AGE

Вопросы права в цифровую эпоху

3/2024

Volume 5

Legal Issues in the **DIGITAL AGE**

3/2024

ISSUED QUARTERLY VOLUME 5

Publisher

National Research University Higher School of Economics

ISSN 2713-2749

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

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

Designer
Andrei Pavlov
Pre-press
Natalya Puzanova

Legal Issues in the **DIGITAL AGE**

Legal Issues in the **DIGITAL AGE**

ISSUED QUARTERLY

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

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

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

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

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

Publication in the journal is free of charge.

All materials are available for free download.

Legal Issues in the Digital Age. 2024. Vol. 5. No. 3.
Вопросы права в цифровую эпоху. 2024. Том 5. № 3.

Digital Age: Civil Law

Research article
УДК: 347
JEL: K15
DOI:10.17323/2713-2749.2024.3.4.30

Obligations in the Digital Environment: Legal Doctrine

Rim Nailievich Adelshin

Russian State University of Justice, 69 Novocheryomushkinskaya Str., Moscow 117418, Russia,

adelshinrn@rsuj.ru, https://orcid.org/0000-0003-3724-7034

Abstract

Aspects of cross-sectoral influence on the spheres of private and its public regulation construct of obligation in the digital environment using the example of utility digital rights. Specific obligation relationships in the form of the exercise of rights under utility digital rights and derivative financial instruments, including under an contract between a forex dealer and an individual, and others that involve the exercise of rights using technical and electronic means. Provisions on changing the norms of the Russian Federation Civil Code regarding new objects of civil rights: utility digital rights, derivative financial instruments or their analogues — digital rights and obligations. The criteria for obligation in the digital environment are considered and conclusions are formulated about the possibility of identifying the properties of obligation: reciprocity, conditionality, potestativeness. A special element is highlighted in relation to obligations in the digital environment. Obligations in the digital environment are presented as a special category of indefinite obligations, digital rights, as new objects of civil rights based on a contract. The results of the action of the norms of Federal Law No. 34-FZ, as well as legislation in general and practice in terms of determining the legal status of participants in relations are analysed. The legal status of the information intermediary determines that it does not have the right to refer to special conditions for exemption from civil liability for violation of intellectual rights under Article 1253.1 of the Civil Code and will be involved in compensation for damage on the grounds common to entrepreneurs, provided for in its Article 401.

Keywords

stochastic obligations; rights in a distributed registry; potestativeness; second right of refusal; virtual obligation; utilitarian digital right; digital financial asset; derivative financial instrument; information intermediary liability; marketplace.

For citation: Adelshin R.N. (2024) Obligations in the Digital Environment: Legal Doctrine. *Legal Issues in the Digital Age,* vol. 5, no. 3, pp. 4–30. DOI:10.17323/2713-2749.2024.3.4.30

Introduction

The structure of obligation in the rapidly growing digital environment infrastructure is quite special. This clearly demonstrates that the digital reality of hybrid transactions is different from a regular civil debt or a duty to perform in its usual form, at least as far as the civil law definition of these relations is concerned. The description of legal phenomena related to cross-sectoral aspects and participation of special subjects in such relations also is quite specific in transactions of this kind.

Because of that phenomenon, and due to the period of validity of changes in the Russian Civil Code introduced by Federal Law No. 34-FZ as well as due to Federal Law No. 259-FZ "On Digital Financial Assets"[1], there is no conclusive answer to the question of the legal nature and structure of obligations in the digital environment; nor is there a mature methodology and a conclusive nomenclature that would put the matter to rest in efforts to develop the global regulation of the smart construct of obligation (even if it is considered a superstructure, still unaccepted in most jurisdictions, and not a civil law construct). Likewise, contractual law theory 2.0 has not taken final shape either. The reason is that this approach, that the doctrine partially terms "technological determinism", is sharply criticized in this area of law. The argument is this case is that it is a technological method that the parties choose to discharge their contractual obligations [Bogdanov D.E., 2023: 35].

Still, the global tasks facing users trying to cope with technology challenges need to be taken into account at least from perspective of gaining competitive advantages of using the technology infrastructure. It creates a cyclic development pattern and calls for a general systemic solution, including legal aspects.

[1] SPS Consultant Plus.

These issues pose a global challenge in the sphere of technological sovereignty policies determine a country's ability to compete in the technology sphere at the global level. Current outlooks for the development of civil law, largely related to the enforcement aspect of digital technology use in property relations, will be determined by the efficiency of regulation model application to the obligations in the digital rights sphere and to the prospects of civil circulation of digital technologies in general. The author believes civil law may regulate all of the above, subject to the following.

Fundamental shifts in technologies affect relations of obligation mediating the relations of exchange and circulation of special objects of civil rights that causes changes in approaches to the regulation of legal categories and institutions that can participate in the circulation. While this phenomenon does not change the idea and purpose of the contractual structure, it adds a special aspect to the way obligations are fulfilled, and, to a some extent, enables to change approaches to the freedom of contract principle. On the whole, the doctrine does not define legal nature of the digital obligation and of the obligation in the digital environment, does not list the attributes characterising this type of obligation, and does not describe limits for application of this legal phenomenon. The question whether general principles of civil law can apply to contractual obligations in their entirety and what is the adequate limit of their application has not been resolved. The fact that there is absolutely no interconnection between legal systems and no synergies between functionality and private interest exacerbates the problems existing in the sphere of high-tech services (sets of platform technological solutions) regulation. E.g., a computer code can influence the shaping of approaches in pricing (anti-competition) of large business structures towards consumers. Also, the information intermediary's legal position can be used dishonestly in this sphere by limiting liability, etc.

The lack of clear-cut rules for regulation of constructs of obligation, the trend to individual regulation without establishing standardised boundaries of these constructs of obligation have given rise to the above-mentioned legal phenomena of a contractual nature. These phenomena tend to obtain a random regime affecting, among other things, correct determination of the list of digital rights. In turn, the development of the civic institution of the object of digital law has led to a cyclical half-result, which gives us reason to believe that it would be premature to ignore the emerging property criteria of such rights; thus, it would be necessary to develop property criteria to involve them properly in the circulation. This state of law and order "naturally" impedes

the technical and infrastructure ability to cope with the global challenges of technological integration and, in effect, obstructs digital sovereignty.

If to look at this as a problem statement and an attempt at an introduction to the theme, we see a clear need for a methodological solution that determines what is the universal (or close to universal) approach for working out ways to develop regulation in this sphere.

1. Descriptive essence of obligation structure in a digital environment

In most cases digital contracts and smart contracts are obligations related one way or another to literal legal contracts; the former ones can be a part of a contract, or a whole contract, or be used to automate the execution of literal transaction.

Obligations in futures transactions with derivative financial instruments are vague. It is a "contract" with no price criteria at the time the parties enter the deal: the price depends on the market (e.g., demand and offer), the terms and conditions of the transaction, and the cost of delivery. In short, this contract is stochastic. In the past, the stochastic nature of such obligations brought about the emergence of terminology that was related to financial instruments in this area and had a clear cross-discipline character. However, after the 2008 global financial crisis, new financial "generators" of market concepts outside of centralised regulation emerged. This gave rise to approaches in law that tend to "expand" towards abstractions and towards a virtualised model of obligation and criteria for valuing this obligation as property already in the decentralised sphere. This is how "stochastically tuned" indeterminate "self-executing", "smart" legal constructs of obligation emerged. However, this fails to address the issue of individual categorisation of the concepts underlying such derivative instruments as digital financial assets ("DFA"), utility digital rights ("UDR") and others, and, consequently, to establish an acceptable balance between the private and public interests of the parties [Kulakov V.V., 2017: 423]; [Egorova M.A., Kozhevina O.V., 2020: 83]; also, this highlights specific peculiarities of their structure—at least, the peculiarities of applying the freedom of contract principle. Special laws in the sphere of the securities market fail to give answers to the above questions, too. Hence, the issue of what should come first, the code or the contract, will remain on the agenda for a long time to come. In this connection, debates continue, and one would logically ask

the question whether a "pure" civil law model is possible as a basis and whether it can apply in full [Kartskhiya A.A., 2019: 13]. In this connection scholars note that the differences between the concept of "code is law" and *lex mercatoria* are expressed in the contradiction of rigid rules, *ex ante* self-executed by software code, and the relationship between special customs and innovative applications that can be applied *ex post* by specialised arbitration courts [Jünemann M., Milkau U., 2021: 1]. Obviously, contract law is in many ways an ex-post instrument for regulating pre-existing contractual relations between counterparties. But as far as smart self-execution is concerned, the transaction that is the basis for the respective obligations is also a private-law regulator that determines the conditions on which the obligations will be formed. Thus, this concept cannot be curtailed: all its parts are important to ensure accurate legal qualification, to categorise concepts for data consolidation and to work out the methodology.

It is still unclear whether law of contract can apply in this case. Is is a controversial issue. The matter is that they were initially developed so as to rely exclusively on technical rules, e.g., the rules embedded in blockchain, and were considered standalone instruments capable of solving various problems that could arise between the parties. However, they failed to stand the real-life test due to the lack of an effective technical legal regulation [Kiviat T., 2015: 608]. Moreover, it is clear that the participants of a distributed ledger not only validate smart obligations but also control their invariability [Bogdanova E.E., 2019: 118].

Therefore, the relevant questions are those that determine the priorities and principled basis at the present moment for the legal regime of such legal concepts and for solving the questions whether synergies are possible when applying general principles of civil law and special principles of digital turnover to solve the problems of law of obligations, corporate law (securities market), and competition law [Inderst R., Thomas S., 2024]. In this connection, it is important to address the point if the institutions and legal remedies of civil law can fully apply to the "laws of the digital market" in general.

2. General description of obligations in the digital environment: the road to conditionality

Participation in a civil obligation means acquiring and executing civil rights and obligations on one's behalf and at one's own financial liability before the creditors, including liability in digital format. Theoretical studies

usually consider legal relations in the sphere of "digital" rights as a dynamic system of "legal relations within the subject of civil law" [Belov A.V., 2007: 75]. And from the view of legal technique they are a legal concept, "the constituent elements of which are objects, subjects, and content" [Volynkina M., 2012: 5].

The civil law method allows, for the purposes of the use of digital rights, to substantiate the conceptual assessment of digital civil turnover, which inherently involves the change of carriers of digital rights through the use of digital technologies that provide sequential mathematical operations of computer code in the form of digital records and which serve as a way to express certification and transfer of digital civil rights to digital objects. This means that the material difference in smart obligations that are initiated and automatically executed is that a smart contract is executed on the contract formation principle by means of a software programme that the parties use to express their will at the time when an agreement is reached on the terms and conditions of the contract, and that a smart contract is a kind of a software veil that covers a regular civil law contract [Željka M., 2021: 166].

Categories such as the presence of virtuality, the digital environment, and its infrastructure require a more comprehensive, renewed understanding of the legal regime of obligations with account of the legal system as a whole. Thus, it is a reason to believe a digital civil smart obligation, unlike its analogue in electronic form, is, according to the previously established criteria, more subjected to the influence of the rules governing the creation of digital technologies. To qualify an obligation that primarily binds, e.g., the execution of a smart contract, a significant starting role will have to be played by legal individual regulators together with technical rules and local acts based on the rules of a distributed data ledger (information system) for such crypto-instruments. That is, the very same regulators can be objects of civil transactions realised as utility digital rights by concluding contracts and issuing tokens for various kinds of services to "support" the platform and with generation of independent values on their basis.

E.g., it should be taken into account that crypto-instruments are the results of IT products (programmes) and of calculations performed by means thereof, i.e., the results of certain algorithms. The software programme, on the other hand, is an intellectual product of human activity. It follows that, at first glance, crypto-assets, as a general rule, cannot be the object of an exclusive right, but they can have distinctive features of and intellectual product– e.g., a programme code that can be activated on physical data carrier.

Hence, the disputed opinion that a crypto-instrument, being an object of digital right, could become an object of absolute right (just as the right of claim was once declared an object of the "absolute" right of obligation [Sazhenov A.V., 2018: 119], has somewhat similar "property features." E.g., the thesis of "thing absolutization" notes: "records in blockchain, limited technologically, represent absolute rights and are similar to natural things: their number is known; they pass from owner to owner in a strictly defined order; they do not contain any *in personam* claims" [Jankowski R.M., 2017: 36]. At the same time, for a possible substantiation of "virtual property", it would be worth mentioning the theory of legal correlates and legal opposites, which deconstructs legal relations into four pairs: claim-rights/duty, privileges/no right, powers/liability, and immunities/disabilities [Hohfeld W.H., 2017: 710].

So, there is a counter-thesis: the idea "digital property" is a new object of civil law follows from the absence of a tangible form; it is an algorithmic code and the result of computer calculations that exists as a virtualised object of law with a value criteria. This code can be used and can circulate outside the IT system whose owner interacts with information intermediaries, and the material value of this virtualised object depends on the number of transactions in the wide sense. While this counter-thesis doesn't enjoy overwhelming support, it still exists as an antithesis to the rejection of the virtual nature of such property. The smart contract proper can also be considered from different perspectives: as a software code, and as an obligation [Efimova L.G., Sizemova O.B., 2019: 30].

So the ideas a close-end joint-stock company may issue the equivalent of stock value in the form of UDRs underscoring its virtual status quo are significant but not critical for the legislator (despite the fact doctrine rejects such transactions, and regulations use them to a limited extent). At the same time, it is impossible to forget the prohibitive background of crypto-asset-for-commodity exchange transactions stipulated in law. Furthermore, some scholars believe that it would be incorrect to introduce the concept in the rules of an individual information system which stipulates that transactions with digital currencies can be performed as with "miscellaneous property": if digital currency is proposed to general public, then it is not related to a particular obligation, either as a means of payment or as an investment. It is an array of electronic data that is generated within a particular information system, has a material value within this system, and there is no particular person obliged to each holder/owner of the electronic data. The exception

is system operators as a special class of information intermediaries according to the rules of the system: normative boundaries/rules have so far only just begun to emerge for them in individual regulation. All these positions and counterarguments give rise to debate and more research.

3. Conditionality and potestativeness

Probably it would be mostly correct to discard the smart contract as an independent regulator. Indeed, basically, the smart contract as a software programme has no substantive legal meaning legal meaning. At the same time, there are no reasons to claim that, broadly speaking, there is no obligation relationship in a transaction when an obligation is executed by means of a smart contract. A smart contract actually pervades the conventional legal relations that are presented in a "digital skin" and are executed by means of the respective digital technologies. And the software decides to execute or terminate an obligation. Therefore, in its essence, the smart contract mediates a concrete obligation relationship that follows from a purchase and sale transaction, a lease, a loan, or a settlement that is tied with the expectation of the proper performance of an obligation by, at least, one party to the transaction. In other words, new types of contractual relations, which are not regulated in the Civil Code, can't be the legal foundation of a smart contract. The novelties in question are as follows: the way of implementing such legal relations, namely by means of crypto-instruments and a blockchain platform; the way of recording such legal relations, namely by means of a programme code or a statement in programming language, the digital object of such legal relations, namely a crypto-asset, crypto-instrument, artificial intelligence, big data, and others. Conditional determinants take a special shape, too. Namely, the obligations are performed by the program in the overall framework of a conditional transaction, and conditional obligations where performance by one party is linked to performance by the counterparty. The priority of performance of a mutual obligation is inherent in the conditional nature itself.

Hence, it is obvious that such action or inaction (the code takes decisions on behalf of both parties, or at least one party) determines the time when the "commanding" nature of such action / inaction manifests itself. This will determine when the condition under the obligation occurs, i.e., when its potestative nature manifests itself. Most probably, it will be necessary to outline this nature in law with respect to such constructs of obliga-

tion despite the fact that potestativeness remains at the discretion of the court and is not applied in positive law. Thus, the digital reality, which is impersonal, abstract, and takes programme code as reference points, is a favourable place for a conditional obligation "to exist in."

If to look at the specificity of the binding nature of a legal relationship implemented through a smart contract, it is worth noting automation inherent in the use of blockchain technology requires that all these types of contractual relationships be conditional, i.e., that they are performed upon the occurrence of certain circumstances set forth by the parties in their written literal agreement. Academic literature has mentioned in numerous papers: performance conditionality is specifically inherent in the execution of an obligation through a smart contract. Scholars point to the conditional nature of a smart contract as one of its characteristics pointing out that the performance of one party's obligation under that sort of a contract is conditional on the occurrence of certain circumstances. Thus, from the point of view of Russian law, this type of relationship may be characterised either as a conditional transaction (Article 157 of the Civil Code) or as a contract in that the performance of one party is conditional on the performance of an obligation by the other party (Article 327.1) [Savelyev A.I., 2016: 123]. In opinion of the author of paper presented, a smart contract has a similar nature: it introduces a conditional aspect to contractual relationships (Art. 327.1) and thus complicates the application of such construct [Kotsar Y.A., 2024: 46].

A party to a smart contract performs its obligations upon the occurrence of certain conditions that can both depend on and be independent of the will of the party as regulated by the provisions of Article 327.1 on the conditional performance of obligations [Grin O.S., Grin E.S., Soloviev A.V., 2019: 55]. The legal fact inherent in a conditional transaction and an obligation with conditional performance leads to a certain legal effect. However, in a conditional transaction, the legal effect manifests itself at the stage when rights and obligations arise or terminate, while in an obligation with conditional performance it appears at the stage when rights are exercised and obligations performed. I.e., obligations with conditional performance may be the legal substance for a legal relationship performed by means of a smart contract.

At the same time, it is not quite correct to consider a smart contract as a purely external form, as a "technological method" of performing obligation. We should agree with the opinion that it is inadmissible to equate

the smart contract only to a specific form of contract, as its use affects the rights and obligations of the parties to the agreement [Akhmedov A.Ya., Volos A.A., Volos E.P., 2021: 20, 79].

Scholars see this influence in the fact that, unlike a contract executed in a regular way, execution through smart technologies is planned for the future, and no outside intervention is possible. Conversely, the execution of an obligation in the "general" version may be subject to modification throughout the life of the contract, again subject to the will of the parties to the contract; this includes circumstances, the occurrence of which determines the fulfilment of a duty.

In light of these issues scholars rightly draw attention to the definition of a smart contract as an "obligation in a digital environment" and to the possibility of applying to such an obligation the principles of general contract law or purely technical principles of platform functioning on the basis of conditionality and reciprocity.

The opinion that the virtuality, the digital environment and its infrastructure require a more complete and new comprehension of the legal regulation of the obligation, taking into account the choice legal remedies in case of non-delivery of the conditional obligation in law as a whole, arises from a certain break-up of relations of obligation (performance by the programme-platform) and from the subsequent choice of the legal remedies, taking into account the definition of Article 328 of the Civil Code. Thus, we believe it is evident that a digital civil smart obligation, unlike its analogue in electronic form, is more subjected to the influence of the rules governing the creation of digital technologies.

Thus, the performance of an obligation in the digital environment will indeed affect the specific nature of this obligation, but will not replace it in its essence. In this regard, if we distinguish between form and content in the smart contract category, it is necessary to should speak exclusively of digital technologies with attention to form. And the content will be the "civil obligation", that is the essence of the legal relations that are performed by means of a smart contract upon the occurrence of the circumstances programmed in the code. Exercise of rights and performance of obligations upon the occurrence of a condition (both an external circumstance and one that depends on the actions of the parties to the obligation) is characteristic of an obligation with conditional performance (Article 327.1). Hence, we can consider a smart contract a form of external expression of this type of obligation.

It would be appropriate to criticize the opinion the smart contract is a conditional transaction. The reason is that it mediates not merely legally significant actions, but precisely the qualitative component of the contract: its performance, and the transition (change of record behind the holder) of the digital asset from one account to another and to its new holder [Efimova L.G., Sizemova O.B., 2019: 30].

These aspects of a smart contract as a conditional transaction imply their separate study in setting the limits and development of approaches to understanding the fundamental basis of freedom of contract in the digital environment in such transactions, which enable understanding the freedom of contract in each part of the transaction responsible for delivery, since the parties regard such performance as an indication in a conditionally separable understanding of the counter-performance of the obligation in one part of the transaction from the other. At the same time, such separable understanding of reciprocity performance may provide an independent qualification criterion.

Programming a smart contract one can use any kind of condition: a contingent condition, a dissolving condition, or a potestative condition. This is determined by the essence of the legal relations form the legal basis of the programme code.

Also relevant is the issue of methods to protect the right in case the programmed condition does not occur. It is impossible to apply here the fictitious occurrence of condition, which is applied in case of violation of an obligation with conditional performance, because this method of protecting the rights is based on evaluations, and any evaluations are totally out of place in the programme code. That said, we believe it is possible to apply the classical remedies, such as damages, in the general course of a lawsuit.

To summarise, it is possible to distinguish the opinions a smart contract is a form of external expression of the rights and obligations arising from "traditional" forms of contractual relations, but implemented and executed on a digital platform using digital tools. A civil law conditional obligation can be the subject matter of a smart contract. This obligation can be performed by computer code programmed for specific circumstances, and it is what the parties have in mind to resolve their issues when they enter into such transactions by joining the platform. Thus, the application of the provisions of the Article 327.1 to relations performed by means of a smart contract establishes a separate type of obligation: the obligation with con-

ditional performance. It is important to note that the conditional relation implemented by means of a smart obligation should be reflected in the law system as a whole rather than only within a regulatory control framework and on a case-by-case basis.

4. Cross-sector linkages and functional approach

The task of correlating private and public principles for the development of methods invariably arises in applying cross-discipline approach for legal regulation of the obligation relationships. This gave rise to the need to study, e.g., the utility component of digital rights.

In view of the above, it would be relevant to study the cross-discipline impact on the legal relationship in the digital circulation of various legal phenomena associated with heterogeneous sector affiliation. This manifests itself in the necessity to divide information law into three conventional groups for the purposes of modernisation: law on information itself; law in the field of modern information technologies; and telecommunications law.

The request for utility reinforces the need to thoroughly analyse the concepts of information and civil law with respect to the regulation of digital relations. In this regard, we find interesting the functional cross-discipline approach. It is synthesis, which partly has a basis of mathematical origin [Efimov A.V., 2022: 95], and partly includes an instrumental approach [Fillipova S.Y., 2013: 350] for a transaction arrangement by means of setting up the digital environment infrastructure (preparing a platform solution) and meeting the public guidelines of the regulators.

It is evident that the mutual definition of the substance of the private element of UDR is predetermined by the public element in the form of a corresponding permission and obligation formalised by a transaction in the field of SaaS, IaaS, and PaaS services. Special attention should be paid when selecting a legal regulatory regime for such intra-functional service UDR as a bridge between private and public legal component through a functional and instrumental approach. In the former case, this will define a basis for the preparation of a correct circulation of such private UDRs, and the latter one will provide a basis for the circulation of investment-grade digital assets (e.g., digital financial assets, hereinafter referred to as DFAs).

The definition of Article 141.1 of the Civil Code does not provide clear criteria for resolving questions about the form of a right in the private sphere

in relation to digital rights. Therefore, upon analysing the scope of its application, we see that we can also apply here the general principles of civil law to contractual obligations to a reasonable extent. Thus, the following questions arise: whether the close concept of the legal regulation model is universal, taking into account the intersectoral relations in the private law of the digital environment, whether it is necessary to specify the content of the norm, and within what limits this should be done.

Scholars note law should be divided into individual areas by the subject of legal regulation, i.e. depending on the differences in the contents of the public relations that law regulates [Venediktov A.V., 1954: 29]. Also, scholars note "interbranch relations in law, including private law, are defined as relations of mutual dependence, conditionality and commonality between legal branches".

Moreover, they clearly state "being inside private law, civil law is interconnected not only with branches of private law, but also with branches of public law—administrative law, criminal law, various branches of procedural law and others, which leads to the possibility of subdividing systemic links of civil law not only into intra-branch and inter-branch ones, but also into interconnections with branches of public law and branches of private law" [Chelyshev M.Y., 2009: 5, 197]. And this is precisely what characterises the primary public component of the UDR.

The conclusion that, in the civil law mode of the digital rights, intersectoral relations play a systemic role facilitating relations of dependence and conditionality between international, administrative, criminal, and civil law requires a multifactor analysis and a functional approach.

The decision on how the foundation can be laid and whether the private model is fully applicable as an established model of digital rights regulation is currently going through the so-called "acceptance stage" [Kartskhia A.A., 2019: 13]. Therefore, answers are required to the questions whether synergies are possible when applying general principles of civil law and special principles of digital circulation to solve the issues of law of obligations and, e.g., financial law and/or corporate law.

And the utility digital rights offer a case of fine-tuned applicability of the qualification of such rights serving as a basis for the principles of "common-public digital law." Here, the question should be answered to what extent there is cross-discipline influence, and to what extent the principles of digital law are identical to special principles of digital circulation and to

what extent they are taken into account: e.g., in particular, the principle of technological neutrality, the principle of identified anonymisation, the principle of personal data security, the principle of crypto-encryption (encrypted) mode of data transmission, and the principle of cyber security. As well as sector principles with mixed affiliation: the principle of credibility of the data ledger, the insertion principle, and various principles of access rights by sector.

Regulation of property and non-property relations in market and commodity circulation is not limited to the norms of civil (private) law only. It also includes the norms of public law (antimonopoly law, law on technical regulation, on cyber security, on intellectual property, on personal data, etc.), which are not without a utilitarian civil law component.

E.g., it has a sense to believe the Law on Personal Data is directly linked to intangible goods, and it is this link that allows to find the reference areas between the law on personal data and civil law, and also, as mentioned above, is the basis for the utilitarian component, which allows to build effective cross-discipline links for their correct introduction in the form of the UDR.

In doctrine, legal relations in the sphere of "digital" rights are usually considered as a system of "legal relations existing within the subject matter of the branch of civil law, and from the point of view of legal technique they are a legal concept, the constituent elements of which are objects, subjects and content" [Volynkina M., 2012: 5]. Civil transactions are dynamic civil-law relations, hence they are "a totality of cases of change of bearers of subjective civil rights" [Belov V.A., 2012: 75]. Utility digital rights bound by appropriate obligation arrangements to users and holders are no exception.

The general approach equates property and civil circulation, viewing it as a "legal expression of commodity-money and market economic relations", that comprises "numerous specific acts of alienation and appropriation of property (goods) committed by owners or other legal owners" [Sukhanov E.A., 2011: 1216].

The norms of civil law, with a private law method of regulating relations, should become the starting point for the qualification of the obligation ensuring the digital civil circulation. In other words, we are talking about mixing legal and individual regulators with technical norms (standards, regulations, etc.), local acts, including within the framework of technological platforms based on the rules (agreements) of a distributed ledger or other

technologies, and with account of the special legal personality of information and technological intermediaries).

General innovative developments in civil circulation of property rights to intellectual property objects promote the method of cross-sectoral and intra-industry regulation. According to Joseph Schumpeter, innovative development is "destructive creativity" [Schumpeter J.A., 1995: 57] that constantly creates the new while ceaselessly destroying the old and is the hallmark of the capitalist formation.

The Utility Digital Right token is an example of UDR realisation by means of a transaction, i.e. a smart contract. It is recognised as a fully automated obligation existing through and in the form of software code, which cannot be modified, cannot be unilaterally terminated, cannot be unilaterally repudiated, cannot be waived, and cannot be materially altered. The public part rules on the issuance of UDR serve as an example of this. I.e., we are dealing with a problem of determining the moment for such a "self-executing" obligation, and into how this relates to other areas. This again raises the question of whether it is a contract at all and whether it needs a precise legal qualification or whether a mathematical algorithm will decide everything.

5. Derivatives market "digitalisation" tools and secondary rights

Even before passing of Federal Law No. 34-FZ on amendments to the RF Civil Code, the automated exercise of several rights and fulfilment of obligations under smart transactions already applied to securities market participants. E.g., Federal Law No. 460-FZ of 29 December 2014 "On Amendments to Certain Legislative Acts of the Russian Federation"[2] provided judicial protection for claims under contracts concluded between a forex dealer and an individual.

By virtue of Para 1, Article 4.1 of the Law "On the Securities Market", a forex dealer on its own behalf and at its own expense concludes with an individual, e.g., a contract on derivative financial instruments, and the obligations of the parties under such contracts depends on the changes in the exchange rate of the relevant currency; the individual in this case may assume obligations that exceed the amount of collateral provided to the forex

[2] Consultant Plus.

dealer. The forex dealer can also conclude so-called contracts for difference (CFD) with a foreign currency or currency pair (Para 3, Clause 1, Article 4.1 of the Law "On the Securities Market").

Such contracts are concluded, executed and terminated using automated systems. The obligation of a forex dealer to use software and hardware tools when carrying out operations in fulfilment of the contract and to use technical tools when concluding individual contracts is directly stipulated by law (clauses 6, 18, 23, 24 of Article 4.1 of the Law "On the Securities Market").

As we continue discussing conditionality and potestativeness raised in this article, we turn to the study of secondary application. Here it is of use to mention and briefly analyse the application of the reciprocity rules under the above-mentioned Article 328 of the Civil Code; in doing so, we should take into account the possibility of comparing "digital format" of performance of an obligation and general secondary performance.

Thus, the classical secondary right to refuse to fulfil an obligation related to the performance of commercial activities by its parties or to unilaterally change the terms of such an obligation may be conditioned, according to the contract of the parties, by the need to pay a certain sum of money/perform an obligation to the other party (Clause 3, Article 310 of the Civil Code)[3]. It, in case of an optional obligation, is pretty much the case in smart execution.

When considering secondary rights incidental to obligations (which may well be the case in a "digital" obligation), their autonomy and the absence of any duty corresponding to the secondary right must be clearly underlined. The presence of a secondary right is predominantly a criterion of optional obligations [Zakharkina A.V., 2013: 172].

Analysing more the right to object as stated in Article 328 concerning reciprocal performance of obligations, it is possible to find here the secondary right consists in suspending performance and setting a time limit for payment of consideration to the debtor under the reciprocal obligation. So, we see a possible overlap with the provisions in the technology obligation when the programme executes a "smart" arrangement, e.g., a specification.

In fact, consideration not only implies but also precedes delivery [Sarbash S.V., 2005: 501]. The priority is inherent in the conditionality.

[3] Ruling of the RF Supreme Court of 20 June 2017. No. 5-KG17-71.

The general basis for the application of Article 328 will be such predictability of non-performance that is related to the actions or inactions of the debtor. An accidental possibility of non-performance may be a ground for suspension of performance only in relations, in which at least one debtor is an entrepreneur. Only in this case this secondary right becomes a protective right, as described above in relations with a forex dealer [Karnushin V.E., 2016: 112], and a unilateral right of refusal arises. It is necessary to keep in mind secondary relations may also arise in situations where a third party (e.g., an information intermediary) is involved in the delivery of a smart instrument under Article 430 of the RF Civil Code.

The contract may provide for the following method of execution. An individual (investor) gives the forex dealer (trader) a login and password to manage a nominal account for the purpose of buying and selling foreign currency on the forex market. In doing so, the parties confirm their will by pressing certain keys. So, the terms of the contract with a forex dealer may stipulate the secondary right of the investor [Karapetov A.G., 2018: 215] to unilaterally withdraw from the contract. The period for exercising this right is limited to the term of the contract. This right can be exercised, among other things, by pressing the corresponding key in one's personal cabinet.

It is worth noting that the refusal to perform the contract implies a waiver of all rights and obligations thereunder, and entails the termination of such rights and obligations [Sukhanova Y.V., 2009: 114]. However, in such disputes the withdrawal from the contract with the forex dealer implies the right of the individual investor to withdraw the funds available in the special account, except for the forex dealer's (trader's) consideration. In this case, in accordance with Clause 11, Article 4.1 of the law "On the Securities Market", if the funds in the nominal account of an individual are not sufficient to satisfy the claims of a forex dealer, the forex dealer's claims that are not satisfied with these funds shall be considered discharged. That is, in this case, an individual is exempt from paying the consideration (or part thereof) to the forex dealer. It should be taken into account that, firstly, in pursuance of Article 421 of the Civil Code, the parties shall be entitled to conclude a contract, both stipulated and not stipulated by the Law or other laws and regulations. The conclusion of a contract between a forex dealer and an individual is stipulated in Article 4.1 of the law "On the Securities Market." Secondly, according to Article 310 of the Code, the contract may grant the right to refuse to fulfil an obligation only to a person who is not an entrepreneur, unless the law allows to include in the contract a condition

on granting such a right to the other party. In fact, by refusing the investor's claim for the return of funds, the court allows the forex dealer in their capacity of a person engaged in the relevant entrepreneurial activity, to unilaterally withdraw from the contract with an individual. This is a violation of Article 310 of the Civil Code and Clause 17, Article 4.1 of the Law "On the Securities Market." The peculiarities of exercising the secondary right under a contract between a forex dealer and an individual are:

in case of unilateral withdrawal from the contract, the individual assumes the risks of the transaction made by the dealer, but is entitled to demand from the latter to pay the amount exceeding the amount of the "risk capital";

in case of unilateral withdrawal from the contract, if there are not enough funds in the nominal account of the individual to satisfy the dealer's claims, the dealer's claims not satisfied with these funds shall be considered discharged;

the right to unilaterally withdraw from the contract may be exercised by changing the login and (or) password, and through the investor's member area, i.e. it is recorded in the programme by pressing the relevant keys;

the right to unilaterally withdraw from the contract may also be exercised by withdrawal of funds from the special account.

Other derivative contracts that are traded in a centralised regulatory environment have similar ways of exercising rights, too. And in turn, the instrument that includes an obligation in a digital environment located in a decentralised data registry, will have almost any combination of the legal tools described in this article.

A smart contract is a fully self-executing contract that exists through and in the form of software code that cannot be changed and cannot be unilaterally cancelled; nor can the exercise of rights under a smart contract be refused. Arguably, this is the most fundamental difference between a contract under which the parties express their through electronic and technical means, and a smart contract. I.e., we are dealing with a problem of determining the time before such a "self-executing" contract is implemented, its implementation, and after its implementation: the sequence of steps needed to end and/or terminate such "hi-tech" contractual relations and the obvious legal implications have to be defined.

Presumably, relations between the parties to a smart contract will fall under the provisions of Articles 157 and 327.1 of the Civil Code regulating stochastic obligations in the decentralised sphere without the regulator's direct involvement. In this case, under Article 327.1 of the Civil Code, the smart contract and individual rights and obligations thereunder shall terminate when certain circumstances occur.

6. Problematic aspects of the parties involved

Information intermediaries are persons working with information (content) created by others on the Internet, act on their own behalf, perform their activities for a fee and have specific requirements for different types of operations with information. The norm on agency in Article 1005 of the Civil Code does not give a deterministic answer to this question either. Due to this uncertainty, scholars believe it is necessary to distinguish between two separate and distinct types of information intermediaries. Firstly, these are persons providing the opportunity to post a piece of information on an information and telecommunications network, including the Internet, and secondly, these are persons providing the opportunity to post a piece of information necessary to obtain the content using an information and telecommunications network, including the Internet.

The concept of an information intermediary first appeared in Russian law in 2013. It was introduced by Federal Law of 02 July 2013 No. 187-FZ "On the Amendments to Legislative Acts of the Russian Federation Concerning Protection of Intellectual Rights in Information and Telecommunications Networks"[4], that complemented Part 4 of the Russian Civil Code with a new Article No. 1253.1. The article establishes a certain range of persons who can act as information intermediaries, regulates their rights, and determines the specifics of liability for infringement of intellectual rights in the information and communication network [Fomina O.N., 2019: 178]. However, the concept of an "information intermediary" needs correction.

Article 1253.1 "Peculiarities of Liability of an Information Intermediary" of the Civil Code offers the following classification:

[4] Federal Law of 02 July 2013 No. 187-FZ "On the Introduction of Amendments to Certain Legislative Acts of the Russian Federation Concerning the Protection of Intellectual Rights in Information and Telecommunications Networks" // Collection of Laws of the Russian Federation. 2013. No. 27. P. 3479.

a person transmitting materials in an information and telecommunication network, including the Internet;

a person providing the opportunity to post materials or information necessary to obtain them using an information and telecommunications network;

a person providing the ability to access materials on that network.

Types of services can be used for classification according to the type of obligation and characteristics of the party to the contractual relationship.

It is particularly evident in the field of obligations involving intermediaries in the cloud format of legal relations and in the sphere of specific features of hosting. The types of cloud storage services include:

infrastructure as a service-IaaS;

platform as a service-PaaS;

software as a service-SaaS.

