IoT Summit Russia
7 June 2016, St. Petersburg
(prepared for RUSSOFT NPO)

WHITEPAPER

THE INTERNET OF THINGS:

Legal Aspects

(Russian Federation)

Version 1.0. For discussion purposes

St. Petersburg
26.05.2016

MAIN CONCLUSIONS

1. The dawn of the era of the Internet of Things is the perfect time to improve the quality of legal regulation. This approach should be both comprehensive and reasonable. Legal terminology and rules should be formally certain, and updated legislation should serve as the springboard for the development of the self-regulation mechanisms.

2. Regulation of the Internet of Things should evolve, at a minimum, in due regard to the principles of user awareness and freedom of participation in the Internet of Things ecosystem.

3. Within the framework of the Internet of Things and Big Data, a special legal construct should be adopted to simplify turnover of information as a subject matter of transactions.

4. Protection of personal data and privacy should be regulated to the extent it can realistically be enforced. The respective norms should be reasonably limited on the basis of a balance of interests.

5. The net neutrality principle should be revised for the context of the Internet of Things – inter alia with regards to critical structures, protection of competition and non-discrimination of various kinds of devices.

6. Potential vulnerabilities of devices pertaining to the Internet of Things shall be compensated with instant-alert requirements and user support.

7. Minimal requirements for interaction (compatibility) among devices and applications should be formulated in order to ensure fair competition, encourage technological advancements, and prevent fragmentation.

8. Legal constructs must be developed that adequately frame and describe automated legally-significant actions occurring within the Internet of Things (without or with minimal participation of subjects).

9. Insofar as the existing legal concepts and approaches are insufficient to ensure a robust protection of the interests of users of decentralized-networks, a legal framework must be created to structure adequately the said relations.

CONTENTS

1. Purpose and goals of the document (version 1.0)

This document is presented in the form of a whitepaper (hereinafter – the "*Whitepaper*"). ***Document version 1.0***, drafted in May 2016, constitutes a brief exposure of a number of the legal aspects of the Internet of Things (hereinafter the ***"IoT"***) in the context of the modern Russian legal system and possible directions of their regulation.

It is not the aim of this document to provide an exhaustive and detailed description of the pertinent legal issues in this sphere, or to propose means of resolving them. The primary objective of the Whitepaper is to start a discussion in order to elaborate:

1) non-contradictory legal terminology in the IoT area;

2) a single vision of the system of IoT legal issues requiring regulation, in due consideration of sector specifics and the status quo of the regulatory framework;

3) a uniform approach to the question of the expediency of delineating various IoT legal aspects into aspects that should be regulated at the legislative level and aspects that it would be viable to leave open to different forms of self-regulation (industry standards, acts issued by professional associations and organizations, etc.);

4) a position as to which IoT legal aspects should be regulated at the national level and which should be regulated at the international level.

The list of IoT issues and aspects considered in this version of the document is not exhaustive[1] and will be supplemented based on the outcome of an open, joint discussion with Russoft NPO members and specialists (http://russoft.org/), as well as with the

[1] For the moment, this document does not touch upon the legal aspects, within the IoT context, of the use of geolocation technologies, the legal aspects of the distribution of radio-frequency spectrum, the potential IoT implications of virtual and augmented reality, electronic payments, 3D printers, etc.

participants of the IoT Summit Russia, which is scheduled to take place on 7 June 2016 in St. Petersburg. The document is open to critique by any other interested stakeholders; suggestions, comments and ideas should be forwarded to *IoT.Russia@dentons.com*.

This document is intended for specialists – irrespective of their particular industry and (or) area of activity – whose sphere of professional interest includes the legal aspects of the IoT, management and strategic planning of the IT business in Russia and the world.

2. What is the Internet of Things?

The term "Internet of Things" has had various definitions. The following general approaches can be taken as examples:

1) The Internet of Things is a "*global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on the existing and evolving interoperable information and communication technologies.*"[2]

2) The Internet of Things is a "*long-term technology and market development based on the connection of everyday objects to the Internet. Connected objects exchange, aggregate and process information on their physical environment to provide value added services to end-users, from individuals to companies to society as a whole.*"[3]

3) "The Internet of Things means "things" such as *devices or sensors – other than computers, smartphones, or tablets – that connect, communicate or transmit information with or between each other through the Internet.*"[4]

4) "*The Internet of Things is the informatization of various objects and their inclusion into a*

[2] Recommendation by the International Telecommunications Union ITU-T Y.2069 "Series Y: Global information infrastructure, aspects of Internet protocol and next-generation networks – structure and functional models of architecture. Terms and definitions for the Internet of Things." Version 1.0 dated 29.07.2012. The text (inter alia, in Russian) is available at: https://www.itu.int/rec/T-REC-Y.2060-201206-I

[3] Report on the Public Consultation on IoT Governance. Published by the European Commission on 16.01.2013. The text is available at: https://ec.europa.eu/digital-single-market/en/news/conclusions-internet-things-public-consultation..

