ADVANT Beiten

LEGAL REGULATIONS OF INFORMATION TECHNOLOGIES IN RUSSIA

Ost-Ausschuss Osteuropaverein der Deutschen Wirtschaft

Ostinstitut / Wismar

Dear readers,

Digitalization is the key to sustained growth, and is a prerequisite for creating a stable competitive edge. That being said, we are standing at the very beginnings of global development. For this reason, the German Committee on Eastern European Economic Relations (CEEER) created recently a Digitalization Working Group to discuss the issues of importance for business and to offer a development platform for joint projects between German companies and companies from the partner countries of the CEEER. B2B has the most potential for cooperation in the area of digitalization, especially when talking about Russian-German economic relations.

To increase and develop this potential, Russian and German companies cooperate to promote the expansion of joint digital projects. It is for this very reason that we created in June 2017 the German-Russian Initiative for Digitalization together with RUIE.

The main topics are digital enterprise, digital power engineering (smart electrical grids), and digital services (public administration, private economy). The development of these areas is of central importance for Russia, but is becoming more and more important for Germany. The Russian populace is very open to digital solutions (a fact that is corroborated, for example, by the high number of users of online stores, digital offers and solutions, for example, in the transport sector).

Digital education aimed at the target group of creative youths must be at the heart of this gradual development. For example, joint German-Russian projects for students and young specialists will ensure professional interaction. They will create a bridgehead for the development of joint projects, in order to bring industrial enterprises and mid-level entrepreneurs together with digital technology specialists.

For the successful economic implementation of German-Russian projects, the regulatory frameworks must be harmonized as much as possible. The issues of commercial use of data, rights of ownership during their transnational use, localization of data storage, big data and cloud solutions, the Internet of things, and regulation of artificial intelligence (in particular, autonomous driving and drones) must be settled, and cannot be made subordinate to protectionist trends.

I am glad that **ADVANT Beiten** has devoted this brochure to the topic of information technology law in Russia and given an overview of current trends. I wish everyone a worthwhile read.

Michael Harms
Managing Director of the CEEER

Dear colleagues,

These days we can hardly imagine our lives without the Internet, smartphones and Facebook. Information technology has a powerful impact on both our private lives, and on business. And this impact is not limited to social networks such as LinkedIn or Xing. A multitude of processes are already performed digitally, from production technologies, building of sales and distribution networks, logistics and communications with the client and advertising, to the drafting of financial reports or submission of tax declarations to the tax authorities. The introduction and dissemination of Industry 4.0, the so-called fourth industrial revolution, will also have an effect on the legal aspect of the economic sector.

Like other lawmakers around the world, Russian lawmakers are trying to keep pace with the new innovations. From the standpoint of state institutions, the new technological revolution influences state security and economic achievements. For example, the publication of personal data that are significant for national security or the adoption of industrial know-how triggers regulatory activity. In addition, after the West introduced sanctions in connection with the Ukrainian crisis, Russian lawmakers have been trying to accumulate as much know-how and as many production facilities as possible in Russia (the so-called localization policy) and, in this way, to become independent of the West. This affects the information technology sphere as well. It is no exaggeration to say that digitalization is the key to the future. The future will belong to him who holds this key.

This is why there has been rapid regulatory growth in this sector and neighboring areas of law over the past few years (in particular, protection of intellectual property). You could even say that some special norms are more important and are applied more often than the ground rules of the Russian Civil Code. The development of digitalization and technological safety and security is running parallel with the development of the corresponding legislation and court practices.

In this brochure, we would like to present a brief overview of the legal framework in the area of information technology and point out the most important regulations.

Prof. Dr Andreas Steininger
Counsel
ADVANT Beiten

CONTENTS

General information on the regulation of information technologies in Russia 8

Regulation of the Internet in Russia 8

Conclusion of a contract 9

Online stores 10

Violation of intellectual property rights 11

Online games 12

eSports 13

Software localisation 14

Localisation of IT equipment 15

Patenting of software 16

Social networks 16

Organiser of dissemination of information on the Internet 18

Blocking websites 19

Personal data 20

Big user data 22

The right to be forgotten 23

Telemedicine 23

The use of VPN technologies in Russia 24

Contacts 27

General information on the regulation of information technologies in Russia

In 2008 the Russian President approved the "Strategy for the Development of an Information Society in the Russian Federation until 2020". In May 2017 a new strategy was adopted for 2017–2030 in connection with the rapid development of information technologies.[1]

A comparison of the two versions of the strategy makes it clear that the authors of the document delved deeply into the topic. The new version is more extensive, contains a list of definitions (such as the processing of big data, the Internet of Things, and cloud computing), determines strategy goals (development of an information infrastructure, creation of a new technological framework for the development of the economy), and describes ways of attaining these goals. At the same time, the creation of a new information society – a knowledge society – is proclaimed as the main goal. This is a society in which the receipt, collection and dissemination of reliable information is of major importance for the development of people, the economy, and the state.