All types of cloud storage allow one to use a particular software without installing the application itself on the user's computer. In other words, the item that we can see does not exist in real life. Instead, there is only something virtual; hence, the user can own only such software. The computer programme itself is installed and the information is stored and processed on the server of the right holder (or partner).

In Para 77 of the Russian Supreme Court Plenum Ruling No. 10 of 23 April 2019 the court independently determines whether a particular person is an information intermediary, taking into account the nature of the person's activities. If a person carries out the activities specified in Article 1253.1 of the Civil Code, it is recognised as an information intermediary with respect to performance of these activities. If a person carries out different activities at the same time, the question of this person's classification as an information intermediary should be decided for each type of activity[5].

In line with the above, and in the light of the doctrine, the following can be classified as an information intermediary of the first type:

telecom operators providing telematic communication services for Internet access [Tereshchenko L.K., Tiunov O.I., 2016: 47].

[5] The Russian Federation Supreme Court Plenum Ruling of 23 April 2019 No. 10 "On the Application of Part Four of the RF Civil Code"// Bulletin of the RF Supreme Court. 2019. No. 7.

information system operators, in cases where they work with information and telecommunication networks in course of their activities [Tereshchenko L.K., Starodubova O.E., 2017: 60].

The said persons shall not be liable for any infringement of the IP rights resulting from this transfer, provided that the following conditions are satisfied at the same time, if they:

do not initiate data transmission and do not determine the recipient of the data;

do not alter the said data as they provide communication services, except for technical changes made to ensure the process of content transfer;

did not know and were not supposed to know that the use of the relevant result of intellectual activity or means of individualisation was unlawful.[6]

The second type of information intermediaries include:

owners of Internet sites, because they determine at their discretion how information is used and posted on the site;

file hosting services that provide the users with space for their files and a 24/7 access to them through the Internet;

torrent trackers users can use to exchange information by downloading it from each other, not from a common server.

search services in case they do not store content or information [Tereshchenko L.K., Tiunov O.I., 2016: 47].

Internet sites in case they represent an information and reference system used to store reference information on goods and/or services, advertising materials, users' information on goods/shops (reviews)[7].

The said persons shall not be liable for any infringement of the IP rights, provided that the following conditions are satisfied at the same time:

the person did not know and was not supposed to know that the use of the results of intellectual activity or means of individualisation contained in the materials or posted information is unlawful;

[6] Russian Federation Civil Code. Part Four. Federal Law of 18 December 2006 No. 230-FZ. Revised 11 June 2021; with amendments and additions in force from 01 August 2021 // Collection of Laws of the Russian Federation. 2006. No. 52 (Part One). P. 5496.

[7] Appeal determination of the Moscow City Court of 10 July 2015 in case N 33-24183/2015 // SPS Consultant Plus.

the person in case of receiving a written claim from the right holder about infringement of intellectual rights with indication of the page of the site and (or) network address on the Internet on that such material is placed, has timely taken necessary and sufficient measures to stop the infringement of such IP rights, which includes deleting this information.[8]

The third type of information intermediaries include hosting providers providing computing capacity power for placing information in an IT system permanently connected to the Internet.

The conditions for exemption from liability for these persons are the same as for the second type of information intermediaries [Tereshchenko L.K., Tiunov O.I., 2016: 49].

These norms, too vague ones, allow endless interpretations of the definition of an information intermediary. Under such circumstances, this includes any person who provides access to contents or information, but also as browser producers, computer manufacturers, and other civil law entities that provide access to Internet sites containing certain materials.[9] This is crucial and relevant because the list of persons in this category is open-ended. In this connection, law enforcement is difficult because it is difficult to categorise a person as an information intermediary, and to identify this person's type so as to determine the grounds for exemption from liability.

It would be interesting to look at the experience of China as a best practice in regulating relations on marketplaces. It is a country of the first order with a fairly advanced system for the provision of access to, transmission, storage of information on the Internet, which often needs licensing. Also, information intermediaries operating in China are obliged to participate in the censorship of information disseminated on the Internet [Van Boom D., 2017: 3].

From the Chinese experience and available practice: the cases are described in: [Huang Y., Lu X., 2019: 220], some recommendations should be considered when such market participants work out the rules.

Marketplaces should actively cooperate with content rights holders and enter into partnership agreements with companies and organisations that

[8] RF Civil Code. Part Four // Collection of Laws of the Russian Federation. 2006. No. 52 (Part One). P. 5496.

[9] Minutes No. 16 of the Meeting of the Scholar Advisory Board of the Intellectual Property Rights Court on 28 April 2017.

have intellectual property rights. The aim is to distribute content legally and hedge the risks of copyright infringement.

Maintain transparency and authenticity: introduce tools to validate the authenticity of goods and content before they are placed on the platform.

Strengthen measures to deal with infringers: this may include removing illegal content, blocking access to the platform, or to banned sellers.

Raise awareness: marketplaces must inform users about the rules of using content and selling goods, and about the negative consequences of copyright infringement.

Promote technological solutions: machine learning and artificial intelligence can be used to automatically detect and remove illegal content [Pokrovskaya A.V. 2024: P. 14].

Approaches to adaptation and ways to incorporate the experiences of such platforms in relation to digital obligation will be explored in future research.

Conclusions

The obligation structure in the information environment and the rapidly growing digital environment infrastructure is quite special. It demonstrates convincingly that the digital reality of hybrid transactions is different from a regular civil duty to perform in its classical manifestation, is subject to cross-disciplinary influence, and is implemented with the participation of marketplaces.

The stochastic nature of such obligations once used to precede the emergence of terminology associated with financial instruments in this area, which had a strong cross-discipline nature.

There is no conclusive answer to the question of the legal nature and structure of obligations in the digital environment; nor is there a developed methodology and a conclusive nomenclature would put the matter to rest in efforts to develop the global regulation of the smart arrangement in the global environment.

The fact there is absolutely no interaction between legal systems and no synergies between functionality and private interest exacerbates problems existing in the sphere of regulating the operation of high-tech services.

Contract law is in many ways an ex-post instrument for regulating pre-existing contractual relations between counterparties. But as far as smart self-execution is concerned, the transaction that is the basis for the respective obligations is also a private-law regulator that determines the conditions under which the obligations will be formed.

To qualify an obligation that primarily binds, e.g., the execution of a smart contract, a significant starting role will have to be played by mixed legal individual regulators with technical rules and local acts based on the rules of a distributed data ledger (information system) for such crypto-instruments. The reason is that these same regulators can themselves be the objects of civil transactions.

Conditional determinants are special ones. They are performed by the program within framework of a conditional transaction and conditioned obligations; performance by one party is linked to performance by the counterparty. The priority of performance of a mutual obligation is inherent in the conditionality itself.

Exercise of rights and performance of obligations under a smart obligation upon the occurrence of a condition (both an external circumstance and one that depends on the actions of the parties to the obligation) is characteristic of the construct of an obligation with conditional performance (Article 327.1 of the Civil Code).

The question should be answered to what extent there is cross-sector influence and to what extent the special principles of digital circulation are identical to the principle of digital law and are taken into account.

In the "smart" version of the optional performance of the obligation, the general secondary right to refuse to fulfil an obligation related to the performance of commercial activities by its parties or to unilaterally change the terms of such an obligation may be conditioned, according to the contract of the parties, by the need to pay a certain amount of money to/perform an obligation before the other party (Clause 3, Article 310).

The general basis for the application of Article 3 will be predictability of non-performance that is related to the actions or inactions of the debtor. An accidental possibility of non-performance may be a ground for suspension of performance only in relations in which at least one debtor is an entrepreneur. Only in this case this secondary right acquires, in fact, the nature of a protective right, as described above in relations with a forex dealer (Section 6 of the Article).

The legal position of information intermediaries at the present time complicates law enforcement in classifying a person as such, as well as in identifying their type as a cause for exemption from liability.

References

1. Akhmedov A.Ya., Volos A.A., Volos E.P. (2022) Concept of Regulation of Relations Complicated by the Use of Smart Contracts. Moscow: Prospekt, p. 20, 79 (in Russ.)

2. Belov V.A. (2007) Object of Subjective Civil Legal Relationship and Object of Civil Circulation: Content and Correlation of Concepts. In: Objects of Civil Circulation: collection of papers. M.A. Rozhkova (ed.). Moscow: Statut, p. 75 (in Russ.)

3. Bogdanov D.E. (2023) Failed Technological Revolution in Contract Law: Apologetics of Traditionalist Interpretation of Contract. *Lex Russica*, no. 3, p. 35 (in Russ.)

4. Bogdanova E.E. (2019) Smart Contract Application in Virtual Property Transactions. *Lex Russica*, no. 7, pp. 108–118 (in Russ.)

5. Bychkov A. (2019) What Information Intermediaries are Responsible for. *New Accounting*, no. 7, pp. 116–131 (in Russ.)

6. Chelyshev M.Y. (2009) Fundamentals of the Doctrine of Inter-sector Relations of Civil Law. Kazan: Kazan State University, p. 5, 197 (in Russ.)

7. Efimov A.V. (2022) Functional Approach to the Construction of Civil and Business Law Norms. *State and Law*, no. 6, pp. 89–96 (in Russ.)

8. Efimova L.G., Sizemova O.B. (2019) Legal Nature of Smart Contract. *Banking Law*, no. 1, pp. 23–30 (in Russ.)

9. Egorova M.A., Kozhevina O.V. (2020) Place of Crypto currency in the System of Civil Rights Objects. *Current Issues of Russian Law,* no. 1, p. 83 (in Russ.)

10. Fillipova S.Y. (2013) Instrumental Approach in the Science of Private Law. Moscow: Statut, p. 350 (in Russ.)

11. Fomina O.N. (2019) Legal Status of Information Intermediary. *Civil Law Bulletin,* no. 3, pp. 171–191 (in Russ.)

12. Grin O.S. et al. (2019) Legal Construct of Smart Contract: Legal Nature and Scope of Application. *Lex Russica*, no. 8, pp. 55–56 (in Russ.)

13. Hohfeld W.N. (1917) Fundamental Legal Conceptions as Applied in Judicial Reasoning. *Yale Law Journal,* vol. 26, no. 8, pp. 710–770. Available at: https://doi.org/10.2307/786270 (accessed: 24.05. 2023)

14. Huang Y., Lu X. (2019) Intermediary Liability for Intellectual Property Infringement in China's E-commerce Marketplaces. *Asian Journal of Law and Society,* vol. 7, no. 2, pp. 213–237.

15. Jankowski R.M. (2017) The State and Crypto Currencies: Issues of Regulation. Available at: URL: http://msu.edu.ru/papers/yankovskiy/blockchain.pdf (in Russ.) (accessed: 30.06. 2024)

16. Jünemann M., Milkau U. (2021) Can Code Be Law? Available at: https://digitalbusiness.law/2021/08/can-code-be-law/ (accessed: 26.12. 2023)

17. Karnushin V.E. (2016) Secondary Rights in the Civil Law of the Russian Federation. In: General Issues of Theory. Secondary Rights. V.P. Kamyshanski (ed.). Moscow: Statut, p. 112 (in Russ.)

18. Kartskhia A.A. (2019) Digital Transformation of Law. *Monitoring of Law Enforcement*, no. 1, p. 13 (in Russ.) DOI: 10.21681/2226-0692-2019-1

19. Kiviat T. (2015) Beyond Bitcoin: Issues in Regulating Blockchain Transactions. *Duke Law Journal*, vol. 65, no. 3, pp. 569–608.

20. Kotsar Yu.A. (2024) Smart Contract as a Form of Execution of Obligation with Conditional Performance. *Law and State: Theory and Practice,* no. 5, p. 46 (in Russ.)

21. Kulakov V.V. (2017) Reasonable Balance of Interests of Participants of Civil Legal Relations: methodological issues of integration of different legal understanding. In: Methodological Issues of Civil Studies. Collection of papers. A.V. Gabov, V.G. Golubtsov (eds.). Issue 2. Moscow: Norma, p. 11 (in Russ.)

22. Željka M. (2021) Smart Contract and Traditional Contract. In: Legal Tech Book. The Legal Technology Handbook. N.Y.: Wiley, pp. 165–166.

23. Pokrovskaya A.V. (2024) Liability of Intermediaries for Copyright Infringement on Marketplaces: Study of China's Experience. *Journal of the Court of Intellectual Property Rights,* no. 6, pp. 14–18 (in Russ.)

24. Inderst R., Thomas S. (2024) Algorithms and Antitrust: A Framework with Special Emphasis on Coordinated Pricing. Available at: https://ssrn.com/abstract=4816287 (accessed: 20.07. 2024)

25. Sarbash S.V. (2005) *Execution of a Contractual Obligation.* Moscow: Statut, p. 532 (in Russ.)

26. Savelyev A.I. (2016) Contract Law 2.0: Smart Contracts as the Beginning of the End of Classical Contract Law. *Civil Law Bulletin*, no. 3, pp. 32–59 (in Russ.)

27. Sazhenov A.V. (2018) Cryptocurrencies: Dematerialisation of the Category of Things in Civil Law. *Statut*, no. 9, pp. 118–119 (in Russ.)

28. Schumpeter J.A. (1995) Capitalism, Socialism and Democracy. Moscow: Ekonomika, p. 57 (in Russ.)

29. Sukhanov E.A. (2011) Russian Civil Law. Law of Obligations: Textbook. Moscow: Statut, 1216 pp. (in Russ.)

30. Tereshchenko L.K., Tiunov O.I. (2016) Information Intermediaries in Russian Law. *Journal of Foreign Legislation and Comparative Law*, no. 6, pp. 46–51 (in Russ.)

31. Tereshchenko L.K., Starodubova O.E. (2017) Riddles of Information Law. *Journal of Russian Law*, no. 7, pp. 56–68 (in Russ.)

32. Venediktov A.V. (1954) The System of the Soviet Civil Code. *Soviet State and Law,* no. 2, p. 29 (in Russ.)

33. Volynkina M. (2012) The Content of the Exclusive Right: Theoretical Aspect. *Copyright and Related Rights,* no. 1, p. 5 (in Russ.)

34. Zakharkina A.V. (2013) The Concept of Optional Obligation in the History of Civil Thought. *Bulletin of Perm State University. Legal Sciences,* no. 4, pp. 170–176 (in Russ.)

Information about the author:

Rim N. Adelshin — Candidate of Sciences (Law), Associate Professor.

The article was submitted to editorial office 31.05.2024; approved after reviewing 28.07.2024; accepted for publication 05.09.2024.

Legal Issues in the Digital Age. 2024. Vol. 5. No. 3.
Вопросы права в цифровую эпоху. 2024. Том 5. № 3.

Digital Age: Labour Law

Research article
УДК: 349.2
JEL: K31
DOI:10.17323/2713-2749.2024.3.31.48

Legal Regulating Electronic Employment Contracts as a Modern Factor of Integration at International Regional Bodies (Exemplified by EEU, CIS and BRICS States Legislation)

Marina Olegovna Buyanova

National Research University Higher School of Economics, 20 Myasnitskaya Str., Moscow 101000, Russia,

mobuianova@mail.ru, https://orcid. org/ 0000-0003-4911-0406

Ekaterina Sergeevna Batusova

National Research University Higher School of Economics, 20 Myasnitskaya Str., Moscow 101000, Russia,

ebatusova@hse.ru, batusovs@gmail.com, https://orcid. org/ 0000-0003-0490-646X

Abstract

The paper provides an analysis of general regulatory patterns concerning the signing, amendment and termination of electronic employment contracts within the Eurasian Economic Union (EEU), Commonwealth of Independent States (CIS) and BRICS as a trend of deepening integration at these international organizations. The core issue in this area is labor mobility in the context of digitization is not regulated internationally with efficiency. It gives rise to a controversy between the need to optimize labor mobility and a lack of comprehensive international instrument on electronic em-

ployment contract to improve legal regulation for more efficient utilization of human capital. The paper analyzes the legislation on electronic employment contracts in a number of EEU, CIS and BRICS member states to come up with recommendations for improving international legal regulation of electronic employment contracts via the relevant international instrument to be drafted. The authors identify a number of general regulatory patterns characteristic of countries such as Russia, Kazakhstan, Kyrgyzstan, Armenia, Belarus, Azerbaijan, Uzbekistan, China, South Africa, India and Brazil, with their national labor law sharing the following features: possibility of HR electronic document exchange for balance of workers' and employers' interests as enabled by regulations; transparent working conditions; electronic employment contract reporting through the software linked to public authorities' websites, and the use of electronic digital signature to sign contracts. This prevents unauthorized amendment of the terms of outstanding employment contracts and allows to track the time when the relevant rights and duties were assigned. The paper comes up with recommendations for better protection of labor rights and duties through the use of electronic tools to conclude employment contracts such as a bilingual online form.

Keywords

electronic employment contract; Eurasian Economic Union (EEU); Commonwealth of Independent States (CIS); BRICS; integration; labor legislation; international legal instrument; labor rights; workers; employer.

For citation: Buyanova M.O., Batusova E.S. (2024) Legal Regulating Electronic Employment Contracts as a Modern Factor of Deepening Integration at International Regional Bodies (Exemplified by EEU, CIS and BRIGS States Legislation). *Legal Issues in the Digital Age,* vol. 5, no. 3, pp. 31–48. DOI:10.17323/2713-2749.2024.3.31.48

Background

In the current environment, the CIS, EEU and BRICS states have to ensure a reliable and independent supply of the goods and services they need. This, however, cannot be done without introducing new business organization methods, improving the national labor productivity and expanding cooperation with friendly countries for supply of labor. One should keep an eye not only on technological upgrading of production processes to introduce new generation equipment but also on the observance of labor rights in HR management processes both in Russia and across international organizations involving this country (CIS, EEA, BRICS). As applied to labor, digital tools are important ways of tracking the work process and the time when the relevant rights and duties were assigned.

The impact of digitization on employment in Eurasian countries was studied in a number of aspects by E.E. Orlova [Orlova E.E., 2022: 228–

234]. General development issues of new digital technologies in the BRICS were explored by I.V. Lazanyuk and S.Yu. Revinova [Lazanyuk I.V., Revinova S.Yu., 2019: 208–213.] while I.A. Filippova has studied the links between information society and regulation of labor relations [Filippova I.A., 2020: 162–182], P.V. Soloviev has devoted his studies to changes to labor legislation in the context of digitization [Soloviev P.V., 2023: 32–37] and K.L. Tomashevsky has explored economic impact of digitization in Belarus and Russia and its harmonization at the Eurasian Economic Union [Tomashevsky K.L., 2020: 398–413]. N.N. Morozova [Morozova N.N., 2019: 71–76] has focused on digital employment problems of specific population categories in Belarus and Russia (CIS states), and the aspects of digital economy and gender issues she has researched with V.M. Bondarenko [Bondarenko V.M., Morozova N.N., 2020: 639–643].

The details of transition to electronic employment contracts were explored by A.V. Raut [Raut A.V., 2023: 123–127]. Other studies focused on the basic issues of the underlying electronic form [Potapova N.D., Potapov A.V., 2017: 52–53] and on the prospects of labor rights protection in electronic employment contracts [Sapfirova A.A., 2020: 162–167]; [Sapfirova A.A. 2021: 8–13] including the balance of general and specific provisions that introduced e-document exchange [Perevalov A.G., 2023: 140–144]. Peculiarities of record-keeping in some countries such as Kazakhstan were discussed in a separate study [Temirova A.B., Yusupov S.A., Tolysbaeva M.S., 2021: 196–200].

It is also noteworthy the methods of digital workplace management and labor regulation are constantly evolving, with decision-making based on big data and data mining currently in expansion. One has to accept I. A. Filippova's view that labor law responds to changes resulting from digitization of new communication types [Filippova I.A., 2020: 176]. It would be useful to disseminate the positive regulatory experience of digitization provided that labor rights are observed. As non-typical forms of employment expand, civil law relations tend to substitute for labor relations even if all attributes of the former are in place. Being a basis of labor relations, the employment contract should thus be entered in electronic form since it allows to establish a set of rights, duties and liabilities as well as other terms of employment while preventing unauthorized amendment.

The trend for deeper integration at international regional organizations like EEU, CIS and BRICS is currently obvious. It is equally true for regulation of labor relations that are now formalized worldwide by an electronic

employment contract we regard as a major factor of harmonization of labor legislation at these international organizations.

While not definitely shaped, this emerging trend has multiple forms such as the development of the Work without Borders international system (job search and staff recruitment) at the EEU[1]; efforts to develop and implement an international digital platform for remote work within the BRICS[2]; and adoption of a number of model regulations on digitization within the CIS like the CIS Model Law on Technology Transfer Support and Regulation[3], CIS Model Law on Digital Space (Infrastructure and Regulation)[4], CIS Model Law on Digital Change in Economic Sectors[5].

Meanwhile, a problem is that while there is no adequate regulation of labor mobility based on the electronic employment contract, common regulatory patterns are observed in this area within the three organizations.

1. Patterns and trends in the legal regulation of an electronic employment contract

The common patterns mentioned point to a need to develop a shared international instrument on the electronic employment contract at these organizations.

These patterns include:

use of e-document exchange by employers to enter into employment contracts;

possible use of public systems to electronically enter into employment contracts;

---

[1] Work without Borders. International job search and staff recruitment system in the territory of EEU states. Available at: URL: https://trudvsem.ru/landing-rbg (accessed: 06.09.2024)

[2] Gazprom Neft to participate in online recruitment platform to be developed for BRICS. TASS news agency of Russia, 8 April 2024. Available at: URL: https://tass-ru.turbopages.org/tass.ru/s/ekonomika/20481771 (accessed: 06.09.2024)

[3] Annex to CIS Inter-Parliamentary Assembly Resolution No. 55-6 of 14 April 2023. Available at: URL: https://etalonline.by/document/?regnum=n22300120 (accessed: 06.09.2024)

[4] Ibid. Resolution No. 55-8. Available at: URL: https://etalonline.by/document/?regnum=n22300122 (accessed: 06.09.2024)

[5] Ibid. Resolution No. 55-9. Available at: URL: https://etalonline.by/document/?regnum=n22300123 (accessed: 06.09.2024)

different status of the electronic signature established to electronically enter into employment contracts;

electronic formalization of amendments to employment contracts;

electronic termination of employment contracts.

It has a sense to analyze these common patterns.

1.1. Use of e-document exchange by employers to enter into employment contracts

The legislation across the CIS, EEA and BRICS enables to an extent the use of e-document exchange to electronically conclude employment contracts. This provision can be envisaged by both the national labor code and the regulations governing employment contracts.

In Russia e-document exchange is enabled by Articles 22.1 and 22.2 of the Labor Code provided electronic communication is agreed between the parties and secured by the worker's electronic signature as necessary.

As for Kyrgyzstan's legal experience, Kyrgyz Republic Law No. 123 "On amending the Labor Code of the Kyrgyz Republic" of 23 December 2022 provides for a possibility to conclude employment contracts electronically in a new wording of Article 58, with Article 360-2 of the Labor Code confirming the use of this form for remote workers. The Labor Code defines e-contracts as electronic instruments signed with electronic digital signature. According to the head of the International Business Council, this will facilitate, for example, "employment of low-mobility individuals, residents of remote areas"[6]. However, no requirements to employers for the use of specific HR document exchange are established by the Labor Code.

In Armenia it was not before 2023 the NA's Standing Commission on Labor and Social Affairs has proposed to discuss the possibility to conclude contracts electronically at the portal of the platform for electronic employment contracts. It is envisaged that a contract will be deemed concluded, once its terms are reviewed and accepted. Meanwhile, fully electronic document exchange was approved by the government in 2009.

[6] Law for remote work has taken effect in Kyrgyzstan. Vesti.kg — News of Kyrgyzstan. Available at: URL: https://vesti.kg/obshchestvo/item/108383-vstupil-v-silu-zakon-reguliruyushchij-distantsionnuyu-rabotu-v-kyrgyzstane. Available at: URL: https://etalonline.by/document/?regnum=n22300123 (accessed: 06.09.2024)

In Azerbaijan, where the implementation of the Strategic Roadmap for the Development of Telecommunications and Information Technologies[7] is underway since 2016, e-document exchange for HR management has been introduced, for example, at the Ministry of Economic Development.

Electronic registration of employment contracts was introduced by Law No. 875-IVQD "On Amending the Labor Code of Azerbaijan" of 27 December 2013, with recruitment regulated by a provision requiring to post a notice on outstanding contracts to the information system based on the list of details to be reported[8].

T. Khalilov and E. Aliyev in their study in digitization has concluded: "Azerbaijan is focused on advancing its digital sector".[9] They have underlined digital tools contribute to transparency of employment processes and protection of workers while the labor market needs to adapt to new challenges in the current context. It is planned to adopt electronic employment contracts and abandon the required notice, with hearings on this issue expected in June 2024[10].

In Belarus e-document exchange can be used, for example, for personal file management, with purely electronic form applicable to warnings, worker consents, bylaw reviews, orders, worker applications. Like in Russia, employers are mainly required to have a bylaw for e-document exchange, maintain unambiguous worker identification and e-document integrity.

In Belarus the employment contract, just like the financial liability contract, is entered, extended and amended in the paper form. For these documents to be entered electronically, it is required to have a personal telephone for unambiguous identification of electronic digital signature, as well as a reliable and continuously operating HR document exchange system.

---

[7] Government of Azerbaijan. 2016. Strategic Roadmap for the Development of Telecommunications and Information Technologies. Available at: https://ict.az/en/news/2006 (accessed: 06.09.2024)

[8] Cabinet of Ministers of Azerbaijan. Resolution No. 183 of 6 June 2014 "On approving the form of the employment contract notice and the rules to post it to the electronic information system, as well as details to be reported by the employer to the Ministry of Taxes following the notice including the rules related to real-time receipt of the posted notice". Available at: URL: https://online.zakon.kz/ (accessed: 06.09.2024)

[9] Available at: https://www.researchgate.net/publication/341733964_Digital_century_new_approaches_to_employment_in_Azerbaijan (accessed: 06.09.2024)

[10] Azerbaijan to Electronically Enter Employment Contracts. Azeri Press Agency. 12 June 2024. Available at: URL: https://ru.apa.az/sotsium/v-azerbaidzane-trudovye-dogovory-budut-zaklyucatsya-v-elektronnom-vide-575705 (accessed: 06.09.2024)

The recommended model employment contract was amended with regard to the employer's duty to arrange for evaluation of workers and to make sure that job titles match skill reference books and occupational standards[11]. Thus, the reform of employment contract has not affected its form.

In India two government-led projects ("Made in India" and "Digital India") were launched to bolster digital economic development with active support of the NASSCOM, a non-governmental association of IT companies.

Digitization of labor relations relies on the Information Technology Act of 2000[12] and the Indian Contract Act of 1872.

The regulatory principles applicable to employment contracts are enshrined in Factories Act No. 63 of 1948[13], Contract Labor (Regulation and Abolition) Act No. 37 of 1970, and Industrial Relations Code of 2020[14].

The Information Technology Act provides for a variety of digital forms of agreement: click-to-sign, e-letter exchange, electronic digital signature. Whatever form is used, an electronic contract is deemed entered pursuant to paragraph 10a of the 2000 Act.

Theoretic research has shown legal regulation of labor is still quite weak in India [Filatkina I.D., Filatkina M.D., Krechetnikov K.G., 2015: 103]. Further introduction of electronic employment contracts will apparently boost employment given that India has the largest population within the BRICS estimated at 1,373.76 million in 2022 and an employment rate of 46.60 percent.[15]

---

[11] Employment Contract Form and Labor Management Rules Adjusted since 1 January 2024. Oshmiany District Executive Committee website. Available at: URL: https://www.oshmiany.gov.by/ru/republic-ru/view/s-1-janvarja-2024-goda-korrektirujutsja-forma-trudovogo-dogovora-i-pravila-vnutrennego-trudovogo-24530-2023/ (accessed: 06.09.2024)

[12] Available at: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf (accessed: 06.09.2024)

[13] The Factories Act 1948 (Act No. 63 of 1948), as amended by the Factories (Amendment) Act, 1987 (Act 20 of 1987). Available at: https://www.ilo.org/dyn/natlex/docs/WEBTEXT/32063/64873/E87IND0 (accessed: 06.09.2024)

[14] Industrial Relations Code 2020 as introduced in Lok Sabha on 19 September 2020. Available at: https://taxguru.in/corporate-law/industrial-relations-code-2020.html (accessed: 06.09.2024)

[15] Employment rate in India. TRADING ECONOMICS. Available at: URL: https://ru.tradingeconomics.com/india/employment-rate (accessed: 06.09.2024)

Employers can themselves introduce HR e-document exchange in entering employment contracts with reliance on labor and information technology laws as long as electronic communication is agreed with workers to be employed.

1.2. Possible use of public systems to electronically enter into employment contracts

In Russia electronic employment contracts can be entered via the portal Work in Russia[16] where contracts for work, job placement and on-the-job practice can also be entered since 1 January 2023.

In Kazakhstan employers are required to observe the form of employment contract since 16 May 2020. One option is to conclude the employment contract electronically at the labor resources portal using the electronic digital signature, or conclude it on paper to be registered with the relevant record-keeping system. [17]

The system does not only facilitate statutory reporting for employers but also given the candidate's prior consent endorsed by electronic digital signature, allows to look at his employment record if the portal used for formalization is integrated with the shared record-keeping system. In addition, the electronic system's portal at https://hr.enbek.kz/ has the information on the worker's side jobs, personal file management, model employment contract and statutory requirements in respect of specific worker categories.

The rules for reporting under employment contracts were introduced by Kazakhstan's Minister of Labor and Social Protection Order No. 353 of 3 September 2020[18]. These rules (apart from the procedure for uploading data to the system) define the main concepts for digital record-keeping such as electronic document and e-government along with information system and code integration.

---

[16] Federal Government Resolution No. 867 On the Shared Digital Platform for Employment and Labor Relations Work in Russia. 13 May 2022 // Collected Laws of Russia. 23 May 2022. No. 21. Article 3446.

[17] Law of Kazakhstan No. 321-VI On Amending Specific Labor Regulations of Kazakhstan. 4 May 2020 // RK Parliamentary Bulletin. 2020. No. 9. Art. 29.

[18] On approval of Rules for submitting and receiving the information on an employment contract in the unified system for recording employment contracts. Registered by the Justice Ministry. 4 September 2020. No. 21173. Available at: https://adilet.zan.kz/eng/docs/V2000021173/compare (accessed: 06.09.2024)

The system requires to enter not only the details of employment contract but also the terms of employment such as the type, location and period of work, first day to report for duty, with the said details to be uploaded within 5 days. Entities employing up to 2,000 workers could upload the details of all outstanding contracts within one year, that is, all contracts should have been registered with the system by September 2021.

In addition, more details can be entered such as working hours and rest time, paid leave, maternity leave, child care (adoption) leave.

The details can be entered in various ways: via the public Electronic Labor Exchange portal, or by integrating the corporate HR (employment contract) system with the shared record-keeping system for employment contracts.

Thus, the employer can choose a software shell at his convenience provided that his system complies with the integration rules approved by Acting Minister of Information and Communications Order No. 123 of 29 March 2018[19] . For using the Electronic Labor Exchange Portal, the employer should have an account with the website and a valid electronic digital signature to endorse the details and terms uploaded to the employment contract database. The details can be entered either by the employer's CEO or HR department head officially authorized to perform this duty.

The following periods (counted in business days) were provided for specific actions: 5 days for provision of information requested by the employer from a public body, 10 days for job reinstatement and employment contract re-entry into force. In the event of error and reinstatement, the worker should be advised accordingly via his account with the e-government website. The information for the worker is posted to his account the day following the employer's entry of the relevant details while a request can be also served to the shared record-keeping system. This makes up a system where several databases are integrated to enable communication between workers, employers and public authorities.

In Azerbaijan before 1 July 2014, employers were required to upload notices on the employment contract status to the public electronic system, with a liability of maximum 3 years in prison for non-compliance. Howev-

[19] Registered by the Justice Ministry of the Republic of Kazakhstan. April 19, 2018. No. 16777. Available at: URL: https://adilet.zan.kz/rus/docs/V1800016777 (accessed: 06.09.2024)

er, the reporting terms were extended. Articles 3, 12, 46 of the Labor Code[20] establish the rules for notices to be registered via the E-Government portal, with employment contracts taking effect after the notice is registered with the system to prevent the employer's non-compliance and tax evasion. Labor rights of workers will be better protected, once the decision is made in June to enter employment contracts electronically through the public portal[21] as the relevant information will be available to public authorities in real time.

It is necessary to discuss how and on what basis the form of employment contract will be digitized in some of the BRICS countries.

In China the State Council developed the Guidance on Actively Promoting Internet Plus Action Plan. Further digitization of labor relations is a step towards implementing the Made in China Strategy for 2025[22] and the National Strategy of Informatization and Development of China passed in 2016. The said strategies undoubtedly have an impact on the development of electronic record-keeping of personnel and electronic employment contracts.

On 1 July 2021 the Guidance on Electronic Employment Contracts[23] was passed to explain the requirements with regard to the e-platform for conclusion of employment contracts; verification and unambiguous identification of the parties; compliance of electronic signature; and contractual performance by the employer. The regulatory framework includes the Civil Code, Law on Electronic Signature, Law on Cyber-security. In 2022, the State Council has approved 2021-2025 Plan for digital economic development.

Legal regulation of labor relies on the Law on Employment Contracts.

The software for electronic contracts is supposed to ensure the authenticity, fullness, exactness and integrity of the data on contractual terms which is essential for such contract to be strong and binding. The platform should support not only the services to conclude contracts but also the protection, integrity, traceability of data as well as confirm the contract's time and date. Moreover, data requests from unauthorized agencies or persons

[20] Approved by Law of Azerbaijan No. 618-IQ of 1 February 1999 (as amended).

[21] Azerbaijan to Electronically Enter Employment Contracts. 12 June 2024. Available at: URL: https://ru.apa.az/sotsium/v-azerbaidzane-trudovye-dogovory-budut-zaklyucatsya-v-elektronnom-vide-575705 (accessed: 06.09.2024)

[22] Approved in 2015.

[23] Available at: https://www.gov.cn/zhengce/zhengceku/2021-07/12/content_5624319.htm (accessed: 06.09.2024)

should be rejected, with the data available only to the contracting parties (worker and employer) and competent public authorities. In addition, the employer should advise the worker on the methods, process and ways of maintaining the electronic digital signature.

The validity of digital certificates, network data and biometric identification should be ensured, with SMS verification codes sent to the mobile telephone and verification process recorded. Digital keys should be issued only by agencies of the digital certification service.

Apart from signing the contract, the employer is under the duty to advise the worker accordingly through the use of digital technologies, remind on the ways to download, save and review the document, as well as provide assistance, with the underlying application required to run on popular hardware to avoid extra costs. A paper copy of the contract should be made available for free upon demand.

The government recommends to employ platform developed by the public authorities. Where different platform is used by the contracting parties, it should comply with the third level of security and support the function of recording the evidence of electronic employment contract which should be registered with the e-government platform on a mandatory basis.

China's Ministry of Human Resources and Social Security under the State Council is responsible for supervision of national labor market policies and social security. Thus, in introducing the "electronic employment contract" and public platforms, this agency is making the control and supervision of compliance with the labor legislation more transparent, in particular, to prevent abuse with regard to wages and mandatory payments to workers.

Liu Dun and Geng Yuan believe public digital platform is shaping a new model of labor relations based on digital technologies, something that upholds the discipline of employment contract administration [Liu Dun, Geng Yuan, 2022: 24, 28].

In South Africa digitization is underpinned by the 2006 Information Society Development Plan, the 2007 Innovation Towards a Knowledge-Based Economy Program, the 2013 National Broadband Policy, 2015 National Integrated ITC Policy White Paper while the major labor legislation instrument is the 1997 Basic Conditions of Employment Act[24]. All the electronic

[24] Basic Provisions of Employment Act 75 of 1997. Available at: https://www.gov.za/documents/basic-conditions-employment-act (accessed: 06.09.2024)

employment contracts are governed by 2002 Electronic Communications and Transactions Act[25] containing requirements to electronic communications and electronic signatures. The latter may be of two types: standard and enhanced one, the second being more resistant to forgery and thus believed to be reliable from a legal perspective. The new type of signatures is believed to have environmental effect as well. The concept of e-contract is wider since it may be concluded both via e-mail, special website or otherwise without the use of paper. Except for voice messages, the Act does not regulate electronic communications. Its approval was for the purpose of promoting small and medium businesses and developing human resources, as well as marketing South African electronic products. Meanwhile, the name reproduced in an electronic letter, a photo of handwritten signature and an electronic signature as such are all deemed signature. In fact, electronic documents could be sent via post offices. The receipt of data is also confirmed by electronic signature or letter. Public authorities may confirm legal facts electronically. Good faith is presumed for the use of e-signature, with the signee assuming the burden of proof in the event of dispute. In particular, the Provision on Accreditation[26] and the duty of protecting data in the database were introduced.