[4] FTC Staff Report "IoT – Privacy & Security in a Connected World." Published in January 2015. The text of the document is available at: https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

single network of networks."[5]

Thus, the IoT assumes, at a minimum:

(a) the existence of a wide pool of devices (including, incidentally, more than just the "usual" Internet terminals – personal computers, smartphones, etc.) connected to the Internet;

(b) collecting a significant array of data about surrounding environment (including both personal data and other information), as well as the sharing of this information amongst the aforementioned devices;

(c) capability for the automated (without direct human intervention) execution by IoT devices of functions that could have legal implications and consequences for people.

The IoT-related "Big Data" category is worth of special mention. Widely-recognized as one of the first sources to describe the unique features of Big Data is the analytical material published by META Group,[6] in which the authors identified the three key attributes of Big Data: data volume, data processing speed, and data diversity. These attributes were reflected in the definition of Big Data proposed by the European regulatory authority in the area of personal data: "*An exponential growth both in the availability and in the automated use of information: it refers to gigantic digital databases held by corporations, governments and other large organisations, which are then extensively analysed using computer algorithms and can be used both for the purposes of identifying general trends and interconnections, as well as for the purposes of influencing the individual subject."*[7] Big Data is one of the factors impacting the legal aspects of the IoT.

[5] "Outlook for the Long-Term Socio-Economic Development of the Russian Federation for the Period Through 2030," drafted by the RF Ministry of Economic Development. The text of the document is available at: http://www.economy.gov.ru as of 30.04.2013

[6] Doug Laney, 3D Data Management: Controlling Data Volume, Velocity and Variety // Application Delivery Strategies, META Group, 6 February 2001, File 949, URL: http://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf.

[7] European Data-Protection Supervisor Opinion 7/2015 dated 19 October 2015 "Meeting the Challenges of Big Data." The text of the document is available at: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-11-19_Big_Data_EN.pdf.

3. The Internet of Things in the world and in Russia

According to Juniper Research, as of year-end 2015, there were already roughly 13.4 billion Internet-connected devices worldwide, with that number poised to nearly triple to 38.5 billion units by 2020.[8] The most visible IoT area is consumer goods (including wearable technologies and vehicles), the most economically-significant – industry, the most critical from the standpoint of personal and public security considerations – medicine and defense technologies, civil-security technologies.

According to rough estimates, Russia currently has 4-8 million devices that are connected to the IoT. In 2016, the M2M connectivity market could surge to 23 million individual units.[9]

The RF Ministry of Industry and Trade[10] has begun working on a roadmap for IoT development in Russia. This work involves a discussion of pilot projects concerning smart-home technologies, smart industrial devices, smart medical instrumentation and smart agricultural equipment. The initiator of the dialog with state power for the purposes of determining the standards governing the implementation of IoT technologies in Russia is the Internet Initiatives Development Fund (http://www.iidf.ru/).[11]

4. Why are the legal aspects so timely?

The various aspects of the IoT (just as with the Internet as a whole) can be regulated in a number of ways, with the law representing but one of them. In terms of methodology, this document is not aimed at providing an analysis of the technical and other non-legal means of IoT regulation; rather it focuses specifically on legal means of regulation, as well as on the identification and demonstration of existing problems and contradictions in the legal

[8] 'Internet of Things' Connected Devices to Almost Triple to Over 38 Billion Units by 2020 // Juniper Research, URL: http://www.juniperresearch.com/press/press-releases/iot-connected-devices-to-triple-to-38-bn-by-2020.

[9] Analytical report by the consulting company Direct INFO "The M2M Market in Russia: 2010 Results, Outlook and Prospects for Development." The full text of the document is available at: http://www.directinfo.net/index.php?option=com_content&view=article&id=126%3A2010-07-06-13-57-09&catid=1%3A2008-11-27-09-05-45&Itemid=84&lang=ru.

[10] http://minpromtorg.gov.ru/.