The strategy asserts that, in the modern world, states whose economies are based on technologies to analyse big data will have a competitive advantage. However, Russia does not have corresponding domestic technologies, and consequently will have to deploy foreign technologies. This complicates the protection of the interests of individuals and the state in the information sector.

Thus, an initial analysis of the strategy indicates that one can assume that the trend towards localisation of information technologies, in particular regarding the processing of big data, will also intensify in the future.

Regulation of the Internet in Russia

The Internet is undoubtedly the most important element in the information technologies sector. In Russian law, the Internet and other information technologies are regulated primarily by Law No 149-FZ dated 27 July 2006 "On Information, Information Technologies and on the Protection of Information" (the "**Information Law**").

1 Decree No. 203 of the President of the Russian Federation dated 9 May 2017 "On the Strategy for the Development of an Information Society in the Russian Federation for 2017–2030".

This Law includes not only a definition of the key concepts for this sector, such as an information system, website, website owner, etc., but also regulates the activity of so-called organisers of the dissemination of information, different online services, and also the blocking of websites in connection with the violation of intellectual property rights or public law obligations (for example, calls for mass disorder).

In addition, specific areas of information technologies ("**IT**") are regulated by other laws, and also by subordinate legislation. For example, the Advertising Law addresses online advertising issues; a significant proportion of issues regarding copyright and trademark rights online are regulated by Part Four of the Russian Tax Code. The Consumer Protection Law plays a key role in online trade. Special laws also regulate personal data and communications (television, radio, requests for frequency allocation, mobile operators, etc.).

Consequently, a detailed description of each of the aforementioned IT sectors (online trade, the processing of personal data in the Internet, online games, advertising, dissemination of information in the Internet, etc.) requires analysis of certain laws.

Conclusion of a contract

In recent years the issue of concluding an online contract lost its recency in connection with the widespread use of such a procedure, in particular in the B2C sector. Therefore this issue will be considered briefly.

Under Russian law, all contracts concluded in the B2C sector and in the B2B sector must be concluded in written form.

A contract is deemed to have been concluded in written form if (i) a single document is signed by both parties, (ii) signed documents are exchanged (or electronic documents are exchanged, for example by e-mail) or (iii) a written offer from a counterparty is implicitly accepted (for example, through the payment of an advance).

As a rule, an online contract is deemed to have been concluded in simple written form through the commission of actions by the buyer (or client) who received the offer by the deadline established for its acceptance, relating to the performance of the terms and conditions of the contract indicated therein (implicit actions). Another example would be when making a purchase from an online store and confirming the order on the seller's website, a buyer agrees to the terms and conditions of the contract and thereby expresses their intent to conclude it.

For example, an end user licence agreement (EULA) is deemed concluded if the respective user accepted the terms and conditions and was thereby registered in the system.

From a legal perspective, nothing prevents the conclusion of contracts by legal entities via e-mail. Nevertheless, in a number of cases, in particular in the B2B sector, it is recommended that the contract be concluded on paper observing the different provisions of accounting, tax and customs law.

Accordingly, it is important to understand the consequences of non-compliance with the rules regarding the written form of the contract. In such instances a contract is not automatically deemed to be invalid; the parties simply lose the opportunity to submit evidence based on witness statements. However, they can use other evidence pertaining to the conclusion of the contract. Consequently, from a practical perspective in the event of a dispute, the conclusion of a contract can be proved as long as there are documents on its actual execution.

Online stores

Turnover of the Russian online market equalled about EUR 22.7 billion[2] in 2018. Turnover was up 59% on the previous year, this is the market's highest growth rate in the nine years it has been measured. Every fifth buyer even used a smartphone to make a purchase. Consequently, the Russian e-commerce market is developing in line with global trends.

From the perspective of Russian law, an online sale and purchase agreement in the B2C sector implies a special form of sale and purchase agreement, a so-called distance contract. Such contracts are regulated by the Civil Code, the Consumer Protection Law, and also subordinate legislation[3]. At the same time, the seller has the same obligations as in the case of a standard sale to a consumer. Moreover, the seller also assumes additional obligations, for example, the seller must offer to deliver the goods to the consumer.

It is important above all that foreign online stores are required from the perspective of international Russian law to follow the compulsory rules of Russian law. In accordance with article 1212 of the RF Civil Code, the choice of law to be applied to a sale and purchase agreement with a Russian consumer may not impair the latter's rights under Russian compulsory rules. In accordance with Russian procedural law, a consumer is

[2] Pursuant to the data of the Russian Association of Internet Trade Companies: https://www.rbc.ru/technology_and_media/03/06/2019/5cf3dab29a79477329e7a402.

