https://doi.org/10.38044/DLJ-2020-1-1-24-38

ARTICLES

TRANSFORMATION OF LAW IN THE CONTEXT OF DIGITALIZATION: DEFINING THE CORRECT PRIORITIES

Elina L. Sidorenko[1,*], Pierre von Arx[2]

[1]Moscow State Institute of International Relations (MGIMO)
76, ave. Vernadsky, Moscow, 119454, Russia

[2]Swiss Federal Institute of Technology in Zurich, The OSCE Programme Office in Bishkek
6, Ryskulova str., Bishkek, 720001, Kyrgyzstan

Abstract

The subject under analysis is the peculiarities around the legal regulation of digital technologies and products arising from digital technologies. The choice of this topic was predetermined by the active development of digital services and digital financial assets, and the necessity to adapt modern legislation to the needs of the digital economy. Despite the fact that several strategies for the development of digital law are being worked out at the level of international organizations, neither in theory nor in practice is there a single understanding of the legal nature of digital technologies and the foundations of their legal regulation.

From this perspective, the purpose of this article is to understand the system and the main categories of the digital economy through the prism of fundamental legal institutions, based both on the traditional principles of scientific analysis and on the results steaming from applied data processing methods.

Using methods of theoretical modeling, idealization, and theoretical experiments, the authors consider the categories of legal personality, security, and tort of digital technologies and products, compare them with similar legal institutions, and determine possible options for integrating new legal categories into traditional rule of law on contracts, liability, and the protection of intellectual rights.

As a result of the study, the authors have assembled their vision of those benchmarks, on which international strategies for regulating the digital economy should be built. The authors proceed from the fact that the adaptive capabilities of traditional law are very limited in relation to digital technologies; furthermore, in relation to many of them, qualitatively new legal models should be developed. The article presents the results of a review of the main legal parameters of digital technologies. Formulations of legal personality and protection are proposed, definitions of digital technology products in civil and copyright law are formulated.

The conclusion reached concerns the inconsistency of approaches to assessing the legal nature of digital objects, and the insufficient consideration of the technical aspects of digital technologies, as well as the need to develop — at the international level — a unified legal strategy for civil and intellectual law regarding digital technologies. This study underlines, among the priority tasks and directions, the issues of legal personality of digital technologies, and the essential mechanisms for the protection of products using digital technologies. The conclusions formulated in the article have important practical and methodological significance, and can be taken into account when reforming the current legislation.

Keywords

digital technologies, legal personality, digital technologies as an object of legal protection, international strategies, legal responsibility, digital law, civil law, intellectual property object

Conflict of interest The authors declare no conflict of interest.

Financial disclosure The study had no sponsorship.

For citation Sidorenko, E. L., & von Arx, P. (2020). Transformation of Law in the Context of Digitalization: Defining the correct priorities. *Digital Law Journal, 1*(1), 24–38. https://doi.org/10.38044/DLJ-2020-1-1-24-38

* Corresponding author

Submitted: 20 Feb. 2020, accepted: 23 Mar. 2020, published: 20 Apr. 2020

СТАТЬИ

ТРАНСФОРМАЦИЯ ПРАВА В КОНТЕКСТЕ ЦИФРОВИЗАЦИИ: В ПОИСКЕ ПРИОРИТЕТОВ

Э.Л. Сидоренко[1,*], П. фон Аркс[2]

[1]Московский государственный институт международных отношений (университет) МИД России
119454, Москва, просп. Вернадского, 76, Россия

[2]Швейцарский федеральный технологический институт в Цюрихе, Офис Программы ОБСЕ в Бишкеке
720001, г. Бишкек, ул. Рыскулова, 6, Кыргызстан

Аннотация

Предмет исследования — особенности правового регулирования цифровых технологий и продуктов деятельности цифровых технологий. Выбор данной темы был предопределен активным развитием цифровых сервисов и цифровых финансовых активов и необходимостью адаптации современного законодательства под потребности цифровой экономики. Несмотря на то что на уровне международных организаций прорабатываются несколько стратегий развития цифрового права, ни в теории, ни в практической деятельности нет единого понимания правовой природы цифровых технологий и основ их правового регулирования.

С этих позиций целью настоящей статьи является осмысление системы и основных категорий цифровой экономики сквозь призму фундаментальных правовых институтов на основе как традиционных принципов научного анализа, так и результатов применения прикладных методов обработки данных.

Используя методы теоретического моделирования, идеализации и мысленного эксперимента, авторы рассматривают категории правосубъектности, охраноспособности и деликтоспособности цифровых технологий и продуктов, сравнивают их с близкими правовыми институтами и определяют возможные варианты интеграции новых правовых категорий в традиционные правовые институты договоров, ответственности, защиты интеллектуальных прав.