[11] Russian associations and funds in the IoT area: Internet Initiatives Development Fund, Russian IoT Research Center (official partner of the Internet of Things Council), Starnet VC, and others.

sphere.

Needless to say, as the IoT continues to spread, the legal shortcomings of existing regulation will become increasingly apparent and conflicts and disputes will begin to emerge. IoT development will entail the adoption of special, general norms aimed at its regulation. The question remains open as to the degree of detail to which IoT relations should be legally regulated – are pinpoint amendments to existing legislation sufficient, or should applicable law be substantially overhauled? Discussions on these issues are being held at different levels at different agencies, including the European Commission[12] and the U.S. Federal Trade Commission.[13]

The Whitepaper assumes that IoT legal regulation should not only (a) establish binding requirements on technologies that could potentially cause harm to human health and safety or be of significance to ensuring the public interest, but also (b) create the necessary prerequisites for self-regulation and the promotion of "best practices."

That said, the following legally-significant IoT architectural aspects underpinning the problematics currently under consideration are particularly striking:

1) The IoT entails a sharp increase in the volume and content of technical information that ceases to have predominately-technical significance and allows for the generation of information about actual subjects (identification of subjects); that is, the line between technical information and personal data is being blurred.

2) In IoT format, the things themselves not only perform their main functions but also automatically accumulate a significant volume of external information – from other Internet-connected things and from the surrounding environment. As a consequence, the gathering of information rises to a qualitatively-new level.

3) The IoT is changing existing approaches to connectivity between objects and subjects.

[12] http://ec.europa.eu/.

[13] https://www.ftc.gov/.

A new relationship format is emerging: users (organizations) are using more than just computer technologies to interact. The full cycle of relations can be implemented at the IoT-device level without the direct participation of their owners. Further significant changes in IoT technologies and social relations should be expected in connection with the development of computer intelligence and related technologies.

4) The spread and scaling of IoT-based solutions is creating new challenges and risks associated with unscrupulous and unlawful activity of varying scope, entailing unauthorized access to devices, altering the algorithms of their operation, or the gathering of confidential information about IoT-network subjects. The widespread integration of IoT devices is increasing these risks by virtue of the growing scale of the possible consequences.

5) With the spread of IoT-connected devices, problems associated with limited resources in the shaping of an integrated, universal environment for the provision of telecommunications services (inter alia, radio-frequency spectrum), compounded by the connection to this environment of a vast number of IoT devices, are becoming more pressing.

On the whole, the IoT is expanding the information space to the world of physical objects, serving as a "bridge" between the different stages of human progress in information society.

5. System of legal issues

The development of Internet regulation (prior to the advent of the IoT) has been the consequence of a number of issues that repeatedly come to the fore at different levels of network architecture and in different legal relations. These issues include, inter alia, identifying users, determining jurisdiction, and establishing the liability of information intermediaries.

These issues rise to a new level in the context of the IoT. The problematics of automated actions, distributed networks and processing of intangibles are being updated. The formulation of concepts for IoT regulation, as well as the elaboration of approaches aimed at resolving specific conflicts of law, must be undertaken in due consideration of the following issues (some of which are closely intertwined with existing legal problems of the regulation of the Internet and information technologies):

1) Legal treatment of information;
2) Personal data and privacy;
3) Neutrality of the Internet of Things;
4) Information security;
5) Compatibility and fair competition;
6) Automated actions;
7) Decentralized networks.

This list is not exhaustive, and the authors anticipate its expansion as a result of public discussion. Needless to say, rapid technological development will give rise to new issues – including those that would be impossible to predict today. Nevertheless, the list reflects the authors' opinion as to certain issues that can already be identified in view of today's legal environment.

Worthy of separate mention is the fact that in terms of the regulation of informational relations, the quality of legal engineering is currently substandard. This problem pertains to more than just the IoT and has been widely recognized for quite some time. Nevertheless, it could have a serious impact on both the development of the IoT industry, as well as on the expansion of IoT-related legal issues. The absence of clearly-defined terminology (reflecting the specifics of IoT technologies, the degree to which certain technologies influence private and public interests, the extent of environmental impact) makes it impossible to apply legal norms uniformly, which could violate the rights and legal interests of IoT-system participants.

6. Fundamental principles of regulation

1) **Principle of awareness**. IoT-service users should be provided with information (be made aware) about what data is being gathered by which devices, how this data is being collected and in what volume, and how and where this data is being stored.