[3] For example, Russian Government Resolution No. 612 dated 27 September 2007 "On Approving the Rules for the Sale of Goods by Remote Means".

entitled to file a claim on the violation of consumer rights at his/her place of residence. This concerns, *inter alia*, instances when foreign sellers advertise online to attract Russian consumers.

As a rule, online stores trade on the basis of general commercial terms and conditions which are based on foreign law. It is recommended that these commercial terms and conditions be reviewed for compliance with the relevant mandatory rules of Russian law.

Personal data processing norms are also among the mandatory rules of Russian law applicable to foreign online stores, in particular the obligation to localise such data on servers in Russia. If these rules are not met, the online store may be blocked in Russia.

As information posted on the website of an online store may be considered advertising in certain instances, foreign online stores must also take account of Russian advertising legislation. The Federal Antimonopoly Service (the watchdog responsible for advertising) takes the position that Russian legal regulations on advertising also apply to advertising posted in the Russian segment of the Internet (on the domains .RU, .SU, .РФ, etc.). This also concerns domains in the foreign segment of the Internet (for example, the domains .COM, .DE) if the websites are available in Russian, which indicates that they are targeting Russian consumers. In this case, the domain administrator is deemed to be sharing the advertisement, and assumes the corresponding liability.

Accordingly, before accessing the Russian market, every foreign online store must study the general legal terms and conditions and Russian market practices.

Violation of intellectual property rights

When dealing with online stores, the topic of violations of intellectual property rights comes up. This concerns primarily trademark violations. Copyright violations, for example, the illegal use of photographs, images, texts, design or databases, are encountered less often.

Trademark violations are so common in online trading and so diverse that it is fairly difficult to describe them in general. Nevertheless, in the case of violations of trademark rights, we can focus here on how the violations occur. In so doing, it is necessary to distinguish whether (a) original goods or (b) counterfeits are being offered for sale.

Offering a counterfeit involving the use of a registered trademark for sale is a classic violation of trademark rights. The right holder may choose from a number of different remedies: from filing a civil law action to making a statement to the police about a violation of the Code on Administrative Offences.

Offering an original product for sale at an online store while posting the respective trademark on the website is a violation of trademark rights, if the goods had been imported into Russia as so-called parallel imports, in other words without the consent of the trademark holder. However, in this situation, a statement may not be filed with the police, as there was no violation of trademark rights in the sense of the Code on Administrative Offences. In this case, it would be possible to send a complaint to the offender, relying on the norms of the Civil Code and demand termination of the trademark violation, citing the possibility that an action might be filed in court.

If copyright is violated on a website, an application for preliminary interim relief may be filed in court. An application may be filed with the Moscow City Court electronically (however, this does not relate to violations of copyright to photographs).

In addition, the right holder can file a written claim against the owner of the website on which the copyright is being violated. Under a special law[4], the website owner is required to check such claims pursuant to the specific procedure and cease the violation.

In general, when it comes to online violations of intellectual property rights, it is worth noting that Russian courts are gradually establishing uniform judicial practice on this issue in favour of the rights holders of the corresponding intellectual property.

Online games

The online gaming sector in Russia is currently regulated by special legislation. Nevertheless, the competent watchdog Roskomnadzor has announced that it is drafting a resolution to regulate online games. Furthermore, the representatives of Roskomnadzor attribute the need to regulate online games to public law issues: chats in online games might be used to coordinate terrorist attacks (something that has already happened, according to certain media reports). Therefore it is likely that Roskomnadzor's regulation will touch the public law aspects of online games.

Regarding the private law aspect of online games, a number of issues remain unresolved. The actual legal nature of purchases in an online game (for example, if

[4] Federal Law No. 149-FZ dated 27 July 2006 "On Information, Information Technologies and on the Protection of Information".

the user buys additional tools to improve his gaming character) is ambiguous. Most online game providers and publishers act on the assumption that this relates to actions within the framework of a software licence agreement concluded with the player. However, in one of its decisions the Commercial Court of the City of Moscow ruled that if a game provides an opportunity to use additional gaming features in order to simplify the gaming process and develop the gaming character more rapidly, this constitutes a paid services agreement[5]. Moreover, the court cited, *inter alia*, the fact that additional features are already contained in the software code when the user initially installed the software; consequently when buying additional features, the user did not receive additional software. This decision of the court of first instance was upheld in the courts of appeal and cassation, which points to effective judicial practice.

In addition, certain courts presume that online games are regulated by Chapter 58 of the RF Civil Code (Gaming and Betting). According to this chapter, the claims of individuals and legal entities related to the organisation of games and betting or participation therein are not subject to court protection. One exception to the rule concerns the claims of any individual who participated in games or betting under the influence of deceit, violence, coercion, etc.

In some instances disputes between the player and online game operator were resolved in favour of the player in connection with compensation for a blocked user account or the loss of an item bought in an online game. However, there have also been diametrically opposing decisions.