В результате исследования выстроено авторское видение тех реперных позиций, на которых должны строиться международные стратегии регулирования цифровой экономики. Авторы исходят

из того, что адаптивные возможности традиционного права весьма ограничены применительно к цифровым технологиям. И применительно ко многим из них должны быть разработаны качественно новые юридические модели. В работе представлены результаты рассмотрения основных правовых параметров цифровых технологий. Предложены формулировки правосубъектности и охраноспособности, сформулированы определения продуктов цифровых технологий в гражданском и авторском праве.
Делается вывод о противоречивости подходов к оценке правовой природы цифровых объектов и недостаточном учете технических аспектов цифровых технологий, а также о необходимости разработки на международном уровне единой юридической стратегии гражданского и интеллектуального права цифровых технологий. В числе приоритетных задач и направлений этой стратегии должна стать проработка вопросов правосубъектности цифровых технологий и основных механизмов охраны продуктов применения технологий. Сформулированные в статье выводы имеют важное практическое и методологическое значение и могут быть учтены при реформировании действующего законодательства

Ключевые слова

цифровые технологии, правосубъектность, цифровые технологии как объект правовой охраны, международные стратегии, юридическая ответственность, цифровое право, гражданское право, объект интеллектуальных прав

Конфликт интересов	Авторы сообщают об отсутствии конфликта интересов.
Финансирование	Исследование не имело спонсорской поддержки.
Для цитирования	Сидоренко, Э. Л., фон Аркс, П. (2020). Трансформация права в контексте цифровизации: в поиске приоритетов. *Цифровое право, 1*(1), 24–38. https://doi.org/10.38044/DLJ-2020-1-1-24-38

* Автор, ответственный за переписку

Поступила: 20.02.2020, принята в печать: 23.03.2020, опубликована: 20.04.2020

Introduction

With the rapid development of the digital economy, there is a need to create coherent, global, and comprehensive legal safeguards, including reliable guaranties of legal protection regulating the use of digital technologies in order to minimize digitalization risks and to legitimize new assets, both tangible and intangible. International organizations and states are actively developing strategies to adapt laws on the use of modern digital technologies. The main problems, however, are that, on the one hand, the proposed strategies are sectoral and address only certain aspects of digitalization, and, on the other hand, the solutions often aim at pursuing a political agenda at the expense of a coherent forward-looking global legal strategy.

Fundamentally, two main approaches to the future of law in the context of digitalization can be identified. The first is the utilitarian approach, which focuses on solving strictly defined functional tasks (financial intelligence, approval of technical regulations, etc.) serving the interests and of sates and specific international organizations. The second is the methodological approach, which would make it possible to have global and comprehensive solutions.

The utilitarian approach

The utilitarian approach is characterized by sectoral international cooperation focused on particular issues. Under the lead of their member states and strict appliance to their mandates, international organizations are developing legal mechanisms to minimize the risks associated to the use of specific digital assets. This approach often reflects political approaches, where some states or groups of states play a leading role whereas others are excluded. The utilitarian approach is about interests.

For example, in its 2019 recommendations, the FATF calls on States to introduce legal regulations for crypto assets in order to prevent the laundering of criminal proceeds[1]. The position the financial regulator holds is supported by the recommendations of the Basel Committee on Banking Supervision on the prevention of risks of using crypto assets by banks. Specific recommendations to develop legal regulation for new digital payment services were made by the European Union, which adopted Open Banking Standard and Revised Payment Services Directive (PSD2), obliging banks to provide financial and technical companies with access to customer information[2].

Speaking of technical regulations, it is necessary to mention the role of the International Organization for Standardization (ISO). For example, ISO is playing a role for defining an international framework for Artificial Intelligence (AI). The ISO subcommittee "ISO/IEC JTC 1/SC" has published 4 standards and plans to develop 12 subsequent standards for Artificial Intelligence; this subcommittee also prepared 21 standards for the Internet of Things and 38 standards for Cloud Technology. ISO also adopted international standards for Unmanned Aircraft Systems (UAS) in 2019. Earlier, in 2015, the European Parliament adopted a resolution on the safe use of Unmanned Aircraft Systems and stressed the importance of developing European framework legislation on the use of drones[3].

There are also some examples of global attempts done by international organizations. For example, the OECD provides universal guidance on how to apply and transform the law with respect to ICOs[4] and establishes general principles for the regulation of Artificial Intelligence[5]. According to the documents, the legislation of individual countries should reflect the following provisions:

1) the focus of AI technology on inclusive growth, sustainable development and welfare;

2) respect for the rule of law, human rights, democratic values and diversity, and strengthening the possibility of human intervention where necessary to ensure a just society;

3) transparency and responsible disclosure regarding information about AI systems;

---

1 FATF (2019, June). Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. Paper presented at the meeting of FATF, Paris. www.fatf-gafi.org/publications/fatfrecommendations/documents/Guidance-RBA-virtual-assets.html

2 Basel Committee on Banking Supervision. (2019). *Designing a Prudential Treatment for Cryptoassets*. https://www.bis.org/bcbs/publ/d490.pdf

3 ISO (2019). *Journey to a New Strategy*. https://www.iso.org/annual-reports.html

4 Organization for Security and Co-operation in Europe (OECD). (2019, January). *Initial Coin Offerings (ICOs) for SME Financing*. https://www.oecd.org/fr/finances/initial-coin-offerings-for-sme-financing.htm

5 Organization for Security and Co-operation in Europe (OECD). (2019, March). *Artificial Intelligence and Freedom of Expression*. https://www.osce.org/representative-on-freedom-of-media/447829?download=true и Organization for Security and Co-operation in Europe (OECD). (2019, May). *Recommendation of the Council on Artificial Intelligence*. https://www.fsmb.org/siteassets/artificial-intelligence/pdfs/oecd-recommendation-on-ai-en.pdf

4) for the reliability and safety of technology, continuous assessment and minimization of risks;
5) developers' and users' responsibility for the operation of digital technology[6].

