КОМИТЕТ ПО ИНФОРМАЦИОННЫМ ТЕХНОЛОГИЯМ И ТЕЛЕКОММУНИКАЦИЯМ

Председатель:
Эдгарс Пузо, Atos

Заместители председателя:
Глеб Вершинин, SAP CIS; **Вадим Перевалов**, Baker McKenzie;
Александра Шмигирилова, Ericsson

Координатор комитета:
Светлана Ломидзе (svetlana.lomidze@aebrus.ru)

ПЕРСПЕКТИВЫ РАЗВИТИЯ РЕГУЛИРОВАНИЯ ТЕЛЕКОММУНИКАЦИОННЫХ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В РОССИИ

ВВЕДЕНИЕ

В 2020 году пандемия коронавируса привела к серьезному повышению спроса на различные ИТ-решения, значительно усилив темпы цифровой трансформации российской экономики. Широкая поддержка усилий Правительства российскими и международными телекоммуникационными и ИТ-компаниями, многие из которых предоставили расширенный доступ к своей инфраструктуре и сервисам, стали залогом устойчивости российской экономики в период самоизоляции.

Цифровая трансформация и достижение «цифровой зрелости» ключевых отраслей экономики и социальной сферы впервые вошли в обновленные цели развития согласно указу «О национальных целях развития Российской Федерации на период до 2030 года», подписанному Президентом РФ 21 июля 2020 года. Правительство РФ ведет разработку показателей уровня цифровой зрелости и соответствующую корректировку национальных проектов, включая программу «Цифровая экономика». Усиленными темпами продолжается реализация курса на импортозамещение за счет широких мер поддержки российских ИТ-компаний, стимулирования государственного спроса на отечественные продукты, а также за счет ограничения конкуренции.

Опыт других европейских стран показывает, что ограничительные меры, направленные на защиту внутреннего рынка, не ведут в долгосрочной перспективе к созданию конкурентоспособных продуктов мирового уровня. Однако при этом возможен обратный эффект, когда на иностранных рынках будут вводиться ограничения в отношении российских продуктов.

РОССИЙСКОЕ ЗАКОНОДАТЕЛЬСТВО О ПЕРСОНАЛЬНЫХ ДАННЫХ

10 октября 2018 года Российская Федерация подписала протокол, вносящий изменения в Конвенцию Совета Европы о защите физических лиц при автоматизированной обработке персональных данных от 1981 года, что позволит сблизить законодательство России и Европейского союза в отношении обработки персональных данных.

2 декабря 2019 года вступил в силу закон о введении значительных штрафов за несоблюдение требований локализации баз персональных данных. Размеры штрафов варьируются от 1 до 18 млн рублей для компаний и от 100 до 800 тыс. рублей для генеральных директоров и иных топ-менеджеров. Штрафы в размере 4 миллионов рублей уже были наложены судом на компании Twitter и Facebook.

21 июля 2020 года Правительство России внесло в Госдуму законопроект (https://sozd.duma.gov.ru/bill/992331-7) о порядке обезличивания персональных данных, требования и методы обезличивания таких данных утвердит Роскомнадзор. Для уничтожения персональных данных в ИТ-системах законопроект предписывает использовать только средства защиты, сертифицированные ФСТЭК или ФСБ, что создаст оператором дополнительные сложности при выполнении требований закона о своевременном уничтожении персональных данных.

ЕВРОПЕЙСКОЕ ЗАКОНОДАТЕЛЬСТВО О ПЕРСОНАЛЬНЫХ ДАННЫХ

25 мая 2018 года вступил в силу Регламент ЕС по общим принципам защиты данных (General Data Protection Regulation). Регламент имеет экстерриториальный характер и применим к ряду российских компаний, которые в случае его неисполнения могут быть привлечены к значительной финансовой ответственности (например, штраф в размере 20 млн евро).

После принятия решения Судом Европейского союза по делу C-311/18 (Schrems II) 16 июля 2020 года, в европейском законодательстве также возникла неопределенность, допустимо ли передавать персональные данные с территории ЕС на территорию России. Полагаем, что решение данной проблемы требует более активного сотрудничества между государственными органами России и ЕС.

ОГРАНИЧЕНИЕ ДОСТУПА К ИНФОРМАЦИИ В ИНТЕРНЕТЕ

В последнее время Роскомнадзор неоднократно указывал на неэффективность механизма блокировок информационных ресурсов (например, веб-сайтов, мобильных приложений), нарушающих информационное законодательство.

18 июня 2020 года Роскомнадзор по согласованию с Генеральной прокуратурой Российской Федерации снял требования по ограничению доступа к мессенджеру Telegram. Решение, принятое Роскомнадзором, дает основание полагать, что сайт или мобильное приложение может быть разблокировано во внесудебном порядке, если компания приняла необходимые меры к исполнению российского законодательства. Полагаем, что подобную практику целесообразно применять и в отношении прочих ресурсов.