Thus, judicial practice in this area remains largely ambiguous or contradictory.

eSports

The area of eSports is closely linked to online games, which in the context of legal regulations is only starting to develop in Russia. The aforementioned issue is not a specifically Russian matter, as this area also remains unregulated in many legal systems.

At the same time, the Russian eSports Federation[6] has operated since 2000; this is a Russian national public organisation, which is responsible for the mass development of eSports (cybersports) in Russia and is a member of the International e-Sports Federation.

[5] Decision of the Commercial Court of the City of Moscow on case No. A40-91072/14 dated 24 November 2014.

[6] https://resf.ru/

Nevertheless eSports were recognised at the end of April 2016[7] as a form of sport ("computer sport"). However, the respective order of the Ministry of Sport did not clarify specifically what this means.

From the perspective of the main conditions of eSports, one should cite the general provisions of the RF Civil Code. Legal relations with a player (or team) regarding participation in a tournament should be assessed in this case as a paid services agreement or as a public tender. Part Four of the RF Civil Code applies to instances of corresponding competitions (copyright and associated intellectual property rights).

Software localisation

Since 1 January 2016, foreign software has been prohibited from participating in state and municipal tenders.[8] Accordingly, a Russian software register[9] was created.

There are two exceptions to this rule: foreign software may be acquired by state institutions if (i) the register does not contain similar Russian software, or (ii) the register contains similar software, but it does not meet the client's requirements in terms of functional, technical, and operating characteristics.

Consequently, in certain cases the participation of foreign software in procurement is possible and is permitted by law. At the same time, this participation will depend on the procurement organiser who in each individual case must substantiate the impossibility of procuring software included in the register and also the need to procure the foreign software.

The criteria for including software in the register concern not only the right holder of the software, but also contain the requirements on the software itself.

To be included in the software register, the right holder of the software should be a Russian legal entity with dominant Russian participation. Consequently, a Russian legal entity should be the majority shareholder of the right holder in the chain of owners.

In this regard, the fact that direct and indirect ownership is defined in accordance with the provisions of Russian tax law is significant. This makes it possible to implement certain corporate arrangements under which a Russian legal entity is de jure the majo-

[7] Order No. 470 of the Ministry of Sport of Russia dated 29 April 2016.

[8] Resolution No. 1236 of the RF Government dated 16 November 1236 "On Establishing a Ban on the Access of Software of Foreign Origin to the Performance of Procurements to Meet State and Municipal Needs".

[9] https://reestr.minsvyaz.ru/reestr/

rity participant, but from the standpoint of corporate law does not have full control over the right holder. In addition, these arrangements will allow a foreign participant to exercise specific corporate control over the Russian right holder and at the same time the foreign participant will not be declared the majority participant.

Another condition for including software in the register is the holding of exclusive rights to the software.

Exclusive rights to software may arise through modifications to existing software. Accordingly, it is important to understand the changes that must be made to the software (for example, the translation of the interface into Russian and the translation of the software into another programming language, the addition of certain functions related to Russian technical standards, etc.) and whether they constitute grounds for the emergence of new exclusive rights to the new software from the perspective of Russian legislation.

According to the data, as of September 2019 5,728 software products have been entered in the register.

As many enterprises with state participation also plan to procure only software that is included in the register (for example, Aeroflot, Rosneft, Gazprom, etc.), it is recommended that foreign investors include their software products on the register.

Localisation of IT equipment

On 12 October 2016 the Russian media reported that there were plans to apply the localisation requirements to the IT sector as well, in other words, to IT equipment. The Russian legislature is promoting the transfer of the production and operation of IT equipment to Russia. According to initial information, a register of Russian IT equipment should be established in 2017. However, as of September 2019 this register had not yet been created.

In future only Russian IT equipment will be able to participate in state and municipal tenders. However, specific regulations regarding the register of IT equipment have yet to be introduced.

Patenting of software

In accordance with the RF Civil Code, technical solutions are protected as an invention. At the same time, solutions are considered in any area pertaining to a product (device, substance, microbial strain, cell culture of plants or animals) or method (performance of actions on a tangible object using physical resources), *inter alia*, on the use of the product or method. An invention is entitled to legal protection if it is new, has an inventive step and is applicable in industry. At the same time, Article 1350 of the RF Civil Code indicates that computer programs may not be registered as inventions.

Nevertheless, the Russian patent agency presumes that this regulation of the RF Civil Code should be interpreted more broadly. If a patent application contains a computer program, then the invention is refused registration. However, if an algorithm for processing specific information is contained, for example, such a technical solution may be declared an invention[10].

In accordance with the electronic database of Rospatent (the Russian patent agency) Microsoft Corporation alone has more than 1,000 registered patents for inventions (valid and invalid). Apple Corporation has almost 100 patents, and in some of them the name indicates that this refers to software patents (for example, an image processing method and system, etc.).