   In practice, this principle can be implemented using IoT technologies themselves, allowing users, for example, to receive and update such information quickly using QR-codes and similar tools.

   Within the scope of the Whitepaper, one proposed option entails considering the question of creating an open **register of IoT devices and solutions**, organized according to the principle of voluntary declaration. The register could contain information about the capabilities of various devices in terms of information gathering and automated connectivity with other devices.

   Such a register could include elements of self-regulation – for instance, a rating by users and (or) industry representatives of such devices and solutions from the standpoint of their various aspects (for example, information security or the protection of personal data) by way of the reactions of authorized participants, analogous to the well-known "likes" on social media.

   Another option would be to consider the formation of a **system of legally-binding principles** that manufacturers would be compelled to observe, and a business environment based on a balance of interests among all IoT participants.

   Both of the aforementioned positions (as well as other possible stances) are subject to further discussion within the scope of the Whitepaper.

2) **Principle of free IoT participation**. Despite the fact that the IoT is an objective trend in the development of information society, discrimination cannot be a factor for individuals and organizations if they do not want to immerse themselves fully in the IoT system.

It should be acknowledged that de facto, the IoT lowers the level of protection of privacy rights and (or) information confidentiality by virtue of the penetration into many spheres of material life and digitalization of a high volume of data.

It would seem that, above and beyond awareness, subjects should be given a real choice as to their participation or non-participation in informational connectivity when using IoT devices (one assumes that IoT devices will soon become extremely widespread and start to crowd out "unconnected" devices). Aside from the traditional solutions associated with equipment and program settings, this principle could also be implemented by way of innovative IoT solutions preventing, on a legal and anonymous basis, the gathering of information or enabling the flexible, secure and simple control of their functionality.

Needless to say, the composition of these principles of the regulation of IoT-based legal relations is subject to augmentation, in due consideration of public discussion.

7. Selected legal issues

7.1. Legal treatment of information

General description: while the importance and value of information as a commodity is growing (information is bought and sold, there is an information market – including, but not limited to, Big Data), the issue of its legal treatment remains undetermined. While information is already becoming an item of economic turnover, there are currently no adequate and fully-fledged legal instruments to deal with it.

Existing legal regulation: in the first version of the RF Civil Code dated 30.11.1994, information is referenced in Art. 128 as an object of civil-law rights. Thereafter, under RF Federal Law № 231-FZ dated 18.12.2006, information was stricken from the number of objects of civil-law rights listed in Art. 128 of the RF Civil Code. In its present version, RF Federal Law № 149-FZ dated 27.07.2006 "On Information, Information Technologies and Protection of Information" regulates relations whose subject matter is information and contains a number of dispositive norms that, while generally making it possible to establish rules of information access, are used in real-world transactions (for instance, the provisions of Art. 6 on information owners). That said, from the standpoint of civil law, such relations are viewed, as a rule, either as services or as relations associated with the results of intellectual activity, including databases and know-how. Neither construction, however, conveys the specifics of informational relations, whether in the context of the IoT or in terms of Big Data.

Solution direction: the time has come for the elaboration of an approach envisioning a direct legal construction that would make it possible to define information as the subject matter of civil-legal transactions.

7.2. Personal data and privacy

General description:

1) The distinction between personal and technical data is becoming blurred – any device can be linked to its owner and his Internet profile; even if data anonymization is declared, in many cases, previously-accumulated information can be used to re-identify the subject.

2) The need is emerging for the formulation of new principles governing the obtainment by device (application) developers (vendors) of the personal-data subject's consent to the use (processing) of his personal data, inter alia, by all IoT-network participants mediating the functioning of the given user device (application) so that the procedure has no significant impact on the development of IoT technologies.

3) The need is emerging for a new evaluation of existing approaches to the ability of law enforcement agencies and IoT-device manufacturers to engage in the gathering and interception of information on social media, as well as the remote control of IoT devices. On the one hand, under the connectivity of devices on the IoT, the volume of personal data and its sensitivity for private individuals is steadily growing, on the other – using an additional volume of generated data on the IoT is poised to become a valuable source of information. The capability for the remote control of devices creates separate risks for private individuals, just as for other IoT users.

4) A market is forming for Big Data, which is essentially serving as the subject matter of transactions. Aside from the issue of the legal treatment of information as an object of legal relations, the extent to which Big Data can be viewed as a commodity in general must be determined.