1.3. Different status of electronic signature for electronic employment contracts

The understanding of digital (electronic) employment contract has evolved with technological progress. While originally it simply meant a contract entered with a remote worker by e-mail and further documented by paper duplicates, it is now a contract to be endorsed by electronic digital signature given the job seeker's consent to electronic communication (e-document exchange), that is, paper-free communication via special software.

In Russia electronic confirmation is governed by Federal Law No. 63-FZ "On Electronic Signature" of 06 April 2011[27].

In Kyrgyzstan, e-signature is a feature of electronic employment contract in accordance with Law No. 123 "On Amending the Labor Code of the Kyrgyz Republic" of 23 December 2022.

---

[25] The Electronic Communications and Transactions Act ("ECTA") // Government Gasette. 2 August 2002. No. 23708.

[26] Regulation Gazette. 20 June 2007. No. 29995.

[27] SPS Consultant Plus.

In India the 2004 Information Technology (Security Procedure) Rules and the 2015 Digital Signature Rules were adopted for the use of electronic records and digital signatures to implement the concept of digitization at work.

The government is authorized to make requirements to the form of electronic signature, method of unambiguous identification of the signee, signature integrity control[28]. Electronic digital signature is issued by a public authority while the law guarantees the legitimacy of contracts signed with electronic signature, requires to ensure the integrity of e-signatures and establishes the methods to ensure security of e-contracts. A contract is legitimate, once it is entered with a legitimate purpose by the authorized parties on the basis of free consent.

In Kazakhstan concept of electronic digital signature is established by Ministry of Labor and Social Protection Order No. 353 of 3 September 2020 mentioned above. However, this concept has inherent defects since the list of features contains, apart from integrity, ownership and authenticity of electronic document, the term itself, that is, "the means of electronic digital signature". As "electronic digital signature" is a feature of "electronic document", it appears that these concepts are defective from the standpoint of formal logic.

In Azerbaijan employers or their authorized representatives are required to use the enhanced electronic signature to endorse amendments to the documentary notice and termination of the employment contract.[29]

In China practical advice including the concept of electronic signature is provided in the mentioned above Guidance on Electronic Employment Contracts[30], with the features (e-message to identify the specific person as a proof of informed performance of actions) differing from those envisaged under Kazakhstan's law. Importantly, e-signature allows to prove the contract's existence prior to and its integrity after signing, as well as to establish the time.

With regard to conclusion of electronic employment contracts and creation of the relevant database, regulations will often require to use electron-

[28] Indian Information Technology Act. Article 10. Available at: https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf (accessed: 06.09.2024)

[29] Available at: https://www.e-gov.az/az/news/read/47 (accessed: 06.09.2024)

[30] Available at: https://www.gov.cn/zhengce/zhengceku/2021-07/12/content_5624319.htm (accessed: 06.09.2024)

ic signature or enhanced electronic signature without specifying whether it is qualified or not.

1.4. Patterns of electronic amendment of the employment contract

Where an employment contract is amended, a distinction is normally made between real amendment of the terms and a need for the employer to make changes due to software errors and not because the terms were incorrectly specified in the contract.

In Kazakhstan, for example, a period of 15 calendar days is provided for amending the terms of an employment contract in the system, with a special period of 30 calendar days envisaged in the event of errors identified in the outstanding employment contract.

In Azerbaijan an amendment to the employment contract will take force, once the employment contract notice formalized by the employer is registered with the electronic system.[31]

A common approach is thus obvious (just like with regard to the conclusion of employment contracts).

1.5. Patterns of electronic termination of the employment contract

Where an employment contract is terminated electronically, the underlying record will normally enable correction of possible errors based on the established procedure and dates.

Thus, a period of three business days is provided for in Kazakhstan to upload the information on the contract's termination. Where corrections need to be made to the system in respect of a contract already officially terminated by the employer, this duty will be assumed by a public agency following the employer's request for correction. The public agency will need to proceed as provided for by the Code of Administrative Procedures mentioned above[32].

[31] Part 1. Article 49. Labor Code of Azerbaijan. Law No. 618-IQ of 1 February 1999 // Collection of Legislative Acts of the Republic of Azerbaijan. 1999. No. 4. Article 213.

[32] RK Parliament Bulletin. 2020. No. 13. Article 66.

In Uzbekistan a period of three business days is provided for to upload and confirm the information on contract termination, with the employer allowed to make corrections within 5 days.

The second option appears preferable from the perspective of opportunities for the worker. However, in this case the software should not only trace corrections being made but provide the evidence that termination was incorrectly documented due to a technical error (rather than violation of the labor law by the employer), otherwise this will question the legitimacy of termination entry. It is also necessary to more exactly determine when the period for correction starts off. Apparently, it should be counted from the date when the three days allowed for the termination entry will elapse rather than from the date of wrong entry.

To terminate an employment contract in Azerbaijan, employers are required to enter a documentary notice of employment contract to the electronic information system.[33]

Moreover, there are different time marks for electronic contracts to take force.

In Azerbaijan it is thus established that each employment contract will take effect following its registration with a special platform of the e-government portal at https://www.e-gov.az/. This system, in operation since 1 July 2014, is designed to ensure public control, increase the collection rate of social contributions and taxes to the budget, and protect labor rights.

In Uzbekistan an employment contract will not take force either unless it is registered by the employer, with the details and terms such as working hours, rest time, probation period (if any), employment type and wage to be formalized within 5 days.[34] A contract is deemed registered, once the entries to the system have been confirmed by the employer representative's electronic digital signature. Side letters to the contract and entitlement to social leave are registered in a similar way.

In China an employment contract will take force, once it has been signed by the parties in the system rather than registered or confirmed by a public agency.

---

[33] Article 3, Labor Code of Azerbaijan // Collection of Legislative Acts of the Republic of Azerbaijan, 1999. No. 4. Article 213.

[34] Republic of Uzbekistan. Cabinet of Ministers Resolution No. 971 of 05 December 2019. Available at: URL: https://lex.uz/ru/docs/4630025#4633148 (accessed: 06.09.2024)

Two different approaches are thus observed. Apparently, the contract's date and time should coincide with the date and time it was registered with the relevant public system, especially since it is technologically feasible to do with the help of modern digital tools.

Conclusion

As follows from the above study of labor legislation across the EEU, BRICS and CIS, legal regulation of electronic employment contracts in these countries has much in common, something that makes a case for an international instrument on digital labor relations to facilitate regional labor mobility.

The proposed international instrument on electronic employment contracts should rely on the positive legal experiences of the EEU, BRICS and CIS states in the field and contain provisions on the concept of electronic employment contract, its contents and the underlying procedure for conclusion, amendment and termination.

Moreover, the international instrument should provide for bilingual contracts to be concluded in the relevant intergovernmental system. It is thus recommended to introduce to the system automatic online translation supported by an application (legal translator) certified by an intergovernmental authority. Focused on a specific worker category — migrant workers from the international organizations' member states — this instrument will contribute to better understanding of contractual terms by these workers and enhance the protection of labor rights.

A special focus in this instrument should be on electronic time stamp of the employment contract to strictly mark the start of labor relationship. The time stamp is important for the emergence of rights and duties (for example, in remote work in the context of time difference). The recording of contractual terms also facilitates control of compliance with labor law. A shared approach to the party identification and recording of contractual terms (not just registration of the contract) can thus improve the protection of labor rights.

Authors of the article believe the proposed international legal instrument will promote the integration of labor practices across international bodies mentioned.

References

1. Bondarenko V.M., Morozova N.N. (2020) Gender aspects of labor market in Belarus and Russia in the times of economic digitization. In: Papers of international conference within the Public Scholar Forum “Hello, Russia!”. *Big Eurasia*: *Development*, *Security*, *Cooperation*, issue 3, part 2, pp. 639–643 (in Russ.)

2. Filatkina I.D., Filatkina M.D., Krechetnikov K.G. (2015) Legal regulation of personnel labor in India. *Bulletin of the Far Eastern Federal Univerisity. Economy and Management*, no. 3, pp. 97–105 (in Russ.)

3. Filippova I.A. (2020) Labor law: challenges of information society. *Law. Journal of the Higher School of Economics,* vol. 13, no. 2, pp. 162–182 (in Russ.)

4. Khalilov T., Aliyev E. (2020) Digital century: new approaches to employment in Azerbaijan. Conference paper. Available at: https://www.researchgate.net/publication/341733964_Digital_century_new_approaches_to_employment_in_Azerbaijan (accessed: 25.06.2024)

5. Lazanyuk I.V., Revinova S.Yu. (2019) ITC technologies in the BRICS countries: from strategy to cooperation. *Business. Education. Law,* no. 1, pp. 208–213 (in Russ.)

6. Liu Dun, Geng Yuan (2022) The model of state digital platform on labor contracts in China. *Digital Law Journal*, vol. 3, no. 1, pp. 20–31.

7. Morozova N.N. (2019) Digital youth unemployment: employment assistance in Belarus. In: N.N. Morozova, Yu. V. Mokhoreva (eds.). Assisting the Tula Oblast students and school graduates for employment and labor market adaptation: papers of research conference. Tula: University Press, pp. 71–76 (in Russ.)

8. Orlova E.E. (2022) Digitization of employment as a new paradigm of the common labor market development in Eurasia. *Transactions of the Vernadsky Crimean Federal University: Jurisprudence,* no. 4, pp. 228–234 (in Russ.)

9. Perevalov A.G. (2024) Correlation between general labor law provisions on e-document exchange and specific regulating work at micro-firms. *Legal Science*, no. 2, pp. 140–144 (in Russ.)

10. Potapova N.D., Potapov A.V. (2017) Electronic employment contract. *Statut and Law*, no. 8, pp. 52–53 (in Russ.)

11.Raut A.V. (2023) Details of transition to electronic employment contracts. *Ural Scholar Bulletin*, no. 5, pp. 123–127 (in Russ.)

12. Sapfirova A.A. (2020) Digitization of employment contract: prospects of legal regulation and protection of labor rights. Digital Law University Dialogues, International Research Conference papers. Chelyabinsk: South Ural State University, pp. 162–167 (in Russ.)

13. Sapfirova A.A. (2021) Digital application of labor law provisions: issues of labor rights protection. *Personnel Worker*, no. 4, pp. 8–13 (in Russ.)

14. Soloviev P.V. (2023) Transformation of labor legislation in the context of digitization. *Labor and Social Law,* vol. 14*,* no. 2, pp. 32–37.

15. Temirova A.B. et al. (2021) Details of introducing the employment contract record-keeping system in the Republic of Kazakhstan. *University Works*, no. 3, pp. 196–200 (in Russ.)

16. Tomashevsky K.L. (2020) Impact of digitization on the labor market and employment relations (from the perspective of theory and comparative law). *Bulletin of Saint Petersburg State University*, vol. 11, no. 2, pp. 398–413 (in Russ.)

Information about the authors:

M.O. Buyanova — Doctor of Sciences (Law), Professor.
E. S. Batusova — Candidate of Sciences (Law), Associate Professor,

The article was submitted to editorial office 26.06.2024; approved after reviewing 17.07.2024; accepted for publication 05.09.2024.

Legal Issues in the Digital Age. 2024. Vol. 5. No. 3.
Вопросы права в цифровую эпоху. 2024. Том 5. № 3.

IT, Industries, Law

Research paper
УДК: 342
JEL: K2
DOI:10.17323/2713-2749.2024.3.49.67

Legal Regulation of Smart Wearable Devices in China

Li Yao
Institute for Foreign-Related Rule of Law, East China University of Political Science and Law, 555 Longyuan Str., Area Songjiang, Shanghai, 201620, China, yaozaihenmang@mail.ru, ORCID 0000-0002-9933-7513

Abstract

A smart wearable device is a portable intelligent gadget worn directly on the body or integrated into clothes or accessories that along with other features such as portability, mobility, sustainability, interactivity and ease of control exploits the natural ability of human body or environment to exchange information with the user, monitor human health and provide entertainment via built-in sensors, wi-fi communication, multimedia technologies, integrated microchips, etc. There are diverse smart wearable devices such as watches, bracelets, massage tools of various types etc., with usage scenarios ranging from general business uses to professional medicine and health care. High demand and technological progress are boosting the market for smart wearable devices that becomes increasingly attractive. Notably, smart wearable devices are not only hardware but also powerful functionalities supported by applications and cloud computing that collect and generate large amounts of operating data, only to cause widespread concern due to the underlying privacy and data security issues. The paper explores how wearable devices collect data and what risks are involved while providing an overview of the applicable regulation in China and explaining the existing gaps (such as the term "consent" to be clarified in the effective law) and personal data anonymization problem, proposing advice for better regulation as well as the ways to specify the provisions for informed consent, dynamic assessment of anonymized data, etc.

Keywords

smart wearable devices; risk; privacy; personal data anonymization; consent; Chinese law.

For citation: Li Yao (2024) Legal Regulation of Smart Wearable Devices in China. *Legal Issues in the Digital Age,* vol. 5, no. 3, pp. 49–67. DOI:10.17323/2713-2749.2024.3.49.67

Background

Rapid progress of the Internet of things, AI, big data and other next generation data technologies have opened up unprecedented opportunities for the development of wearable devices ranging from the early simple pace-counters to today's multi-functional watches for health and fitness monitoring, mobile payments etc., and up to such devices as smart clothes and AR/VR glasses and headsets. Thus, on 5 June 2023 Apple presented the Vision Pro headset at the WWDC which, compared to the existing VR glasses, integrates the AR (Augmented Reality) technology activated by a lever in the upper part of the headset which, based on the Apple Watch operating system logic and the proprietary spatial computing technology, allows users to see floating virtual interfaces in their real environment. As a fantastic feature, multiple built-in sensors make Vision Pro sensitive to movements of the user's eyes and hands for easy control of the virtual interface with eyes, gesture and voice without joystick or other interactive device. VR devices exemplified by Vision Pro are crucial for access to the metaverse, with numerous types of these devices such as VR glasses, VR helmets and digital VR gloves already available. On 23 April 2024, Meta, a specialist in virtual reality and metaverse, announced the launch of the Meta Horizon OS quest system, with Asus and Lenovo already under contract with Meta for forthcoming production of MR headsets based on Meta Horizon OS. For more natural user experience, Meta Horizon OS integrates numerous self-monitors and other technologies for four new types of communication including hands, eyes, face and body monitoring. While Meta's previous Quest platform had control regimes based on the use of joystick or buttons, new Meta headsets for multi-modal AI control support based on numerous key technologies for 3D simulation, rendering, man-machine engagement, high resolution displays, AR capabilities and

virtual avatars will continue to offer breathtaking and interactive virtual reality experience in a limited environment. With Google 2024 I/O annual conference taking place as planned on 14 May 2024, a number of new AI functions and forthcoming products including Google's own Project Astra multi-modal AI assistant combined with AR glasses promotional videos were announced. Project Astra is expected to memorize and analyze what it sees in addition to audio, text and visual data processing capabilities typical of conventional multi-modal AI macro-models. Wearable devices have largely improved daily life. To encourage further development of the industry, China has implemented the relevant policies for rapid growth of wearable devices in medicine, health care and consumer goods sectors. Meanwhile, there is an expansion of smart wearable devices relying on man-machine engagement and user behavior-related big data that record physiological conditions and behavioral path on a permanent basis thus inevitably creating specific risks to be addressed by law.

1. China's policies in respect of smart wearable devices

A large-scale electronic industry in China is the result of many years of development, with smart wearable devices forming a mature segment of important intelligent products. Boosted by the increasing domestic and international demand and more sophisticated technologies, all types of electronic products have been improved in terms of their design, quality, performance and other aspects, only to encourage domestic producers of wearable devices to further upgrade R&D, production and branding, with competent public authorities introducing a number of measures in recent years.

In June 2016, the State Council published the Framework of the 2030 Healthy China Action Plan: "Developing and promoting digital intelligent devices for health care. Supporting health-related AI research and development, 3D biological printing technologies, medical robots, large medical equipment, auxiliary devices for health and rehabilitation, smart wearable devices and the relevant micro-sensor devices"[1].

In February 2022, the State Council published the 14th five-year plan for development of the anti-ageing national program and pension security

[1] Available at: https://www.gov.cn/zhengce/2016-10/25/content_5124174.htm?eqid=9d4da6bb000833c0000000046496f297 (accessed: 15.06.2024)

stressing demand for "rehabilitation treatment of neurological disorders, post-traumatic cognitive brain disorders, support for people in paralysis, revolutionary brain-computer interface and other technologies, assistive robots for rehabilitative support for various injuries, and implementation of the action plan for development of intelligent service robots, R&D of wearable dynamic devices for ECG monitoring and other equipment for physiological parameter testing, portable health monitoring equipment, self-service and other health monitoring tools, as well as development of new types of microchips for signal recording and intelligent digital health terminals"[2].

In April 2023, the Ministry of Industry and Information Technology issued a circular to support joint innovations and 5G+ Smart Tourism development: "Encouraging the development of 5G applications based on the smart tourism information platform, promoting in-depth integration of digital products such as 5G cameras with embedded AI, VR/AR terminals and smart wearable devices with intelligent tourism products, as well as further promoting 5G intelligent tourism products"[3].

In July 2023, the State Council issued the Notice on consumption recovery and support measures: "Encouraging the consumption of smart wearable devices and intelligent products, as well as develop new usage scenarios for electronic products"[4].

In January 2024, the State Council issued the Opinion on promoting Silver Hair Economy and improving the well-being of elderly individuals: "Improving the list of intelligent products for healthy ageing, promoting a new generation of information technologies and mobile terminals, smart wearable devices, service robots and other intelligent devices for homes, communities, institutions and other settings, developing smart products for health management, care and psychological comfort of the elderly"[5].

As follows from the above national policies, thanks to breakthrough achievements in such innovative areas as AI, data storage and computing,

[2] Available at: https://www.gov.cn/zhengce/zhengceku/2022-02/21/content_5674844.htm (accessed: 15.06.2024)

[3] Available at: https://www.gov.cn/zhengce/zhengceku/2023-04/12/content_5751000.htm (accessed: 16.06.2024)

[4] Available at: https://www.gov.cn/zhengce/content/202307/content_6895599.htm (accessed: 17.06.2024)

[5] Available at: https://www.gov.cn/zhengce/zhengceku/202401/content_6926088.htm (accessed: 17.06.2024)

brain-computer engagement technologies, and promoting the metaverse concept, the usage scenarios of smart wearable devices, ever wider and diverse, will apply not only to gaming, entertainment and tourism but also health management, intelligent medical services, sports and fitness, smart furniture and care for the elderly, and to the development of intelligent, individual and traceable user services.

2. Data collected by smart wearable devices and relevant risks

Broader usage and convenience of smart wearable devices comes at a cost of permanent "surveillance" of users by these devices. Shaped by the information age, smart wearable devices carry cameras, sensors, chips and other sophisticated equipment sensitive to physiological conditions of human body and able to collect real-time data and engage with a cloud or software for personalized reporting, only to make the underlying usage scenarios highly sensitive to personal data collection as manifested by the following:

Firstly, automatic real-time collection of data. In traditional devices, information is normally collected partially and in a fragmented way while smart wearable devices are capable of continuous collection of data that can follow changes to the human health in real time. The man-computer engagement logic is that the line between man and machine, body and environment gradually fades. In mobile scenarios, wearable devices are linked to human body thus connecting people, behaviors, scenarios and networks, with the body and media mixed together, reality and virtuality mapping over each other, so that human biometric data, information on health, fitness, geographic position and environment is monitored round the clock. Surveillance permeates our daily life like air and water. As has been noted in literature, "thanks to round-the-clock following, monitoring, reminding and feedback, smart wearable devices, like smart companions, become a kind of replacement for human limbs, a technological shadow body where the subject is digitally assembled from different behavioral patterns to become a walking digital man embedded, every time he opens his eyes, into a heterogeneous environment of multidimensional time that is real and virtual, private and public" [Xu T., 2022: 163].

Secondly, pervasiveness. A smart shadow companion, the wearable device not only collects static biometric information such as cardiac rate, myo-electricity, pulse, blood pressure, oxygenation, body temperature etc.,

but also assesses and recognizes the user's behavior and state (whether he sits or stands, runs or jumps, works or sleeps, walks or falls), location and environment (weather conditions, barometric pressure, altitude) and other related data. In short, the wearable device can present a full picture of human health and daily activities by generating the user's exact profile. Types of data collected by wearable devices embrace virtually all human states over the day: at work, a smart watch will remind users: "please take a walk, do not sit still"; during physical exercising, "steps, cardiac rate, blood oxygenation, arterial tension, palpitation"; during sleep — state and time of sleep. Relying on novel technologies, VR products can not only collect users' external biometric data such as iris diaphragm, fingerprints, body height, constitutional type, voiceprints etc., but also physiological information by monitoring heartbeat and muscular response. The progress of the brain-computer interface has resulted in mind control, only to mean that the data detection "pinhole" can go deep "under the skin" and assess human brain data such as thinking, consciousness and memory, one by one. BrainLink, a smart headband developed in China, is advertised to monitor the user's brain, for example, whether it is tense, relaxed or tired [Wei Z., Shi H., Cao T., 2020: 19]. Once illegally transferred and sold, such data can be applied in many ways, not only violating the right to privacy but also creating major social problems such as discrimination at employment, thus adding up to the dilemma of science and technology ethics.

Thirdly, more parties involved in the process. Wearable devices have more segments of information flow including data collection, storage, use exchange, provision and deletion which may involve consumers, patients such as elderly people and children, service providers, health institutions, governments and other multilateral subjects, with a higher risk of leakage and unauthorized processing. In contrast, traditional health care assumes a process focused on in-patient consultations with lower-risk circulation of information within the hospital. Meanwhile, proprietary technologies of wearable medical devices are focused on digital data processing and transfer via wireless communications including diffraction bio-signals, navigation, cloud storage, fingerprint identification, data requests, fees, filming, screening, AI, medical visualization, nanoinjections, connectivity, resource and energy distribution, etc. [Liu X., 2020: 39-41].

Fourthly, multiple use. When marketed, Apple Watch was advertised as "saving lives ruined by mobile phones" while it would penetrate inside the body under the pretext of "exercising for health" [Song M., Xu S., 2020:

47]. While users assess and monitor the state of their health and regulate physical exertion through the use of wearable devices posting the results to social platforms in real time, it feels as if they were filmed by a security camera. The use of personal data in wearable devices has gone well beyond simple health monitoring to serve secondary purposes. If we integrate and process the information collected by wearable devices, we will get indirect data of substantial informative value. For example, body data collected by these devices can be professionally analyzed to generate user health reports, with a back office to tell on this evidence whether the user has suffered or will suffer from certain disease; credit or insurance companies to charge higher premiums or even assess the feasibility of insurance services in view of the reported state of health. Correlation analysis of cardiac rate, oxygenation, deep sleep and other data can help to detect whether the user suffers from cardiovascular diseases while businesses can use these data to offer certain medical goods and drugs. As another example, the extent of papillary dilatation can reveal a preference for something, and eye-tracking technology can tell whether the user has recognized something by the movement of his eyes; if we link this data with the user's location or address, we can recommend a fitness center, restaurant or other recreational site. Using personal data brings enormous potential to businesses leading to re-use of personal data. At this moment, "the user becomes a link in production chain where he will permanently generate both data and feedback on data usage" [Hu L., 2018: 91].

The growing use of wearable devices and supporting applications is fraught with three main threats related to the extent and sensitivity of data being collected: privacy, data use and exchange, and also the risk of hacking.

Firstly, a new type of privacy risk. Smart wearable devices collect real-time data on pulse, blood pressure, respiratory rate, sleep, physical exertion, dietary preferences, lifestyle etc., while health data are currently the most confidential type of information. While users voluntarily collect and analyze the said data via wearable devices to generate personalized reports, they might be unaware that these devices can collect their other data along the way. Moreover, with technological change smart wearable devices are able to make and accept calls, send and receive messages, make instant payments meaning that the wearable device should have real-time connectivity to the user's smartphone, with supporting mobile applications constantly collecting different data from the smartphone in the background. While all data collected by smart wearable devices are accessible to their manufacturers, the user collecting the data is unaware what information

is collected. This results in information asymmetry and round-the-clock privacy threat to the user.

Secondly, risks of unauthorized data use: what the collected data will be used for and whether they will be made available to third parties. In the age of big data, data are as valuable as oil, and it is only natural that smart wearable devices in contact with the user round the clock 7 days a week will use this advantage. Many companies share the collected data with the third parties to maximize their profits. Thus, consumption data are sold to advertisers for better targeted advertising while physiological data and those on habits for physical exertion can be made available to insurers for higher premiums. Since firms increasingly use consumer data in new and different ways, it may result in a loss of control over users' personal data when wearable device manufacturers and their partners will know more about users than users themselves. With more data transferred and used, the leakage risk is higher. Where personal data are transferred and processed by several entities, users will find it hard to understand where their data go and why they are processed, only to create a "black box effect".

Thirdly, risks of hacking. Under the current design and development pattern, the focus is on higher performance and lower weight of wearable devices, with a majority of manufacturers unaware of security issues and even willing to compromise for the sake of performance thus increasing the risk of hacking. While the data collected by smart wearable devices are normally not encoded, abusers can have access to user personal data and location via the Bluetooth connectivity to monitor user actions and even remotely control the devices, only to threaten the security of persons and property. Some studies have demonstrated that personal health data is information on someone's physical or psychic health received in process of preventive care, diagnostics, treatment etc. It is a symbol related to a particular person reflecting individual traits and enabling identification [Tian Y., Zhang Y., 2021: 50]. In 2022, 41 percent of advanced persistent threats (APT) will be related with the government and health care, with attacks on health care to account for 15 percent of total APT attacks in China, second only to the government sector[6]. Malware or application errors can equally result in unauthorized access to data saved in wearable devices, with design errors at the top of statistics of vulnerability causes[7].

[6] Available at: https://www.qianxin.com/threat/re-portdetail?report_id=151 (accessed: 17.06.2024)

[7] Available at: https://www.topsec.com.cn/uploads/2024-01-04/5573280d-c531-4b57-8407-deaa347472e91704359364603.pdf. (accessed: 18.06.2024)

3. China's regulatory framework and gaps

3.1. Legal regulation overview

At this stage, China's personal data protection law mainly splits into two parts: private and public law.

As to civil law, personal data protection in China is largely governed by the Civil Code of the People's Republic of China (hereinafter Civil Code of China) and by the Law on Personal Data Protection. The Civil Code of China explicitly considers biometric information as personal data in the "personal rights" section protectable together with the right to privacy, with relevant legal remedies available to civil law subjects[8]. The Law on Personal Data Protection provides for persons' right to informed consent to personal data processing that could be withdrawn, and for processing agents' duties to classify and manage personal data[9].

From the perspective of the Criminal Code of the People's Republic of China (hereinafter Criminal Code of China), the main crimes related to personal data security[10] are offenses against personal data of individuals (Article 253.1) while the Supreme Court and Procurator General Office in their Explanation on applying legal provisions to personal data-related criminal offenses have stated: "Illegal ownership, sale or presentation of personal data shall be deemed an aggravating circumstance envisaged by Article 253.1 of the Criminal Code of China where it has occurred in one of the following situations:... 4) illegal ownership, sale or presentation of over 500 personal data units such as information on housing, communication records, physiological and health data, transactional and other data likely to impact the security of persons or property"[11]. Other offenses are related in the Criminal Code to illegal penetration and destruction of computer systems (Article 285); non-compliance with data security duties (Article 286.1); and illegal use of data networks (Article 287.1).

---

[8] Available at: https://www.gov.cn/xinwen/2020-06/01/content_5516649.htm (accessed: 18.06.2024)

[9] Available at: https://www.jxrtvu.com/xdjyjszx2023/2022/0906/c3642a29877/page.htm (accessed: 19.06.2024)

[10] Available at: http://www.law-lib.com/law/law_view.asp?id=768114&page=2 (accessed: 19.06.2024)

[11] Available at: https://www.spp.gov.cn/xwfbh/wsfbt/201705/t20170509_190088.shtml(accessed: 19.06.2024)

As to administrative law, China's legislative framework on personal data security is scattered across a variety of regulations, standards etc. For example, the Data Security Technology Specifications for Personal Data Protection (GB/T 35273-2020)[12] consider medical and physiological data, biometric personal data as personal confidential information. Standards are crucial for bio-data security. With rapid progress of web technologies over the last few years and new issues emerging in related areas one by one, legislation, being subject to rigid procedures, is obviously a laggard. Therefore, standards are used in practice largely to settle and standardize specific issues. The Chinese Government and market players have also developed a number of standards on collecting and protecting personal biological data. Thus, the Telecommunication Terminal Industry Forum Association issued in 2020 a group standard "Specifications for minimum required evaluation of personal data to be collected and used by APP: data on persons"[13]. According to China's Standardization Law[14], a group standard is the one jointly developed by a civil society organization under the law to satisfy market demand and support technological innovation and coordination between the relevant market players as agreed between the organization's members or presented for voluntary acceptance under the organization's statute, and designed largely by actors with a certain degree of influence over the industries in question.

Because of the late emergence of personal data legislation in China, provisions for protection of individuals' biological data are still scattered across sectoral laws. Though the adoption of the Law on Personal Data Protection has filled some legal gaps in specific areas, its content is still dominated by broad provisions on personal data collection, usage and processing while multiple standards developed in response to practical needs, albeit more detailed, are not binding and systematic.

3.2. Existing legal gaps

Limited computing and storage capacities allow to upload and store large amounts of personal data on platforms while a majority of wearable devices

[12] Available at: http://nic.swu.edu.cn/__local/1/FE/8B/5DC92A975E617561B685BDDE3DA_B7B6D500_FE10A.pdf (accessed: 19.06.2024)

[13] Available at: https://www.ttbz.org.cn/Pdfs/Index/?ftype=st&pms=40991 (accessed: 19.06.2024)

[14] Available at: http://www.npc.gov.cn/zgrdw/npc/xinwen/2017-11/04/content_2031446.htm (accessed: 20.06.2024)

do not enable user control for preventing personal risks in these processes such as timely request for, correction, deletion or withdrawal of consent. Where users' personal data are uploaded to a cloud, violations cannot be stopped by powering off or switching off the device since data circulating between several data controllers are aggregated in different directions at different levels under specific scenarios, sectoral needs and business models [Xu T., 2018: 169]. Health care services provided by wearable devices such as Apple HealthKit, Google Fit, Huawei Hi Health etc. rely on big data analysis to collect large amounts of personal data on users' health in real time, as well as to monitor, screen and prevent a wide range of health issues. However, few people believe they have a right to decide what personal information will be collected by wearable devices and how it will be used. Obviously, consent is at the core of personal data protection in wearable devices [Man H., Guo L., 2023: 121]. Firstly, such consent is a manifestation of the party's autonomous will. Smart wearable devices can perform medical operations for physical health monitoring or detection of potential health problems where there is medical agreement between the user and the data processor, with the latter required to seek prior consent since the user is autonomous. On the other hand, wearable devices collect large amounts of medical data from the human body in real time and by providing health care services to users become a tool for medical research. To guarantee the user's rights and interests as a subject and to seek consent, the theory should go back to considerations on the duties of health personnel during the Second World War — Permissible Medical Experiments of The Nuremberg Code (1947): "The voluntary consent of the human subject is absolutely essential. This means that the person involved should have legal capacity to give consent; should be so situated as to be able to exercise free power of choice, without the intervention of any element of force, fraud, deceit, duress, overreaching, or other ulterior form of constraint or coercion; and should have sufficient knowledge and comprehension of the elements of the subject matter involved as to enable him to make an understanding and enlightened decision"[15].

The meaning of the term "consent" still needs to be specified in the effective Chinese law. As applied to wearable devices, the user's consent primarily refers to private domain, with para 1, Article 13 of the Law on Personal Data Protection ruling that data processors may process personal data upon a person's consent while under para 4, Article 13, no user con-

[15] Available at: https://cirp.org/library/ethics/nuremberg/ (accessed: 20.06.2024)

sent is required in emergency situation where someone's life and health are at stake[16]. While not an issue in the traditional production sectors, it is a problem in the industry of wearable devices widely used in medicine and health care where the user has a discretion in respect of medical interventions and should be able to independently decide whether the interests of his health prevail over those of his personal data, since users are often as much fearful of disclosure or unauthorized use of data as of any disease. The terms applicable to mandatory data processing in emergency should be made more specific. As the personal data subject cannot control whether his medical data is sent while instantly generated data such as pulse, blood pressure, body temperature as well as ECGs, brain waves etc., are no longer filtered by the brain before being sent by the subject and instead are automatically collected by the device, the data collection "consent" envisaged by the effective law is not sufficient.

At the same time, Article 4 of the Law on Personal Data Protection explicitly excludes anonymized data from protected personal information with an intent to fully realize the value of personal data for economic and social development once such data is cleared of individuality through the use of this mechanism, and thus to strike a balance between the use and protection of personal data [Zhang X., 2018: 48]. However, in practical terms it is often hard to tell whether personal data have been sufficiently anonymized as technologies and data used for re-identification are ever evolving to defy any forecast [Esayas S. Y., 2015: 3]. Some studies have shown that it is practically impossible to fully remove the risk of re-identification of anonymized personal data [Qi Y., 2021: 52]. Pursuant to Article 73 of the Law on Personal Data Protection, anonymization is a process whereby personal data are processed in such a way that they no longer identify a natural person and cannot be recovered. However, the Law contains no clue as to the extent of technical processing required to achieve the standard of non-identifiability and non-recovery.

Data processors will currently use personal data for profit-making largely under three business models: macro-economic decision-making; marketing of a specific business; and click bait [Shen J., 2022: 93]. Meanwhile, data likely to be used for the said purposes are practically impossible to anonymize, especially in areas such as user profiles and personalized recommendations [Ding X., 2019: 82]. The more detailed and complete are

[16] Available at: https://xxzx.lfyjzjxy.com/uploads/editor/98/0f4bdfcab2389b06ae0d5b2fa99753.pdf (accessed: 20.06.2024)

personal details contained in data, the more accurate are the outcomes obtained through an algorithm and thus its contribution to the accuracy of marketing. Thus, from the data processor's perspective, personal data anonymization is paradoxical: if data is not anonymized, there is no way to disseminate and use personal information; meanwhile, anonymized data that could be disseminated and used have no value. A strife towards absolute data security is clearly not the only purpose of law: it is equally important to promote the use of information and data, and to support the digital economy. Ideally, there should be a balance between data security and conveniency of data usage.

4. Proposals to improve the law and address gaps

4.1. Specifying legal provisions for informed consent

Despite China's effective laws clearly establish the principle of informed consent, the detailed provisions on personal data collection by wearable devices are in a sense inadequate, only to complicate adaptation to new situations and risks in the context of ongoing progress of modern information technologies. With regard to specific rules to seek consent, it is proposed to: firstly, allow for users' right to consent in substance; for documents such as data privacy, downloading and exchange statements, provide for the regime of partial consent or full refusal instead of full consent, with users to choose either option depending on their needs or preferences while applications should not interfere with or limit the use of different health management services provided by wearable devices if the user has opted for partial consent or full refusal. Secondly, health data and other physiological information such as cardiac rate, blood oxygenation, blood pressure, body temperature, brain waves, ECG etc. collected by sensors and IOT units on wearable devices, once tracked and integrated, can easily disclose the user's past clinical record and particular states of health. Pursuant to para 2, Article 28 of the Law on Personal Data Protection, the following three conditions are to be met for processing sensitive personal data: specific purpose; reasonable necessity; rigorous protective measures. With regard to wearable devices, data processors are required to specify the type and amount of biometric data they collect and the underlying purpose. Since the Chinese law does not establish a list of specific purposes of biometric data collection, operators should explain the purpose of each biometric data unit to be collected in authorization requests in simple

language understandable to users. Thus, if the operator only indicates that "certain part of information will be used for gaming functionalities", the requirement of "specific purpose" will not be met; it should be stated instead that information will be used to support a certain functionality in the specific part of the game, with vibration, animation etc. used to clearly tell the user that full awareness is required before the "agree" button is pressed. It should be noted that at the data usage stage the data processor should process personal medical data to the minimum extent required to achieve a specific user-allowed purpose. Under Article 14 of the Law on Personal Data Protection and Article 38 of the Policy for Ethical Review of Bio-Medical Research Involving Human Subjects[17], a new written user consent should be sought where the specific purpose, method and type of data processing, as well as the program, amount and content of research have been changed. Individual users should also be aware of their rights and give attention to the specific terms of service, personal data collection/privacy protection agreement for VR applications, and report equivocal or unfounded terms to consumer associations and other bodies while the government should provide for convenient ways to lodge complaints.