Social networks

Social networks are used not only by individuals, but also by companies as part of professional communications (XING, LinkedIn). There is no special legal regulation of social networks in Russia[11]. The operators of such social networks write their own terms of use.

The popularity of social networks means that bad-faith actions are frequently committed in this area. The user account page is an Internet web page, and consequently may contain various items of intellectual property: from copy-righted texts and images to databases and trademarks. In some cases, they can be used by third parties acting in bad faith. There have been instances when third parties have created a group in a social network named as the official representative office of a famous company. Furthermore

[10] Order No. 87 of Rospatent dated 25 July 2011 "On the Entry into Force of the Manual on the Expert Examination of Applications for Inventions".

[11] Draft Law No. 145507-7, which is intended for the legal regulation of social networks, was introduced to the State Duma of Russia back in April 2017, but as of September 2019 had not yet passed even the first (preliminary) reading.

the group posts photographs of the company's goods and uses its corporate style (colours, logos, etc.). The name of this group may also foster the impression that it is the official group of the company.

The use of social networks is regulated by so-called user agreements, which frequently contain requirements on the creation of groups or communities. For example, these regulations prohibit (i) the false depiction of ties to a specific individual or legal entity, (ii) the publication of specific information by parties not authorised to do so, (iii) the creation of third party profiles.

As a rule, the administration of a social network creates an e-mail address that may be contacted in the event of violations. Some social networks even create a special procedure for filing reports on violations. It regulates the next steps of the social network, the applicant, and the alleged offender.

In certain instances it can suffice to simply eliminate the violation through this procedure. Nevertheless our experience shows that not even the world's famous networks react adequately even in cases of explicit violations of rights.

Alternatively Russian legislation can be cited if rights are violated. In this case, it is worth bearing in mind that under Russian legislation social networks act as so-called information intermediaries. Information intermediaries are companies that transfer material online or provide an opportunity to post information or grant access to specific information online. Consequently, a social network is a classic information intermediary.

At the same time, under Russian law an information intermediary is only liable if it is guilty, as in general an information intermediary cannot influence the information and materials posted on its resource or control them.

Consequently, a complaint must first be sent to the social network, with a demand that the offence be terminated. And it is only in cases where the social network does not react to such a complaint that the social network is to blame and that claim may be filed on this basis.

It goes without saying that a complaint may be sent not only to the social network, but also directly to the respective group administrator (information on the group administrator is publicly available in all social networks).

Organiser of dissemination of information on the Internet

Russian legislation contains the concept "organiser of dissemination of information in the Internet" ("**Disseminator of Information**"), which to all intents and purposes includes the owner of the websites on which electronic messages are transferred, delivered and processed.

At the same time, some of the subordinate legislation clarifying the concept of Disseminator of Information makes it possible to conclude that this relates first and foremost to social networks, Internet forums, mail services, etc.

The Disseminator of Information is required to notify Roskomnadzor of the start of its activity and this body also maintains the corresponding register[12].

At the same time, please note that the disseminator of information is required to store in the Russian Federation any information on the receipt/transfer, delivery and/or processing of electronic messages (in the form of texts, audio recordings, images or videos, etc.) for a period of 12 months. Effective 1 July 2018, in addition to the foregoing information, disseminators of information will be required, *inter alia*, to store the contents of electronic messages, audio recordings, images or videos.

The Disseminator of Information is required to submit the corresponding information to the competent state authorities (in particular, the police and the Federal Security Service).

Failure to comply with the obligation to notify Roskomnadzor of the commencement of online activities may lead to the imposition of a fine on the organiser of up to RUB 300,000 (approximately EUR 4,100), while failure to comply with obligations relating to information storage may result in a fine of up to RUB 500,000 (approximately EUR 6,900).

[12] http://97-fz.rkn.gov.ru/

Blocking websites

The Information Law contains a number of instances where the state watchdog Roskomnadzor may restrict access to a network address (domain or website).

This is possible if materials are posted on the website whose dissemination in the Russian Federation is prohibited (for example, on the production and use of drugs and psychotropic substances, on ways of committing suicide, etc.).

If such information is identified (by individuals or the state authorities), then a corresponding report may be filed with Roskomnadzor. After a review, Roskomnadzor notifies the entity hosting the prohibited information on the website. The hosting provider must duly notify the website owner and inform it that it must delete the prohibited information. If there is no reaction from the website owner and the hosting provider itself does not limit access to the resource, Roskomnadzor notifies the telecommunications operator, and it restricts access to the website. At the same time, the website is listed in a special register.

Website access restrictions can also be established in another way: for example, Russian domain registrars operate according to rules that establish the right of the domain registrar to terminate delegation of the domain on the basis of a written decision of the deputy head of an investigative agency. Please note that this rule applies only to domains registered in the .RU or .RF zones, although in practice some Russian registrars serving domains in other zones also terminate delegation of domains in these other zones.