Existing legal regulation: RF Federal Law № 152-FZ dated 27.07.2006 "On Personal Data" provides a broad definition of the concept of "personal data" ("any information pertaining, whether directly or indirectly, to an identified of identifiable person," Clause 1, Art. 3). Moreover, it establishes a series of legal requirements governing the processing of personal data, including the need to obtain the consent of the personal-data subject aside from a number of exceptions, not all of which are applicable to real-world relations in the IoT context, and also imposes on operators a set of obligations in terms of personal-data protection. In this case, IoT issues intersect with Big Data issues. There are well-founded doubts, for example, as to whether in such conditions the principle of personal-data processing on the basis of specific and predetermined objectives can be observed, and, objectively speaking, the opportunity to obtain the personal-data subject's consent simply does not exist in all cases. The value of personal-data anonymization diminishes in situations where it is statistically possible to obtain other "auxiliary" data from numerous additional sources, whose number is steadily growing.[14] Furthermore, the existing regulation of generally-accessible personal data may also be insufficient to meet current requirements.

Solution direction:

1) The development at the official level of an approach based on a balance of interests between the protection of personal data and need for technological progress. Such an approach must be grounded in the principle of the formal certainty of legal norms (currently in question within the framework of personal-data legislation) and reasonable restriction of the concept of personal data in such a way that allows for the consistent and predictable application of applicable norms while protecting the

[14] See, for example: *A.I. Savelyev* "Problems of the Application of Personal-Data Legislation in the Era of Big Data" // Law Journal of the Higher School of Economics – 2015. № 1. S. 54-61.

"minimum threshold of privacy rights." Interpretation could be built around the idea of positive identification based on the array of data currently at the operator's disposal (partially supported by case law).

2) In the context of the IoT and Big Data, the question is becoming not whether or not to transfer data to a particular operator (Internet resource), but whether or not to transfer data to the Internet as a whole – after such a transfer, data begins to "live its own life," inter alia, via its full or partial accumulation and processing by an indefinite range of devices and systems. The subject's consent can be expressed to the fact of such transfer in general. At the same time, additional workup entails the issue of what to do with data on a specific subject that can be gathered independently of his will (for example, via the placement in public places of sensors that collect information on all of the subjects in the area).

3) Concerning additional capabilities for law enforcement agencies and manufacturers to gain access to user devices for the purposes of information-gathering or remote control (including "backdoors"), opinions are polarized – from "crypto-anarchism" to an ultra-conservative state-oriented approach. In this context, all solution options require an open search for compromise between various pressure groups and the "weighing" of constitutional principles. Taking the public interest into account is an objective necessity, insofar as the expansion of technological capabilities means the emergence of new opportunities for their abuse.

4) It would be worthwhile to consider the issue of the delineation, aside from personal data, of an additional category of information, the urgent nature of whose protection comes to the fore at the intersection of the IoT and Big Data. At issue is data that is not "personal" in the strict sense of the word, but which – even without identification of the subject – violate privacy rights and (or) other rights and legal interests.

Moreover, on the whole, it is impossible to agree with any approach that assumes the total rejection of anonymity in information-telecommunication networks, now encompassing the IoT as well.

7.3. *Neutrality of the Internet of Things*

General description: the well-known principle of *network neutrality* assumes that communications networks are open for the exchange of information without discrimination in terms of type and (or) source of traffic. In terms of the "regular" Internet, where the potential for discriminatory preferences in favor of certain content providers depending on the volume of paid services is at issue, such a principle may be justified. In the IoT context, however, there is the issue of particularly "socially-significant" or "economically-significant" traffic associated with "critical" elements (for example, wearable technologies monitoring health status or critically-important industrial Internet).

Against this backdrop, it would seem prudent to suggest that exceptions from the principle of neutrality (whose emergence can be logically predicted at this stage) should be both transparent and reasonable. That said, a balance must be observed between the public interest, associated with the functioning of critical elements, and the assurance of fair competition and prevention of abuse. As it pertains to the IoT, this principle could be formulated more broadly – as IoT neutrality and non-discrimination among various IoT devices, as opposed to merely the neutrality of the Internet as a network built on the TCP/IP protocol.