This approach was supported by the G20, which, in its ministerial declaration, established 5 principles for regulating AI, which are largely consistent with the OECD principles[7].

The impetus for this elaboration of financial law was set by the European Commission, which prepared 30 recommendations for the development of law in the context of digitalization. The importance of adapting existing regulations to the introduction of new technologies was stressed, and a call was made to overcome the fragmentation of the law on the regulation of fintech and to ensure equal legal conditions for technology companies. Specific recommendations included: the importance of preserving personal and depersonalized data, ensuring the openness of systems, and compliance with the ethics of using digital technologies.

The UN plays an active role in implementing the security agenda. The General Assembly Resolution called for ensuring information security and improving national legislation in response to the steady increase in digital crime. The report submitted to the 74th session of the UN General Assembly also deserves attention. It stresses the need for legislative mechanisms to contain the risks associated with the mass use of inexpensive smart devices, gaps in information decryption, etc. It is important to emphasize that, according to experts, the priorities of law transformation include: involving technical experts in the legislative process, updating domestic legal acts on cybercrime, and developing legal mechanisms to control transnational crime.

The principles and provisions for transforming law contained in the Council of Europe Convention on Cybercrime are continued in directives and framework decisions of the European Union on the legal framework for the functioning of various segments of the digital economy. Most of the legal acts are aimed at regulating legal relations in the field of civil and financial law, but their provisions provide a basis for the adoption of criminal law rules, and significantly increase responsibility for criminal offenses in the IT sphere.

The methodological approach

The second approach considers creating a global and comprehensive model of legal regulation. It is necessary to understand what the foundations of digitalization are. The global approach allows the fundamentals of digitalization to be addressed by integrating essential dimensions such as the ethical, societal, technological and political aspects of digitalization. While the utilitarian approach is about developing numerous sectoral laws and strategies, the need to understand the status of digital technologies and its impact for the humankind remains. The methodological approach is about values and responsibilities; it implies a balancing act between rapid technological developments and the choice of a model of society. Thus, the law must prevail and the digital foundation shall be a legal one. There is a need to create coherent, global and comprehensive legal safeguards. The precise way to solve international approach remains to be seen: either to use the traditional law

[6] Organization for Security and Co-operation in Europe (OECD). (2019, June). *OECD Principles on AI.* https://www.oecd.org/going-digital/ai/principles/

[7] G20. (2019, June 9). *Ministerial Statement on Trade and Digital Economy.* http://trade.ec.europa.eu/doclib/press/index.cfm?id=2027

constructions, or the creation of a new legal order. The prevalence of the law for ensuring digital world order should not be put into question.

Inclusive growth and international cooperation in the sphere of the digital economy is essential. It requires the development of a strategy dealing with digital law transformation, as well as the establishment of models aiming at preventing digitalization risks.

Currently, many challenges cannot be tackled due to the lack of an internationally recognized comprehensive legal framework. It is imperative to find answers to a number of strategic questions, such as the legal nature of new digital technologies and their products, the possibility of adapting traditional legal instruments to new legal phenomena, or the development of a unified approach to the legal regulation of the digital economy at the interstate level, amongst others. Unfortunately, these issues are not currently being addressed either by the scientific community or by international organizations. In this regard, it is more urgent than ever to develop a single theoretical framework for digital legislation and choose a vector for its development. Future international and national legislations shall set legal guarantees for the development of digitalization and at the same time minimizes its risks.

Some international organizations are trying to apply a global methodological approach in line with their comprehensive approach to security. The implementation of digital technologies can solve many economic as well as social problems, and can be used as confidence-building tools between states.

The digital transformation has traditionally been discussed by the OSCE in a comprehensive manner. Within its politico-military dimension, the OSCE has developed the first set of confidence and security building measures between states in the cyber sphere. The digital economy became an important tool for cooperation among states, where economic cooperation and security are important element for building trust and confidence, thus preventing conflicts, as well as enhancing the welfare of citizens. Digital economy has the potential to foster sustainable and inclusive economic growth and development, connectivity, transparency, and accountability.

The protection of the private sphere is also a fundamental issue discussed within the human dimension and in a cross-dimensional manner at the OSCE. As part of its international activities, the organization encourages further research and discussion of end-to-end technologies; it also advocates the need to develop principles and recommendations that will maintain a balance between the security aspects of digitalization (such as controlling content leading to radicalization or criminal acts) and respect for the private sphere and people's freedom to create digital content. The OSCE Mission in Bishkek has developed and launched the first in the history of Central Asia Master's Program in Digital Jurisprudence, aimed at training specialists to ensure proper regulation of new digital technologies. The following specialists are being trained under this program: digital lawyers for state and municipal administration, digital lawyers for corporations, and digital security lawyers.

The current EU Critical Information Infrastructure Protection Agenda is built on five principles: readiness and prevention; detection and response; mitigation and recovery; international cooperation; and harmonization and unification of legislation in the EU countries.