4.2. Helping users to truly exercise the right to withdraw consent to personal data processing

While the Law on Personal Data Protection stipulates that consent to personal data processing may be withdrawn[18], this makes little practical effect. In this regard, application developers may be required to clearly specify the user's right to withdraw consent and the path to the relevant button for the user to decide whether to give or withdraw consent, and to ensure the ease of the button's use in absence of artificial obstacles (like heaping it up with settings). Firstly, where the data processor has been changed at the data usage stage as a result of liquidation following merger,

[17] Available at: https://www.gov.cn/zhengce/2016-10/12/content_5713806.htm (accessed: 23.06.2024)

[18] Article 15. Where personal data are processed upon a natural person's consent, such consent may be withdrawn. The personal data processor should arrange for a convenient way to withdraw consent. Withdrawal of consent shall not affect the validity of personal data processing operations consented by the natural person before such withdrawal. Article 16. The personal data processor should not deny the provision of goods or services on the basis that a natural person does not give or withdraws consent to personal data processing, except where personal data processing is required to provide goods or services.

division or bankruptcy, the name and contact details of the data recipient should be clearly communicated to the user with the help of animation or voice message within a prior reasonable period based on the principle of specific purpose and the user's reasonable trust in the data processor, with the user entitled to withdraw consent. Secondly, since users assume the main risk under the health management scenario, the user has a discretion to withdraw consent to physiological data processing and may exercise the right to remove unnecessary, irrelevant or obsolete physiological data processed and controlled by the data processor. Thirdly, users have the right to withdraw from medical research projects at any time while data processors should timely stop processing personal medical data following a withdrawal request and timely provide feedback to the data subject. Withdrawal of consent by the user does not affect the validity of prior operations to process personal health data consented by the user. Once the purpose of research has been reached, the data processor should step in to delete such data. Fourthly, it is proposed to implement arrangements for the "loss" of device, that is, where a wearable device has been lost, stolen, abandoned etc., convenient and fast channels will be provided to users to report the loss and lodge complaints, with the device to be automatically "blocked" and the stored personal data timely deleted in the background mode, once the event of loss has been conformed.

4.3. Improving legal provisions for emergency personal data processing

Constraints that make it impossible to obtain data processing consent in a situation of major risk to human life and health can do a considerable harm to users. There is only one legal basis to force wearable devices to process personal medical data, that is, para 4, Article 13 of the Law on Personal Data Protection: "Life and health of natural persons should be protected in emergency". Researchers believe that the Civil Code and the Law on Personal Data Protection reflect pluralistic rules of consent [Xiao X., 2022: 176]. However, the above law-protected interests and rights to protection of life and health, as well as the right to information belong to users who, given their compliance with social order, morals and public interests, have a discretion to decide on their affairs and even life, and thus cannot neglect their own will. In our view, paragraph 4, Article 13 of the Law on Personal Data Protection is close to *negotiorum gestio* (Article 979, Civil Code of China) whereas processing personal medical data to avoid

harm to the user's rights and interests is *negotiorum gestio* because of the need to protect the user's interests presumed to be the user's intent. To avoid unauthorized processing of data by smart wearable devices, the following conditions should be met: firstly, major risk: user's life and health should be at risk; secondly, data processing urgency; and, thirdly, data minimization principle. From the perspective of comparative law, GDPR clearly defines the principle of data minimization[19].

4.4. Dynamic anonymized data assessment

The consequences of de-identification are by no means static since they are rooted in continuous technological progress and massive buildup of data and information. The Article 29 Working Party (2014a) analyses the force and limits of anonymization techniques against the EU legal background of data protection and provides recommendations to handle these techniques by taking account of the residual risk of identification inherent in each of them[20]. ICO call for views: Anonymization, pseudonymization and privacy enhancing technologies guidance chapter 4 (Accountability and governance): "Your governance procedures should address what you will do if you are concerned that the risk of re-identification has increased, e.g., due to technological developments or increased availability of additional information that when linked to the anonymized data may facilitate re-identification. You should consider introducing measures to mitigate these risks"[21].

Thus, the ranking of de-identified personal data should be dynamic, with data processors required to keep the de-identification effect under permanent control through a risk assessment mechanism implemented to specify the systemic processes, subjects of supervision and liability for regular assessment of risks regarding de-identified personal data [Xia Q., 2022: 102]. The risk of re-identification of de-identified personal data may vary depending on the evolution of information environment, data users, technological development levels and other pertinent factors. Thus, data processors should re-assess the re-identification risk on a permanent basis or following changes to the relevant factors, with de-identification to be performed again based on assessment results.

[19] Available at: https://gdpr-info.eu/art-5-gdpr/ (accessed: 25.06.2024)

[20] Available at: https://www.aepd.es/documento/88197.pdf (accessed: 25.06.2024)

[21] Available at: https://www.lexology.com/library/detail.aspx?g=f443dc16-49e8-49e6-b2be-cdd59c04e884 (accessed: 26.06.2024)

In addition, once explicit identifiers were processed with the help of technology, the data processor must store additional data separately and not disclose them together with core information. For example, where all full names in a large personal data block are replaced with a specific type of identifiers using pseudonymization, the data processor is required to store separately and withhold any additional data that allows to recover full names. Meanwhile, the data processor is required not to perform re-identification and, if personal data with removed explicit identifiers have been transferred, contractually prohibit re-identification to the recipient (Han X., 2018: 72). Should the recipient re-identify data in violation of the contract with the data processor, he will assume liability. Should the recipient re-identify personal data by removing explicit data identifiers or by processing for other than originally specified purpose to the detriment of the rights and interests of personal data subjects, he will be liable to such data subjects for damages and other tort obligations. Data subjects may require compensation of damages both from data recipient and data processor. Once compensation was paid, the data processor has the right to recover damages from the recipient. Under Article 1197 of the Civil Code of China, the data processor shall assume joint liability in the event of a failure to act where he was or should have been aware of the data recipient's illegal conduct.

4.5. Innovative technologies to prevent hacking attempts

In response to the risk of personal data leakage and hacking attempts, wearable device manufacturers should introduce innovative technologies and take appropriate action to assume social responsibility. Conventional electronic devices (computers, smartphones, watches etc.) come with data protection technologies such as private data encoding, secure application and developer audit tools, access control and authentication technologies designed to limit data collection etc. Data protection in smart wearable devices should be based on unique data properties such as safer file types and formats for multi-modal data profiles collected by wearable devices, proprietary data collection modules added to wearable device hardware to characterize engagements with users for numerous aspects of biological information, as well as using several data authentication methods such as biometry and virtual identifiers to mitigate the risk of intrusion and fraud for wearable devices.

Conclusion

While a combination of smart wearable devices and applications is likely to satisfy users in their strife for entertainment and health as well as better living standards, these gadgets will keep watch over users round the clock to collect data that can attract advertisers, research institutions and even hackers. Over the last few years, the problem of data privacy and security has come under increasing scrutiny and, as individuals are becoming aware of the need for privacy and security, there is a need in tougher regulation of smart wearable devices from this perspective. Now that the technology of wearable devices is rapidly progressing, there is no assurance that it will expand across all spheres of life and work unless we guarantee that data collection does not undermine privacy and security. Market players should also join forces to ensure compliance of wearable devices with biometric data collection and processing requirements.

References

1. Ding X. (2019) User Profiles, Personalized Recommendations and Personal Information Protection. *Huan qiu fa lv ping lun* = Global Law Review, no. 5, pp. 82–96 (in Chinese).

2. Esayas S.Y. (2015) The role of anonymization and pseudonymization under the EU data privacy rules: beyond the "all or nothing" approach. *European Journal of Law and Technology,* no. 2, pp. 1–20.

3. Han X. (2018) Legal Regulation of Anonymous Information in the Era of Big Data. *Da lian li gong da xue xue bao (She hui ke xue ban)* = Journal of Dalian University of Technology (Social Science Edition), no. 4, pp. 64–75 (in Chinese)

4. Hu L. (2018) On the Architecture of Cyberspace and Its Legal Implications. *Dong fang fa xue*=Oriental Law, no. 3, pp. 87–99 (in Chinese)

5. Liu X. (2020) Patent Analysis of Global Wearable Medical Intelligent Devices Based on "Wisdom Buds". *Zhong hua yi xue tu shu qing bao za zhi*=Chinese Journal of Medical Library and Intelligence, no. 8, pp. 37–42 (in Chinese)

6. Man H., Guo L. (2023) Personal health information protection in wearable devices — a consent-centered study. *Fa xue lun tan*=Law Forum, no. 2, pp. 121–131 (in Chinese)

7. Qi Y. (2021) A Review of China's Personal Information Anonymisation Rules and Alternative Choices. *Huan qiu fa lv ping lun*=Global Law Review, no. 2, pp. 52–66 (in Chinese)

8. Song M., Xu S. (2020) Wearables as media: dataization and regulation of the body. *Xian dai chuan bo*=Modern Communication, no. 4, pp. 46–50 (in Chinese)

9. Shen J. (2022) The Rights Architecture and the Unfolding of the Rules of Data Property. *Zhong guo fa xue*=China Law Journal, no. 4, pp. 92–113 (in Chinese)

10. Tian Y., Zhang Y. (2021) The Protection of Personal Health Information in the Era of the Civil Code. *Bei jing hang kong hang tian da xue xue bao (She hui ke xue ban)*=Journal of Beijing University of Aeronautics and Astronautics (Social Science Edition), no. 6, pp. 47–58 (in Chinese)

11. Wei Z., Shi H., Cao T. (2020) Research progress of intelligent wearable devices at home and abroad. *Zhong guo yi xue zhuang bei* = China Medical Equipment, no. 10, pp. 18–21 (in Chinese)

12. Xu T. (2018) Privacy Dilemma and Remedy Path in the Age of Artificial Intelligence. *Xi nan min zu da xue xue bao (Ren wen she hui ke xue ban)*=Journal of Southwest University for Nationalities (Humanities and Social Sciences Edition), no. 6, pp.166–170 (in Chinese)

13. Xu T. (2022) Data Intelligence Regulation: Privacy Risks and Protection of Wearable Devices. *Jiang xi she hui ke xue* = Jiangxi Social Science, no. 12, pp. 162–170 (in Chinese)

14. Xiao X. (2022) Pluralistic Consent Rules for Personal Information Processing — Understanding and Interpretation Based on the Consent Hierarchy System. *Zheng zhi yu fa lv*=Politics and Law, no. 4, pp. 158–176 (in Chinese)

15. Xia Q. (2022) Improvement of Notification Obligations and Dynamic Anonymization of Personal Information Protection in Cyberspace. *Jiang han lun tan*=Jianghan Forum, no. 3. pp. 95–103 (in Chinese)

16. Zhang X. (2018) Discussion on the Main Contradictions of China's Personal Information Protection Law Legislation. *Ji lin da xue she hui ke xue xue bao*=Journal of Social Sciences of Jilin University, no. 5, pp. 45–56 (in Chinese)

Information about the author

Li Yao — Doctor of Sciences.

The article was submitted to editorial office 05.07.2024; approved after reviewing 15.08.2024; accepted for publication 05.09.2024.

Legal Issues in the Digital Age. 2024. Vol. 5. No. 3.
Вопросы права в цифровую эпоху. 2024. Том 5. № 3.

E-Government

Research article
УДК:342
JEL: K4
DOI:10.17323/2713-2749.2024.3.68.87

Artificial Intelligence in the Judiciary: Issues and Outlooks

Anna Vladimirovna Belyakova
Institute of Legislation and Comparative Law under the Government of the Russian Federation, 34 Cheremushkinskaya St., Moscow 117218, Russia,
belyakova.av@gmail.com, ORCID: 0000-0003-4241-4511

Abstract

Application of artificial intelligence in governance and in public, economic, and political life draws the attention of many researchers from various areas of science. They study how AI affects the development of economics, law, philosophy, and medicine. They also look at how AI introduction affects various industries from an ethical and moral point of view. E.g., there is a risk that robotic systems will replace humans and labour relations will transform completely, or that goods-money relations change as marketplaces and online platforms appear. In the era of rapidly developing technology and information processes, introducing digital products and algorithms into governance and into social and economic relations is an objective necessity, so these processes gain momentum. Legal science, the legal system and law in general have to adapt to changes in society, economy, science, technology, politics, and governance. The judicial system is no exception in this situation. By multitasking and speeding up production cycles, digital and electronic products simplify and optimise production processes. At the same time, there are risks to overuse artificial intelligence and minimise the human factor. Replacing skilled staff with robots and IT systems does not always optimise processes and can result in fatal errors. Technical progress fosters the growth of fraudulent and other criminal schemes that involve information technology because it helps perpetrators to abuse law, violate personal boundaries, and constitutional and legal guarantees. The author analyses various aspects of the introduction of AI into the judicial system, and examines the

reasons for and ramifications of the use of digital products and services for justice and society. The methodology of the study is based on general research ways like analysis, synthesis, generalisations and dialectical methods. Other methods include formal logical and comparative legal studies.

Keywords

AI; neural networks; justice; judicial system; justice digitalisation; information technology; judicial discretion; concept of judicial law.

Acknowledgements: The paper was prepared for presentation: "Artificial Intelligence in the Judicial System: Justice "without a Face"? at 12th Conference "Law in the Digital Age" at the Faculty of Law of the National Research University Higher School of Economics on 1 December 2023. Author is deeply indebted to organizers of conference. Special thanks are due to Professor Irina Yurievna Bogdanovskaya.

For citation: Belyakova A.V. (2024) Artificial Intelligence in the Judiciary: Issues and Outlooks. *Legal Issues in the Digital Age,* vol. 5, no. 3, pp. 68–87. DOI:10.17323/2713-2749.2024.3.68.87

Introduction

The research examines social relations pertaining to the use and application of new and emerging technologies in the judicial system, and analyses particular aspects concerning AI in the administration of justice. In particular, it draws attention to the establishment of objective truth by means of "pre-set algorithms."

AI use affects worldview, perception, consciousness and legal awareness, and changes the ways and mechanisms of performing familiar processes. In other words, it transforms objective reality in favour of virtual reality. This applies not only to socio-economic relations, but also to legal relations. Conventional approaches are receding into the background. The new millennium is the time for using new information, IT, and robotic processes in all spheres of human relations. This isn't just any latest trend, but logical incremental development of the society and production. In this connection, many questions arise that are awaiting their solutions. E.g., what areas and activities can be entrusted to robots? Can application of robots be accepted in the legal sphere? These questions, alongside many others, are still waiting to be answered.

In the past decades mankind has seen quick development of digital technologies that in everyday life is not perceived as a "new era" or a period of

paradigm shift in socio-economic and political relations. The issues related to full integration of various technical and digital products and resources into all spheres of life and public authorities have been gaining more and more relevance. At the same time, traditional and conservative approaches have increasingly been relegated to the background. Such technologies are not only IT, ICT, information modelling, virtual space, robots, machine-readable law, etc., but also artificial intelligence, which is increasingly being used in various fields. As these technologies evolve, more and more questions on their relation to the rights, freedoms and lawful interests of citizens arise.

And here, introducing IT in various spheres of public life and in socio-economic areas is one of the priorities of national policy in the Russian Federation [Khabrieva T.Y., Klishas A.A., 2020].

One may see digitalisation products developed, implemented and used everywhere: in the agro-industrial complex, educational process, judicial system, urban planning, housing and utilities sectors, as well as in ecology and environment protection and many other areas of human activity. It should be noted that despite their diverse nature, IT-related problems are equally important not only in the design phase but also in the implementation and utilisation phases.

Economy and public administration are developed to increase efficiency, improve the quality of functioning, and optimise and simplify individual tasks and processes. A number of problems should be noted here. They include peculiarities in practical implementation and in public administration (including legal regulation because the number of laws and regulations on particular issues in the area under consideration has been growing exponentially). Other aspects that have to be taken into account include the lack of specialists with cross-disciplinary experience, lack of coordination between the private and public interest, and the inability to organise interaction between practitioners and subjects of state regulation and administration. Another issue, which is just as serious, is insufficient funding and the lack of private investments, as well as the lack of a system of interaction between governmental entities that would take into account the interests of public at large, including entities engaged in entrepreneurial and other business activities in the said areas, and end product users.

In author's opinion, judicial system is facing the greatest risks here. As information technologies are adopted everywhere, the number of court cases may only grow than decrease because the technologies not only help optimise processes but also open up opportunities to abuse procedural rights and law in general.

Therefore the author is sure the questions raised in the article should be considered, together with a number of other aspects, from the perspective of the modern concept of judicial law. It, in turn, with a logical and structured approach, may help to form an adaptive judicial system in current realities.

1. From Digitalisation of Justice to Artificial Intelligence in the Judiciary

Digitalisation of various spheres of life is a worldwide trend. The aim is to provide the best organisational, technical, technological, production and industrial conditions for the development of society.

The use of digital products in professional relationships or in public administration can streamline individual processes, speed up data transfer, and help to aggregate and analyse large amounts of information. Thus, it is a unique form of optimising certain activities using specialised software, and the justice system is no exception here. This digital optimisation of professional activities is meant to make human work easier, reduce the time to complete the tasks at hand, and accelerate the achievement of goals. Here, the specialist (employee) coordinates and manages the process, and not the other way round. In other words, "whoever sets the search string is in charge." And in this case, it should be the human operator, not digital algorithms set by someone else.

E.g., in various spheres and areas, artificial intelligence is beginning to discredit itself, in terms of the quality of information provided[1] and work performed[2].

It is quite difficult to introduce digital products in the Russian Federation, for a number of reasons. Firstly, such services are not 100% accessible in Russia. Hence, to promote the society's digitalisation, maximum accessibility to advanced digital technologies must be ensured for state and municipal authorities, representatives of the business community, and for

[1] Global audiences suspicious of AI-powered newsrooms, report finds. Reuters, 18 June 2024. Available at: https://www.reuters.com/technology/artificial-intelligence/global-audiences-suspicious-ai-powered-newsrooms-report-finds-2024-06-16/ (accessed: 24.06. 2024)

[2] Amazon's next Big Bet on Cashless shopping is a smart grocery cart. Gismodo, 14 July 2020. Available at: https://gizmodo.com/amazons-next-big-bet-on-cashless-shopping-is-a-smart-gr-1844377270#:~:text=Meanwhile%2C%20for%20items of%20the%20item (accessed: 24.06. 2024)

individuals. To this end, it is necessary not only to increase funding the field, but also to ensure accessibility at all levels, and to create "adjacent", interdisciplinary specialities and areas that integrate IT with other fields. Without the development of an interdisciplinary approach, we do not believe it is possible to fully computerise and digitalise the processes involved in different areas of government regulation.

Secondly, the lack of software and information systems of a proper level and quality does not contribute to the development of digital infrastructure in this area either. It is of great importance to form a unified information space and unified databases, regularly updated and extended. Access to them would simplify interaction not only between government agencies (interdepartmental interaction), but also directly between agents active in various socio-economic areas of Russia. To achieve this, it is necessary not only to ensure that the data and information provided is updated regularly, but also to create: interdepartmental "cloud technologies" allowing stakeholders to quickly exchange information, to extend and correct it in real time; individual servers; software to ensure data protection, including protection of personal data. It is necessary to structure the information and data provided, to establish logical interrelationships, and to form a "complete cycle" of production and processes, including the stages of public administration.

All of the above are, in the author's opinion, organisational and technical reasons affecting difficulties in the development of digital and information services, including artificial intelligence in public administration. These reasons include the need to develop certain specialities and specialised education, as well as to build a logical and structural interaction in this area between society and the business sector, on the one hand, and government and municipal authorities and other stakeholders, on the other hand. So, a centralized approach needs to be developed at the federal level.

The legal reasons are there is no unified conceptual framework related to digitalisation. E.g., the terms used include expressions such as "digital technologies", "information and communication technologies", "electronic technologies", etc., which is not quite correct.

Issues of a similar nature fall within the scope of different legal acts. There is no uniform and consistent system of concepts and categories describing this most important issue; nor is there a structure and hierarchy in legal regulation. The basic regulatory legal act in the field is Federal Law No. 149-FZ of 27 July 2006 "On Information, Information Technologies, and

Information Protection."[3] Its content should be taken into account in further work in this area. Legal regulation in Russia is highly differentiated: general provisions are defined in the National Programme "Digital Economy of the Russian Federation"[4], the Strategy for the Development of Information Society in the Russian Federation for the years 2017-2030,[5] and many other programmes, strategic documents, local regulations and regulatory legal acts.

E.g., in the area of justice, digital services have been introduced in a stepwise manner. In 2013[6], Article 155.1 "Participation in a court session through the use of video-conferencing systems" was introduced into the Russian Federation Code of Civil Procedure. A similar provision is contained in Article 153.1 of the Russian Federation Arbitration Procedure Code; the article was enacted in 2010[7]. The Russian Federation Code of Administrative Proceedings contains a similar norm in its Article 142. These provisions are further elaborated in Clause 1.5 of the Regulations on the Organisation of Video-Conferencing in Federal Courts of General Jurisdiction approved by Order No. 401 of the Judicial Department of the Russian Federation Supreme Court of 28 December 2015. In the arbitration court system, they are elaborated in the ruling of the Plenum of the Supreme Arbitration Court of 25 December 2013 No. 100 (as amended 11 July 2014) "On Approval of the Instruction on Case Management in Arbitration Courts of the Russian Federation (first, appellate and cassation instances).[8]" The legal basis for the development of e-justice elements in Russia was established in the period of 2010–2013. However, due to the lack of technical equipment and sufficient funding for its development, the process remained uncompleted.

---

[3] Collection of Laws of the Russian Federation No. 31 (part 1). 2006. July 31. P. 3448.

[4] Approved by the Presidium of the Presidential Council for Strategic Development and National Projects, Minutes No. 7 of 04 June 2019). // Consultant Plus Legal Information System.

[5] Presidential Decree No. 203 of 09 May 2017 on the Strategy for the Development of the Information Society in the Russian Federation for 2017–2030 // Collection of Laws of the Russian Federation No. 20. 2017. May 15. P. 2901.

[6] Federal Law of 26 April 2013 No. 66-FZ "On Amendments to RF Civil Procedures Code." Rossyiskaya Gazeta, 2013, 30 April.

[7] Federal Law of 27 July 2010 No. 228-FZ (as amended on 28 June 2014) "On Amendments to RF Civil Procedures Code." Rossyiskaya Gazeta. 2010, 2 August.

[8] Ruling of the Plenum of the Supreme Arbitration Court of 25 December 2013 No. 100 (as amended on 11 July 2014) "On Approval of the Instruction on Case Management in Arbitration Courts of the Russian Federation (first, appellate and cassation instances)" // Consultant Plus.

Further digitalisation of the justice system will be linked to the implementation of the federal target programme "Development of the Judicial System of Russia for 2013-2020."[9] The Concept of Computerization of the Supreme Court of the Russian Federation[10] regulating specifics of the development of digital technologies in the justice is already in force. To implement the above Programme, Order of the Judicial Department under the Supreme Court of the Russian Federation of 17 February 2017 No. 25 "On Approval of the Instruction on Case Management in the Judicial Department of the Supreme Court"[11] was issued to regulate a number of basic concepts of e-justice. Also, Order of the same Judicial Department No. 168 of 11 September 2017 "On Approval of the Procedure for Filing Documents to Justices of the Peace in Electronic Form Including in the Form of an Electronic Document"[12] was issued to regulate the peculiarities of filing documents of claim via the Internet.

On 27 December 2016 order of the Judicial Department of the Supreme Court No. 251 "On Approval of the Procedure for Filing Documents to Federal General Jurisdiction Courts in Electronic Form Including in the Form of an Electronic Document"[13] was issued that regulates the peculiarities of electronic justice in RF general jurisdiction courts.

In 2019, the "Concept of Information Policy of the Judiciary for 2020-2030" was approved[14]. A document of strategic informational value, it aims to develop and introduce information technology into the judicial system.

The digitalisation of justice is described in greater detail in the "Concept of Computerisation of the Supreme Court"[15], but this document is limited in scope: it applies only to the Supreme Court of Russia.

Pursuant to Federal Law No. 440-FZ of 30.12.2021 "On Amendments to Certain Legislative Acts of the Russian Federation" (entered into force 1

[9] Government Decree No. 1406 of 27 December 2012 No. 1406 (as amended 03 October 2018) "On the Federal Target Programme "Development of the Judicial System of Russia for 2013-2020."// Consultant Plus.

[10] Approved by Order of the Supreme Court of the Russian Federation of 10 December 2015 No. 67-P // Consultant Plus.

[11] Consultant Plus.

[12] Judicial Acts Bulletin, No. 10, 2017, October.

[13] Judicial Acts Bulletin, No. 2, 2017, February.

[14] Approved by the Council of Judges of the Russian Federation on 5 December 2019 (document is not published) // Consultant Plus.

[15] Approved by Order of the Chairman of the Supreme Court No. 9-P of 15 February 2021 (document is not published) // Consultant Plus.

January 2022), spot amendments and additions were made to the Code of Civil Procedure, Code of Arbitration Procedure, and Code of Administrative Procedure on the use of electronic documents in court proceedings, and on the possibility of remote participation in court hearings through video-conferencing.

Thus, the evolution of information and communication technologies has led to the formation of the "e-justice model", which is a fundamentally different way of justice.

The "Concept for the Development of Machine-Readable Law Technologies" of 2021[16] is also of interest with regard to the development of "machine-readable law technologies in court proceedings and electronic document management mechanisms used in court proceedings."

At the same time, there is still no legal act regulating the basics and the peculiarities of digitalisation of justice in the Russian Federation.

In practice, however, we can already speak about a trend to compel interested persons to submit applications "in electronic form only"[17] as there have been many such cases[18].

E.g., in case No. A43-17925/2015, the interested party submitted a petition to the court through the electronic filing system to authorise participation in the court session by video-conference, and, if such participation was not technically possible, to postpone consideration of the case. The court ignored the above petition and considered the claim in the applicant's absence, thereby violating the principles of access to justice, legal equality, equality of rights and adversarial proceedings enshrined in the procedural legislation of the Russian Federation[19].

---

[16] Approved by the Government Commission on Digital Development, Use of Information Technologies for Improving the Quality of Life and Business Environment, Minutes No. 31. 15 September 2021 (document is not published) // Consultant Plus.

[17] Appellate ruling of the Appellate Collegium of the RF Supreme Court No. APL19-262 of 30 July 2019 // Consultant Plus.

[18] See: Decision of the RF Supreme Court No. ACPI19-79 of 23 April 2019 // Consultant Plus Legal Information System; Appellate ruling of the Appellate Collegium of the RF Supreme Court No. APL19-121 of 16 May 2019; Decision of the RF Supreme Court of No. ACPI18-1290 07 February 2019 // Consultant Plus.

[19] Ruling of the Arbitration Court of the Volgo-Vyatsky District No. F01-5281/2016 of 26 December 2016 in case No. A43-17925/2015 // Consultant Plus.

2. Artificial Intelligence in Court is Not a "Sci-Fi Future" but the Current Reality

Only a few years ago, the legal community actively discussed the introduction of certain elements of electronic (digital) justice into the national system of justice. Less than five years later, we are observing a new, more advanced phase of the introduction of digital algorithms into the national justice system and public administration. The sci-fi future has turned out to be a lot closer than we thought. At the same time, are things as straightforward as we would like them to be? We don't think so. The reason is that the widespread introduction of artificial intelligence into public life, including everyday life, will lead (and in some cases has already led) to changes in all its spheres.

Many questions still need to be answered. E.g., in national legal regulation AI is defined as "A set of technical solutions that allow imitating human cognitive functions (including search for solutions without a predetermined algorithm) and obtaining results at least comparable to or exceeding the results of human intellectual activity when performing specific tasks. The set of technical solutions includes information and communication infrastructure, software (that, among other tools, uses machine learning methods), and processes and services for data processing and solution search."

The concept was regulated in 2019 by the Presidential Decree "On the development of artificial intelligence in the Russian Federation." The Decree has approved the National Strategy for the Development of Artificial Intelligence until 2030,[20] which outlines further development in this area. This document, among other things, gives a definition and describes the tasks and methods of artificial intelligence; the criteria for project selection were approved in Order of the Ministry of Economic Development No. 392 of 29 June 2021 "On Approval of the Criteria for Determining Whether Projects Belong to Projects in the Sphere of Artificial Intelligence."[21] Chapter IV "Intelligent Decision Support Systems," which defines the spheres of interaction between social life and artificial intelligence, is of

[20] Decree of the President of the Russian Federation No. 490 of 10 October 2019 "On the Development of Artificial Intelligence in the Russian Federation" (together with the "National Strategy for the Development of Artificial Intelligence until 2030") // Collection of Laws of the Russian Federation No. 41. 2019. October 14. P. 5700.

[21] Available at: http://pravo.gov.ru (accessed: 29.07.2021)

interest. Item 43 "Decision development on the basis of open data sources and unstructured information, including for use in intelligent decision support systems for solving strategic issues and (or) adaptive dynamic control of complex objects" seems to us the most interesting in the context under review[22]. The present-day justice system finds it important to consider information processing and "interpretation of processed data" (Para. "c" of Chapter I "General Provisions" of the "Strategy for the Development of Artificial Intelligence" and Para 41, 43 and 46 of the "Order on Approval of the Criteria for Determining Ownership of AI Projects"), and legal scholars specialising in procedural law emphasise this. E.g., L.V. Borisova, in analysing the international experience of AI application, discusses the advantages of using AI in the professional activity of a judge [Borisova L.V., 2020].

Thus, it follows from the content of this paragraph that AI may be used in justice in decision-making by analysing publicly available and unstructured information. This raises the question, "How can a fair, legitimate, and informed decision be made if the digital algorithms used in the judicial system can be based on unverified and unreliable facts from publicly available sources?" In other words, we see that evaluations and expert data are levelled, notions are substituted, and the meaning of "high skills" and "professionalism" in a particular field is devalued—because AI used in various spheres of public life and public administration, one way or another, will be capable of performing analysis according to the parameters set by the developers.

The arguments a digital algorithm is devoid of feelings and emotions, is not subject to mood swings, and thus can make a weighted, objective and informed decision are questionable. The reason for this is objectivity, as a positive criterion of artificial intelligence, is a product of highly intellectual activities of a professional, or, in some cases, a group of professionals (developers) with certain personal convictions. And they can arbitrarily incorporate these convictions into the algorithm they develop. Any information products and digital products function according to strictly defined parameters and algorithms formed and set by customers and developers. This includes the parameters that AI should use to self-learn and the data it analyses and predicts. I.e., there will be elements of subjective

[22] Order of the Ministry of Economic Development of the Russian Federation No. 392 of 29 June 2021 "On Approval of the Criteria for Determining Whether Projects Belong to Projects in the Sphere of Artificial Intelligence." Registered in the Ministry of Justice of Russia on 28 July 2021 under No. 64430 // Consultant Plus.

evaluation in the numerical algorithm one way or another [Broussard M., 2020]; [Tsvetkov Yu. A., 2021][23].

As the theme of implementing AI in public administration is getting more and more popular, this raises a range of questions that modern society needs to address. First, is the quality level of the AI programmes that are being developed acceptable for making law-forming decisions? Second, have interdisciplinary programmes been developed to train specialists in AI and other areas of social life? Third, are both public authorities at all levels of government and stakeholders sufficiently equipped technically and technologically? There is no unambiguous answer to these questions, as modern society is fragmented and differentiated. It should also be noted that some districts and regions do not have proper and stable access to the Internet and that there is an uneven level of interest in the use of technical means in the Russian Federation[24].

However, what we are currently witnessing is just the initial adjustment of the national society and the technification of state administration, including the judiciary.

A substantial number of research studies have been conducted on the issue of computerisation, technification and digitalisation of social relations and all spheres of state regulation (where justice and the judiciary are no exception). A lot of authors are convinced technification and digitalisation will improve many processes, including the administration of justice. But the things are not that simple. The reason for this is not only that the information technologies that are being developed differ for certain social groups in terms of quality, accessibility and affordability, but also possible technological (production) shortcomings. This raises the question: is it possible to entitle AI to pass rulings on human fates in the administration of justice? I would venture to suggest that, for a number of reasons, this is extremely premature at this point in time.

In addressing this topic, it is necessary to consider the digitalisation of justice from the point of view of options that facilitate the administration

[23] The AI used in the US justice system to make parole decisions is a vivid illustration. This system predicted propensity for repeated offences twice as often for African Americans as for other individuals. Hence, this bias was embedded in the criteria that formed this algorithm. So there is a predisposition to make errors in data sampling.

[24] The Market in Russia and the CIS. Tadviser.ru, 2024, 20 June. Available at: https://www.tadviser.ru/index.php/:Интернет-доступ_(рынок_России)?ysclid=lnk28leuke21107550 (accessed: 24 June 2024)

of justice within the time limits established by law, to study the problems and outlooks for the use of information technology in justice, look at the execution of judicial acts and the judicial system as a whole, rather than as separate elements of one system [Tikhomirov Yu. A., Belyakova A.V., 2023]. It includes the need to research the promotion of AI in public administration from a predictive point of view, not from an idealistic one. E.g., doctrine studies the transformation of the economy in the context of global digitalisation [Kucherov I.I., Sinitsyn S.A., 2022] and in other legal relationships [Pashentsev D.A., 2022]; [Tereshenko L.K.,2023]; [Golovanova N.A., Gravina A.A., 2019]. The collective monograph edited by Professor Yu .A. Tikhomirov is a predictive research in this area [Tikhomirov Yu. A., 2019]. It tells about the main processes of robotization of social and economic relations from the point of view of transformation of legal relations.

The theme is also highly popular in procedural legal science. E.g., the team of authors under the guidance of Professor V.V. Yarkov studied the issues of civil and administrative proceedings, including the influence of IT on modern proceedings [Yarkov V.V. et al., 2021]. Representatives of the modern procedural school at the O.E. Kutafin University have also contributed to the development of this area. A team of authors led by E.G. Streltsova prepared a book on the possibilities of using digital technologies in civil and administrative proceedings [Streltsova E.G. et al., 2022].

Yu.A. Tsvetkov has written a very informative and relevant paper. It offers an analytical forecast of AI development in national justice, tells about the peculiarities of judicial activity in the modern information and communication society, and describes the issues of correlation between technical means and their application in judicial activity. The author of the present study shares the scholar's view that "justice is "human, all too human"" [Tsvetkov Yu. A., 2021]. In this regard, it is useful to draw attention to a number of key aspects in the use of AI in the judiciary. The point is that, despite a fair number of publications on this issue, there is still a need for research from a different angle, namely, in the context of the correlation of the content of jurisprudence, jurisprudence, justice, and artificial intelligence.

3. Artificial Intelligence in the Judiciary: Justice without a Face?

To answer the question whether AI can administer justice, we must refer to the essence of justice and clarify what exactly the court does when

interested persons go to law. According to conventional definitions, justice is interpreted as "the legally regulated activity of the court (at all levels and instances) to consider and resolve criminal and civil cases on the merits" [Ryzhakov A.P., 2015].

In particular, the views expressed in legal science that some of the functions should be transferred to a "robot judge" [Kovalenko K.E. et al., 2020: 171] are extremely controversial for a number of reasons.

The judiciary constitutes one of the three branches of state power. This implements the principle of separation of powers guaranteed in Article 10 of the RF Constitution. In pursuance of Article 118 of the Constitution, justice is administered only by the court: a particular judge performs legally established activities which involve consideration and resolution of cases (in the narrow sense) referred to as legal proceedings. Thus, justice is a special jurisdictional activity aimed at protecting the infringed rights, freedoms and legitimate interests of citizens. The special status of the judiciary consists in the fact that only persons with higher legal education are allowed to perform this professional activity; such persons must also meet other requirements established by federal law. In other words, to qualify for work in this area the person must meet stringent criteria, and a professional degree is the main criterion.