The Information Law establishes a special procedure regarding access restrictions on websites that disseminate information violating copyright and associated rights. Roskomnadzor may restrict access to such websites, but only if it has a court order of Moscow City Court (a ruling on the introduction of preliminary interim relief).

As soon as a court grants such an application for preliminary interim relief, the applicant is entitled to send it to Roskomnadzor. Roskomnadzor will act pursuant to the established rules and send a notice to the website owner on the need to restrict access to the contested information.

The Information Law contains a declarative norm to the effect that the website owner must delete information violating copyright or associated rights when it receives a complaint from the owner of these rights. At the same time, it does not establish any specific liability for failure to comply with the demand of the right holder. However, the website owner's failure to take the required measures might affect the civil law classification of such actions and affect its subsequent civil law liability.

If the website owner does not react to the complaint of the right holder, the latter may take court action.

An interesting option for defending the rights of the right holder is to file a claim against the hosting provider of the offending website. Interaction with the hosting provider may result in the offending site being cut off from the Internet by the hosting provider, i.e. a temporary suspension of the operation of the website (until the owner concludes an agreement with a new hosting provider).

Personal data

Over the past few years, the legal community and many foreign companies have taken particular note of any topic related to personal data, primarily owing to the entry into force on 1 September 2015 of a law on the mandatory localisation in Russia of the processing of the personal data of Russian citizens.

In order to clarify this topic, it is necessary to focus on the general concepts used in personal data legislation. Federal Law No. 152-FZ dated 27 July 2006 "On Personal Data" (the "**Personal Data Law**") provides an extremely general definition of personal data as any information that relates directly or indirectly to an identified or identifiable individual. The definition is not very clear and is overcomplicated, in particular given that information is understood by the law to mean any data, regardless of the form of presentation.

For example, is the business telephone number of an individual part of this individual's personal data? And what about the personal bank account number? To all intents and purposes, in both cases the information relates to an individual, but the nature of this link differs.

The definition in the previous version of the Personal Data Law was more precise and understandable from the perspective of its legal drafting: any information relating to an identified or identifiable individual based on such information. In other words, if an individual can be identified based on the business telephone number (which would be impossible, for example, if this was a general phone number), then such information might be classified as personal data.

The definition of personal data raises a number of issues and the only argument of the Russian watchdog (Roskomnadzor) in favour of such a definition is that the legislation of the European Union also defines personal data in a fairly broad manner.

In one of its rulings, the RF Supreme Court cited examples of personal data: surname, first name, patronymic, year, month, date and place of birth, address, family, social and property status, education, profession, income[13]. Consequently, in each specific instance it is necessary to clarify whether the specific data constitute personal data.

In terms of personal data localisation, one important participant is the personal data operator, in other words, the person organising the processing of personal data or processing the data. It follows from this definition that any employer is a personal data operator, as every employer processes the personal data of its employees.

The law imposes specific obligations on the personal data operator on how to appoint the person responsible for personal data processing, publish internal regulations on personal data processing issues, and adopt organisational and technical measures to guarantee the safety of personal data.

Before processing personal data, the operator is required to notify Roskomnadzor that it will begin such processing. At the same time, the Personal Data Law contains a number of exceptions to this rule.

According to the legal norm in force since 1 September 2015, in case of the collection of personal data the operator must arrange for the recording, classification, accumulation, storage, clarification (updating, changes), and extraction of the personal data of Russian citizens, using databases located in the Russian Federation.

To all intents and purposes this norm obliges any operator of the personal data of Russian citizens to use information infrastructure (servers, computers, etc.) located in the Russian Federation.

After the entry into force of this innovation, the Ministry of Communications and Mass Media published the relevant clarifications on its website. In particular it clarified that the new requirements of the Personal Data Law applied solely to operators that collect personal data. As the collection of personal data is understood by the Law to mean the targeted process of obtaining personal data, localisation refers only to the personal data obtained by the operator as a result of the targeted organisation of the collection of such data, and not as a result of the accidental receipt thereby of such data (for example, as a result of e-mails which contain personal data, or due to the normal course of business, namely the conclusion of contracts and the receipt thereby of the personal data of the employees of the counterparty).

[13] See Ruling No. APG15-7 of the RF Supreme Court dated 24 June 2015.

Furthermore, the Ministry clarified the specific situations in which a foreign company that has no branches or representative offices in the Russian Federation is required to comply with the requirements of the Personal Data Law. For example, if the online activities of a foreign company target Russian citizens, then this company is required to comply with the requirements of this law. The use of the domain names .RU, .SU or .RF, or the existence of a Russian-language version of a website, for example, demonstrate that a company is targeting Russian citizens in its activities. These interpretations are not binding, but may serve as guidelines to an understanding of the goal of legislative regulations on the localisation of personal data.