Results

The paper analyses the needs and requirements for adapting the rule of law, in order to address the legal challenges arising from the development and the use of digital technologies and their products. It considers the categories of legal personality and protection of digital technologies, as well as the foundations of their legal regulations. The paper defines ways to protect intellectual property rights in the digital sphere, and considers the development of legislation in terms of establishing the responsibility of both developers and users of digital programs.

In addition, the article reveals the author's model for considering the legal status of digital technologies through the prism of general issues of status regulation and establishing responsibility and applied aspects of the application of individual technologies (Artificial Intelligence, Internet of Things, Blockchain, big data, etc.).

The paper notes the trend in the digital sphere of law being marginalized, and emphasizes the limited adaptive capabilities of traditional legislation in the regulation of digital technologies. The authors propose the development of fundamentally new legal constructions for digital technologies regarding their legal personalities and ability to be protected; this would allow the goal of the progressive development of the digital economy and the technical capabilities of individual technologies to be taken into account.

Discussion

Modern scientific literature does not address the legal status of digital technologies, or the use of its products, in a holistic manner. As illustrated below, experts focus their main attention on specific technical issues and practical solutions concerning particular topics.

For example, the issues of legal regulation in the sphere of Artificial Intelligence predominantly sit within the framework of the technology reliability evaluation (Yu & Alì, 2019); its possible application in certain areas of activity, in particular in jurisprudence (Mowbray et al., 2019); or inciting changes in modern tort and contract legislation (Hacker et al., 2020). Specialists mainly address issue of recognizing AI as an object of civil rights, and an object or a subject of intellectual activity.

The legal regulation of drones and other breakthrough technologies' application is addressed with regard to specific legislation reform (aviation (Bassi, 2020), transportation (Bassi, 2020), health care (Konert et al., 2019), information (Marquès, 2019) and others. In scientific literature, great importance is attached to the regulation of smart contracts in terms of securities exchange (Lee & Joseph, 2019) declaration of the parties' intent (Gomes & Silvana, 2018), and de jure formalization of smart contracts (Liu & Huang, 2019).

Crypto assets management is also addressed. The majority of works are devoted to basic financial law principles (Giudici et al., 2020), the regulation of the digital payment instruments market (Huang et al., 2020), taxation (Sixt & Himmer, 2019) and norm-setting principles in the field of digital finance (Edwards, Hanley, Litan & Weil, 2019).

The issue of the status of big data legal is equally urgent; examples of these issues include its use in legal activities (Goanta, 2017; Custers & Leeuw, 2017), legal control (Lei, 2019), and models and assessment of legal risks related to big data use (Low & Mik, 2019).

We shall not attempt a detailed analysis of all legal challenges related to digitalization, but rather outline two clusters of issues that need to be addressed as a priority, both at national and international levels. The first cluster shall focus on the general aspects of transformation of digital law: adaptive capacities of modern, civil, financial legislation in digital transformation; the legal nature of digital technologies as an object of civil rights; and any specificities of contractual relations in digital economy. The second cluster shall focus on the implementation of particular technologies, such as the Internet of Things, AI, big data, machine learning, drones, robots, and similar areas, which require detailed scientific analysis and restrictive application.

While assessing the prospects for the development of law in the context of digitalization, scientists are considering two possible scenarios: the first one foresees the restructuration of traditional legal models in order to accommodate new digital issues; the second one foresees fundamental changes in the current legislation aiming at replacing traditional legal framework with more abstract and universal models.

The conflict between the two scenarios is most visible in the analysis of protectability and legal identity of digital technologies. Protectability of digital technologies means their ability to act as objects of civil and intellectual rights. In this regard, it is important to consider whether emancipation is permissible between the real right/right in rem and copyright from traditional legal institutions.

Emancipation opponents challenge the fact that Artificial Intelligence and machine learning can become the foundation for the law, or they can replace fundamental principles of the law, as these principles have developed over the centuries through so-called 'consolidating learning' in AI, whilst human behaviour is inherently too irrational and inconsistent (Fernández-Villaverde, 2020).

Proponents, by contrast, see emancipation as a natural conflict of public and private interests in the digital world (Entin, 2017) and recognize the possibility for digital technologies to obtain their legal identity if they acquire functional autonomy, value, and economic utility (Kharitonova, 2019).

In the current Russian legislation, objects of civil rights, along with property rights, include digital rights. They constitute a type of property rights and are mentioned along with intellectual rights, which provides some researchers with a reason to deny the possibility of attributing digital objects to copyright protection. They are defined as the right of obligation or other rights; their exercise, disposal, or restriction is possible only within the information system (Article 141.1, the Civil Code of the Russian Federation) and therefore they have a very limited meaning or application. A whole cluster of issues related to exercising these rights outside the digital environment — namely, results of the rights implementation (big data consolidation and analysis, machine learning results, etc.) — remains outside the regulatory mechanisms.

While Russian law provides for the regulation of digital rights as part of information law, in English law the protection of digital rights is related to the protection of property. This approach is in line with the spirit of the following statement: Digital rights are monetary in nature and therefore should be protected as things (Rahmatian, 2013). From this point of view, digital technologies acquire the status of objects of civil law, as well as products manufactured using these technologies.