It is worth noting the work of a judge is based on knowledge of jurisprudence (in the Soviet period the term "legal science" was predominantly used)[25]. In addition, there is the moral and ethical significance of law and justice, which is explored by philosophy and sociology of law. Following ideas of the German philosopher of law Gustav Radbruch [Radbruch G., 2004], it is admissible to conclude "law is the pursuit of order, and justice is designed to ensure this order". In view of the above, to summarise, it is of use to raise the question of whether a robot judge can carry out one of the forms of state activity, namely justice? Also, can it search for objective truth and justice when considering and resolving a particular case on the merits? To feel and understand what is happening in the courtroom means to show empathy. Knowledge of the law, judicial practice, and other knowledge and skills are not enough to fully carry out professional activities; it is necessary to feel and understand, to predict and analyse details, to see and hear everything that is happening in its entirety.

[25] Jurisprudence (legal studies) is the science of law that includes body of practical knowledge of current legislation and judicial practice, in the narrow sense (The Great Soviet Encyclopaedia in 65 vols. Vol. 46. Moscow, 1940. P. 656.

There has been a devaluation of the professional and creative activity of lawyers (that includes all members of the legal profession). The activity of a lawyer consists, first of all, in interpreting the law, clarifying its meaning and content by specifying those concepts that are expressed in verbal form in the regulatory legal acts. Interpretation is the process of knowing the law as the law is formulated as a general abstract rule, as a behaviour. Its content is revealed through specific features and provisions that enable to know the meaning of the law and to apply it in a particular case, namely through factual circumstances. The fact is that the norm of law has a general character and covers a larger range of relations; at the same time is indirectly detailed by other norms of law, thereby formulating a system regulation of particular social relations [Bratus S.N., 1975].

Since the national judicial system is the only "available" way for the majority of interested parties to restore the violated rights, freedoms and legitimate interests, we deem it necessary to look at how fairness in decision-making and establishing of objective (judicial) truth correlate in a case when AI is used in the judicial system. Objective (judicial) truth in a case is of great importance in the present conditions of society's development because professional use of AI and digital services allows not only to draft any document, but also to conceal the true psycho-emotional attitude of the participants of the judicial process on a particular issue when a case is considered through online meetings. In this context, the role of the judge's discretion increases because the court's leadership in the judicial process must be strengthened in order to establish the truth of the case. Even the most state-of-the-art and efficient software or digital algorithm would not be able to fully establish the sufficiency and reliability of the evidence presented, identify cause-and-effect relationships, or determine the moral and ethical attitude of the parties to the case or to a particular question arising in the course of the trial.

Just like other digital services, AI functions according to the parameters set by the developers, so the question arises: is it possible at the stage of development of this software to predict the development and change of social relations, which, in turn, will be realised in a particular sphere of legal relations, and will subsequently influence the resolution of disputes in court? We expect not only the risks that the provided evidence base can be distorted or consciousness manipulated, but also that a new layer of litigation can arise, as interested parties will be forced to apply to the judicial authorities in order to protect their infringed rights. As an example, we can cite the

creation and dissemination of false and damaging information about the life and personality of certain citizens, and the creation of a negative image both online and offline through AI and other digital services and products [Kapitonova E.A., 2024]; [Sviridova E.A., 2024]).

Justice is one of the most common concepts used in the field of law, judiciary, and jurisprudence. At the same time, it is also in the plane of moral and philosophical judgements and is a starting point in the deliberation on the correlation between AI and justice, since national legislation defines this category, directly or indirectly, in codified legislative acts. Justice is an evaluative category, and it correlates with the judge's internal convictions (judicial discretion) in passing a judgement. The author would like to emphasise that the ubiquitous dominance of AI in the professional activities of legal specialists, including judges, may lead or has already led to the erosion of fundamental human values. Neural networks[26], that are at the basis of any AI, process queries and create certain selections; this shapes perceptions and, as a consequence, professional convictions on a particular issue. It is hard to believe it is possible to eliminate the use of AI. Therefore, we should note that such a legal phenomenon as technical (information) abuse may arise, which will provoke (and in some cases has already contributed to) the emergence of lawsuits for debt collection from individuals or legal entities, which will also subsequently lead to additional disputes about such payments. In this connection, the leadership of courts needs to be strengthened, as information systems and digital algorithms (products) cannot currently be made perfect.

Judicial discretion is exercised only in cases where there is no direct legal regulation on an issue, no uniform judicial practice on the category of cases in question, and no clarifications from higher courts. In such cases, the judge will have to exercise his or her professional, practical and life experience in resolving a particular dispute, and this will be the judge's discretion.

The most complete explanation of the judicial discretion concept is given in one of Professor V.V. Momotov's papers in relation to the consideration of cases arising in the field of digitalisation of substantive relations: "Using a variety of forms of interpretation of law and his or her judicial expertise, the judge creates a specific legal regulation for the litigants. We regard this

[26] Neural networks are computing systems or machines designed to simulate the analytical activities of the human brain. Neural networks belong to the area of artificial intelligence and are used for recognising hidden patterns in raw data, for grouping and classification, and for solving problems in the field of AI, machine and deep learning.

as already a complex fusion of regulatory, factual and moral judgements of the judge about the outcome of the dispute" [Momotov V.V., 2023].

Electronic document management (where the original documents are generated electronically and signed with an electronic signature)[27] has become ubiquitous. This in turn forms the ICT system for the administration of justice. On the one hand, as a result of the introduction of digital products and AI in the modern justice system, the automation of the judicial process simplifies the professional life of judges, but on the other hand, organisational and technical issues (e.g., the development of machine-readable documents) and the issues related to the protection of the rights, freedoms and legitimate interests of interested parties have not been fully resolved. (E.g., the issue of how abuse of the law by an unscrupulous participant in the process can be prevented).

So there is a fair question: is it possible to implement judicial discretion in software and digital algorithms? In discussions of the development of AI in the administration of justice, legal scientists have repeatedly expressed views on the prospects for the development of "machine-readable law" and "robot judge", namely, the use of automated systems that allow to consider the case materials and make decisions without the involvement of the interested parties and the judge. And it is the exercise of judge's discretion and inner convictions in the context of the implementation of digital algorithms that does not receive sufficient attention in such discussions.

The judge exercises his/her inner conviction at all stages of the consideration and resolution of the merits of the case. The conviction is based on the professional knowledge and skills, legal thinking, legal consciousness, life and professional experience and moral and ethical attitudes of each judge. Here we should not deny the interrelation of legal and psychological knowledge in the judge's professional activity, which, intertwined, enable the judge to determine the objective truth of the case. Based on his or her professional and life experience, the judge can objectively assess the substance of the dispute. In doing so, the judge will be guided not only by legal knowledge, but also by knowledge in the field of sociology and psychology, as the parties in some cases tend to distort the facts and interpret them inappropriately.

Judicial discretion, in turn, is a more complex legal category: it consists in analysing the particularities and formulating conclusions in each par-

[27] Federal Law No. 63-FZ of 06 April 2011 (as amended on 19 December 2022) "On Electronic Signature." Rossyiskaya Gazeta. 2011. 8 April.

ticular case, with account for the evidence presented and the legislation in force. The judge uses internal conviction to assess the situation and the behaviour of the parties, and uses discretion to adopt and issue a judicial act, which may subsequently be reviewed by a higher instance. The judge's discretion is reflected in the reasoning and operative part of the judgement, where the judge's perception of the evidence presented and the resulting judge's inner conviction on a particular case is justified.

The judge's inner conviction, which guides him or her in considering and deciding the merits of the case, including the judgement, must be, "fair discretion based on a firm conviction of conscience" and on "considerations of all the circumstances of the case." While digital technologies make it possible to make distances shorter and overcome time zones, in our times the issues of conscience and fairness of court decisions remain no less relevant [Tikhomirov Yu. A., Belyakova A.V., 2023].

Therefore, it is necessary to revive the concept of judicial law development. It should take into account the modern reality not only from the point of view of the actual implementation of legal relationships, but also from the point of view of the need to use the predictive function of modern legal science, since the list of aspects considered is truncated. It means more research needs to be done, and other not less important aspects of the use of digital products and their implications in justice need to be addressed

The author believes one of the sections of the modern concept of judicial law should focus specifically on the use of the latest technology in the administration of justice, with due regard to the whole range of issues, since the above arguments, conclusions and reasoning need to be considered in terms of their direct or indirect interrelationship. And the development of the concept of judicial law can contribute to this.

Conclusion

The implications of introduction of AI and other new technologies in various areas of public life could be quite ambivalent, and the judiciary system is no exception here. An inconsistent, incomplete and haphazard introduction and use of individual digital products in the administration of justice can lead to fatal consequences that have cumulative and delayed effects. The slogan that AI can enable a reduction in the number of court cases is controversial. On the one hand, it's true. On the other hand, it may lead to the emergence of new categories of cases that will need to be

overcome by recourse to national jurisdictions, as the author, inter alia, has previously written.

Conservatism can be a drawback in some areas, and an advantage in others. The author believes that in this area, conservatism expressed in consistency, structure, logic, and systemic approaches, and accompanied by the use of predictive function, can help prevent falling into "digital chaos" because justice and the judicial system are particularly confronted with various kinds of "distortions" in the realisation of social relations.

Justice and the judicial system are associated with the implementation of a number of functions. One of them is government activity aimed to protect the violated rights, freedoms and legitimate interests of interested persons. In this regard, we deem it necessary to note that there is no digital algorithm that could take over the implementation of the state function of administering justice. This area of government activity is highly vulnerable because inconsistency in the implementation of digital services can lead to risks that can have fatal consequences. It is not only that digital algorithms are not capable of understanding questions of justice, objective truth, understanding and awareness of everything that is going on, forecasting, analysing, critical insight and critical legal thinking. At the moment, there is no software available to train neural networks in "three-dimensional perception." And legal science demands not only to have knowledge, skills and abilities, but also requires the ability to apply them in all areas of life, to be a whole and self-sufficient person both in personal and professional activities. In other words, it is about a holistic perception of the past, present and possible future. Only humans are capable of this, so far.

There are areas of legal field where a technical glitch can "deliver a deadly blow", and the judicial system is one of them. Consequently, the author proposes to address the conceptual aspects of the development of justice and the judicial system from the perspective of "judicial law."

Therefore, in view of all the aforesaid, it is necessary to "revive" the concept of judicial law with account for the latest trends and developments. This may help not only to bring about coordinated changes to the existing justice legislation, but also to overcome and anticipate the risks that may arise from the ubiquitous dominance of information technology in the present society.

References

1. Borisova L.V. (2020) E-justice as a Form of Judicial Defence in Russia. *Issues of Russian Law,* no. 6, pp. 105–111 (in Russ.)

2. Bratus S.N. (1975) The Legal Nature of Judicial Practice in the USSR. *Soviet State and Law,* no. 6, pp. 13–21 (in Russ.)

3. Broussard M. (2020) *Artificial Intelligence: the Limits of Possible.* Moscow: Alpina, 361 p. (in Russ.)

4. Golovanova N.A., Gravina A.A. et al. (2019) Criminal Justice in Context of Digitalization. Moscow: Kontrakt, 212 pp. (in Russ.)

5. Kapitonova E.A. (2024) Fake Images Created by Neural Network: Social and Legal Risks and Issues of Qualification. *Law*, no. 1, pp. 39–48 (in Russ.)

6. Khabrieva T.Y., Klishas A.A. (2020) Commentary to Law on Constitutional Amendment of 14 March 2020 on Improving Regulation of Issues of Organization and Functioning of Public Power. Moscow: Norma, 240 pp. (in Russ.)

7. Kovalenko K.E., Pechatnova Y.V. et al. (2020) The Robot Judge as Resolution of the Contradictions of Judicial Discretion (legal aspects). *Legal Bulletin of Dagestan State University,* no. 4, pp. 169-173 (in Russ.)

8. Kucherov I.I., Sinitsyn S.A. et al. (2022) Digital Economy: Current Areas of Legal Regulation: textbook. Moscow: Norma, 376 pp. (in Russ.)

9. Law Enforcement and Judicial Bodies of Russia (2015) N.A. Petruchio, A.S. Hamycin (eds.): a textbook. Moscow: State University of Justice, 434 pp. (in Russ.)

10. Momotov V.V. (2023) The Space of Law and the Power of Technology in the Mirror of Judicial Practice: A Contemporary View. *Russian Law Journal*, no. 2, pp. 112–123 (in Russ.)

11. Pashentsev D.A. et al. (2022) Gaps in Law in the Context of Digitalisation: a collection of papers. Moscow: Infotropik Media, 472 pp. (in Russ.)

12. Radbruch G. (2024) Philosophy of Law: textbook. Moscow: Mezhdunarodnye otnosheniya, 238 pp. (in Russ.)

13. Ryzhakov A.P. (2015) Law Enforcement Bodies: textbook. 4th ed. Moscow: Delo i Servis, 590 pp. (in Russ.)

14. Streltsova E.G. et al. (2022) Digital Technologies in Civil and Administrative Proceedings: Practice, Analysis, Prospects. Moscow: Infotropik Media, 336 pp. (in Russ.)

15. Sviridova E.A. (2024) Rules for the Use of Deem Fake Technologies in US and PRC Law: Adaptation of Foreign Experience in Legal Regulation. *Modern Law*, no. 3, pp. 119–123 (in Russ.)

16. Tereshchenko L.K. et al. (2023) Human Rights in the Information Sphere Amid Digitalisation: a guide. Moscow: Infotropik Media, 244 pp. (in Russ.)

17. Tikhomirov Yu.A. et al. (2019) Legal Concept of Robotization. Moscow: Prospekt, 240 pp. (in Russ.)

18. Tikhomirov Yu.A., Belyakova A.V. (2023) Discretion in Context of Digitalisation. *Russian Justice*, no. 6, pp. 5–16 (in Russ.)

19. Tsvetkov Yu.A. (2021) Artificial Intelligence in Justice. *Law*, no. 4, pp. 91–107 (in Russ.)

20. Yarkov V.V. et al. (2021) Issues of Civil and Administrative Proceedings. Moscow: Statut, 460 pp. (in Russ.)

21. Yurchenko A.K. (2023) Evaluating Designer's Labor Productivity in Creating a Service Object through AI Technologies. *Law and Business*, no. 1, pp. 30–32 (in Russ.)

Information about the author:

A.V. Belyakova — Candidate of Sciences (Law), Leading Researcher.

The article was submitted to editorial office 25.06.2024; approved after reviewing 15.08.2024; accepted for publication 05.09.2024.

Legal Issues in the Digital Age. 2024. Vol. 5. No. 3.
Вопросы права в цифровую эпоху. 2024. Том 5. № 3.

Research article
УДК: 343
JEL: K14
DOI:10.17323/2713-2749.2024.3.88.102

Child Neglect and Juvenile Delinquency Prevention Bodies: Priorities and Prospects in Context of Digitization

Ludmila Vladimirovna Saenko[1], Pavel Andreevich Nepomnyaschiy[2]

[1, 2] Saratov State Law Academy, 104 Chernyshevskogo Str., Saratov 410056, Russia,

[1] saenko7@yandex.ru, ORCID id: 0009-0001-7284-9252

[2] neppavel@mail.ru

Abstract

The paper explores one of the priority issues faced by the country and society — preventing child neglect and juvenile delinquency with a special focus on cooperation between bodies for prevention of the deviant behavior. The study comprises an analysis of possibilities to address the problems arising in this regulatory area through the implementation of digital tools such as automated information systems. From this lens, the authors also explore the issue of developing and introducing the modern Profilaktika automated information system. Conceptual provisions for possible use of federal information systems by bodies for prevention of child neglect and maltreatment have been developed. In terms of methodology, analysis and synthesis of statistical information and comparative law are primarily used by the authors. The provisions substantiated by the paper can be useful for development of the relevant regulatory framework.

Keywords

record-keeping of minors; child neglect; prevention; prevention bodies; automation; information system.

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

For citation: Saenko L.V., Nepomnyaschiy P.A. (2024) Child Neglect and Juvenile Delinquency Prevention Bodies: Priorities and Prospects in Context of Digitization. *Legal Issues in the Digital Age,* vol. 5, no. 3, pp. 88–102. DOI:10.17323/2713-2749.2024.3.88.102

Background

Preventing child neglect and juvenile delinquency is a policy area of public administration where the use of information technologies is of primary importance, in particular, since the law requires multiple bodies to be involved in this activity at the federal, regional and local levels, only to considerably complicate interagency cooperation. The problem could be solved by the development and introduction of a shared federal-level information system but there is no legal mechanism to use such digital tool.

The study presented purports to analyze possible ways of improving performance of the child neglect prevention bodies through the use of automated information systems as well as to explore possible use of the distributed ledger technologies and AI in such systems. It is set to research the importance of the institution of childhood in Russia's public policies; identify the main operational problems of child neglect and juvenile delinquency prevention bodies; propose ways for improving the said bodies' performance through the introduction of an automated information system; and to explore the opportunities for the use of distributed ledger technologies and AI in such information systems. With the child neglect and juvenile delinquency prevention system at its focus, authors explore automated information systems as a tool to enhance its performance.

1. Children at the heart of public policies in Russia

Future generations are pivotal for the development of society and a defining vector for any country. The extent and quality of children's ethical, physical and psychological development largely determine qualitative and quantitative indicators of the population, as well as national situation in general. Happy and safe childhood has been a national priority for countries and societies as often discussed at research events. Thus, pursuant to UN guidelines, any juvenile delinquency prevention program should be under-

pinned by youth well-being guaranteed from early childhood[1]. Meanwhile, a lack of assistance for social adaptation is likely to develop in children the stereotypes of permissiveness and illegal ways for satisfying one's demands.

Improving the situation of children and families has been a social policy priority in Russia over the last few years. Following amendments to the country's Constitution in 2020, the protection of childhood became a constitutional objective which is indicative of the national efforts to protect this institution as much as possible by putting in place specific implementation mechanisms and guarantees. Pursuant to Part 4, Article 67.1 of the Constitution, children are a major public policy priority in Russia[2], with the year of 2024 announced by the President the Year of Family[3] to mark a number of reforms in legal regulation of this important social sphere.

It is not for nothing that the national legislator has devoted so much attention to the institution of childhood. Statistical data and negative trends in this regulatory field are a cause of concern and require response from public authorities.

The indicators of child neglect have risen dramatically as a result of deteriorating living standards, parental attempts to make public institutions responsible for children's education, as well as declining prestige of the family as a social institution, growing alcohol and drug addiction and a number of other negative background developments. These factors combined are prompting a reform of the discussed regulatory area.

According to the unified interagency information and statistical system (UIISS), a total of 56,934 neglected children were identified in Russia in 2023 (3,121 fewer than over the previous year), with the indicator still believed to be high[4]. As reported by the Ministry of Interior, minors ac-

[1] UN Guidelines for the Prevention of Juvenile Delinquency (The Riyadh Principles; UN General Assembly Resolution 45/112 of 14 December 1990) // Available at: URL: https://www.un.org/ru/documents/decl_conv/conventions/juveniles_deinquency_prevention.shtml (accessed: 12.06.2024)

[2] Constitution of the Russian Federation (adopted by popular vote on 12 December 1993 as amended by popular vote of 01 July 2020). Available at: URL: http://www.pravo.gov.ru. 04.07.2020 (accessed: 20.05.2023)

[3] Presidential Decree No. 875 "On the Year of Family in Russia" of 22 November 2023 // Collected Laws of Russia, 27 November 2023. No. 48. Article 8560.

[4] Number of identified neglected and abandoned children // Unified interagency information and statistical system. Available at: URL: https://www.fedstat.ru/indicator/ 36186 (accessed: 12.06.2024)

counted for 22,340 or 3 percent of the total delinquency in 2023[5]. In a vast majority of cases, juvenile delinquency is largely caused by neglect, that is, non-existent or considerably slackened control by families or public authorities over personal development of minors.

In 2023, crimes against minors in the Saratov Region grew by 4.9 percent (from 1,665 to 1,746), including by 91.1 percent (from 856 to 1638) against infants. A total of 24 minors involved in vagrancy and beggary were identified, 14.29 percent less than in the same period previously (25 in 2021, 28 in 2022). Juvenile delinquency in the region was down by 2.2 percent (407 to 398), its specific share of total crime still at 2.6 percent as in the previous year. Meanwhile, in 2023 the Volga Federal District witnessed a 57.9 percent rise in juvenile drug-related delinquency (3.2 percent share of total crime), with overall rise across Russia at 27.8 percent (2.3 percent share of total crime)[6].

Statistical data clearly suggest that preventive focus on neglected minors is crucial for lower incidence of children's criminal and otherwise deviant behavior, as well as for their well-being.

2. Operational aspects of child neglect prevention bodies

An analysis of law enforcement practices shows that the child neglect prevention system is not fully adequate for addressing social demands and realities of the moment. Practical response to social problems should be underpinned by theoretical provisions as practices cannot develop without a normative framework.

Child neglect prevention relationships are governed in Russia by Federal Law No. 120-FZ "On the Principles of the Child Neglect and Juvenile Delinquency Prevention System" of 24 June 1999 ("FL No. 120")[7] whereby a

[5] Summary of delinquency in Russia in January–December of 2023 // Ministry of Interior site, statistics and analysis section. Available at: URL: https://media.mvd.ru/files/application/5095078 (accessed: 12.06.2024)

[6] 2023 Saratov Oblast child neglect and juvenile delinquency prevention report (annexed to Resolution No. 1/1 of 27 February 2024 of the Saratov Oblast interagency commission for juvenile affairs and protection of children's rights), p.p. 51, 61, 65 // Available at: URL: https://saratov.gov.ru/upload/iblock/8cc/vp5x8la9a1dbo07nu1w8j4s0boztar8f/Otchet-o-rabote-za-2023-god-Saratovskaya-oblast.pdf (accessed: 12.06.2024)

[7] Federal Law No. 120-FZ "On the Principles of the Child Neglect and Juvenile Delinquency Prevention System" of 24 June 1999 // Collected Laws of Russia.1999.

neglected child is defined as the one whose behavior is out of control due to a failure to perform or unduly performance of upbringing, education and/or maintenance duties by parents (legal representatives) or public officers.

It is clear from analysis of this definition the duties of education and control are to be assumed not only by parents and legal representatives but also the system of public bodies at large. Thus, pursuant to Article 4 of FL 120-FZ, the child neglect and juvenile delinquency prevention system comprises:

commissions for juvenile affairs and protection of children's rights;

social protection governance bodies;

federal, regional and local level education authorities;

adoption and guardianship authorities;

bodies for youth affairs;

health authorities;

employment services;

bodies of the Ministry of Interior;

penitentiary bodies (pre-trial detention centers, juvenile detention centers and corrective services).

Federal law thus invokes a wide range of authorities and agencies for preventive action concerning children's life.

On the one hand, the cross-cutting nature of the system and diversity of agents for preventive action should guarantee a comprehensive approach and effective prevention. Meanwhile, this vast system dealing with children at all levels of public administration from federal to local authorities cannot reverse the trend of growing child neglect.

For a majority of researchers, the reason is inadequate mechanism for cooperation between the prevention system bodies [Lugovskaya A.A., 2017: 253], a position shared by the authors. As noted by the research community, a need in interagency cooperation will arise where the agents have intersecting interests with fully or partially overlapping functional purposes [Usheva T.F., 2021: 269]. A prevention system should be systemic and comprehensive [Mironov V.S., 2020: 222]. A need to design and introduce a

No. 26. Article 3177.

single comprehensive structure for prevention and rehabilitation of deviant children/teenagers is invoked [Vasilieva A.N., 2022: 57]. With this assumption in mind, a mechanism for child neglect prevention should rely on robust interagency cooperation across the board.

In fact, federal and regional executive authorities will almost invariably delegate public child neglect prevention powers to local level bodies as provided for by Articles 19, 20 of Federal Law No. 131-FZ "On the General Organizational Principles of Local Government in Russia" of 06 October 2003[8]. This practice is widespread among public authorities in constituent territories.

The delegation of powers is undoubtedly caused by a need in direct engagement between competent agencies and the social category in question, with the best results achieved only if the relevant powers are exercised by lower level (grass root) bodies, that is, those as close as possible to the population.

However, the diverse and uncoordinated action by control agents at the municipal level clearly suggests that a way of forming a child neglect prevention system will not allow to deal optimally with the issues at this stage.

Firstly, this operating mechanism will make commissions for juvenile affairs and protection of children's rights directly dependent on funding available to the respective municipality.

Secondly, while the said commissions are required to coordinate action across the child neglect prevention system as a whole, they do not have adequate resources at their disposal to perform this function. In delegating public powers to municipalities, regions will not always designate sufficient sources of budget funds for commissions to fully implement their coordinating role. In doing so, they will at times fail to support the implementation of relevant powers, that is, allocate adequate funds to the commissions, which is an evident violation of the federal provisions for inter-budget transfers.

And thirdly, the very fact that commissions for juvenile affairs are normally local government institutions, that is, grass root public authorities, will complicate — and even exclude with regard to a number of issues — any coordinated action with higher level bodies. Researchers doubt whether the commissions will be able to ensure coordination with federal agencies in charge of education [Popova V.I., 2007: 65].

[8] SPS Consultant Plus.

This context suggests that coordination within the child neglect prevention system is plagued by a number of issues to be removed by the legislator as a matter of priority. One implication of this failure is a lack of operational cooperation and consistent action between the discussed authorities as observed in enforcement practices.

A vivid demonstration of harm from a lack of adequate engagement between child neglect prevention authorities is a situation that persisted in the Khabarovsk Region for quite a while. In November 2014, the Khabarovsk Center for Social Aid to Families and Children has received a request for aid to K. and her underage daughter who qualified for social protection [Lugovskaya A.A., 2017: 251]. The family's living conditions were dire: they lived in a house with stove heating. Out of work, K. did not have a permanent source of income, lost her dwelling and was not registered at her domicile. The Center helped her to make a document file and to find a job with a crisis management center while the family details were sent to the Khabarovsk district commission for juvenile affairs and protection of children's rights.

In December 2014, K. with the child on her hands was detained by the police in a state of heavy intoxication as evidenced by administrative offense report. In April 2015, she was fired from the crisis management center after a drunken brawl. A report sent to the police also contained the information on possible threat to life and health of a minor. From June through December 2015, K. and her daughter would repeatedly change their domicile where K. cohabitated with different persons and led a life of dissipation.

In February 2016, K. had a criminal case opened up against her for having beaten her daughter. It was only eighteen months after her asocial behavior had been noted that the pre-trial investigation found that while the family had been many times subject to police scrutiny, no preventive action was taken.

As was found by the prosecutor's office, this failure was caused by a lack of adequate cooperation within the prevention system, with the respective agencies scattered across the city and reporting to different departments, only to fail to detect the family's asocial drift at an early stage and take preventive action. Though some facts on the family were periodically reported to judiciary authorities, occasional action did not reveal a systemic focus to prevent asocial behavior. The deteriorating situation of this family resulting in adverse implications was caused by the fact that relevant information was not available to the prevention system's bodies.

This example suggests a need in partnership between public and non-public actors to prevent child neglect. There should be a robust system for professional engagement between specialists as well as fruitful application of human, financial and organizational resources for family support and effective assistance to children in hardship.

3. Digitization as a prerequisite of better performance of the child neglect prevention system

While the available studies of interagency cooperation to prevent child neglect are anything but numerous, those analyzing various aspects of information technologies to be used for this purpose are even fewer. They largely praise the benefits of e-document exchange compared to paper within a specific agency [Khlivenko L.V., 2011: 100–104]. Meanwhile, it is the overarching opportunities brought by digitization that we believe to be a factor of reform of the prevention system to ensure coordinated action.

As follows from the above examples of enforcement practices, rapid information exchange should be regarded as a priority method of dealing with the problems faced by the system.

A context for introducing information technologies into various spheres of social and personal life is currently being created everywhere across Russia. In laying down a new technological basis for operations of public authorities, the national legislator is pursuing the purpose of "applying new technologies at public authorities in Russia for better governance" as formulated in the Information Society Development Strategy[9]. As a rule, digitization of social relations relies on the introduction and use of automated information systems ("AIS").

Such applications have been created virtually in all spheres of social life across the board: judiciary (SIS Pravosudiye), public prosecutor supervision (AIS WEB-Nadzor), executive branch (SIS Gosuslugi), employment relations (AS Trud, Rabota v Rossii) etc. The main distinctive feature of these systems is that they operate at the federal level due to a need in cooperation of the entire public system to deal with a particular issue. Researchers note a need to engage IT professionals in this sector for addressing specific tasks and problems [Krasnoschechenko I.P., 2022: 74].

[9] Presidential Decree No. 203 "On the 2017-2030 Information Society Development Strategy for Russia" of 09 May 2017 // Collected Laws of Russia, 2017, Article 3659.

In our view, the established trend for digitization of public relations should be also reflected in the child neglect prevention system where some actors already have and use their own departmental information systems that allow to promptly receive and process relevant information. Thus, the guardianship system has assessed positively the benefits and convenience of intra-agency operations via automated systems, with the AIS *Opeka* allowing to accumulate and process the details of abandoned minors and their guardians (legal representatives).

However, this standalone system will accumulate only the operational information of the said agency and its structural subdivisions with regard to guardianship of minors while other bodies even in similar roles within the child neglect prevention system will be unable to upload or download relevant information. Thus, commissions for juvenile affairs currently cannot coordinate automatic engagements within the system, primarily because their operations are not duly digitized in technological terms.

The experience of regional databases on neglected children and their families is of true academic interest. While not all constituent territories are technologically capable of developing and maintaining such record-keeping systems, they have been formed in a number of regions to considerably improve the performance of prevention bodies in the respective territories. Thus, the Tumen Oblast has a regional interagency databank of families and children in need of special care[10], with the regional department of social development in charge of organization and coordination. The software complex allows a shared access to aggregate information within the prevention system for personalized record-keeping of each person/family subject to control while tracking each agency's interventions with minors and their parents. A complex of interventions (rehabilitation program) including the implementation of interagency technologies and social services is developed for each person registered in the database. The experience of developing and maintaining such comprehensive databases has been accumulated by the Vologda, Tambov, Rostov Oblast, Altai Territory, Saint Petersburg, as well as a number of other Russian regions.

Meanwhile, as has been observed in literature with good reason, "a vast majority of the regional and municipal level commissions neither use AIS

[10] Tumen Oblast Law No. 205 "On the system for prevention of child neglect and juvenile delinquency and for protection of children's rights in the Tumen Oblast" of 06 October 2000 // Tumenskiye izvestiya. 12 October 2000.

in their operations nor recognize the need in information engagement within the prevention system as priority objective" [Yusupaliev B.S., 2013: 181].

In a study conducted by the Saratov State Law Academy [Ilgova E.V., 2021: 104–113] it is also noted that the available AIS are primarily constrained by impossibility of information exchange between child neglect prevention bodies.

In addition, researchers note a lack of proper regulation of personal data protection in the relevant information systems as well as issues of compliance with the established confidentiality regime within the prevention system [Tchausskaya O.A., Kuznetsova I.O., 2020: 114].

Unfortunately, the issues of automatic data exchange between prevention agencies are yet to be addressed by federal law. The peculiarities identified in the course of this study generally support the need in and feasibility of a shared federal AIS to be developed and introduced in the area under discussion. The main purpose of a database on families with minors in need of special public care is to introduce a comprehensive approach to child neglect prevention. That system will ensure the protection of rights and legitimate interests of children and their families and will automatically generate a plan of customized protective action.

Regional law for regulation of automation, as was noted above, is currently more detailed than federal law. The regional experience of such systems as well as positive and negative aspects of such collaborative practices should be carefully studied.

The introduction of a shared federal AIS for coordinated action to prevent child neglect will obviously require a detailed legal framework for regulation of rights and duties of the parties to information exchange.

It is pleasing that legislative authorities take the child neglect problem to heart by proposing a number of draft laws to develop a federal database of neglected children and their families. For example, a draft proposed by the interagency working group for draft federal law "On Protecting Minors' Rights and Preventing Abusive Behavior and Misconduct" envisages a state information system for information support of protective and preventive action in Part 1, Article 33. Under the 2024 work plan of the Ministry of Education the draft law should be refined in the 4th quarter of 2024[11].

[11] 2024 work plan of the Ministry of Education of Russia (approved on 9 April 2024, No. SK-9/02int) // SPS Garant.

It has a sense to discuss the benefits of such system in detail.

Coordinated action within the child neglect prevention system will be ensured. In the previous section, we discussed in detail the operational problems of the competent bodies largely caused by a lack of shared information platform. An AIS will support a concerted action for prevention of child neglect.

Children's rights and legitimate interests will be protected. In the first place, the system will enable the implementation of major constitutional guarantees: protection of maternity, paternity and family, rights to education, health, employment, social security, leisure etc.

The system will enable ongoing control over socially disadvantaged families and children, a benefit of special importance in the context of permanent migration of this population category. Thus, where the individuals registered with regional AIS migrate elsewhere in Russia, they are likely to fall out of sight of executive bodies. Meanwhile, a shared federal database will have the details of all persons under control even if they change their domicile, with no effect on the quality of preventive action. Advised of the interventions performed in respect of neglected children at their previous domicile, the prevention bodies will be able to carry on as due.

It makes sense to discuss a potential shared AIS based on the distributed ledger technology (blockchain) to largely enhance the system's degree of security and prevent unauthorized access to restricted data. Moreover, the distributed ledger technology has been considered in literature for a number of years as an efficient way to expedite and improve the quality of administrative decision-making and reduce budget expenditures [Fialkovskaya I.D., 2020: 216]. In our view, it would be reasonable to introduce a closed (centralized) form of blockchain where there is a "super-user" and at the same time the information system's operator vested with enhanced administrator rights.

Adequately trained modern AI technologies are able to automatically analyze web information to identify elements of offenses by or in respect of minors, as well as facts of child neglect and problems in individual families. In cross-system collaboration, such algorithms can promptly retrieve and analyze information from different data systems. As a result of data comparison, a neural network can propose changes to methodologies and fresh ideas for different public awareness events. In our view and also in line with public digitization policies for widespread introduction of AI technologies, the initiators of AIS to be developed should consider possible use of neural networks as part of the system's software.

For this legislative initiative to take its place in the regulatory system, it should be obviously supported by Russia's supreme legislative authorities — chambers of the Federal Assembly. Meanwhile, as explicitly envisaged by Article 33, the drafters go beyond the adoption of a federal law. As part of the initiative, it is also proposed to issue a Government Resolution containing "a list of details to be uploaded as well as the information system's organization and maintenance procedure". In the context of this study, we have made proposals on the contents of this bylaw.

Thus, the list of details should include:

information used by prevention bodies for interventions to address minors and their families in accordance with sectoral and departmental regulations;

nformation used for personalized record-keeping of minors;

nformation to be reflected in statistical reports.

The procedure for the system's organization and maintenance is such that before any intervention targeting minors and their families, a prevention body should seek consent for processing personal data to be uploaded to the AIS within one business day. Then the body for ongoing control of the neglected child will draft and upload to the AIS a prevention plan and an individual rehabilitation/adaptation program within three business days.

The adaptation plan for the neglected child and his family at risk should specify the bodies and institutions responsible for interventions and the relevant dates. The AIS should promptly reflect changes to the rehabilitation program, analysis of the progress of prevention plan, information on specific interventions being implemented, as well as decisions to de-register a person.

The authors share the view established in the doctrine that it makes sense to adopt a federal law for regulation of the relations involved in AIS organization, operation and upgrading [Smagina T.A., 2020: 112].

Our list of details to be uploaded to the AIS as well as the procedure and specifics of record-keeping within the system can be helpful in drafting the relevant Government Resolution and other regulations.

The Profilaktika shared state automated information system (AIS Profilaktika) is developed by the autonomous no-profit Center for the Study and Network Monitoring of Youth Environment, an accredited IT organi-

zation, as part of the National Education Project and the Federal Patriotism Promotion Project[12]. The Profilaktika is currently at the restricted beta testing stage in a number of regions and has already shown high potential for positive outcomes such as lower software development costs for regions, faster operational data exchange and decision-making, as well as ongoing performance monitoring of interventions to prevent child neglect and juvenile delinquency.

The most prominent of that AIS declared objectives include a shared methodological framework for customized interventions by competent authorities and institutions, automatic performance monitoring and reporting, as well as a shared secure data environment to accumulate, store and retrieve the relevant information.