Existing legal regulation: in the Russian Federation today, the principle of [network] neutrality is not explicitly regulated. At the same time, this principle is implied by the general norms of current legislation, which also envisions certain restrictions: i.e., the restriction by a communications provider of a subscriber's actions in the event that said actions pose a threat to the normal functioning of the communications network (Para. 2, Clause 27 of the Rules Governing the Provision of Telematic Communications Services), or the priority use of communications networks by the state authorities in the event of emergencies (Art. 66 of the Law on Communications). Also worthy of note is the brief Core Document on network neutrality drafted by members of the working group on network neutrality at the RF Federal Anti-Monopoly Service (RF FAS).[15]

[15] http://fas.gov.ru/documents/documentdetails.html?id=14145

Solution direction: formulation of a principle of IoT neutrality which, while assuming that exceptions from the principle be reasonable and fair, guards against the possible abuse of such exceptions.

7.4. *Information security*

General description: by virtue of its very essence, IoT software necessarily entails certain vulnerabilities that cannot be eliminated in view of economic realities and the level of technical sophistication of the concerned devices. Moreover, there is often no automatic-update function available for the software installed on IoT devices. On the other hand, the availability of such an automatic-update function assumes the capability for the remote control of devices, including by unauthorized parties, which could also lead to serious consequences. This gives rise to the general problem of the quality of devices and related services, as well as the issue of manufacturer liability in this regard.

Existing legal regulation: comprehensive regulation of the information-security system has been evolving in Russia over the past several years. At the same time, it should be noted that the norms of Russian legislation in the area of information security do not as yet contain the comprehensive solutions required against the backdrop of the anticipated widespread expansion of the IoT and its significance.[16] Most of the regulatory acts in this sphere have differing areas of focus and scopes of regulation. They reflect approaches to ensuring information security that are largely tailored to regulation of the Internet in its present-day form. There are serious doubts as to whether they fully meet the specifications and intended purpose of IoT technologies and devices (in particular, "wearable technologies," self-driving vehicles, other devices designed for personal use) or factor in the unique aspects of the threat to information

[16] See, for example: RF Government Regulation № 608 dated 26.06.1995 "On the Certification of Information-Security Tools;" FSTEC of Russia Order № 31 dated 14.03.2014 "On approval of the Requirements for ensuring information security in systems for the automated control of production and technological processes at critically-important facilities, potentially-hazardous facilities, and facilities posing an elevated level of danger to public health and safety and environmental safety;" RF Government Regulation № 1236 dated 16.11.2015 "On establishing a ban on the clearance of software originating from foreign states for the purposes of engaging in procurements intended for the satisfaction of federal and municipal needs."

security posed by IoT software.

<u>Solution direction</u>:

1) Amendments should be made to the draft law "On the Security of the Critical Information Infrastructure of the Russian Federation,"[17] provided the final version of the draft law is aimed at the comprehensive regulation of information-security issues, including devices intended for personal use, in order to determine what should be classified as "critical infrastructure" for IoT purposes within the legal context, and provided that it is compiled in due consideration of international standards and practices in terms of establishing the rights and responsibilities of critical-infrastructure operators, procedures for confirming the compatibility of front-end applications (devices) associated with critical infrastructure, information-security requirements, etc.

2) Requirements should be formulated for IoT, API[18] operating systems, other tools for connectivity with the software of IoT devices and user applications, in terms of mandating that such software supports certain information-security standards that ensure the security of information exchange and meets the applicable requirements governing user-authentication procedures. An additional measure might involve a mechanism allowing for device manufacturers to alert users of critical device failures having an impact on their overall level of information security, as well as the responsibility of IoT device manufacturers (application developers) to arrange for the monitoring and support of their products (at least in terms of the elimination of critical faults) throughout the entire lifecycle of the respective products.

7.5. Compatibility and fair competition

<u>General description</u>: there is no one standard or well-developed practice for the unrestricted and stable connectivity of various devices. This complicates interaction

[17] See: Draft Federal Law "On the Security of the Critical Information Infrastructure of the Russian Federation," URL: http://www.consultant.ru/law/hotdocs/27694.html.

[18] API – Application Programming Interface.

among IoT subjects which, among other things, has a negative impact on security. A related issue deserving of separate attention is the matter of intellectual-property rights to solutions and protocols pertaining to IoT devices, as is the task of ensuring fair competition in the given field.

Existing legal regulation: as of today, coordinated efforts in this area are being made at the level of the International Telecommunications Union (ITU). The general provisions of the Law on Fair Competition could potentially be interpreted in the context of this aspect of the IoT (collusion among business entities, prohibition against the abuse of dominant position, etc.).