Thus, the Anglo-Saxon law makes it easy to answer the questions about who owns (a) a new code of a self-learning program, which embodies 'experience' in executing commands; (b) the rights to products made by such programs and robots; and (c) who bears property or other liability for the

negative effects of digital technologies or their products. However, other countries' experiences are not sufficient for the sustained and successful development of the digital economy. It is important to develop a one-size-fits-all approach for civil matters with regard to digital technologies, products, and rights.

We believe that this approach should be based on the following methodological provisions:

1) Recognition of digital product as an object of civil rights shall not be based on its material essence or economic value. As a rule, digital objects have a comprehensive legal nature and can be considered both from the intellectual and the proprietary standpoint;

2) Digital technologies' assessment shall be based on a legal model, allowing for compliance with the legal nature of the relationship, and which is capable of balancing private and public interests in digital circulation;

3) When developing a universal approach to digital technologies regulation as a subject of civil rights, objective emancipation of digital law from traditional legal institutions shall be taken into account. In other words, the adaptive capacity of traditional law in relation to digital technologies is very limited due to the multifunctional nature of objects, technical saturation, uncertainty in task management, and possible risks related to their integration into civil circulation.

With regard to the development of intellectual rights in the digital sphere, it is important to note that one of the most pressing issues is the choice between granting digital benefits to individuals or recognizing them as public domain. However, it is obvious that it is not possible to take a decision as long as the legal nature of the rights of digital products is not determined; this is particularly the case concerning AI.

Challenges emerge from the objective characteristics of digital products: technology results being highly repeatable, the low human creative contribution, the automation of some processes, the impossibility to distinguish between creative and noncreative components, the complexity of distinguishing between the author's rights and those of the compiler, and so on. Such challenges are also encountered while referring to digital platforms and platform solutions, databases, data processing algorithms created during machine learning, etc.

The digital economy poses a question for the law on how to protect intellectual activity products and fully respect the interests of creators, users, and investors. Three possible models related to intellectual products' protection are considered by scientists and in practice:

1. Consider digital technology products through the prism of copyright. This approach is based on European Union Directive 96/9/EC (EC, 1996) and is valid for cases where digital objects meet the criterion of originality for data selection and processing. However, this approach negates the difference between the author and the technology owner. In addition, there may be difficulties in distinguishing authorship when, for example, one author creates their product based on another author's digital solution (digital platform, block chain registry, cloud technology), or when some data is transferred from the creator's database system to another system without their consent. Moreover, the proposed solution is in conflict with one of the basic copyright principles — protecting a product that has an original, unchangeable, and one-off form. Digital solutions typically have multiple pre-

sentation formats, coding methods, and techniques, which precludes considering them as indivisible original products.

2. Digital technologies regulation in neighbouring rights' format. This approach is common for Russian law, where the activity of database or other digital products creators can be determined as organizational and technical (Maggon, 2006). In this case, database architecture creators and developers acquire an exclusive right to their intellectual products in general. However, the boundaries of neighbouring rights are blurred, and the risk of digital products users' rights being violated increases.

3. Establishing an independent institute of intellectual rights in digital objects, combining both property and non-property rights, as well as reflecting the technological specificity of protected objects (Lauts, 2019). The development of a fundamentally new mechanism will allow a correct model for managing digital products use to be designed (products created by robots, self-learning program codes, etc.).

The next important aspect is to provide a legal capacity to digital technologies. This proposal has already exceeded its theoretical framework. There are proposals to recognize robots and robotics products as subjects of rights of obligation and to consider them as agents in concluding contracts with third parties acting on behalf of their owner and in their own name (Neznamov & Naumov, 2008). Arizona law gives delivery robots same rights as pedestrians, but they must abide by the same rules: they cannot run into somebody and must give way to other pedestrians. The state of Utah is currently considering a bill with the same wording.

The traditional law identifies legal identity as a combination of legal capacity, active capacity, and delictual dispositive capacity. Currently, three types of legal capacities are recognized: physical persons, corporations, and public legal entities. At the same time, this list has gradually expanded, as necessary, to include new circulation parties and to adjust the theoretical foundations of legal identity. In particular, granting legal identity to corporations requires changed approaches to understanding the will, interest, and motive of the subject. Moreover, it does not seem appropriate to deny digital technologies' legal identity due to the lack of a will component (Ponkin & Redkina, 2018).

It is much more important to evaluate technologies through the prism of corporations' legal identity: namely, from the standpoint of autonomy and decision-making. Learning ability and the ability to independently change the action algorithm can supplement these characteristics.

However, it should be noted that modern digital technologies have different degrees of autonomy. Can the same legal identity rules apply to them, or should they be differentiated? In modern law, there is no solution to this issue yet. If the legal identity of AI and other digital technologies is recognized, it will be important to address such issues as public liability insurance, criteria for determining the possible risk related to robotic activities, setting out the rules for digital tort and the procedure for recording, and registering new legal entities.

In general, the very idea of the legal identity of digital technologies is reasonable; however, it often equated with the legal identity of persons. According to experts, the legal identity of robots may be recognized similarly to the recognized legal identity of international organizations, for example the UN (Chung & Zink, 2017).