An analysis of the publicly available AIS Profilaktika user manual (version 1.0 of 2021)[13] has shown that the information and user interface will be organized into five main blocks: Minors; Parents/legal representatives; Families; Prevention system; and Archive. The AIS will provide access to the methodological and regulatory framework as well as restricted access to information and reference systems. Users are supposed to access the system with a login and a password which we believe to be a drawback. As the system will accumulate law-protected confidential information on minors and their families, it makes sense to introduce two-factor authentication with enhanced qualified digital signature followed by a code from SMS sent to the user's confirmed telephone number.

Three-factor authentication should be required for administrators and moderators, with biometric data such as finger and voice prints to be added, otherwise there will be a high risk of compromised user passwords and information leakage. User workstations should be subject to a high degree of protection certified by authorized FSB or FSTEC specialists.

---

[12] Available at: URL: https://www.cism-ms.ru/natsproecty/536/?ysclid=lxbs3j613z706320937 (accessed: 12.06.2024)

[13] AIS Profilaktika, automated information system of the commission for juvenile affairs and protection of children's rights. User manual, version 1.0. 2021 // Available at: URL: https://kdn.avo.ru/documents/4987981/0/%D0%90%D0%98%D0%A1+%D0%9F%D1%80%D0%BE%D1%84%D0%B8%D0%BB%D0%B0%D0%BA%D1%82%D0%B8%D0%BA%D0%B0%28%D1%80%D1%83%D0%BA%D0%BE%D0%B2%D0%BE%D0%B4%D1%81%D1%82%D0%B2%D0%BE%29+%281%29.pdf/391e064d-a4d7-fb9d-20d0-2affdbab1397?t=1682321460433&ysclid=lxbu1kasmp574958400 (accessed: 12.06.2024)

The AIS developers have made public their position and the system's conceptual design at different research events and publications [Burlakov M.E., 2023: 5–9]. With the Center's staff actively conducting training workshops since April 2023 for regional and municipal bodies/institutions to use the system for better interagency collaboration, its deployment across Russia is forthcoming, only to add urgency to the problem of developing a regulatory framework for AIS operations.

Conclusion

Thus, the importance of developing and introducing a shared federal automated information system as electronic platform for interagency collaboration within the child neglect prevention system cannot be overestimated in the current context. In view of the system's bulky design, a shared information platform to exchange, collect, analyze and systematize data is the only feasible option for concerted action.

Once introduced, the AIS Profilaktika is expected to have a positive impact across the child neglect prevention system, with timely IT research and development helping to promptly remove operational errors and upgrade the system's capabilities.

Additional studies may be focused on the issue of observance of rights and legitimate interests of neglected minors registered for record-keeping with automated information systems.

References

1. Burlakov M.E. et al. (2023) Digitizing the child neglect and juvenile delinquency prevention system in Russia. *Society*, *Economics*, *Management*, vol. 8, no. 3, pp. 5–9 (in Russ.) DOI: 10.47475/2618-9852-2023-8-3-5-9.

2. Fialkovskaya I.D. (2020) Prospects of using blockchain for public administration. *Bulletin of Nizhnyi Novgorod State University*, no. 2, pp. 213–217 (in Russ.)

3. Ilgova E.V., Zaikova S.N. (2021) Functionalities of automated information system for child neglect and juvenile delinquency prevention in Russia. *Bulletin* of *Saratov Law Academy*, no. 5, pp. 104–113 (in Russ.) DOI: 10.24412/2227-7315-2021-5-104-113.

4. Khlivenko L.V. et al. (2011) Automating document exchange at guardianship bodies. *Bulletin of Voronezh State University,* no. 1, pp. 100–104 (in Russ.)

5. Krasnoschechenko I.P. (2022) Social adaptation of minors in Russia: transformation, risks, threat reduction strategies. *Applied Legal Psychology*, no. 2, pp. 67–76 (in Russ.) DOI: 10.33463/2072-8336.2022.2(59). 067-076.

6. Lugovskaya A.A. et al (2017) The interagency collaboration in the child neglect and juvenile delinquency prevention system. *Proceedings of Tomsk State University*, no. 3, pp. 249–254 (in Russ.)

7. Mironov V.S. (2020) Preventing child neglect and juvenile delinquency in the context of digitization. In: Sustainable development of the digital economy, industries and innovative systems. Papers of a research conference. Saint Petersburg: Politekh-Press, pp. 220–222 (in Russ.) DOI: 10.18720/IEP/2020.7/65.

8. Popova V.I., Gulin K.A. (2007) Room for improving child neglect prevention system in the region. *Economic and Social Changes in Region: Facts, Trends, Prognosis,* no. 5, pp. 61–71 (in Russ.)

9. Saenko L.V. (2023) Protecting children via family law from perspective of traditional values. In: The role of jurisprudence and social sciences in the development of modern society: papers of a research conference. Vladivostok: Far Eastern Federal University, pp. 311–314. DOI: https://doi.org/10.24866/7444-5493-7.

10. Smagina T.A. et al. (2020) Upgrading regulatory mechanism of data exchange in the child neglect and juvenile delinquency prevention system: a socio-legal study. Saratov: Law Academy, 236 p. (in Russ.)

11. Tchausskaya O.A., Kuznetsova I.O. (2020) Pressing IT development issues in the child neglect and juvenile delinquency prevention system. *Politics of Law and Life*, no. 4, pp. 108–117 (in Russ.)

12. Usheva T.F. (2021) Implementing training course “Interagency collaboration between specialists in education and social sector” on the basis of reflective approach. In: Interagency approach to supporting persons in hardship: theory and best practices. Papers of a research conference. Irkutsk: University, pp. 267–273 (in Russ.)

13. Vasilieva A.N., Portnyagina A.Yu. (2022) Organizing juvenile delinquency prevention at education departments. *Modern Pedagogical Education*, no. 4, pp. 54–57 (in Russ.)

14. Yusupaliev B.S. (2013) Information and reference system development exemplified by the database of the commission for juvenile affairs. *Polzunov almanakh*, no. 1, pp. 181–182 (in Russ.)

Information about the authors:

L.V. Saenko — Candidate of Sciences (Law), Associate Professor.
P.A. Nepomnyaschiy — Lecturer.

The article was submitted to editorial office 20.06.2024; approved after reviewing 07.08.2024; accepted for publication 05.09.2024.

Legal Issues in the Digital Age. 2024. Vol. 5. No. 3.
Вопросы права в цифровую эпоху. 2024. Том 5. № 3.

International Law And Cybersecurity

Research article
УДК: 341
JEL: K33
DOI:10.17323/2713-2749.2024.3.103.128

Collective Countermeasures in Response to Cyber Operations under International Law

Ekaterina Aleksandrovna Martynova
Center for Technology and Society, Fundação Getulio Vargas (FGV) Law School, 190 Praia de Botafogo, Rio de Janeiro, CEP: 22250-900, Brazil,
eamartynova@hse.ru, ORCID id: 0000-0002-8995-4462

Abstract

The paper examines the application of collective countermeasures — i.e., measures taken by non-injured states — as a means of cooperative non-institutionalized response to malicious cyber-enabled activities undertaken or controlled by a state. Particularly, the paper investigates: the right of the state not injured by a cyber operation to take countermeasures against the perpetrating state under current international law; and state positions towards collective countermeasures and possible grounds for the development of a more supportive attitude within states to this form of collective reaction. General research and special legal methods, as well as game theory, are employed to test the hypothesis the concept of collective countermeasures has been gaining nascent and fragmented support by states in terms of its applicability in the context of cyber operations. The author concludes this emerging trend reflects the general tendency of states to join forces to halt malicious activities in cyberspace and impose political and economic costs upon the perpetrators. This allows one to assume that collective countermeasures in response to cyber operations might become an expectable means of reaction by 'like-minded' states. Their legitimation might, therefore, be determined not only (or not so much) by the development of international law due to the practical difficulty in harmonizing positions among states on this issue at the current stage, but rather as a part of the general political trend of uniting the efforts of states to bring wrongdoers in cyberspace to responsibility.

Keywords

cyberspace; cyber operations; state responsibility; countermeasures; Tallinn Manual 2.0; game theory.

For citation: Martynova E.A. (2024) Collective Countermeasures in Response to Cyber Operations Under International Law. *Legal Issues in the Digital Age,* vol. 5, no. 3, pp. 103–128. DOI:10.17323/2713-2749.2024.3.103.128

Introduction

The article examines whether a state, or a group of states, not injured by malicious cyber activities can employ countermeasures in assistance to the victim-state or independently of the latter. The term 'collective countermeasures' in the title of the paper, as well as the alternative term 'third-party countermeasures', are not defined in any legal source, including the most authoritative document on states responsibility — Articles on Responsibility of States for Internationally Wrongful Acts ('ARSIWA').[1] As will be described, the application of countermeasures by a non-injured state has been discussed by the UN International Law Commission (ILC) and the Sixth Committee of the UN General Assembly within the development of ARSIWA, as well as in legal scholarship, and turns out to be a truly divisive issue. In certain cases the distinction is made between 'third-party countermeasures' as measures taken by a non-injured state in the interest of the injured state, sometimes on behalf of or at the request of the latter, and 'collective countermeasures' as a means of congregate reaction to enforce a communitarian norm [Delerue F., 2020: 454].

The concept of third-party countermeasures under general (not cyber-specific) international law was examined in detail by Martin Dawidowicz in his seminal *Third-Party Countermeasures in International Law* [Dawidowicz M., 2017]. The academic discussion of collective responses to hostile cyber-enabled actions has intensified against the backdrop of increasing 'naming and shaming' of particular states in the systematic commission of wrongdoings in cyberspace [Finnemore M., Hollis D.B., 2020]. The body of scholarship on countermeasures presents a relative consensus that international law does not entitle a state, other than the victim-state,

[1] UNGA Res. 56/83. Articles on Responsibility of States for Internationally Wrongful Acts. 12 December 2001. UN Doc. A/RES/56/83.

to take countermeasures in response to a cyber operation [Tsagourias N., 2015]; [Henriksen A., 2015]; [Corn G., Jensen E.T., 2018]. At the same time, publications by European and American authors in recent years have increasingly expressed cautious support for the possibility of using collective countermeasures in cyberspace. In particular, there are arguments that international law has been evolving since ARSIWA to permit collective countermeasures in the cases when collective obligations are violated [Roguski P., 2020: 36]; that limited acceptability of collective countermeasures is justified by political reasons, such as the technological impossibility for some states to respond to a cyber-attack without the help of more cyber advanced allies [Haataja S., 2020: 49]; and — more generally — that international law does not contain a clear prohibition on collective countermeasures, and the overall development of international law towards a collectivist approach confirms rather than denies the legitimacy of collective countermeasures [Schmitt M.N., Watts S., 2021: 182, 200].

The Russian doctrine considers the concept of collective countermeasures, or countermeasures in the collective interest, both in the general theory of international responsibility [Lukashuk I.I., 2004: 355]; [Lipkina N.N., 2013: 49–50]; [Keshner M.V., 2017: 130–132] and, in particular, in the context of the legitimacy of collective coercive measures applied by the European Union, and other (often informal) associations of states, against the Russian Federation [Kozheurov Ya. S., 2015: 182]. Russian specialists tend to question the validity of such measures from the standpoint of the current development of international law [Kononova K. O., 2010: 16]; [Keshner M.V., 2015: 37, 47]. At the same time, the issues of the legality and practice of collective countermeasures as a response to hostile actions in cyberspace remains significantly understudied in the Russian doctrine. It appears that the specifics of cyberspace, cyber operations and responses to them, as well as the positions formed in official statements of states, predetermine the importance of reconsidering the legality of collective countermeasures specifically in relation to cyber operations. In this paper the terminological distinction between ‘collective countermeasures’ and ‘third-party countermeasures’ is provided when it is relevant to the issue under discussion; otherwise, the term ‘collective countermeasures’ is used as a more general term due to its prevalence in the literature devoted to state responsibility.

The paper aims to contribute to the current discussion on the admissibility of collective countermeasures in the cyber context in two ways. First, the most recent state practice and *opinio juris* have been analyzed including

the Official compendium of voluntary national contributions by states on the subject of how international law applies to the use of information and communications technologies (hereinafter Compendium)[2] and recently adopted national strategies on cyber security (particularly, the US National Cyber Security Strategy of 2023), as well as multilateral declarations on this matter. Second, the tools of analysis used in this paper include general scientific and special legal methods, along with application of beyond-positivistic research approaches to international law. Among the general research methods, the method of analysis was used, including the study of positions of states on the application of international law in cyberspace. The method of synthesis was employed to generalize the approaches of states to the legality of the measures applied to respond to cyber threats. The study also involved the application of methods of formal logic. In particular, the method of induction was used to identify collective countermeasures as a separate group of potential ways to influence states that allegedly commit malicious acts in cyberspace. The foresight method was employed to outline possible trajectories for the future development of states' cyber response strategies, in particular in analysing possible consensus-building on the legality of collective countermeasures in the context of cyber operations. Apart from the 'expository' tradition in legal research, contemplating study of legal texts, this study was conducted in the tradition of a methodological approach designated in literature as 'International Law and Economics' [Danielsen D., 2016: 453–488]. Namely, it employed game theory analysis to assess the possibility of a collective response to cyber operations by means of countermeasures, taking into account not only black-letter law, but also current political processes and incentives for states to act in a particular way.

The paper presented is structured as follows. The next section provides a brief overview of the concept of countermeasures in international law and positions of states on their applicability in cyberspace. Section Two describes the drafting history of ARSIWA with respect to the application of countermeasures by a state other than the state injured by an internationally wrongful act, which can be applied to understanding of why states are in

[2] Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by states submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace in the Context of International Security, 13 July 2021. UN Doc. A/76/136. Available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/189/48/PDF/N2118948.pdf?OpenElement (accessed: 05.07.2024)

most cases indecisive in supporting collective countermeasures in the cyber context. Section Two also provides a beyond-positivistic analysis and suggests an assessment based on game theory to enrich the discussion on the admissibility of collective countermeasures based on political rather than purely legal grounds. Section Three is a comclusion.

1. Countermeasures and State Responsibility in Cyberspace

1.1. Notion of 'countermeasures' and its applicability in the cyber context

When a state is directly injured by another state's violation of obligations owed by the latter state to the former, international law allows to state to take countermeasures. The fact that there was a prior violation precludes the countermeasures from being themselves wrongful,[3] as countermeasures are understood as 'measures that would otherwise be contrary to the international obligations of an injured state *vis-à-vis* the responsible state, if they were not taken by the former in response to an internationally wrongful act by the latter in order to procure cessation and reparation.'[4]

The substance of countermeasures is temporary non-performance by the state applying countermeasures of its international obligation (or several obligations simultaneously[5]) towards the responsible state.[6] Their purpose is to induce a wrongdoing state to comply with obligations of cessation and reparation towards the state taking the countermeasures. Accordingly, countermeasures may not have a coercive character;[7] they should be instrumental, but neither punitive[8] nor forcible.[9] Countermeasures should be

[3] Gabčikovo-Nagymaros Project (Hungary v. Slovakia), Merits, Judgment of 25 September 1997. ICJ Rep. 7, at 55 para 83: countermeasures might justify otherwise unlawful conduct 'taken in response to a previous international wrongful act of another state and ... directed against that state'.

[4] International Law Commission. Articles on the Responsibility of States for Internationally Wrongful Acts, with Commentaries (2001). UN Doc. A/56/10 (ARSIWA w. Commentaries). Part Three. Chapter II, para 1.

[5] ARSIWA w. Commentaries, commentary (6) to Art. 49.

[6] Ibid. Art. 49, para 2.

[7] ARSIWA w. Commentaries, commentary (3) to Art. 18.

[8] Ibid. Commentary (1) to art 49.

[9] ARSIWA. Art 50, para 1(a).

temporal ones[10] and reversible as far as possible.[11] They cannot coerce the wrongdoing state to violate obligations to third states[12] or involve any departure from certain norms of international law, including *jus cogens* norms.[13] Neither can they affect any dispute settlement procedure that is in force between the two states,[14] nor impair diplomatic or consular inviolability.[15]

As is well known, states conceptually affirm application of international law, and in particular the Charter of the UN, in the cyber context.[16] The Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security ('the GGE') has specifically addressed in several reports international obligations of states regarding internationally wrongful acts using information and communication technologies ('the ICTs').[17] The UN Open-Ended Working Group ('the OEWG') concluded in the 2021 Final Substantive Report on the need for further development of rules, norms and principles of responsible behavior of states in cyberspace.[18] However, none of the final reports of GGE or OEWG published to date contains their conclusions or proposals on the applicability of countermeasures in response to malicious activities in cyberspace.

Another widely cited source on the application of the norms of international law in the cyber context — the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations [Schmitt M. N., 2017] (hereinafter the Tallinn Manual 2.0) representing views of the international group of experts not including specialists from Russia — on the contrary, offers

[10] Ibid. Art. 49, para 2: 'for the time being'.

[11] Ibid. Art. 49, paras 2 and 3, and Art 53; ICJ, Gabcíkovo-Nagymaros Project, at 56–57, para 87.

[12] ARSIWA w. Commentaries, commentary (3) to Art. 18.

[13] ARSIWA Art. 50, para 1; Application of the Convention on the Prevention and Punishment of the Crime of Genocide, Counter-Claims, Order of 17 December 1997, ICJ. Reports 1997, at 258, para 35: 'in no case could one breach of the Convention serve as an excuse for another'.

[14] Ibid. Art. 50, para 2(a).

[15] Ibid.

[16] The General Assembly welcomed this affirmation of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE) on numerous occasions: see UNGA Res. A/70/455. 23 December 2015.

[17] GGE Report 2013. UN Doc. A/68/98, para 23; GGE Report 2015. UN Doc. A/70/174, para 13; and GGE Report 2021. UN Doc. A/76/135, para 25.

[18] OEWG. Final Substantive Report 2021. UN Doc A/75/816, paras 8, 24.

comprehensive rules and commentary on countermeasures. The group of international experts who authored the Tallinn Manual 2.0 starts with a general statement about the right of a state injured by a cyber operation to employ countermeasures, 'whether cyber in nature or not', if the operation constitutes a breach of an international legal obligation owed by the wrongdoing state.[19] The Tallinn Manual 2.0 then clarifies the requirements for the countermeasures to be considered lawful, including limitations of the purpose and targets of countermeasures, their compliance with peremptory norms of international law, and the mode of their execution.[20]

Since recently (and particularly after the publication of the Tallinn Manual 2.0), several states began to indicate their position on the applicability of countermeasures as a means of response to malicious use of ICTs. Thus, Australia has specified, in 2017, that a state injured by malicious cyber activity attributable to another state may apply countermeasures if they are non-forcible, proportionate and aimed at compelling the perpetrator state to cease the wrongful conduct;[21] in 2020 Australia has reaffirmed, in a comprehensive case study, its position on the legality of countermeasures in response to hostile conduct using ICTs if the measures applied meet the requirements of proportionality, reversibility, non-forcible character, compliance with fundamental human rights, humanitarian obligations and peremptory norms of international law.[22] Canada enumerates similar constraints for states to take countermeasures in response to cyber operations; herewith, the position of Canada is quite specific in respect of the attribution of the relevant malicious conduct to the responsible state: a state taking countermeasures is not obliged to provide detailed information equivalent to the level of evidence required in a judicial process to justify its cyber countermeasures; however, the state should have reasonable grounds to believe that the state that is alleged to have committed the internationally wrongful act was responsible for it.[23]

---

[19] Tallinn Manual 2.0. Rule 20.

[20] Ibid. Rules 21–23.

[21] Australia's International Cyber Engagement Strategy 2017. Available at: www.internationalcybertech.gov.au/about/2017-International-Cyber-Engagement-Strategy (accessed: 05.07.2024)

[22] Case studies on the application of international law in cyberspace, published February 2020. Available at: www.internationalcybertech.gov.au/sites/default/files/2020-12/australias-oewg-non-paper-case-studies-on-the-application-of-international-law-in-cyberspace.pdf, at 3 (accessed: 05.07.2024)

[23] Government of Canada. International Law applicable in cyberspace. Available at: www.international.gc.ca/world-monde/issues_development-enjeux_developpement/

France, in its submission to the OEWG in 2021, indicated it considers itself entitled to take cyber-related countermeasures 'designed to (i) protect its interests and ensure they are respected and (ii) induce the state responsible to comply with its obligations',[24] thus broadening the legitimate purpose of the application of countermeasures by indicating the goal of protection of interests without specifying their scope. Germany and Norway, likewise, have stated that malicious use of ICTs can be responded to by countermeasures; at the same time, they share a cautious approach to their application due to 'multifold and close interlinkage of cyber infrastructures not only across different states but also across different institutions and segments of society within states'[25] and the difficulties in the attribution of cyber operations to the responsible state.[26] Switzerland,[27] the UK[28] and the US[29] similarly maintain that a state injured by malicious cyber-enabled activities which constitute internationally wrongful acts may resort to countermeasures subject that general requirements contemplated by international law to this means of response are met. Overall, there is agreement among the named states that countermeasures may be both of cyber and non-cyber nature.

China stands out from the crowd claiming that the law of state responsibility 'has not yet gained international consensus', and '*there is no legal basis at all* for any discussion on its application in cyberspace'.[30] More generally, China questions the utility of enforcing rules on countermeasures enshrined in ARSIWA in the cyber context — instead, it advocates for the

---

peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng#a9, para 34-36 (accessed: 05.07.2024)

[24] International Law Applied to Operations in Cyberspace, Paper shared by France with the Open-ended working group established by resolution 75/240. Available at: https://documents.unoda.org/wp-content/uploads/2021/12/French-position-on-international-law-applied-to-cyberspace.pdf, at 4 (accessed: 05.07.2024)

[25] Position Paper on the Application of International Law in Cyberspace, submitted by Germany to OEWG. 2021. Available at: https://documents.unoda.org/wp-content/uploads/2021/12/Germany-Position-Paper-On-the-Application-of-International-Law-in-Cyberspace.pdf, at 13–14 (accessed: 05.07.2024)

[26] Compendium, 72–73.

[27] Ibid, 90–91.

[28] Ibid, 118.

[29] Ibid, 142.

[30] China's Contribution to the Initial Pre-Draft of OEWG Report. Available at: https://front.un-arm.org/wp-content/uploads/2020/04/china-contribution-to-oewg-pre-draft-report-final.pdf, at 5 (emphasis added) (accessed: 06.07.2024)

application of general principles of international law reflected in the UN Charter. To date, this position appears to be a rare exception and is rather intended to emphasize the commitment of Chinese experts to the idea of the development of new international treaties to establish binding rules of state behaviour in cyberspace [Huang Z., Ying Y., 2021: 555–558].

Another BRICS country, Brazil, also takes a cautious stance on responding to cyber operations by countermeasures: 'Brazil considers that there needs to be further discussions on the legality of countermeasures as a response to internationally wrongful acts, including in the cyber context'.[31] This wariness is based on the premise that the ARSIWA provisions on countermeasures went beyond codification of customary norms and represent a progressive development of international law,[32] which at least calls into question the states' obligation to follow them, as well as concerns about the feasibility of meeting the procedural requirements of application countermeasures in the ICTs environment.

Unlike retorsions being 'unfriendly conduct which is not inconsistent with any international obligation of the state engaging in it',[33] acts (or omissions) that constitute countermeasures would normally be wrongful unless certain conditions are met.

Firstly, the existence of an internationally wrongful act towards the states applying countermeasures should be established.[34] This necessitates the attribution of the relevant conduct to the responsible state [Shany Y., Schmitt M. N., 2020]; [Lahmann H., 2020] and qualification of a cyber operation as a violation of a particular obligation which the responsible state owes to the injured state. The literature on the application of international law in cyberspace considers the possibility of qualifying cyber operations, inter alia, as violations of the principle to respect state sovereignty [Rusinova V., Assaf A., Moshnikov D., 2020]; [Coco A., Dias T., van Benthem T., 2022]; the principle of non-intervention [Watts S., 2015]; the prohibition of the use of force and/or qualification of the cyber incident as an armed attack [Roscini M., 2014].

[31] Compendium, 22.

[32] Max Planck Encyclopedia of International Law. Countermeasures (2015).

[33] ARSIWA w. Commentaries. Chapter II. Countermeasures, commentary (3).

[34] ICJ, Gabcíkovo-Nagymaros Project, at 55 para 83: 'In the first place it must be taken in response to a previous international wrongful act of another state and must be directed against that state'.

Secondly, the countermeasures applied must comply with the proportionality test, i.e. they should take into account the gravity of the internationally wrongful act and the rights in question.[35] The Tallinn Manual 2.0 offers a rather vague definition of 'injury', which is taken into account when assessing proportionality of countermeasures applied in response to malicious cyber-enabled activities: it 'is not to be understood to require damage. Instead, simple breach of an international legal obligation suffices to make proportionate countermeasures available to the injured state.'[36] It seems that such an approach contradicts the position of the ILC which points to proportionality as 'an essential limit'[37] of the intensity of countermeasures, which also serves as a protection for the injured state itself from being subjected to the rules of responsibility. The mandatory proportionality of countermeasures was confirmed by the majority of states that declared their position on the state responsibility for malicious activities in cyberspace (including, during the sessions of the OEWG): among them, Germany underlines that states should be especially cautious and prudent when determining whether the applicable constraining criteria for cyber countermeasures are met, and if such actions satisfy the standards for countermeasures, a state may — *a maiore ad minus* — engage in cyber reconnaissance measures to investigate options for countermeasures and evaluate the potential danger of side effects.[38]

Finally, countermeasures may be justified only if taken against the wrongdoing state and do not affect third parties.[39] This requirement is of particular importance in the context of cyber-enabled countermeasures because, as noted by Brazil, 'cyber operations can be designed to mask or spoof the perpetrator, which in turn increases the risks of miscalculated responses against innocent actors'.[40]

---

[35] ARSIWA. Art. 51; Case Concerning the Air Service Agreement of 27 March 1946 between the United States of America and France, Decision of 9 December 1978, UN Reports of international arbitral awards, Vol. XVIII, at 443-444 para 83.

[36] Tallinn Manual 2.0, commentary 2 to Rule 23.

[37] ARSIWA w. Commentaries, commentary (1) to Art. 51.

[38] Position Paper on the Application of International Law in Cyberspace, submitted by Germany to OEWG, 2021. Available at: https://documents.unoda.org/wp-content/uploads/2021/12/Germany-Position-Paper-On-the-Application-of-International-Law-in-Cyberspace.pdf, at 13–14 (accessed: 06.07.2024)

[39] ARSIWA. Art. 49, para 1 and 2.

[40] Compendium, 22.

2. Substantive and Procedural Requirements to Countermeasures: Is *Lex Specialis* Needed for Cyber Countermeasures?

Apart from the substantive restrictions described above, the use of countermeasures must meet certain procedural requirements. Article 52 of ARSIWA imposes two main procedural duties on a state intending to resort to countermeasures: to call upon the wrongdoing state to comply with its obligations[41] (obligation also known as '*sommation'*[42]*); and to notify the responsible state of its intention to apply countermeasures and offer negotiation. That said, in emergency circumstances, the injured state is permitted to forego the requirement of notification and offer negotiations and take urgent* countermeasures 'as are necessary to preserve its rights'.[43] Such relief, however, does not apply to the *sommation*.

The Tallinn Manual 2.0 provides a non-exhaustive list of examples where urgent cyber countermeasures can justify waiver of prior notification requirement: (i) when the injured state needs to take prompt action to protect its rights and prevent further harm;[44] and (ii) when prior notification of the intent to take a countermeasure will make it meaningless.[45] While the minority of experts, authors of the Tallinn Manual 2.0 came to the conclusion that customary international law (specifically, Article 52(1)(b) ARSIWA) requires the injured state to seek negotiations before taking countermeasures, the majority of them rejected this requirement and argued that an injured state may take countermeasures before seeking negotiations.[46]

An analysis of available states' positions on the applicability of the requirements set forth in Article 52 of ARSIWA to cyber-related countermeasures has revealed the following. First, a number of states which have expressed their position on applicability of the rules on countermeasures

[41] ARSIWA. Art 52(1)(a). Jurisprudence on sommation: Air Service Agreement, at 444, paras 85-87; Gabcíkovo-Nagymaros Project, at 56, para 84. See also: G. Arangio-Ruiz. Fourth Report on State Responsibility. 1992 YILC. Vol. II, 22, para 6ff.

[42] ARSIWA w. Commentaries, commentary (3) to Art. 52.

[43] Art. 52(2) of ARSIWA, ARSIWA w. Commentaries, commentary (5) to Art. 52: temporal relationship between the operation of subparagraphs (a) and (b) of paragraph 1 is not strict. Notifications could be made close to each other or even at the same time.

[44] Tallinn Manual 2.0, commentary 11 to Rule 21.

[45] Ibid. Commentary 12 to Rule 21.

[46] Ibid. Commentary 13 to Rule 21.

in response to cyber operations (including Australia, Denmark, Estonia, and Germany) omit addressing procedural requirements altogether. Out of this group of states, Canada indicates that the precise scope of certain procedural aspects of countermeasures, such as notification, 'needs to be further defined through state practice given the unique nature of cyberspace'[47] (leaving, however, open the question of whether requirements contemplated by ARSIWA are generally appropriate for the cyber domain).

Second, only two states, Italy and Norway, distinguish between the two requirements stipulated by Article 52(1) of ARSIWA: to call upon the responsible state to fulfill its obligations, and to notify it of the decision to take countermeasures and offer to negotiate. Herewith, Italy indicates that derogation from both requirements is possible in cases of emergency[48], which contradicts the idea of urgent countermeasures implied by the ILC. Norway seems to be the closest to the provisions of Article 52(2) of ARSIWA, indicating that urgent countermeasures can be taken without prior notification 'if providing such notification might reveal sensitive methods or capabilities or prevent the countermeasures from having the necessary effect', and not saying the same regarding the requirement to request the responsible state to fulfill its obligations.[49]

Finally, the rest of the states mention only one of the procedural requirements or indicate both but do not differentiate exceptions, in cases of an urgent countermeasure. For instance, France acknowledges the obligation of the victim-state to notify the responsible state of its intention to take countermeasures, which the obligation can be derogated from if the injured state needs to protect its rights (but doesn't mention the *sommation*).[50] Switzerland indicates that 'the responsible state can only impose countermeasures if it has first called for the violation(s) to cease and has announced what measures it is planning to take' and, at the same time, '[e]xceptions may be made for cyber operations requiring an immediate response in order for the injured state to enforce its rights and prevent further damage'[51]

[47] Government of Canada. International Law applicable in cyberspace (no. 33), para 36.

[48] Italian Position Paper on 'International Law and Cyberspace' submitted to OEWG (2021) at 7.

[49] Compendium, 72–73.

[50] 'International Law Applied to Operations in Cyberspace'. Paper shared by France with the Open-ended working group established by resolution 75/240, at 4.

[51] Compendium, 90–91.

(do these exceptions apply for both the *sommation* and notification requirements?). The US mentions only the requirement to call upon fulfilment by the responsible state of its obligations and permits derogation from this requirement to preserve the injured state's right — a position which contradicts Article 52(2) of ARSIWA.

There are several possible explanations for this range of positions expressed by states (to set aside the probability that states omitted an analysis of procedural requirements while preparing their submissions for some technical reasons or because they considered them insignificant).

Potentially, states do not consider procedural requirements stipulated by ARSIWA applicable in the cyber context due to its specific nature. Thus, *lex specialis* might be required to define the pre-requisites for responding to malicious cyber operations by countermeasures. Policy arguments to support such *lex specialis* may include indication of the special covert and sensitive nature of cyber capabilities can be revealed by prior notification of countermeasures, especially if they are themselves of cyber nature.[52] Moreover, such notification can make the countermeasures meaningless or quite weak one.[53] One more possible reason is that cyber incidents may be ongoing and high speed, and notification exception can be introduced to procure the possibility of a timely response. Also, it is sometimes considered that public warnings that malicious activities in cyberspace are unacceptable and will lead to countermeasures usually have no effect on 'hostile states such as Russia and China', thus, 'this exception has the potential to become the norm'.[54] It seems that despite the general attractiveness of the idea to develop *lex specialis* for the use of countermeasures in cyberspace, given its specific nature, the lowering of procedural conditions for this means of response carries significant risks, first of all — the danger of escalation, potentially in both cyber and kinetic domains. Moreover, as pointed out by Brazil, there is an increased risk of responding against an innocent actor, as

[52] J. Wright. Attorney General of the United Kingdom, in his speech 'Cyber and International Law in the 21st Century' (23 May 2018) did not agree states are always legally obliged to give prior notice before taking countermeasures against wrongdoing states, and that it would 'not be right for international law to require a countermeasure to expose highly sensitive' defense capabilities.

[53] Compendium, 72–73.

[54] Deeks A. Defend Forward and Cyber Countermeasures. Hoover Working Group on National Security, Technology, and Law. Aegis Series Paper No. 2004. 2020. Available at: www.lawfareblog.com/defend-forward-and-cyber-countermeasures (accessed: 01.07.2024)

cyber operation can be designed to conceal the offender, and the waiver of procedural requirements (particularly, the *sommation*) precludes the possibility for such an actor to validate its lawful conduct.

Another possible explanation is that states do not assume the need to develop *lex specialis*, but rather, most of them did not consider it possible at all to determine as of the date of their contributions the procedural requirements for countermeasures to be applied in the cyber context. In that case, it remains to join Canada's aspirations states practice will further clarify the exact procedural limits of countermeasures as a lawful response to malicious activities in cyberspace.[55]

As an interim summary of what has been discussed above, it can be noted that applicability of the law of state responsibility, including countermeasures, is generally accepted by those states which have expressed their position on the matter, except for China which questions the binding character of ARSIWA, and Brazil which hesitates rules relating particularly to countermeasures are of customary nature. Similarly, there is sufficient consistency in states' positions regarding the fundamental preconditions for countermeasures (the cyber operation should constitute an internationally wrongful act and be attributed to the wrongdoing state), as well as major substantial requisites of lawful countermeasures in response to cyber incidents (they should be addressed to the wrongdoing state, be proportionate, non-forcible, compliant with international law, including *jus cogens*).

Contrary to the general agreement on these points, there is little clarity on the procedural pre-requisites applicable to countermeasures as a response to cyber operations. Article 52 of ARSIWA vests two major requirements on the state intending to take countermeasures: (i) to call upon the responsible state to comply with its obligations, which aims to give this state a chance to evaluate its conduct and, if necessary, to correct it; and (ii) to notify the responsible state of the decision to take countermeasures and offer to negotiate. Review of states' positions revealed particularly a lack of consensus regarding the 'urgent countermeasures' in the cyber context. Although the position expressed, in particular by Italy, on the possibility of waiving both the *sommation* and notification requirements in cases of emergency is understandable from a political standpoint, its expansion can generate dangerous uncertainty. Reports of Special Rapporteur James Crawford on state responsibility demonstrate hot debates on the procedural

[55] Government of Canada. International Law applicable in cyberspace, para 34-36.

requirements to countermeasures during the work of ILC.[56] The requirement of *sommation* is considered by the Special Rapporteur as classical, reflecting a general practice and confirmed by Arbitral Tribunal in the *Air Service Agreement* and by ICJ in the *Gabčíkovo-Nagymaros Project*.[57] Taking into account that the injured state makes a decision on countermeasures based on its sole assessment of the other state, the *sommation* requirement serves a safeguard against an unlawful and premature resort to countermeasures, and their potential misuse. In this sense, application of the 'urgency exception' to the *sommation* requirement, and not only to the prior notification, should not become a 'new norm' for cyber-related countermeasures.

3. Collective Cyber-Related Countermeasures Under International Law

3.1. Drafting History of Article 54 ARSIWA: from Bilateral Model to the 'Saving Clause'

Two articles of ARSIWA, Article 48 and Article 54, deal directly with situations when a non-injured state can invoke state responsibility. Article 48(1) provides for the invocation of responsibility by a non-injured state if the obligation breached protects a collective interest of a group of states including that state, i.e. obligation *erga omnes partes,*[58] *or if the obligation breached is owed to the international community as a whole, i.e. obligation erga omnes.*[59] Thus, in both cases the state invoking responsibility acts not in its individual capacity as an injured party, but in the collective interest — either, of a group of states or the international community.[60] Para (2) of Article 48 specifies the claims available to the non-injured state in these cases: to request from the wrongdoing state cessation of the internationally wrongful act, and reparation. The list of remedies is exhaustive,[61] and it does not include countermeasures.