Big user data

Back in summer 2016 the plans of the Russian watchdog Roskomnadzor to create a big data operator for user data came to light. First and foremost it should control the use of big user data and prevent the illegal use of such data.

A draft law[14] was introduced into the State Duma at the end of 2018, which was intended to make amendment to the Law on Information concerning the regulation of big user data, but as of September 2019 it had not yet passed first reading. Accordingly, at present big user data remains a concept that has yet to be defined in Russian legislation.

At the same time, there have been trends to classify big user data as personal data. At the same time, big user data should also include data on the activities of individuals, for example, data on how and where they make purchases, how often they use their smartphones, which websites they visit, etc.

For the time being the concept of big user data has also not yet been determined in Russian judicial practice. However, the first claims related to the processing of big user data have already appeared. For example, at the start of 2017 the well-known Russian social network VK filed a claim[15] against a software manufacturer whose software scans social networks and collects various kinds of information on its users, which has all the signs of big user data. The value of this information lies in the fact that this information could, for example, help banks to assess the solvency of potential borrowers, help advertisers in the targeted advertising of products, etc. According to the claimant, this software overloaded the servers of the social network due to the constant scanning of personal accounts, and also violates the Claimant's exclusive rights to the social network's user database. This dispute has been examined by commercial courts of the

[14] http://asozd2.duma.gov.ru/main.nsf/(Spravka)?OpenAgent&RN=571124-7

[15] http://kad.arbitr.ru/Card/1f33e071-4a16-4bf9-ab17-4df80f6c1556

first and appellate instances, which took different positions, after which their decisions were overturned by the Intellectual Property Court, and the case was sent to the court of first instance, where it is currently under consideration.

The right to be forgotten

The right to be forgotten means that an individual may in certain circumstances demand the deletion of links to more out-of-date or obsolete information on himself/herself from search engine results.

Both Russia and the EU recognise the right to be forgotten. A law enshrining this right entered into force on 1 January 2016. Pursuant to the law, the operator of a search engine that disseminates online advertising targeting Russian consumers is required at the individual's request to block the following information in search results: (1) information whose dissemination violates the legislation of the Russian Federation, (2) incorrect information or (3) out-of-date information.

Pursuant to the data of Russia's largest search engine Yandex, it received more than 3,600 applications for the deletion of search results in the first months after the entry of the law into force. Furthermore, most requests were attributed to the fact that corresponding search results contained reliable but more out-of-date information.

Only a third of the requests were granted. This small number is attributable to the fact that the search engines are unable to check whether information is correct. Instead, the applicant is required to prove that the information is incorrect, for example, by a corresponding court decision.

Telemedicine

On 1 January 2018, Federal Law No. 242 dated 29 July 2017 went into effect. This is the first law in Russia to regulate certain issues related to medical assistance using telemedicine technologies.

This law provides a definition of telemedicine technologies, which are understood to mean information technologies that provide for the remote interaction of medical personnel among themselves and with patients, the identification and authentication of such persons, the documentation of the actions they take when conducting case conference, consultations, and remote medical observation of the patient's health.

In accordance with this law, medical assistance using telemedicine technologies must be provided in compliance with the legislation on personal data and the provisions of medical secrecy, using a uniform identification and authentication system, the requirements on which[16] are approved by the Russian Government.

Specifically, the law permits medical consultations using telemedicine technologies, in which the consulting doctor may revise a previous course of treatment (provided that the doctor establishes a diagnosis and recommends treatment in a single visit). Remote observation of the patient's health is also permitted after an in-person visit.

The use of VPN technologies in Russia

Federal Law No. 276 dated 29 July 2016 which prohibits the use of special software or services if they enable users to gain access to websites blocked in Russia, entered into force on 1 November 2017.

This law has triggered numerous questions, in particular from foreign companies. Some companies believe that the law will make it difficult or completely impossible to communicate with their Russian subsidiaries through VPN technologies.

In view of this fact, a more detailed study of the law is recommended. The law prohibits the owners of specialist software, information networks, website, and also corresponding equipment (collectively "VPN Technologies") from providing technologies that make it possible to circumvent the ban on access to websites blocked in Russia.

Consequently, VPN Technologies are not prohibited as such: only the use of these technologies to provide access to websites blocked in Russia is prohibited.

VPN Technologies may be understood to mean, *inter alia*:

- virtual private networks (VPNs);
- anonymous proxy servers;
- certain types of routers;
- other software or technical equipment that performs similar functions.

[16] Russian Government Resolution No. 977 dated 28 November 2011.

The law targets the owners of such VPN Technologies, but not their users. Operators of search engines disseminating advertising that targets Russian consumers over the Internet are also subject to the law. Such search engines should stop providing links to blocked websites.