It is also important to consider the autonomy of digital objects. Human dependence on technology will determine its delictual dispositive capacity. It is important to mention a number of applied aspects with regard to law transformation in the digital environment. In particular, AI application issues need to be resolved. It is difficult to identify persons who are responsible for digital device errors. Experts widely discuss the liability of IBM's Artificial Intelligence (AI) system "Watson for Oncology" in South Korea, and its legal identity, and argue that liability should be placed on Watson's creators and the relevant medical personnel.

Establishment of legal guarantees for AI and robots security is widely discussed alongside activity regulation issues. In particular, Chessman raises the issue of applying animal handling rules to robots — up to the establishment of responsibility for the abuse of robots or AI — as contemplation of this abuse can cause mental harm to humans (Chessman, 2018). The active introduction of AI and machine learning makes the process of determining any possible limits for the use of technology in legal activities a challenge. Some authors deny this possibility, and stress that legal decision-making cannot be automated as it contains too many value judgments; norms are contextual, and reliant on intuition as well as fairness in any of its forms (Wachter et al., 2020). This approach seems to be extremely categorical, especially in light of the long-standing use of digital technologies by lawyers. The issue is how this participation shall be formalized, and how to determine the machine's liability for the final decision. Ryan Catterwell's fair comment was that machine learning and AI could be used for automated contract interpretation.

However, if some provisions may well be interpreted by a machine, others may not. There are two main constraints: 1) some provisions are relative, intuitive, and rather a "question of perception"; 2) some provisions can be interpreted only in the light of the views of the parties and their circumstances. Therefore, machine learning can only help lawyers, not replace them in contract interpretation (Catterwell, 2020). The separation of human and machine power in decision-making is therefore justified. AI can assume the function of data processing and analysis, and a person can make decisions based on their critical analysis of information prepared by AI.

Many issues also arise while using the Internet of Things. Lawyers emphasize that the personal data which users of "smart" things provide is insufficiently protected; devices often collect and exchange information without the owner being aware of it, or can exchange information across borders, amongst other violations. (Mohamed & Zulhuda, 2015). The problem is that the current legislation, and in particular the EU General Data Protection Regulations (GDPR), does not take into account the use of the Internet of Things and smart homes; literal application of regulations may impose an unreasonably high liability on device designers in some cases, or may create cyber security risks in other cases (Chen et al., 2019).

The issue of personal data protection also arises in connection with the use of cloud technologies. Even the current strict General Data Protection Regulation (GDPR) cannot be applied in practice for personal data processing in cloud technologies, in particular due to its inability in identifying data controllers or providers; moreover, the fact that the programme has collected data may remain secret (Fosch Villaronga & Millard, 2018). The exchange of data in the data cloud is no less problematic. Currently, much data — including the data needed for criminal investigation by Country-1 — may be under the control of Country-2. However, international mutual legal assistance treaties do not

allow Country-1 obtaining their cloud data in Country–2; mere international courtesy leaves too much discretion, as *Microsoft Ireland* or *the Yahoo! Belgium* case law demonstrated. Therefore, experts suggest that countries should start negotiations on international information exchange agreements (Yunquera, 2018).

As for legal regulation of digital technologies, we cannot but mention the applied aspects of using unmanned aircraft (drones). Although the legislation in many countries, including Russia, incorporates norms limiting the use of drones, protection of privacy remains an issue. In particular, no country in the world provides landowners with adequate legal protection against the malicious actions of drone owners who may use drones to actually invade foreign land, photograph everyone without any permission, or otherwise interfere with their privacy (Holden, 2016). The issue of the information collected by the drones and the possibility of its use by the owners has not been addressed either (Kaminski, 2015).

Conclusion

Summarizing the findings of this study, it is important to emphasize that modern legislation is only beginning to establish rules for the use of digital technologies. On an international level, discussions currently focus on two possible strategies: to foster the digital economy development (progressive advance strategy) or to minimize the risks related to its use (security strategy). On the state level, attempts are made to address the problem in a palliative manner through selective legal solutions and the adoption of national programmes aiming at finding cross-cutting solutions.

While not denying the importance of this work, there is the need for a more coherent and systematic approach to the development of digital law by addressing two fundamental issues: (1) Can traditional legal constructs be adapted to the digital economy, or are innovative laws needed? (2) How can a model for the universalization of transnational technologies law be designed?

The solution of the first issue directly depends on how modern jurisprudence will assess the legal identity of, and the ability to protect, digital technologies. The study showed that, in the light of digital development, the marginalization of traditional law is evident; therefore, the use of old structures can only lead to mosaic regulation without reserves for further development.

The progressive development digital economy is undergoing is impossible without the development and adoption of fundamentally new legal structures with a long-term commitment. In particular, the legal identity of technologies, copyright and neighbouring law, machines liability, and insurance need to be fundamentally reviewed.

It is also important to note that these models shall be developed at the level of the international community rather than on the level of individual states; this ensures the laws are universal.