Article 54 in Chapter II of ARSIWA on countermeasures addresses specifically measures taken by non-injured states. It provides for the right of

[56] J. Crawford, Special Rapporteur. Fourth Report on State Responsibility. 2001. UN Doc. A/CN.4/517, para 67.

[57] Ibid. Para 69.

[58] ARSIWA w. Commentaries, commentary 6 to Art. 48.

[59] Ibid. Commentary 8 to Art. 48.

[60] Ibid, Commentary 1 to Art. 48.

[61] Ibid, Commentary 11 to Art. 48.

any state which is entitled to invoke state responsibility under Article 48 (1) to take 'lawful measures' against that wrongdoing state 'to ensure cessation of the breach and reparation in the interest of the injured state or of the beneficiaries of the obligation breached'.[62] The term 'lawful measures', rather than 'countermeasures', was incorporated deliberately in order 'not to prejudice any position concerning measures taken by states other than the injured state',[63] and thus to include acts of retorsion.

The origins of such a cautious approach can be traced in the convoluted drafting history of ARSIWA. The early drafts were based on the distinction proposed by Special Rapporteur Ago between 'international crimes', i.e. the serious breach of particular obligations most important for the international community, and 'international delicts', i.e. breach of other obligations.[64] The allocation of particular wrongdoings to the category of international crimes could justify collective reaction[65] and give the green light to third-party countermeasures, especially if the notion of an 'injured state' included all states when a wrongdoing by a state constituted an international crime.[66] However, the first reading of Article 40 [1996] on the notion of 'injury' was based on the traditional bilateral model of enforcement. That was strongly opposed by Special Rapporteur Crawford who noted that 'here is no longer (if there ever was) any a priori reason to reduce all relations of responsibility to the form of a bilateral right-duty relation of two states'.[67] Crawford proposed to consider a state injured by a breach of a multilateral obligation if the obligation in question is an obligation *erga omnes* or *erga omnes partes*, and, herewith, the breach specifically affects the state, or 'necessarily affects' the enjoyment by that state of its rights or the performance of its obligations.[68] This distinction, according to Crawford, was to determine the

[62] Art 54 ARSIWA.

[63] ARSIWA w. Commentaries, commentary 7 to Art. 54.

[64] Ibid, 74.

[65] Ibid, 79.

[66] W. Riphagen, Special Rapporteur. Fifth Report on the Content, Forms and Degrees of International Responsibility. 1984. UN Doc. A/CN. 4/380 at 3, Art. 5; Sixth Report on (1) the Content, Forms and Degrees of State responsibility, and (2) the 'Implementation' (mise en oeuvre) of International Responsibility and the Settlement of Disputes, at 5–8 (for commentary to his draft Art. 5).

[67] J. Crawford, Special Rapporteur. Fourth Report on State Responsibility. 2000. UN Doc. A/CN.4/507, 29, para 84.

[68] Ibid. 39, formulation of draft art 40 bis 'Right of a State to invoke the responsibility of another State'.

right of the state to invoke responsibility of another state for a breach of a multilateral obligation: any state party to such an obligation could take countermeasures 'at the request and on behalf' of a state directly injured by the breach (if there was such a directly injured state).[69] In cases of serious breaches of an obligation *erga omnes*, any state could take countermeasures to the extent necessary 'to ensure the cessation of the breach and reparation in the interests of the victims'.[70] It is in this latter case that the model of bilateral interaction between the wrongdoing and the victim-states was replaced by the use of collective, or solidarity, measures [Koskenniemi M., 2001: 346].

Crawford's conception of different categories of 'injured states' and corresponding right to take countermeasures in case of a breach of collective obligations raised hot debates in the ILC and the Sixth Committee. The main concerns of those opposing to the right of states to take countermeasures in response to a breach of *erga omnes* obligations laid in the fears of abuse by powerful states of this right[71] as well as intervention in competence of the UN Security Council to address situations of the most serious breaches of collective obligations.[72] Thus, the final wording of Article 54 of ARSIWA as a 'saving clause' appears to be a necessary compromise after the ILC established that at the time of drafting ARSIWA customary international law did not contemplate the right of states to take countermeasures in the general or collective interest.[73]

One might wonder, to which extent the practice of the International Court of Justice has been influencing the long-years discussion of collective countermeasures in the ILC and its drift between the models of bilateral and collective enforcement in the cases when communitarian norms are breached. In fact, the concept of collective countermeasures has not been much discussed by the ICJ with a remarkable exception of the *Nicaragua* case in which the Court examined whether the support provided by the US to *contras* can be justified as a third-party countermeasure against Nicaragua

[69] Ibid. 108, formulation of draft art 50A 'Countermeasures on behalf of an injured State'.

[70] Ibid. 108–109, formulation of draft art 50B 'Countermeasures in cases of serious breaches of obligations to the international community as a whole'.

[71] UN Doc. A/C.6/55/SR.18, at 11, para 59–62 (Cuba); UN Doc. A/C.6/55/SR.15, at 5–6, para 29, 31 (India).

[72] ILC, Summary Records of the Meetings of the Fifty-Third Session 23 April — 1 June and 2 July — 10 August 2001, 2001 YILC, Vol. I, at 41 para 49.

[73] ARSIWA w. Commentaries, commentary 6 to Art 54.

which supported armed rebels in Costa Rica, El Salvador and Honduras.[74] The Court was firm in its conclusion only victim-states (i.e. Costa Rica, El Salvador and Honduras) could apply countermeasures and not the US as a third party in that situation.[75] At the same time, the ICJ in a manner left the door ajar by saying that 'a use of force of a lesser degree of gravity [than an armed attack] cannot produce any entitlement to take collective countermeasures involving the use of force'.[76] This gave commentators the grounds to suggest that the Court considered collective countermeasures potentially justifiable if taken in response to a grave violation of an *erga omnes* obligation [Dawidowicz M., 2017: 71] and created a sort of an 'echo camera' with the corresponding discussion in the ILC.

3.2. Collective Countermeasures in Cyberspace: To Be or Not to Be

Rule 24 of the Tallinn Manual 2.0 stipulates only the victim-state may apply countermeasures. Herewith, the accompanying commentary to Rule 24 indicates that there was some disagreement among the experts on the permissibility for a non-injured state to apply countermeasures: some of them left such possibility open, provided that the injured state requests assistance; the majority, however, noted with a reference to the *Nicaragua* case that 'countermeasures taken on behalf of another state are unlawful'.[77] The latter group was also divided over whether the non-injured state can assist the injured state in its countermeasures — thus, on the possibility of solidarity measures, and not third-party countermeasures in a narrow sense. Some experts equated the assistance to a victim-state and third-party countermeasures which makes such helping illegal.[78] Others, on the contrary, differentiated the assistance to take countermeasures and taking them on behalf of another state, which means that helping in legal countermeasures is legal itself.[79] Finally, some experts proposed to evaluate solidarity measures for compliance with the obligations owed by the assisting state to the wrongdoing state: if the activities that make up the assistance (e.g.,

[74] Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States), Merits, Judgment of 27 June 1986. ICJ Rep. at 127, para 248.

[75] Ibid. 127, para 249.

[76] Ibid.

[77] Tallinn Manual 2.0, commentary 7 to Rule 24.

[78] Ibid. Commentary 9 to Rule 24.

[79] Ibid.

instructions or technical help on hacking-back) violate obligations of the assisting state to the responsible state, such assistance in unlawful.[80] The diversity of views among the experts — authors of the Tallinn Manual 2.0 indicates, inter alia, that there were (and still remain) legal and political arguments both for and against permissibility of collective and/or third-party countermeasures in the cyber context.

This brings us, first, to the analogy of collective self-defence, the right to which is contemplated by Article 51 of the UN Charter as a measure until the Security Council effects its reaction on the threat to the international peace and security. This analogy, however, could justify only third-party countermeasures at the request of the injured state, if the requirements developed in respect of the application of Article 51 to the 'real world' armed conflicts could be transferred into cyberspace with a qualification of a cyber operation as an armed attack.

Another approach could be to justify collective countermeasures as a means to defend collective interest in cyberspace. This, first, requires identifying collective obligations that can be breached by cyber operations. It appears that the known episodes of malicious use of ICTs do not violate the traditional *erga omnes* obligations enlisted by the ILC, such as prohibition of aggression and genocide, protection from slavery and racial discrimination, the right of peoples to self-determination.[81] Identification of a cyber-specific community interest is sometimes suggested in the literature, for instance, the obligation to protect the 'public core of the internet' [Roguski P., 2020: 37–40]. No less important is the question of whether protection of such collective interest (if it is established for the cyber context) a priori justifies its enforcement by third-party countermeasures. It appears that international law in its present state does not contemplate such automatic standing, and clarification on this issue has yet to be developed in the state practice which will depend, in particular, on the inclination towards a bilateral or collectivist model of enforcement.

Alternatively, the permissibility of third-party countermeasures can be supported by a political, rather than purely legal, argument that the malicious cyber-enabled activities should not go unanswered if the victim-state is unable to take countermeasures on its own, in particular due to its low cyber capabilities. In other words, the injured state should not be left alone in a situation of hostile actions in cyberspace. This line of argumentations

[80] Ibid.

[81] ARSIWA w. Commentaries, commentary (9) to Art. 48.

seems to be configuring the position of Estonia who is to date the main advocate for the legality of third-party and collective countermeasures. In her speech on the annual Cyber Conference of NATO Cooperative Cyber Defence Centre of Excellence in May 2019, then-president of Estonia, Kersti Kaljulaid, stressed the importance for the non-injured states to be able to take countermeasures 'to support the state directly affected by the malicious cyber operation'.[82] Later Estonia has reaffirmed its position in the Compendium: 'If a cyber operation is unfriendly or violates international law obligations, injured states have the right to take measures such as retorsions, countermeasures or, in case of an armed attack, the right to self-defense. These measures can be either individual or collective'.[83] Thus, Estonia supports collective and third-party countermeasures as a means of response to malicious cyber operations.

At the same time, there are quite convincing arguments against such an approach. First, granting the states not directly affected by a cyber-attack the right to respond to it by means of countermeasures could open the way to widespread abuse of that right and the emergence in powerful states of a sense of self as the world cyber police. Second, as rightly pointed out by Brazil,[84] whose position has already been cited above, the difficult task of the attribution of a cyber-attack to a state and overall covert nature of cyber operations raise the risk of ill-founded measures against a clean handed state (and, consequently, the risk of invocation of responsibility of the state applying countermeasures). Finally, the significant risk of escalation, potentially spreading to the kinetic domain, due to the high speed of cyber actions proceeding, should be taken into account.

These considerations, perhaps, may explain the more restrained position of the states, other than Estonia, that expressed their attitude towards collective countermeasures in cyberspace. France unambiguously stated that collective countermeasures are not authorised by international law, and therefore France considers itself entitled to take countermeasures only if it is a victim to malicious cyber actions and not in response to violation

[82] K. Kaljulaid, President of the Republic at the opening of Cy Con 2019. Speech in Tallinn. 29 May 2019. Available at: www.president.ee/en/offiial-duties/speeches/15241-president-of-the-republic-at-the-openingof-cycon-2019/index.html (accessed: 05.07.2024)

[83] Estonian positions on 2021-25 United Nations Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security. 2021, 16.

[84] Compendium, 22.

of another state's rights.[85] Canada seems to be hesitating: on the one hand, it underlines the absence of sufficient state practice or *opinio juris* to answer in affirmative that collective cyber countermeasures are permitted under international law; on the other hand, it recognizes the possibility of technical or legal assistance to the victim-state if the latter does not possess necessary capabilities for a response.[86] Herewith, Canada does not address the issue of qualification of such assistance as third-party countermeasures and its legality under international law.

Overall, the number of states that have expressed their position on the admissibility of collective countermeasures in the cyber domain is too limited to conclude on the support or denial by the international community of this means of reaction to cyber operations. Having said that, one can make an assumption of an increase in the number of supporters of collective cyber countermeasures in the future, not only (or not so much) due to the development of international law in this area, but rather as part of the general trend of uniting the efforts of states to bring trouble-makers in cyberspace to responsibility. Thus, as the next section appeals to the toolbox of economics, namely game theory, — to assess the arguments for and against countermeasures as a potential collective response to cyber operations beyond the purely legal discussion but taking into account also current political processes and incentives for states to act in a particular way.

3.3. Application of Game Theory as an Auxiliary Means to Assess the Applicability of Collective Countermeasures in Cyberspace

The section seeks to provide an additional lens in the form of methodology from the discipline related to international law, namely economics, in order to create a more comprehensive view of the reasons why states are willing to cooperate in their responses, or conversely, refrain from such cooperation. Game theory — the 'study of mathematical models of conflict and cooperation between intelligent rational decision-makers' [Myerson R.B., 1991: 1] — appears to be an adequate tool for developing a stereoscopic view of the motivation for states to unite or disunite in their response to new threats, including cyber-related ones.

---

[85] International Law Applied To Operations In Cyberspace, Paper shared by France with the Open-ended working group established by resolution 75/240. Available at: https://documents.unoda.org/wp-content/uploads/2021/12/French-position-on-international-law-applied-to-cyberspace.pdf, at 4 (accessed: 06.07.2024)

[86] Government of Canada. International Law applicable in cyberspace, para 37.

A game-theoretical analysis has been widely addressed in the international relations literature and, more recently, in the literature on international law [Ohlin J. D., 2011]. The tools of game theory are employed as a part of a beyond-positivistic approach to answering the question of why states obey international law [Tesón F., 1998: 74–76]; [Chinen M.A., 2001]; [McAdams R.H., 2009]; [Konyukhovskiy P.V., Holodkova V.V., 2017].

Assuming that states are rational actors that seek to maximize payoffs and reduce costs, cooperation in the cyber security sphere would be mutually beneficial for states wishing to protect their interests in cyberspace. From the standpoint of rational choice doctrine, states tend to cooperate due to the payoffs underlying such cooperation even in the absence of international treaties [Guzman A., 2008: 26]. In certain cases states use the informal instruments to reassure their willingness to cooperate — as, for instance, declaration of alignment of third countries (particularly, EU Candidate Countries Turkey, North Macedonia, Montenegro and Albania; Bosnia and Herzegovina; EFTA States Iceland and Norway and EU Associates Ukraine and Georgia) with EU cyber-related sanctions,[87] or declaration by the EU of solidarity with the US on the impact of the Solar Winds cyber operation.[88] As a step further, formal international agreements are executed such as the Malabo Convention. In light of coordination games theory (that are games which contemplate coordination of players' actions to achieve the goals of their cooperation), agreements serve to formalize arrangements between the parties and increase stability of the agreed regime on complicity, especially in the situation when the incentives for informal cooperation may weaken over time. In other words, international treaties apparently facilitate cooperation of states in a coordination game in the setting of uncertainty about the players' payoffs in the future [Guzman A., 2008: 26, 28].

The rational choice assumption provides various avenues for the analysis not only of the incentives for states to cooperate and comply with obligations under international agreements, but also the application of counter-

[87] The text of the declaration is available at: www.consilium.europa.eu/en/press/press-releases/2020/06/19/declaration-by-the-high-representative-on-behalf-of-the-eu-on-the-alignment-of-certain-third-countries-concerning-restrictive-measures-against-cyber-attacks-threatening-the-union-or-its-member-states/# (accessed: 06.07.2024)

[88] Council of the EU. Declaration by the High Representative on behalf of the European Union Expressing Solidarity with the United States on the Impact of the Solar Winds Cyber Operation.

measures as strategic interaction. Such situations of strategic interaction between the players, or 'games', are divided in a number of classes.

The interaction 'cyber operation — reaction' can be qualified as a cooperative game. States as game players are bound, at least in theory, with the commitments enforced under international law, including the principles of sovereignty and non-interference in the internal affairs of other states. As these commitments can be enforced through outside parties, the game is deemed cooperative.[89] In non-cooperative games, although players can cooperate with each other, any cooperation must be self-enforcing.[90] Cooperative game theory contemplates forecasting coalitions that the players will form, their collective actions and group payoffs. In non-cooperative theory, a game is a detailed model of various moves available to the players, the analysis of individual payoffs and Nash equilibria.[91] In a cooperative game, players other than the state applying countermeasures and the target can join the game at each decision stage, at their discretion, as 'white knights' in cooperation with the applicant of the countermeasures or 'black knights' on the side of the designated wrongdoer [Eyler R., 2008: 37]. Each episode of the application of countermeasures undermines reputation of the target as an actor that complies with the undertaken commitments. A bad reputation of a state violating its international obligations raises costs for this state in future cases of cooperation, not only in that particular game, but also other scenarios of cooperation with different players [Guzman A., 2008: 34–35]. In this sense, the retaliatory role of countermeasures correlates with the reputational damage effect that complicates for the target process of cooperation with other players and increases its cost.

Conclusion

The paper has examined collective, or third-party, countermeasures as a potential means of response to malicious cyber-enabled conduct of a state. An analysis of state positions reveals almost complete agreement on general

[89] Non-Cooperative Game. Dictionary of Game Theory Terms, Game Theory.net. Available at: www.gametheory.net/dictionary/Non-CooperativeGame.html (accessed: 06.07.2024)

[90] Ibid.

[91] Cooperative Game Theory: Characteristic Functions, Allocations, Marginal Contribution. 2007. Available at: https://web.archive.org/web/20160527184131if_/http://www.uib.cat/depart/deeweb/pdi/hdeelbm0/arxius_decisions_and_games/cooperative_game_theory-brandenburger.pdf, 1 (accessed: 06.07.2024)

applicability of the law of state responsibility, including countermeasures, in cyberspace, but a lack of clarity on the procedural pre-requisites applicable to the countermeasures as a response to cyber operations. Appeal to the drafting history of ARSIWA has shed light on a shift from the traditional bilateral model of enforcement to the collective, or solidarity, measures and, finally, to a 'saving clause' as a necessary compromise within the drafters. Development of inter-state relations demonstrates states overall willingly cooperate to increase reputational, political and economic pressure for malicious actions in cyberspace. The cooperation has so far taken the forms of collective accusations and collective economic sanctions. At the same time, several states (the US in the first stance) demonstrate the desire to expand the toolbox of measures applied collectively to respond to malicious cyber incidents, regardless of their legal qualification. Returning to the hypothesis posed at the beginning of this study, it is now possible to conclude that states may be willing to join in the application of such measures, driven by the considerations of rational choice and (or) conditions of being in an alliance or a coalition of 'like-minded' states. The use of collective countermeasures, thus, may at some point become a logical step towards increasing the joined efforts of states, including within the framework of alliances, to counter cyber incidents.

References

1. Chinen M. A. (2001) Game Theory and Customary International Law: A Response to Professors Goldsmith and Posner. *Michigan Journal of International Law*, vol. 23, no. 1, pp. 143–189.

2. Coco A., Dias T. and van Benthem T. (2022) Illegal: The Solar Winds Hack under International Law. *European Journal of International Law*, vol. 33, no. 4, pp. 1275–1286.

3. Corn G. and Jensen E.T. (2018) The Use of Force and Cyber Countermeasures. *Temple International & Comparative Law Journal*, no. 32, pp. 127–136.

4. Danielsen D. (2016) International Law and Economics: Letting Go of the "Normal" in Pursuit of An Ever-Elusive. In: Orford A. and Hoffmann R. (eds.) The Oxford Handbook of the Theory of International Law. Oxford: University Press, 1045 p.

5. Dawidowicz M. (2017) *Third-Party Countermeasures in International Law*. Cambridge: University Press, 438 p.

6. Delerue F. (2020) *Cyber Operations and International Law.* Cambridge: University Press, 513 p.

7. Finnemore M. and Hollis D. B. (2020) Beyond Naming and Shaming: Accusations and International Law in Cybersecurity. *European Journal of International Law*, vol. 31, no. 3, pp. 969–1003.

8. Eyler R. (2008) *Economic Sanctions: International Policy and Political Economy at Work*. N. Y.: Palgrave MacMillan, 251 p.

9. Guzman A. (2008) *How International Law Works: A Rational Choice Theory*. Oxford: University Press, 260 p.

10. Haataja S. (2020) Cyber Operations and Collective Countermeasures under International Law. *Journal of Conflict and Security Law*, vol. 25, no. 1, pp. 33–51.

11. Henriksen A. (2015) Lawful State Responses to Low-Level Cyber-Attacks. *Nordic Journal of International Law*, vol. 84, no. 2, pp. 323–351.

12. Huang Z., Ying Y. (2021) Chinese Approaches to Cyberspace Governance and International Law in Cyberspace. In: N.Tsagourias and R. Buchan (eds.) Research Handbook on International Law and Cyberspace. 2nd ed. Cheltenham: Edward Elgar Publishing, 634 p.

13. Keshner M.V. (2015) Collective countermeasures taken against the Russian Federation: the issue of legitimacy. *Russian Law Journal,* vol. 101, no. 2, pp. 32–38 (in Russ.)

14. Keshner M.V. (2015) *Economic sanctions in the modern international law*. Moscow: Prospekt, 184 p. (in Russ.)

15. Keshner M.V. (2017) *Law of international responsibility*. Moscow: Prospekt, 240 p. (in Russ.)

16. Kononova K.O. (2010) 'Collective countermeasures': a question on the legitimacy of their existence and the vector of development in international law in the 21th century. *Mezhdunarodnoe publichnoe i chastnoe pravo*, no. 6, pp. 13–16 (in Russ.)

17. Konyukhovskiy P.V. and Holodkova V.V. (2017) Application of Game Theory in the Analysis of Economic and Political Interaction at the International Level. *Contributions to Game Theory and Management*, no. 10, pp. 143–161.

18. Koskenniemi M. (2001) Solidarity Measures: State Responsibility as a New International Order? *British Yearbook of International Law*, vol. 72, no. 1, pp. 337–356.

19. Kozheurov Ya.S. (2015) The War of "Sanctions" and the Law of International responsibility. *Russian Law Journal*, vol. 101, no. 2, pp. 179–182 (in Russ.)

20. Lahmann H. (2020) *Unilateral Remedies to Cyber Operations: Self-Defense, Countermeasures, Necessity, and the Question of Attribution*. Cambridge: University Press, 326 p.

21. Lipkina N.N. (2013) Countermeasures and sanctions as means of ensuring of the implementation of international obligations. *Law, Legislation, Person,* vol. 17, no. 2, pp. 48–55 (in Russ.)

22. Lukashuk I.I. (2004) *Law of international responsibility*. Moscow: Wolters Kluwer, 405 p. (in Russ.)

23. McAdams R.H. (2009) Beyond the Prisoner's Dilemma: Coordination, Game Theory, and Law. *Southern California Law Review*, vol. 82, no. 2, pp. 209–258.

24. Myerson R.B. (1991) *Game Theory: Analysis of Conflict*. Harvard: University Press, 568 p.

25. Ohlin J.D. (2011) Nash Equilibrium and International Law. *Cornell Law Review*, vol. 96, pp. 869–899.

26. Roguski P. (2020) Collective Countermeasures in Cyberspace — Lex Lata, Progressive Development or a Bad Idea? 12th International Conference on Cyber Conflict. DOI: 10.23919/CyCon49761.2020.9131715.

27. Roscini M. (2014) *Cyber Operations and the Use of Force in International Law.* Oxford: University Press, 307 p.

28. Schmitt M.N. (ed.) (2017) Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge: University Press, 598 p.

29. Rusinova V., Assaf A., Moshnikov D. (2020) Dispute on sovereignty in cyberspace: content, limits, and prospects for the development of positivistic discourse. *International Justice*, vol. 19, no. 3, pp. 55–66 (in Russ.)

30. Schmitt M.N., Watts S. (2021) Collective Cyber Countermeasures? *Harvard National Security Journal*, no. 12, pp. 373–411.

31. Shany Y., Schmitt M.N. (2020) An International Attribution Mechanism for Hostile Cyber Operations. *International Law Studies*, vol. 96, pp. 196–222.

32. Tesón F. (1998) *A Philosophy of International Law*. New York: Routledge, 208 p.

33. Tsagourias N. (2015) The Law Applicable to Countermeasures against Low Intensity Cyber Operations. *Baltic Yearbook of International Law Online*, no. 14, pp. 105–123.

34. Watts S. (2015) Low-Intensity Cyber Operations and the Principle of Non-Intervention. In: Ohlin J., Govern K. et al. (eds.). Cyber War: Law and Ethics for Virtual Conflicts. Oxford: University Press, 320 p.

Information about the author:

E.A. Martynova — Cyber BRICS Fellow.

The article was submitted to editorial office 07.08.2024; approved after reviewing 30.08.2024; accepted for publication 05.09.2024.

Legal Issues in the Digital Age. 2024. Vol. 5. No. 3.
Вопросы права в цифровую эпоху. 2024. Том 5. № 3.

Legal Informatics

Research article

УДК: 340
JEL: K 24
DOI:10.17323/2713-2749.2024.3.129.153

eLegalls-as-a-Service: Towards Developing Cloud-based Legal Tech System to Aid Lawyering in the Digital Age

Sugam Sharma
Iowa State University (ISU) Startup Factory/eLegalls.com, 1805 Collaboration Pl, Ames, Iowa, USA 50010,
info@elegalls.com, sugam.k.sharma@gmail.com, ORCID: 0000-0002-0762-3900

Ritu Shandilya
Mount Mercy University, Cedar Rapids, Iowa, USA 52402,
rshandilya@mtmercy.edu, ORCID: 0009-0000-8205-9302

Divya Dwivedi
Supreme Court of India, 40 Hanuman Lane, Connaught Place, New Delhi, India 110001,
divyadwivedi04@gmail.com, ORCID: 0000-0002-6086-7090

Millie Pant
Department of Applied Mathematics and Scientific Computing, Indian Institute of Technology Roorkee, India 247667,
pant.milli@as.iitr.ac.in, ORCID: 0000-0002-7668-7887

Abstract

Legal Tech Jurisprudence is not as developed as it was hoped for, compared with other fields of study. As a result, legal tech has not advanced globally as would have been preferred and remains primal in nature. The situation is more disappointing when it comes to developing or underdeveloped countries. While tech is critical in countries like India, which is going through digital transition currently, the justice system is still functioning in centenarian ways. For some reason, the system has not yet begun to fully harness the potential of modern IT technologies, which may consist of AI, ML, DL, NLP, etc. but not limited to these technologies. A lawyer, who is an integral part of the justice system, still continues to handle most tasks manually or with the help of an assistant, which often becomes challenging and cumbersome while dealing with complex legal issues that involve humongous contracts, for example. It is problems like these that can be very well handled with the help of technologies, being dubbed as legal informatics (LI), to help elevate the quality and quantity of lawyering and the core of jurisprudence. To try and resolve this problem and find an amicable solution to an extent, we have designed and developed an LI-enabled and proposedly cloud-based innovative computational system, called *eLegalls* and to be delivered as *eLegalls-as-as-Service*, and this paper illuminates and elaborates its potential in providing the hassle-free lawyering in digital age.

Keywords

e-Legalls-as-a-Service; cloud; legal; informatics; law; tech; lawyer.

Acknowledgments: Dr. Sugam Sharma would like to acknowledge the CodeX at Stanford Law School, Stanford University, USA, where he is the regular participant in the CodeX meets. This has helped him to better understand the contemporary research and future trends in Legal Informatics arena. The authors also acknowledge Professor Santosh Kumar of Dar- Es-Salaam University to help review the mathematical content of this paper. The authors would like to acknowledge Shwetank Shekhar Dubey, News Editor, Times of India for his help in editing.

For citation: Sharma S., Shandilya R., Dwivedi D., Pant M. (2024) *e-Legalls-as-a-Service*: Towards Developing Cloud-based Legal Tech System to Aid Lawyering in the Digital Age. *Legal Issues in the Digital Age,* vol. 5, no. 3, pp. 129–153. DOI:10.17323/2713-2749.2024.3.129.153

Introduction

Legal Tech Jurisprudence has not started to evolve as one would have hoped for in comparison to other domains of law. Emerging technologies have time and again proved their mettle by serving humans and benefiting humanity as well. Field that has the most impact on our daily lives is Law and that fraternity has ignored the technologies largely till date. After pandemic hit, there was a

huge hue and cry for usage of virtual courts in many countries and this was not only from practicing lawyers, but also from judiciary too. One cannot agree more than ever that legal court system needs to change its functioning on day-to-day basis and must involve as much technology as possible. Lawyers will have to come to terms with technology as a helping mechanism and not an enemy of sorts. In the past, scientific communities, along with legal scholars and computer scientists, have initiated communications to converge together their isolated expertise and efforts to energize a judicial system with the potential and power of modern technologies like Artificial Intelligence (AI), Machine Learning (ML), Deep Learning (DL), and Natural Language Processing (NLP), etc.; and, concept of applying modern technologies in legal domain is termed as Legal Informatics (LI).

As evolution of LI and LI-enabled models has been relatively slower and, therefore, it requires swift advancements to upgrade and to eventually become part of Legal Tech Jurisprudence. In developing countries with large population, like India, technological urgency to enhance the legal system with LI capabilities is more manifested. In Indian Legal System, court proceedings are very slow and number of cases are very high, and as a result, the decision-making process to react final verdict often takes too long, sometimes decades. It has been often reported that the Indian Justice System lacks requisite number of judges to adjudicate current, pending and piled up court cases. Although, the argument may be true in nature, but it does not help towards the betterment of system. Hence, possibly by the motivation being manifested by the success of technological advancements in other fields of study, the legal community has started exploring the possibilities of usage of technology in the system of law (LI) and, therefore, some thin traces of LI are witnessed in literature today. Currently, some of the visible LI developments globally include the conversion of paper form of legal documents, such as court proceedings and cases into digital form, research and development (R&D) of AI exploration in jurisprudence aiming to produce efficient software tools to search and extract digital documents from legal corpus; a few legal software tools are aiding, particularly, legal scholars and experts in reporting searched cases in a graph with their citations as nodes and vertices, respectively. Although, the development of LI is slow, any major change is yet to be seen where law and justice stand firm with its expectations and promises to be faster, fair and financially feasible, even for the feeble and frail fraternities.

The legal court system primarily consists of three main players — judge, lawyer, and parties involved in litigation. The lawyer is an integral,

indispensable and intrinsic part of a judicial system and is the primary and only connection between judge and parties; lawyers also share the ethical responsibilities of ensuring smooth proceedings and fair justice delivery. Although, each aspect of jurisprudence is in need of urgent and swift technological intervention to ameliorate them; however, the efforts in this paper are focused mainly on improving the lawyering aspect and to facilitate lawyers in their case-related activities. In this digital era, a majority of lawyers or attorneys still deal with their cases on paper, overflowing their dockets. Management of these long documents, and also dockets, often is a challenge for the lawyers and always involves additional unproductive time consumption, which also somewhere directly or indirectly contributes to the delay in justice delivery. There is a viable possibility and a good scope of improvement on this front and in this research work, we provide a technology-enabled computational solution, called *eLegalls* (prototype), for lawyers so they can manage and handle their cases efficiently. The *eLegalls* is architected to be lawyer-centric, equipped with several pertinent features and functions that are highly beneficial to lawyers in their case management activities and effectively discharging their duties in an efficient manner. To make *eLegalls* more robust, secure, affordable and easily accessible, we further leverage another popular service delivery technology, cloud computing, and propose to deliver *eLegalls* as eLegalls-*as-a-service (eLaaS)*.

The remaining paper is structured as follows. Literature on contemporary LI research is compiled in Section 2. Section 3 briefly explores basic cloud computing technology and also outlines its expansion into legal context. Section 4 illustrates architecture of *eLegalls*, with focus on its lawyering core. In Section 5, technical development and implementation of *eLegalls* prototype are illustrated with pertinent test cases. Section 6 discusses current legal tech landscape and outlines some interesting LI-enabled emerging legal techs along with their classification, including *eLegalls*.

1. Literature Review

J.B. Ruhl et al. consider legal systems are complex systems and the use of complexity science can help produce better and improved legal system [Ruhl J.B. et al., 2017: 1377–1378]. The study of conventional legal system is majorly based on empirical observations with unnoticeable scientific experimentation and has not explored various perspectives of complexity

science yet. The complexity of legal system is bound to grow in near term, which consequently will push legal industries to investigate new technological solutions and support and to expand technology footprints in legal domain. The complex legal systems always produce complex datasets with distinctive compositions, for example- case decisions, executive orders, legal regulations, legal contracts, legal records, legal opinions, networks and citation networks of cases (Figure 1), etc. Big data science, in combination of modern IT and its allied AI, ML, DL, and NLP technologies, is expected to reshape the traditional legal studies and to improve skills and pragmatic understanding, which ultimately will ameliorate and upgrade the quotidian legal operations. Complexity science when introduced into legal research is anticipated to open avenues to address intrinsic legal questions and concerns, that may help elevating and enhancing a judicial system and refining policy-making to match the societal expectations from legal system. Goswami's thesis on LI primarily explores the information retrieval of legal data, which is dubbed as legal information retrieval (Legal IR). Legal IR retrieves legal documents, for example, legal judgments, case laws, acts, articles, etc. Legal documents are generally exceptionally lengthy and also are written in complex legal language with long sentences; lawyers and other legal experts often require to refer these court documents in their work-related activities. However, legal language complexity and convoluted lengthy legal sentences make their comprehension tedious and tardy. To address this issue, Goswami relies on supervised algorithm and created an auto catchphrase retrieval mechanism for legal content to draw catchphrases out of complex court judgement to impart the gist to quickly understand a judgment. LegalIR runs on database of court judgments,

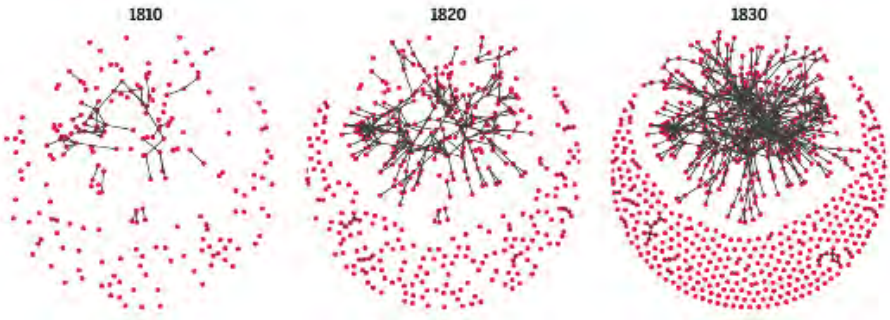


Fig. 1. United States Supreme Court citation network (1805–1835) (Ruhl et al., 2017). Nodes are the Cx(s) and the edges are citations of the Cx(s). The Cx(s) citation span is (1791–2015)

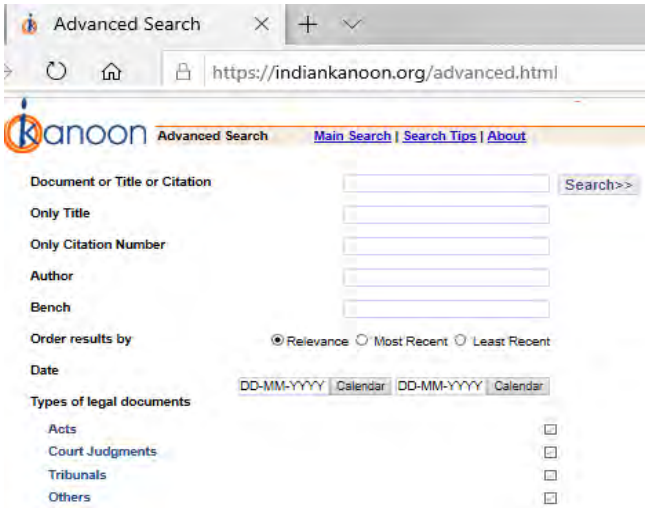


Fig. 2. Indian Kanoon search engine

Source: https://indiankanoon.org/advanced.html.

acts, legal articles, etc. and outsmarts Indian Kanoon (Figure 2) and Manupatra (Figure 3), the online search engines for Indian jurisprudence, in efficiency and accuracy [Goswami J.J., 2018]. Lettieri et al. investigate the possibilities and potential benefits of applying computer visualization in legal domain and called it Visual-LI [Lettieri N., Malandrino D., 2018: 241–246]. Know Lex [Lettieri N., Altamura A., Malandrino D., 2017a: 332–345] (Figure 4), which is equipped with several efficient features, provides the thorough visual analyses of legal documents through its online web interface. The objective of development of Know Lex is to provide a testbed to legal community to study and understand relationships of heterogeneous legal documents. EU Case Net [Lettieri N., Altamura A., Faggiano A., Malandrino D., 2016: 56] (Figure 5) can be considered as a web-based testbed to extensively support to conduct study to develop new tools and techniques for analytics on legal corpora. The objective is to create an online laboratory for legal community to study legal science and legal system in Europe. The study examples include, better understanding of case network of the European Court of Justice (ECJ) of law, conducting visual analytics on ECJ judgements to deduce relevant observations. Crime Miner [Lettieri N., Malandrino D., Vicidomini L., 2017b: 32–54] (Figure 6) equips investigators to find innovate techniques to study and explore crime and its societal implications. Crime Miner offers mining, visualization and analytics operations and SNA techniques to investigate and understand

Fig. 3. Manupatra online legal research

Source: http://www.manupatrafast.com.