In connection with the adoption of this law, Roskomnadzor will initially identify all the owners of VPN Technologies.

In so doing, Roskomnadzor will contact hosting providers and cooperate with the law enforcement authorities.

Roskomnadzor will then send notices in Russian and English to the owners of VPN Technologies on the need to connect to a special information system in the Internet which contains information on the websites banned in Russia.

Owners of VPN Technologies are required to connect to this system and restrict access to the websites indicated in the system.

The law stipulates the adoption of a wide range of bylaws, which will clarify certain issues. At present such bylaws (some of them) only exist in draft form. Accordingly, a detailed analysis of such bylaws is not worthwhile.

If an owner of VPN technologies does not comply with the law, then its website may be blocked in Russia.

The law does not stipulate any other penalties.

However, if the owner of the VPN Technologies subsequently ensures compliance with the law, it will once again be granted access to Russian users.

The law includes an exception to the general rule.

For example, owners of VPN Technologies who

- previously determined the user community of such VPN Technologies and
- use such VPN Technologies for technological purposes for the performance of their activity

are permitted access to websites blocked in Russia.

In connection with this fact, we would like to point out that the wording of this exception looks fairly ambiguous, as neither this law, nor other laws (or bylaws) contain any interpretation of the term “technological purposes”.

Accordingly, such “technological purposes” could be understood to mean a fairly wide range of factors. In view of such positions, this “flexible” wording is even handier for the owners of VPN Technologies.

It is worth noting here that at the draft law stage this exception had been worded more clearly and included a single criterion: use of VPN Technologies by individuals employed by the owner of such VPN Technologies.

In light of this law, we should point out the following: As a rule, companies do not develop their own VPN Technologies, but instead procure them from developers (suppliers). Consequently, if you use VPN Technologies that are owned by a third party, there is a risk that Roskomnadzor’s notice might be sent to this third party and might be ignored. As a result, this VPN Technology would be blocked for Russia.

Accordingly, we recommend that you check the relevant legal relations with the suppliers of the VPN Technologies, and where possible compel the owners of such VPN Technologies to comply with corresponding Russian legislation.

Contacts

Falk Tischendorf
Rechtsanwalt | Partner
Head of CIS
ADVANT Beiten
Falk.Tischendorf@advant-beiten.com

Taras Derkatsch
Lawyer | Ph.D. | Associate
ADVANT Beiten
Taras.Derkatsch@advant-beiten.com

ADVANT Beiten in Russia
Turchaninov Per. 6/2
119034 Moscow
T: +7 495 2329635
www.advant-beiten.com

Our offices

BEIJING
Suite 3130 | 31st floor
South Office Tower
Beijing Kerry Centre
1 Guang Hua Road
Chao Yang District
100020 Beijing, China
beijing@advant-beiten.com
T: +86 10 85298110

BERLIN
Luetzowplatz 10
10785 Berlin
Germany
berlin@advant-beiten.com
T: +49 30 26471-0

BRUSSELS
Avenue Louise 489
1050 Brussels
Belgium
brussels@advant-beiten.com
T: +32 2 6390000

DUSSELDORF
Cecilienallee 7
40474 Dusseldorf
PO Box 30 02 64
40402 Dusseldorf
Germany
dusseldorf@advant-beiten.com
T: +49 211 518989-0

FRANKFURT
Mainzer Landstrasse 36
60325 Frankfurt/Main
Germany
frankfurt@advant-beiten.com
T: +49 69 756095-0

FREIBURG
Heinrich-von-Stephan-Strasse 25
79100 Freiburg im Breisgau
Germany
freiburg@advant-beiten.com
T: +49 761 150984-0

HAMBURG
Neuer Wall 72
20354 Hamburg
Germany
hamburg@advant-beiten.com
T: +49 40 688745-0

MOSCOW
Turchaninov Per. 6/2
119034 Moscow
Russia
moscow@advant-beiten.com
T: +7 495 2329635

MUNICH
Ganghoferstrasse 33
80339 Munich
PO Box 20 03 35
80003 Munich
Germany
munich@advant-beiten.com
T: +49 89 35065-0

Imprint
This publication is issued
by BEITEN BURKHARDT Rechtsanwaltsgesellschaft mbH
Ganghoferstrasse 33, 80339 Munich, Germany
Registered under HR B 155350 at the Regional Court Munich/
VAT Reg. No.: DE811218811
For more information see:
https://www.advant-beiten.com/en/imprint

EDITOR IN CHARGE:
Falk Tischendorf

ADVANT member firm offices:
BEIJING | BERLIN | BRUSSELS | DUSSELDORF
FRANKFURT | FREIBURG | HAMBURG | LONDON | MILAN
MOSCOW | MUNICH | PARIS | ROME | SHANGHAI

advant-beiten.com

09/2022