REFERENCES:

1. Catterwell, R. (2020) Automation in contract interpretation. *Forthcoming, Law, Innovation and Technology Journal*, *12*(1), 81–112. https://doi.org/10.1080/17579961.2020.1727068
2. Chen, J., Edwards, L., Urquhart, L., & McAuley, D. (2019). Who is responsible for data processing in smart homes? Reconsidering joint controllership and the household exemption. *Edinburgh School of Law Research Paper Forthcoming*, *8*(2), Article 21. http://dx.doi.org/10.2139/ssrn.3483511
3. Chessman, C. F. (2018, June 29). *Not quite human: Artificial Intelligence, animals, and the regulation of sentient property*. SSRN Electronic Journal. http://dx.doi.org/10.2139/ssrn.3200802
4. Chung, J., & Zink, A. (2018). Hey Watson, can I sue you for malpractice? Examining the liability of artificial intelligence in medicine. *Asia-Pacific Journal of Health Law & Ethics*, *11*(2), 51-80.
5. Custers, B. H. M., & Leeuw, F. (2017). Legal Big Data: Toepassingen voor de rechtspraktijk en juridisch onderzoek [Legal Big Data: Applications for legal practice and legal research]. *Nederlands Juristenblad*, *34*, 2449–2456. https://www.openrecht.nl?jcdi=JCDI:ALT82:1
6. Edwards, F. R., Hanley, F., Litan, R., & Weil, R. L. (2019). Crypto Assets Require Better Regulation: Statement of the Financial Economists Roundtable on Crypto Assets. *Financial Analysts Journal*, *75*(2), 14–19. https://doi.org/10.1080/0015198X.2019.1593766
7. Entin, V. L. (2017). Avtorskoye pravo v virtual'noy real'nosti (novyye vozmozhnosti i vyzovy tsifrovoy epokhi) [Copyright in virtual reality (new opportunities and challenges in digital age)]. Statute.
8. Fernández-Villaverde, J. (2020, March 20). Simple rules for a complex world with artificial intelligence. *PIER Working Paper 20-010*. http://dx.doi.org/10.2139/ssrn.3559378
9. Fosch Villaronga, E., & Millard, C. (2018, December 23). Cloud robotics law and regulation. *Queen Mary School of Law Legal Studies Research Paper 295/2018*.
10. Giudici, G., Milne, A., & Vinogradov, D. (2020). Cryptocurrencies: Market analysis and perspectives. *Journal of Industrial and Business Economics*, *47*, 1–18. https://doi.org/10.1007/s40812-019-00138-6
11. Goanta, C. (2017, October). Big law, big data. *Law and Method*, Special Issue – Comparative Law. https://doi.org/10.5553/REM/.000029
12. Gomes, S. (2018). Smart contracts: Legal frontiers and insertion into the creative economy. *Brazilian Journal of Operations & Production Management*, *15*(3), 376–385. https://doi.org/10.14488/BJOPM.2018.v15.n3.a4
13. Hacker, P., Krestel, R., Grundmann, S., & Naumann, F. (2020, January 19). Explainable AI under contract and tort law: Legal incentives and technical challenges. *Artificial Intelligence and Law*. https://doi.org/10.1007/s10506-020-09260-6
14. Holden, P. (2016). Flying robots and privacy in Canada. *Canadian Journal of Law and Technology, 14*(1), Article 3. http://dx.doi.org/10.2139/ssrn.2571490
15. Huang, R., Yang, D., & Loo, F. (2020). The development and regulation of cryptoassets: Hong Kong experiences and a comparative analysis. *European Business Organization Law Review*, *21*, 319-347. https://doi.org/10.1007/s40804-020-00174-z
16. Kaminski, M. E. (2015). Robots in the home: What will we have agreed to? *Ohio State Public Law Working Paper No. 292*, *51*(3), 661–677. http://dx.doi.org/10.2139/ssrn.2592500
17. Lauts, E. B. (Ed.). (2019). Sovremennyye informatsionnyye tekhnologii i pravo [Legal regime for Artificial Intelligence modern information technologies and law]. Statute.
18. Konert, A., Smereka, J., & Szarpak, L. (2019). The use of drones in emergency medicine: Practical and legal aspects. *Emergency Medicine International*, *2019*, Article 3589792. https://doi.org/10.1155/2019/3589792
19. Lee, J. (2019, January 31). *Smart contracts for securities transactions on the DLT Platform (Blockchain): Legal obstacles and regulatory challenges*. SSRN Electronic Journal. http://dx.doi.org/10.2139/ssrn.3523317