Solution direction: minimum criteria must be formulated and utilized for the connectivity (compatibility) of devices and applications made by different manufacturers, inter alia, for the purposes of preventing anti-competition practices, encouraging technological progress and guarding against fragmentation. Another option might be to consider compelling manufacturers to provide any third-parties' access to the API of devices and applications, which could also be problematic in terms of ensuring the privacy rights of technology users. It might also be appropriate to propose measures for the presales expert examination of devices in terms of their compatibility (on the basis of minimum requirements governing the compatibility of IoT devices). Worthy of separate attention in the context of ensuring fair completion is the issue of proprietary technologies.

7.6. Automated actions and automated agreements

General description: against the backdrop of the IoT, the issue of the legal qualification of legally-significant automated actions is coming to the fore. The number of interactions among devices occurring without the direct participation of humans is growing, thereby complicating the resolution of issues pertaining to liability for the potential harm and damage caused by such devices.

Transactions executed in electronic form or via electronic interaction among devices are expected to become widespread. The blanket nature of device connectivity, coupled with its varying forms of application, requires the expansion and adaptation of rules governing the conclusion of agreements and allowable forms of agreements (human-readable agreements, machine-readable agreements, blocking of the unilateral waiver or modification of obligations, prevention of misleading terms and conditions, protection of the weaker party and adhesion agreements). Fundamental changes will be caused by the advancement of artificial-intelligence (AI) technologies, which elevate the level of autonomy of controlling-software modifications.

Blockchain technology[19] is poised to play a key role in the conclusion and performance of agreements executed in electronic form, insofar as it creates a trusted execution environment (TEE) for the consolidation of contractual terms, recording of obligation performance and indexing of rights (both to electronic items, as well as to physical objects). The conclusion of transactions and transfer of ownership rights under their execution, inter alia – to physical objects, could be performed by algorithms constructed by humans but with a minimum of their direct participation or without such direct participation at all.

<u>Existing legal regulation</u>:

1) Existing law contains certain special constructions aimed, to a certain extent, at automated actions, such as Art. 498 of the RF Civil Code on the retail sale of goods via the use of automated terminals. The number of such norms is critically low. Separate norms are only indirectly associated with automated actions, such as the norms envisioned by the Law on Information and the RF Civil Code which, whether explicitly or implicitly, regulate legal relations featuring the participation of information intermediaries.

   At the same time, against the backdrop of the IoT, automated actions are rising to a new level where, among other things, the format for interaction between subjects

[19] In broad strokes, the term "Blockchain" is currently used to denote a distributed database that contains a history of entries on all manner of transactions in the broadest sense of the word and which, by virtue of its architecture, includes "natural protection" against fraud and abuse. One example of Blockchain use – crypto-currency. Over the long-term, discussions are centering on the use of this technology in a wide array of fields, from jurisprudence to management, and the topic merits separate analysis.

and objects is changing. A sizeable share of legal relations in this area are fundamentally beyond the scope of even the most general norms of existing legislation, which could lead to unpredictable regulatory enforcement.

2) In the sphere of consumer relations, it is impossible to exclude significant conflicts between real-world practice and the requirements of the Law on Consumer Protection.

3) The situation is made all the more complicated by the fact that jurisdictional issues are gaining newfound prominence against the backdrop of the IoT, which calls into question the possibility of their resolution on the basis of classical approaches (including concepts of the operation of law in space and in terms of the range of concerned parties, determination of applicable law and location of action execution, determination of dispute-resolution venue).

4) Existing legal instruments aimed at the conclusion of transactions in electronic form were developed, in the best-case scenario, in the context of Internet format Web 1.0, with minor adaptations for Web 2.0. Direct regulation is limited to the provisions of the RF Civil Code on transactions and agreements. To a significant extent, a number of the general norms envisioned by the Law on Electronic Signature allow for the possibility of self-regulation, but nevertheless fail to exclude the necessity of seeking recourse to real-world and direct contact among subjects at certain stages, which could hinder the development of the automated-agreement system.

Solution direction:

1) It is necessary to determine the jurisdiction applicable to the activities (legal relations) of IoT participants (in all senses, including the operation of law in space and in terms of the range of concerned parties, determination of applicable law, determination of dispute-resolution venue). Moreover, it is essential to determine the legal status and provide a clear definition of IoT operators (in view of the fact that the majority of IoT operators will in some capacity serve as information intermediaries), as well as to analyze existing legislation on information

intermediaries in order to formulate a reasonable and balanced approach to the thresholds of their liability within the context of the IoT.