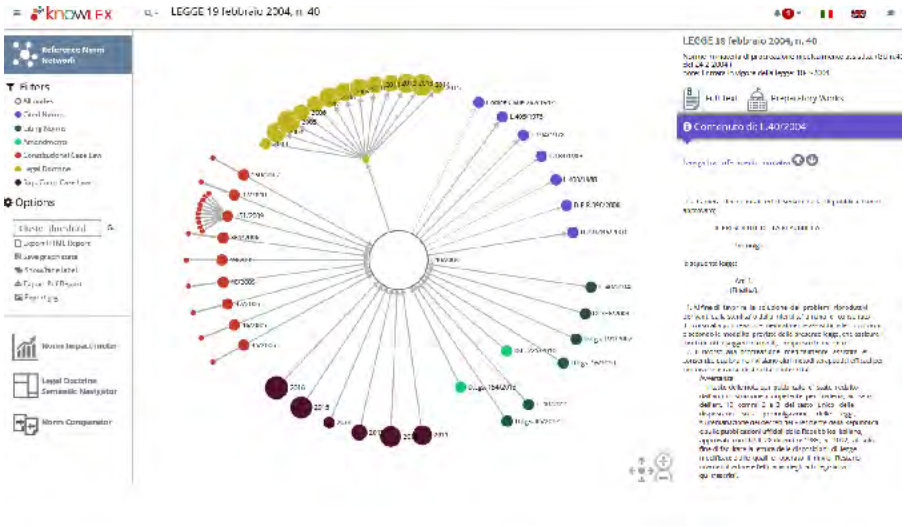


Fig. 4. KnowLex: the Norm Graph Navigator

behavioral and functional patterns of notorious individuals or entities from crime database, which includes phone tapings and personal records with former represents edge and latter is a node or vertex of a graph in SNA data analysis to understand and manifest the connection of individuals or entities complicit in phone conversations. Typically, legal documents are generated

Fig. 5. EUCaseNet: Citations network graph of the first 350 judgments in terms of in-degree and their citation network

Fig. 6. CrimeMiner: The wiretaps graph

in a regulated standard format with smaller font size and thin line spacing and are excessively lengthy. Also, the language of written legal documents is highly technical, flooded with legal jargons, and consequently, is beyond

easy comprehension of an ordinary educated individual with no prior legal understanding. The words and expressions in legal documents are interpretable to various meanings, which potentially change legal discourse and consequently the outcomes. As a result of above, a reader does not fully understand a legal document and also legal communication easily and often requires support from legal experts. Therefore, the notion of design patterns from the IT world is injected into legal document design as an important instrument. Design patterns providing solutions to legal design issues, help to develop legal documents in various simple formats, highly suitable for ordinary readership with no legal domain knowledge. In recent times, several good legal design patterns are introduced, but are underused mostly, probably because of the missing central legal design patterns repository; consequently, searching for a pertinent design pattern becomes a tedious process. Therefore, in the view of rehashing and tailoring complex legal documents to be coherent and comprehensible to a specific audience, A. Rossi et al. have created a design language to restructure the legal design patterns into a desired format. The goal is to gather and accumulate the dispersed, disorganized, and diverse legal resources and solutions and then to attach relevant examples and contextual descriptions to them to improve their utilization and to smoothen the legal communications throughout in legal domain [Rossi A., Ducato R. et al., 2019: 517–526]. Waltl et al. are the first few investigators, who study the possible use of AI in LI, more specifically, the explainable AI, which potentially can enable tagging of proper explanations along with the court decisions in a judicial process. The authors suggest that explainablility in AI can be an additional intrinsic category of ML algorithms, see: [Ruhl J. B. et al., 2017: 1377–1378].

2. Cloud Computing in Legal Space

In recent years, cloud computing has emerged as a powerful and revolutionary service-oriented delivery paradigm, primarily because of its on-demand and abstract architecture for complex, large-scale, and data-intensive applications [Alam T., 2021: 108–115]; [Sharma S., 2015]; [Varghese B., Buyya R., 2018: 849–861]. The on-demand nature of cloud paradigm makes it highly cost-effective to users; and also, as cloud environment hides the software-supported complex hardware infrastructure and its cumbersome and overwhelming technical details from the end users, this together encourages them to avoid establishing an expansive local server-level hardware infrastructure and rather offload their complex

applications into cloud. The cloud services are still broadly classified into three traditionally categories:

Infrastructure-as-a-Service (IaaS). This is an important paradigm of cloud environment, which is being used heavily in practice globally. The IaaS model provides the complex infrastructures as simple abstract services to the end users. The enterprise IT infrastructures are constituted by various several comprehensive software, hardware and network resources organized in a more modular fashion; and this modularity facilitates easy customization of the environment to accommodate and support the varying needs of the end users. Amazon Web Services (AWS) [Wittig M., Wittig A., 2018] is the most popular and widely used commercial cloud IaaS model today.

Platform-as-a-Service (PaaS). As name suggests, PaaS model facilitates and provides a secure, mature, and vigorous but flexible platform to the users, where they can develop software systems. The platform is furnished with all the necessary software artifacts; platform itself can either be housed in a localized hardware environment, belonging to a PaaS provider or be served through IaaS. A PaaS cloud can be accessed and used either by PaaS specific APIs or GUI. Google App Engine [Python J., Go P., 2015: 35] is one of the most popular PaaS cloud platforms.

Software-as-a-Service (SaaS). SaaS is a highly popular and most used resource-rich and repository-intensive cloud paradigm, which provides the software to end users in the form of service. The SaaS repository is composed of a sea of diverse sets of simple and complex software services, which are readily available to use. Google [Geewax J. J. J., 2018] as SaaS provider is providing several software as SaaS service, for example Gmail, Google Doc, etc. A SaaS provider owns up full responsibilities to deliver operational services and also its underlining intertwined hardware and software infrastructure. Most SaaS vendors also support their users with efficient GUIs to offer easy and smooth interaction.

Because of on-demand nature, easy accessibility and integration, flexible and affordable (pay as you) pricing model, the cloud computing acceptability has grown across almost all the domains such as healthcare, medicine, business, data science (*Data-as-a-Service*, *Data Integrity-as-a-Service*, *Data Mining-as-a-Service*, *Database-as-a-Service*) [Sharma S.,

2015], etc. In legal domain, most of the discussion is still centered around the legal issues triggered due to inception and evolution of cloud computing itself as disruptive technology such as data (in cloud) privacy and security violation, data breach and loss, hacking, copyright infringement liability, etc. [Morningstar Law Group, 2015]. The cloud data and service usage across cross-borders has further added the legal complexity such as who owns the data and service, who has legal jurisdiction over the cloud data and services, etc., [Reingold B., Mrazik R., D'Jaen M., 2010: 1-6]. Nations are developing new rules, regulations, laws, litigations, and jurisdictions to address the above-mentioned legal issues. The United States has now enacted and established the CLOUD Act, which enables it (with other foreign countries and vice-versa) to lawfully access the data, stored off-shores, required on court orders [Mulligan S. P., 2018: 3–28].

Although, the LI space is still evolving [Sharma S., Gamoura S., Prasad M.D., Aneja A., 2021: 218–235], however, with its evolution, the cloud-usage in legal world is gradually expanding; more and more legal entities are growing and adopting cloud environment for their service and legal data delivery [Corrales M., Fenwick M., Haapio H., 2019]; [Murley D., 2009: 101]; [Dykstra J., Riehl D., 2012: 1]; [Black N., 2013: 593]. And this motivates us also to develop *eLegall*s in a way, which could be easily and smoothly deployed and served from cloud environment as an effective SaaS model and we propose to deliver it as *eLegalls-as-a-Service*.

3. Design and Architecture

In this section the design and architecture aspects of the system are illustrated with special focus on lawyering support of *eLegalls*. Various elements, integrated with the system are also depicted. Also, formal definition is given to core constituents of *eLegalls* from the theory building point of view and theirs abbreviation are summarized in Table 1 [Sharma S., AL R. S., 2021:16–31].

Table1. Abbreviation of *eLegalls* terms

S. No.	Term	Abbreviation
	Victim	V_L
	Complainant or plaintiff	CP_L
	Case, complaint or report	C_x

S. No.	Term	Abbreviation
	Litigant	L_L
	Lawsuit	L_x
	Accused or defendant	AD_L
	Police or law enforcement agency	P_AL
	Lawyer, advocate or attorney, litigator	L_AL
	Judge or magistrate	J_L
	Judiciary, jurisprudence, judicial system, or court of law	J_CL

1. Victim (V_L) is defined as an individual, who experiences suffering as a result of the action of someone ($AD_L(s)$).

2. Complainant or plaintiff (CP_L) is defined as any individual who reports the case against the $AD_L(s)$ in a PA_L *or* JC_L.

3. Case/Complaint (C_x) is defined as the written document deposited to the $PA_L(s)$, with the detailed information about the event that agonizes V_L or CP_L.

4. Litigant (L_L) is associated as a party in a C_x as $V_{L,}$ $AD_{L,}$ or CP_L.

5. Lawsuit (L_x) is dubbed as C_x submitted to the JC_L by a CP_L for adjudication or arbitration.

6. Accused or defendant (AD_L) is someone -individual, group, or entity- who stride to defend themselves in a JC_L on the $C_x(s)$ against them.

7. Police or law enforcement agency (PA_L) is the government-run entity, which is responsible to administer, implement and enforce the good laws and order.

8. Lawyer, advocate or attorney, litigator (LA_L) is someone, who has undergone rigorous educational training to study and understand the laws and the legal system and subsequently is authorized to practicing the law. The $LA_L(s)$ advocate and argue in a JC_L with the aim to derive the decision and final outcome in favor of their clients.

9. Judge or magistrate (J_L) is someone, who is equipped with government-enabled authorities, responsibilities, and power to adjudicate the $C_x(s)$, presented in the JC_L before him/her and delivers the fair judgements eventually in JC_L.

10. Judiciary, jurisprudence, judicial system, or court of law (JC_L) is a system, which consists of the people with judicial understanding and government-enabled authority and power to resolve the $C_x(s)$ or $L_x(s)$ and other disputes through the fair adjudication and arbitration.

Figure 7 depicts the architecture of *eLegalls-as-a-Service*. The core components of system are *eLegalls* and $LA_L(s)$ and Law Firm(s). It can easily be seen that *eLegalls* is hosted in cloud along with its dedicated *Data Store*, which consists of (relational) *Database* and *Files* storage in the cloud as well. The *Database* is relational in nature and contains relevant textual data. The *Files* storage houses the large legal documents and the information to access these documents are stored in tables of relational *Database* object. The architecture also shows abstraction of prominent functional services, offered under *eLegalls-as-a-Service* — 1) *Register new lawyer,* 2) *Update case status*, 3) *Case status*, and 4) *Create a new case*.

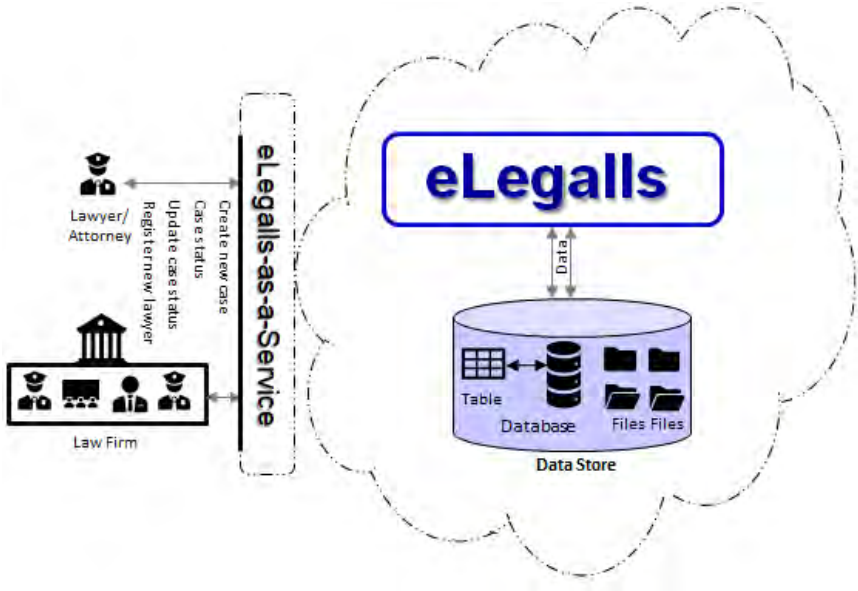


Fig. 7. Architecture of eLegalls-as-Service. In this figure, it can be easily observed, the eLegalls system resides in cloud and is served as eLegalls-as-Service to external world, particularly, lawyers/attorneys or law firms. The Data Store consists of Database and Files storage components, which store the related legal data in relational format (tables) and files such as legal documents

4. Development and Implementation of *eLegalls* System

Figure 8 is the design mockup of *eLegalls*, which primarily consists of following modules -*Report new case*, *Case status*, and *Lawyer*. Although, similar to the complex nature of legal system, the design of *eLegalls* in its entirety is quite complex, but for simplicity and easy understanding, a basic section is shown here. As mentioned earlier, in this paper, the focus is to illuminate the lawyering core of *eLegalls,* therefore, in this design image, the *Lawyer* module is shown selected and active, where a LA_L (with dummy name "*R J Malani*") is logged in. After successful logging, LA_L is able to perform several tasks such as "*Add new comments"* to update case status of an existing C_x, *"Upload new file"* to upload new legal documents, etc.

Fig. 8. Basic design mockup of eLegalls

In the following section 5.1, we further explore the implementation aspect of lawyering-centered basic components of *Lawyer* module; the demonstration of each item is supported by a pertinent use case scenario. And thereafter, in section 5.2, we briefly explain the technologies used for

the implementation; also highlighted in this section is the data model, which suffices current data engineering needs and also will be potentially able to accommodate the scalability and high availability system requirements.

4.1. Lawyer module implementation

eLegalls's Lawyer module is highly beneficial and immensely useful to $LA_L(s)$ in their C_x management and to help them better prepare with the organized and updated documents to effectively aid their lawyering activities and advocacy in JC_L(s). The *Lawyer* module consists of a few submodules and each one of them is independently development and implemented.

4.1.1 New LA_L to eLegalls

To operate and avail the *eLegalls* system, the new LA_L has to register with it for the first time through a simple but secure user interface (see Figure 9). During the registration process, the system requires the LA_L to enter pertinent information such as *Bar ID*, *Expertise*, etc. along with the important documents, which are to be uploaded. Upon the successful registration, the system sends a confirmation auto email to the LA_L, which also carries the confidential login credentials. The accuracy of the LA_L*'s Expertise* parameter is crucial to the system as this information is later used to match the C_x types to suitably assign it to the most appropriate $LA_L(s)$. Presently, the *eLegalls's* prototype functions with some basic authentication mechanism, however, as the prototype advances and expands into a mature product, a more sophisticated and robust authentication process such as AD, LDAP, etc. will be integrated into the system [Vazquez A., 2019: 123–155].

4.1.2 Existing LA_L login

Figure 10 is the user interface developed in this module; this enables a registered LA_L for the successful login. The interface requires the LA_L *to* input the correct login credentials, which were sent to him/her through the auto email during the first-time registration process. In case, if a LA_L forgets the credentials or has not yet registered with the system, this interface also provides links to navigate a LA_L to other appropriate interfaces.

4.1.3. Case status update by LA_L

The module is quite important and useful for $LA_L(s)$ when it comes to management and updating of a C_x in *eLegalls* system. Figure 11 shows that

Fig. 9. Lawyer (New LAL registration). This sample example demonstrates, how a new LAL can register themselves with eLegalls system. After the successful submission, the system sends an auto email to the LAL with the login credentials

Fig. 10. Lawyer (Existing LAL login) - This interface assists the LAL to login using the valid credentials.

a new C_x is created and system has assigned an auto generated unique C_xN (L87020445290010) to this C_x. This C_xN is used to surf and search this C_x throughout all the use case examples.

On successful login (in Figure 10), a LA_L is navigated to graphical interface, which facilities LA_L to retrieve the entire most up-to-date case history and to further update C_x status. Figure 12 provides a use case example of a C_x update scenario. The LA_L enters C_xN (L87020445290010) into the designated field and a single click on "Go" button renders entire C_x status. The LA_L decides to update a C_x status and adds more content to it. The newly updated content becomes immediately available in C_x status display with the valid C_xN and this example scenario is shown in Figure 13.

4.2. Frontend and backend technologies

The *eLegalls* prototype is developed in modular design using modern computer technologies. The frontend and backend of the system are

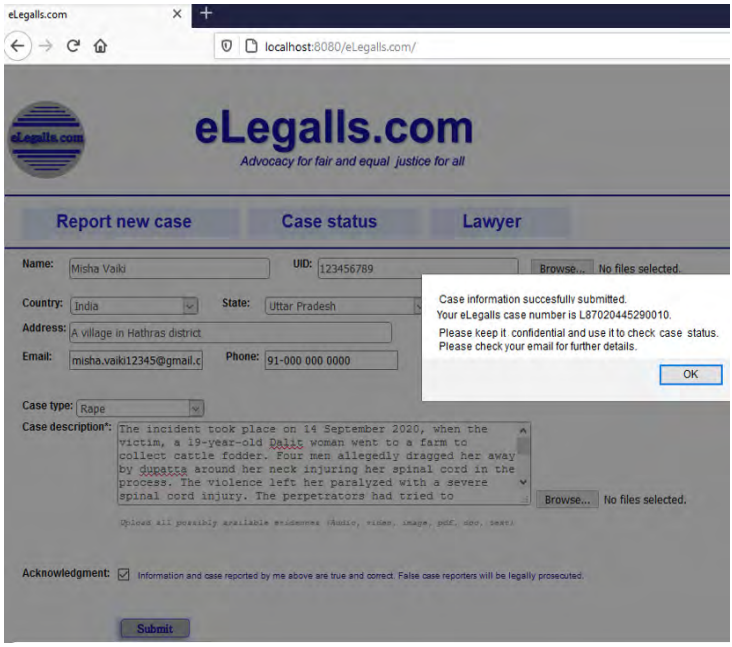
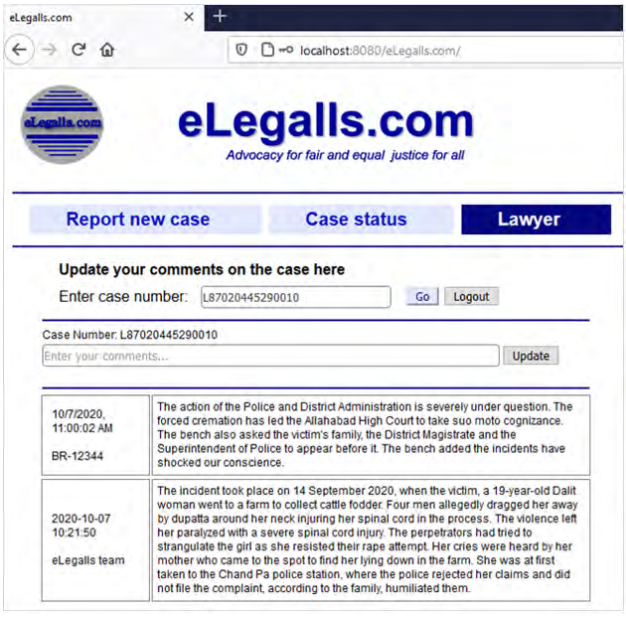


Fig. 11. Create a new case in eLegalls system- This interface enables the process to generate a new Cx. On the successful submission of a Cx, the eLegalls generates a confidential and unique identification number (CxN) for a Cx. This CxN is tagged with a Cx and is used as a reference for that Cx

Fig. 12. Lawyer (Case status update (LAL)). A click on Go button with a valid Cx number entered, renders the textbox to update the Cx status. The authorized LAL can enter the long comments and clicks on the Update button.



F*ig. 13.* Lawyer (Case status update (LAL)). A click on the Update button prepends the new comments to the Cx status list. The newly updated comments are readily available to the LAL and CPL or a VL (with valid Cx number) tout de suite to view and read.

implemented using the following programming languages — J2EE 1.8, Servlets, Jsp, Jspf (Java server pages fragments to improve code security), Html 5, JQuery, and CSS. The project is developed, built, integrated and tested in Eclipse Juno integrated development environment (IDE) [Araujo R.F., 2013]; [Hickson I., Berjon R., Faulkner S. et al., 2016]. In *eLegalls* software prototype development, modular design is further enforced by enabling and implementing efficient software design patterns such as DAO [Ngaogate W., 2020: 27–31]. Additionally, to have clean and compact code in development process, annotation-based codebase programming is preferred wherever possible [Guérin S., Polet G., Silva C. et al., 2021]. The data engineering, management and data transition in *eLegalls* system are facilitated through SQLite relational data model [Oh G., Kim S. et al., 2015: 1454-1465].

5. Discussion on Legal Tech Landscape

One of the primary objectives of emerging LI research and innovation is to alleviate deeply rooted and globally pervasive manual activities in jurisprudence and to exploit the unbounded benefits of the IT and its allied modern technologies to achieve it. More specifically, evolving LI has great potential to develop the manual legal and litigation procedures, practices, and proceedings into an efficient and automated civil justice system with some degree of intelligence. AI-supported LI systems are expected to predict $C_x(s)$ outcomes with high degree of accuracy and therefore, can aid speeding up decision delivery of $C_x(s)$, when augmented with $J_L(s)$ and within $JC_L(s)$. Furthermore, these predicted outcomes at early stage can be immensely advantageous to $CP_L(s)$, $AD_L(s)$, and $LA_L(s)$; specifically, $LA_L(s)$ can repeatedly adjust the input parameters and produce more refined predictions and eventually achieve the most beneficial outcome to their $C_x(s)$. As a result, the most optional final input parameters can be used as supportive factors by $LA_L(s)$ to defend and substantiate their arguments in JC_L to improve, enhance and strengthen the winnability of their $C_x(s)$. In their recently published overarching work on legal tech and its impact on civil procedure, Engstrom and Gelbach have extensively elaborated on current status and future evolution of legal tech [Engstrom D.F., Gelbach J.B., 2020], which is the basis and motivation of this discussion that is primarily centered around the emerging legal techs. In recent years, LI research and LI-enabled legal techs have slowly begun to develop their minuscule footprints; however, substantial LI research presently is still

practically futuristic, formulaic, and foreseeable with remote imagination to realization of robot-judges [Markou C., 2017]; [Volokh E., 2019] and robot-lawyers [Fitch A., 2020]; [Merchant G., Covey J., 2018]; [Markovic M., 2019: 325]. As, LI research inevitably expands, LI-enabled legal tech space inexorably expands, and as a result, the scope of disruptive stress by the legal tech evolution on existing jurisprudence also expands; which further raises some critical questions about adaptability of emerging LI-enabled new legal tech world, filled with unbounded technical challenges, by JC_L*'s* active players, particularly, $J_L(s)$ and $LA_L(s)$; additional obvious concerns are related to the momentum of adoptability, how swiftly, these legal actors are able to accommodate the convoluted complexities and tedious intricacy of new legal tech, when new modern legal tech world begins to rejig, reorganize, and revolutionize the existing civil procedure and civil justice system. The growth of LI-enabled legal tech arena is expected to affect all major legal players of JC_L and strikes on two key challenges- overly lengthy legal procedure and proceeding's time which often runs through years to decades, and extremely unaffordable financial stress, incurred and imposed due to JC_L proceedings.

For better understanding the entire legal tech space, it is advisable and important to segregate them into an appropriate category based on the nature of operations. Therefore, in this section, the emerging legal tech world is further fragmented into a coarser classification.

Legal matchers assess the given expertise of $LA_L(s)$ and aid matching the perspective $CP_L(s)$ to $LA_L(s)$. Additional support to $LA_L(s)$ includes basic operations such as maintaining legal records of $C_x(s)$. Examples — Ravel[1], Lexicata[2], Atticus[3], Avvo[4], etc.

Legal searches aid $LA_L(s)$ in smooth and easy searching of legal documents of their interest, e.g. case decisions, legal proceedings, statutes. Examples are: Judicata[5], Case Text[6], etc.

Legal decision predictors auto predict probable decision of $C_x(s)$ or $L_x(s)$ with a good degree of accuracy. The end users, particularly LA_L(s), can

[1] home.ravellaw.com (accessed: 20.05.2022)

[2] clio.com/?cta=lexicata (accessed: 16.12.2023)

[3] atticus.com (accessed: 20.05.2022)

[4] avvo.com (accessed: 29.12.2023)

[5] judicata.com (accessed: 16.12.2023)

[6] casetext.com (accessed: 12.04.2024)

generate various outcomes of C_x/L_x, based on varying inputs; and, can exploit such input/output combinations to properly formulate, drive and strengthen their future legal arguments for the same C_x/L_x in $JC_L(s)$. Examples are: Case Crunch[7], Lex Machine[8], eLegalls[9], etc.

Legal analytics facilitate $LA_L(s)$ to perform extensive analyses on various legal documents of distinct nature. Examples are: Gavelytics[10], Fast Case[11], etc.

Legal document discovers enable the detection and discovery of relevant documents during legal process and proceeding and label them suitably to the C_x at hand. Examples are: Exterro[12], Everlaw[13], etc.

Legal document developers offer various types of templates of legal documents to aid $LA_L(s)$ to further designing, drafting and developing final and fair simple, moderate and complex legal documents. Examples are: Rocker Lawyer[14], Legalmation[15], etc.

Legal managers are legal tech graphical dashboards, which offer and enable $LA_L(s)$ to administer numerous business operations. Examples are: Brevia[16], Law Geek[17], United Lex[18], Ravn[19], etc.

Legal auto assisted servers are online platforms, which aid and offer legal advice, and legal resolutions in lawsuits and disputes, especially to destitute, $CP_L(s)$ and $AD_L(s)$. Examples are: Legal Zoom[20], Nolo[21], Modria[22], etc.

---

[7] case-crunch.com (accessed: 20.05.2022)

[8] lexmachina.com (accessed:16.12.2023)

[9] elegalls.com (accessed: 16.12.2023)

[10] gavelytics.com (accessed: 30.06.2024)

[11] fastcase.com (accessed: 12.04.2024)

[12] exterro.com (accessed: 16.11.2023)

[13] everlaw.com (accessed: 16.11.2023)

[14] rocketlawyer.com (accessed: 30.06.2024)

[15] legalmation.com (accessed: 16.11.2023)

[16] ebrevia.com (17.01.2024)

[17] lawgeex.com (16.11.2023)

[18] unitedlex.com (accessed: 25.12.2023)

[19] imanage.com/product/artificial-intelligence (accessed: 25.12.2023)

[20] legalzoom.com(18.09.2023)

[21] nolo.com(accessed: 18.09.2023)

[22] tylertech.com/products/Modria (accessed: 16.11.2023)

Majority of the above legal tech examples are based on IaaS, PaaS or SaaS paradigm of cloud computing technology and serve their users in flexible and affordable pay-per-service mode. Although, the classification above is backed up by a smaller set of legal tech examples for each class, but some of them are likely to cut across multiple categories.

Similarly, our *eLegalls* system is also based on SaaS cloud model and is proposed to serve the end users as *eLegalls-as-as-Service*. The fully developed and completely operational *eLegalls* will also intersect through multiple classes — *Legal matcher* and *Legal managers*. Presently, global legal tech landscape is yet sparsely developed and most of these tech tools are still in their nascent stages. However, with rapid upward trajectory of LI and LI-research, faster growth of LI-supported legal tech tools is also inexorable, which will potentially restructure, reshape and transform the current jurisprudence into a faster, fair, and cost-effective civil justice system.

Conclusion

IT support into jurisprudence, globally, is still in nascent stage and legal world has not yet accessed and exhausted the full potential of IT and its allied technologies; they are: AI, ML, DL, NLP, etc. Particularly, in underdeveloped nations, IT-driven legal ecosystem is apparently either remote or rather imaginary as there are not even thinner traces of LI-centered communications exist yet in several such nations. In developing nations with even enough digital progress and infrastructure, the enthusiasm and manifestation for serious efforts to reshape, repair and transform the senile, lax, and leaden legal system into a LI-enabled faster and fair jurisprudence are yet to be seen. In $JC_L(s)$, legal procedures and practices largely are continued to be conducted and executed in archaic manner. $LA_L(s)$, who are important and inseparable constituents of $JC_L(s)$ still manage and administer their lawyering activities in mediaeval manual fashion, which when viewed from modern digital tech era, cannot be considered -time and effort- efficient. As LI technology evolves, $LA_L(s)$ should also explore new methods and mechanisms.

In that paper we designed, developed and implemented a cloud-based legal tech solution, *eLegalls,* for $LA_L(s)$ as an alternative to their current burdensome and cumbersome lawyering in digital age. *eLegalls* is to aid efficient handling of lengthy legal documents and legal contracts and better managements of legal $C_x(s)$. *eLegalls*, that proposedly serves as a SaaS-

based cloud technology, *eLegalls-as-a-Service*, potentially replaces most manual efforts and $C_x(s)$ management activities of $LA_L(s)$ and equips them with appropriate technology and assists with technology-drive lawyering. Future work includes the expansion of *eLegalls* to further enrich it with more in-need features and functions with the goal to completely eliminate manual efforts and needs of $LA_L(s)$ in handling and managing their $C_x(s)$. Eventually, *eLegalls* will be shaped into an efficient, effective, and robust LI-enabled cloud-based legal tech, which serves and contributes towards emancipating $JC_L(s)$ from archaic, outmoded, and obsolete practices.

References

1. Alam T. (2021) Cloud Computing and its role in the Information Technology. *IAIC Transactions on Sustainable Digital Innovation,* vol. 1, pp. 108–115.

2. Araujo R.F. (2013) Getting Started with Eclipse Juno. Mumbai: Packt Publishing, 256 pp.

3. Black N. (2013) Lawyers, Cloud Computing, and Innovation: How Cloud Computing Facilities Innovation in the Delivery of Legal Services. *ISJLP*, no. 9, p. 593.

4. Corrales M., Fenwick M., Haapio H. (eds.) (2019) *Legal Tech, Smart Contracts and Blockchain*. Singapore: Springer, 276 p.

5. Dykstra J., Riehl D. (2012) Forensic collection of electronic evidence from infrastructure-as-a-service cloud computing. *Richmond Journal of Law & Technology*, vol. 19, p. 1.

6. Engstrom D. F., Gelbach J. B. (2020) Legal Tech, Civil Procedure, and the Future of Adversarialism. *University of Pennsylvania Law Review*, vol. 169, p. 1001.

7. Fitch A. (2020) Would You Trust A Lawyer Bot with Your Legal Needs? *Wall Street Journal*. 10 August.

8. Geewax J.J.J. (2018) Google Cloud Platform in Action. N. Y.: *Simon and Schuster, 632 pp.*

9. Goswami J.J. (2018) Legal Informatics. Doctoral dissertation. Dhirubhai Ambani Institute of Information and Communication Technology.

10. Guérin S., Polet G., Silva C. et al. (2021) PAMELA: an annotation-based Java Modeling Framework. *Science of Computer Programming*, p. 102668.

11. Hickson I., Berjon R., Faulkner S. et al. (2016) HTML5. A vocabulary and associated APIs for HTML and XHTML. *W3C Recommendation*

12. Lettieri N., Altamura A., Faggiano A., Malandrino D. (2016) A computational approach for the experimental study of EU case law: analysis and implementation. *Social Network Analysis and Mining*, vol. 6, no. 1, p. 56.

13. Lettieri N., Altamura A., Malandrino D. (2017a) The legal macroscope: Experimenting with visual legal analytics. *Information Visualization*, vol. 16, no. 4, pp. 332–345.

14. Lettieri N., Malandrino D. (2018) Cartographies of the legal world. Rise and challenges of visual legal analytics. In: 22nd International Conference Information Visualization, pp. 241–246. IEEE.

15. Lettieri N., Malandrino D., Vicidomini L. (2017b) By investigation, I mean computation. *Trends in Organized Crime*, vol. 20, no. 1–2, pp. 31–54.

16. Marchant G., Covey J. (2018) Robo-Lawyers. *Litigation Journal*.

17. Markou C. (2017) Are We Ready for Robot Judges? *Discover Magazine*. Newsletter, pp. 1–3.

18. Markovic M. (2019) Rise of the Robot Lawyers. *Arizona Law Review*, vol. 61, p. 325.

19. Morningstar Law Group (2015) The Laws of Cloud Computing: Weathering the Storms of Cyber piracy, Hacking, and IP Infringement. Available at: https://morningstarlawgroup.com/insights/cloud-computing-legal-issues/ (accessed: 16.04.2023)

20. Mulligan S.P. (2018) Cross-border data sharing under the CLOUD Act. *Congressional Research Service*, pp. 1–28.

21. Murley D. (2009) Law libraries in the cloud. Retrieved from Law library Journal, vol. 101, no. 2. Available at: http://www. aallnet. org/main-men/publications/ilj/LLJArchives/Vol1-101/pub_iij_v10l (accessed: 20.11.2023)

22. Ngaogate W. (2020) Integrating Flyweight Design Pattern and MVC in Development of Web Application. In: Proceedings of 2nd International Conference on Information Technology and Computer Communications, pp. 27–31.

23. Oh G., Kim S. et al. (2015) SQLite optimization with phase change memory for mobile applications. *Proceedings of the VLDB Endowment*, vol. 8, no. 12, pp. 1454–1465.

24. Python J., Go P. H. P. (2015) Google App Engine. *Development*, vol. 1, p. 35.

25. Reingold B., Mrazik R., D'Jaen M. (2010) Cloud Computing: Whose Law Governs the Cloud? Part III. *Legal Works, West Law*, pp. 1–6.

26. Rossi A., Ducato R. et al. (2019) Legal Design Patterns: Towards A New Language for Legal Information Design. In: Internet of Things. Proceedings of the 22nd International Legal Informatics Symposium IRIS. Weblaw, pp. 517–526.

27. Ruhl J.B. et al. (2017) Harnessing legal complexity. *Science*, no. 355 (6332), pp. 1377–1378.

28. Sharma S. (2015) Evolution of as-a-Service Era in Cloud. *Ar Xiv preprint arXiv*:1507.00939 (accessed: 25.04.2022)

29. Sharma S., Gamoura S., Prasad M. D., Aneja A. (2021) Emerging Legal Informatics towards Legal Innovation: Current status and future challenges and opportunities. *Legal Information Management,* vol. 21, no. 3–4, pp. 218–235.

30. Sharma S., AL R.S. (2021) ELegalls: Enriching a legal justice system in the emerging legal informatics and legal tech era. *International Journal of Legal Information*, vol. 49, no. 1, pp. 16––31.

31. Varghese B., Buyya R. (2018) Next generation cloud computing: New trends and research directions. *Future Generation Computer Systems*, no. 79, pp. 849–861.

32. Vazquez A. (2019) Integrating LDAP with Active Directory and Kerberos. In: Practical LPIC-3 300. Berkeley (Cal.): Apress, pp. 123–155.

33. Wittig M., Wittig A. (2018) Amazon web services in action. N.Y.: Simon and Schuster, 552 pp.

34. Volokh E. (2019) Chief Justice Robots. *Duke Law Journal,* vol. 68, p. 1135.

Information about the authors:

S. Sharma — PhD, Founder/CTO.
R. Shandilya — PhD, Associate Professor.
D. Dwivedi — LLB, Advocate.
M. Pant — PhD, Professor.

The article was submitted to editorial office 10.04.2024; approved after reviewing 20.06.2024; accepted for publication 30.08.2024.

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.