20. Lei, C. (2019). Legal control over Big Data criminal investigation. *Social Sciences in China*, *40*, 189–204. https://doi.org/10.1080/02529203.2019.1639963
21. Lin, C., Shah, K., Mauntel, C. & Shah, S. (2017). Drone delivery of medications: Review of the landscape and legal considerations. *American Journal of Health-System Pharmacy*, *75*(3), 153-158. http://doi.org/10.2146/ajhp170196
22. Liu, Y., & Huang, J. (2019). Legal creation of smart contracts and the legal effects. *Journal of Physics: Conference Series*, *1345*(4), Article 042033. http://doi.org/10.1088/1742-6596/1345/4/042033
23. Low, K., & Mik, E. (2020). Pause the Blockchain legal revolution. *International and Comparative Law Quarterly*, *69*(1), 135–175. https://doi.org/10.1017/S0020589319000502
24. Maggon, H. (2006). Legal protection of databases: An Indian perspective. *Journal of Intellectual Property Rights, 11*, 140–144.
25. Marquès, M. C. (2019). Drones recreativos: Normativa aplicable, responsabilidad civil y protección de datos [Recreational drones: Legal framework, civil liability and data protection]. *Revista de Derecho Civil, 6*(1), 297–333. https://www.nreg.es/ojs/index.php/RDC/article/view/380
26. Modh, K. (2015, November 25). *Drones and their legality in the context of privacy*. SSRN Electronic Journal. http://dx.doi.org/10.2139/ssrn.2773598
27. Mohamed, S., & Zulhuda, S. (2015). The concept of internet of things and its challenges to privacy. *South East Asia Journal of Contemporary Business, Economics and Law*, *8*(4), 1–6.
28. Mowbray, A., Chung, P., & Greenleaf, G. (2019, June). Utilising AI in the legal assistance sector-testings role for legal information institutes. Paper presented at the 1st International Workshop on AI and Intelligent Assistance for Legal Professionals in the Digital Workplace (LegalAIIA),Canada. http://dx.doi.org/10.2139/ssrn.3379441
29. Neznamov, A. V., & Naumov, V. B. (2018). Strategiya regulirovaniya robototekhniki i kiberfizicheskikh sistem [Regulation for the robotics and cyberphysical systems regulation]. *Zakon*, 2, 69–89.
30. Ponkin, I. V., & Redkina, A. I. (2018). Iskusstvennyy intellekt s tochki zreniya prava [Artificial intelligence from the point of view of law]. *RUDN Journal of Law*, *22*(1), 91–109. https://doi.org/10.22363/2313-2337-2018-22-1-91-109
31. Rahmatian, A. (2013). Originality in UK copyright law: The old "skill and labour" doctrine under pressure. *International Review of Intellectual Property and Competition Law*, 44, 4–34. https://doi.org/10.1007/s40319-012-0003-4
32. Sanz Bayón, P. (2019). Key legal issues surrounding smart contract applications. *KLRI Journal of Law and Legislation*, *9*(1), 63–91.
33. Sixt, E., & Himmer, K. (2019, July 15). *Accounting and taxation of cryptoassets*. SSRN Electronic Journal. http://dx.doi.org/10.2139/ssrn.3419691
34. Wachter, S., Mittelstadt, B., & Russell, C. (2020, March 3). *Why fairness cannot be automated: Bridging the gap between EU non-discrimination law and AI*. SSRN Electronic Journal. http://dx.doi.org/10.2139/ssrn.3547922
35. Yu, R., & Alì, G. (2019). What's inside the black box? AI challenges for lawyers and researchers. *Legal Information Management*, *19*(1), 2–13. https://doi.org/10.1017/S1472669619000021
36. Yunquera Sehwani, R. (2018). One cloud in the sky and conflicting laws on the ground: Regulating law enforcement access to e-evidence in cloud computing in the European Union and the United States (Unpublished thesis). *College of Europe,* Belgium. http://dx.doi.org/10.2139/ssrn.3271580
37. Zimmerman, E. (2015, February 12). *Machine minds: Frontiers in legal personhood.* SSRN Electronic Journal. http://dx.doi.org/10.2139/ssrn.2563965

The authors' contribution:

Elina L. Sidorenko — scientific editing, general formulation of research tasks, analysis of legal definitions of digital technologies and digital technology products, identification of signs of legal capacity and security of artificial intelligence, determination of the development directions of civil and copyright law.

Pierre von Arx — scientific editing, determination of research methodology, analysis of the characteristics of the regulation of the digital economy in the framework of international organizations.

Вклад авторов:

Сидоренко Э.Л. — научное редактирование, общая постановка исследовательских задач, анализ юридических определений цифровых технологий и продуктов цифровых технологий, определение признаков правоспособности и охраноспособности искусственного интеллекта, определение направлений развития гражданского и авторского права.

Пьер фон Аркс — научное редактирование, определение методологии исследования, анализ особенностей регулирования цифровой экономики в рамках международных организаций.

Information about the authors:

Elina L. Sidorenko* — Dr. Sci. in Law, Professor of the Department of criminal law, criminal procedure and criminalistics, Director of the Center for digital economics and financial Innovations, Moscow State Institute of International Relations (MGIMO), Moscow, Russia.
12011979@list.ru

Pierre von Arx — Ambassador, Head of the OSCE Programme office in Bishkek, Ph.D., Professor of Swiss Federal Institute of Technology of Zurich, retired general-staff colonel, Bishkek, Kyrgyzstan.
pierre.vonarx@osce.org

Сведения об авторах:

Сидоренко Э.Л.* — доктор юридических наук, профессор кафедры уголовного права, уголовного процесса и криминалистики, директор Центра цифровой экономики и финансовых инноваций, Московский государственный институт международных отношений (университет) МИД России, Москва, Россия.
12011979@list.ru

Пьер фон Аркс — посол, глава Программного офиса ОБСЕ в Бишкеке, Ph.D., профессор Швейцарского федерального технологического института в Цюрихе, генерал-полковник в отставке, Бишкек, Кыргызстан.
pierre.vonarx@osce.org