2) The popularization and broad application of automated agreements will rest on the formulation of the formal languages capable of describing such agreements. On the one hand, this task is closely aligned with self-regulation, while on the other, in view of the weighty role played by the state in the economy, it could reasonably be assumed that the state might be interested in standardizing approaches to the description of automated agreements (to formal languages). The use of formal languages requires a review of existing approaches to norms governing the form of agreements, interpretation of agreements, and the regulation of fraud and error issues in the course of agreement conclusion, as well as to the contesting of agreement forms – clearly, rules will be required that clarify a person's ability to reliably familiarize themselves with the texts of the documents and conduct negotiations. Case law, or the regulator, will need to formulate approaches to distinguishing between the identity of programming codes and agreements.

3) Ensuring the opportunity for IoT development will require the clarification of key institutions of civil law, including the concept of obligation, the securing of obligation performance, as well as the definition of fault and liability for breach of performance. These institutions will need to be adjusted in order to ensure party balance in terms of obligations, as well as for the purposes of protecting the weaker party. Excessive regulation of substantive issues will slow commerce and impede growth in the accessibility of the resources, services and benefits offered by the IoT.

4) Automated agreements will clearly feature the broad use of Blockchain technology. In this respect, legislators will need to resolve the issues associated with the use of private Blockchain and validity of agreements. Moreover, it would be prudent to expect the expansion of private registers of various types of property based on Blockchain technology – as well as the attempt by legislators to regulate the activities of such registers for the purposes of preventing abuse.

7.7. Decentralized networks

General description: decentralized (peer-to-peer, single-rank) networks are already a well-known technology, one whose significance is steadily climbing against the backdrop of the IoT. A prime example of this technology is Blockchain. The urgency of information-security issues is prompting the need for a modification of existing regulation in terms of the creation, use and (or) export/import of devices into the IoT, insofar as this will entail the expanded use of encryption tools.

Existing legal regulation: existing legislation and current approaches to its interpretation scarcely allow for the consistent application of legal norms to any legal relations evolving within the scope of decentralized networks. From the legal standpoint, the issue boils down to the particularities of the functions performed by the various nodes of such networks. While the technical side of legal relations might be clear, for legal purposes, a picture of participants is emerging in which each plays an active role, and frequently – a picture assuming one form of regulation or the other. Some well-known examples: torrent trackers, in which each "sharing" participant is automatically viewed as a content distributor, with all of the ensuing consequences; in the case of crypto-currency like Bitcoin, each operator of a network node – from the standpoint of classical legal approaches – can be viewed as an "issuer." Anticipated growth in the use of decentralized networks, in both the private and public sectors, requires changing approaches to existing legislation which, in the majority of today's cases, has no capacity, a priori, for consistent application to distributed networks.

Solution direction: formulation of a new legal approach tailored to the structure of distributed networks and reflecting its decentralized nature, assuming the absence of any set "decision-making center" on which liability could be imposed in the event of a bad-case scenario. The key task – avoiding a situation in which a comprehensive set of obligations could be imposed on each of the independent and inter-coordinating network nodes as if it were the sole "decision-making center," insofar as such a situation would be absurd and render regulatory-enforcement decisions impossible to execute. The need is emerging for the establishment (under self-regulation or at the standards level) of general rules that would broadly cover all participants of the respective legal relations within the scope of a decentralized network.

8. Conclusion

The IoT is creating new and fundamentally-complex "rules of the game" for the legal system. The classical and as-yet unresolved legal issues of the Internet (including user identification, the legal status of information intermediaries, and issues associated with the determination of jurisdiction) are evolving and intensifying at this stage in the development of information society.

Gaining particular urgency are issues related to the legal treatment of information, the processing of personal data and privacy rights, network neutrality and information security. A new area is emerging for the discussion of device compatibility – an issue whose social and economic importance is gaining a new dimension. Problems of automated actions and distributed networks are becoming more pronounced. Automated agreements are making it necessary to take a fresh look at classical legal institutions of contract law.

This is but one aspect of the legal issues coming to the fore against the backdrop of the IoT (as well as in the era of Big Data). Considerable overlap between the law and technical regulation exists in other areas as well (although this largely pertains to the determination of substantive technological requirements), including the distribution of radio-frequency spectrum and technological regulation as a whole.

Technological progress always outpaces the law, yet the law remains one of the most important instruments for the organization of social and economic life, and reasonable compromises are essential. Against the backdrop of the future "IoT world," the legal system must provide the basic prerequisites for self-regulation and dispute resolution.

26 May 2016 , St. Petersburg