ХРАНЕНИЕ ПОЛЬЗОВАТЕЛЬСКИХ СООБЩЕНИЙ И ИНФОРМАЦИИ О ПОЛЬЗОВАТЕЛЯХ

Сохраняется неопределенность в отношении реализации «пакета Яровой», в частности, в отношении обязанности операторов связи и организаторов распространения информации по хранению текстовых сообщений, голосовой информации, изображений, звуков, видео и иных сообщений пользователей услугами связи. С 1 июля 2018 года указанные данные должны храниться до 6 месяцев с момента окончания их приема, передачи, доставки и (или) обработки.

В связи с пандемией COVID-19, операторы связи и бизнес-сообщество рассчитывают на ослабление/изменение некоторых требований закона.

БЕЗОПАСНОСТЬ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

1 января 2018 года вступил в силу Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации».

В конце мая Минцифры России предложило осуществить переход на «преимущественное использование» российского ПО и оборудования на объектах КИИ. В соответствии с этим предложением владельцы объектов КИИ будут обязаны перейти на преимущественное использование ПО из российского реестра и реестра программного обеспечения ЕАЭС (Евразийского экономического союза) до 1 января 2021 года, российского оборудования – до 1 января 2022 года.

Принятие предлагаемых требований в текущем виде может привести к сбою обеспечивающих функционирование объектов КИИ ИТ-систем, а у субъектов КИИ возникнут существенные необоснованные затраты на закупку нового оборудования и ПО при еще не истекшем сроке жизненного цикла уже установленного оборудования и ПО. Кроме того, существует риск нарушения договоренностей ВТО в случае принятия актов, ограничивающих покупку иностранной продукции субъектами КИИ, многие из которых являются негосударственными компаниями.

РЕКОМЕНДАЦИИ

- Привлекать экспертов международных ассоциаций и профессиональных объединений к участию в рабочих группах и экспертных советах исполнительной и законодательной властей при проработке правового режима актуальных для современной цифровой экономики концепций (большие данные, интернет вещей и т. д.).
- Выработать сбалансированный подход к распределению затрат между бизнесом и государством в отношении реализации «пакета Яровой».
- Выработать официальную позицию по европейскому регламенту (GDPR), возможности трансграничной передачи персональных данных из ЕС в Россию и наоборот, а также подходы, позволяющие эффективно имплементировать изменения, предусмотренные модернизированной Конвенцией Совета Европы, в российское законодательство о персональных данных.
- Дать официальные разъяснения и создать условия для более широкого практического применения операторами п. 7 ч. 1 ст. 6 Закона 152-ФЗ (обработка персональных данных необходима для осуществления прав и законных интересов оператора или третьих лиц) для целей обоснования обработки персональных данных.
- Дать официальные разъяснения для бизнеса в отношении:
  - применения Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» к компаниям;
  - механизма оценки и принятия решений в соответствии с Федеральным законом «О безопасности критической информационной инфраструктуры Российской Федерации».
- Отказаться от принятия нормативно-правовых актов, предписывающих частным компаниям осуществить переход на «преимущественное использование» российского программного обеспечения и оборудования на объектах критической информационной инфраструктуры.
- Ускорить принятие законодательной базы для новых технологий, чтобы исключить отставание от мирового рынка высоких технологий.

СОСТОЯНИЕ И ТЕНДЕНЦИИ РАЗВИТИЯ РОССИЙСКОГО ТЕЛЕКОММУНИКАЦИОННОГО РЫНКА

Российский рынок телекоммуникаций по-прежнему отличается высокой степенью консолидации.

Количество телефонов, смартфонов, планшетов и модемов, подключенных к мобильному интернету (основному драйверу роста доходов операторов) в России составляет около 100 миллионов.

Инновации стимулируют развитие общества, полностью охваченного подключением к Интернету. Развивается перспективный сегмент рынка – интернет вещей (IoT), предполагающий подключение к сети различных объектов. Уже сегодня подключения M2M в мире демонстрируют годовой рост в 40%. С появлением IoT этот сегмент ожидает взрывное развитие.

На данный момент по объему Enterprise-рынка интернета вещей среди российских отраслей с большим отрывом лидирует транспортная отрасль – 13,1 млрд рублей. Эта сумма в значительной степени формируется системами автотранспортной

телематики (они составляют порядка 44% от текущего количества всех M2M-подключений).

Еще одним востребованным сегментом корпоративного ИКТ-рынка является информационная безопасность. Согласно прогнозу IDC, к 2022 году среднегодовой темп роста рынка корпоративных ИБ-услуг составит 3,9%. Этому способствует рост числа киберугроз – одно только развитие интернета вещей в ближайшие годы спровоцирует лавинообразное увеличение числа устройств, подключенных к глобальной сети. Наличие угроз с такого количества неуправляемых или слабо управляемых устройств приведет к необходимости обеспечивать защиту как существующих онлайн-сервисов, так и вновь подключаемых объектов.

Новое поколение мобильной связи 5G является сейчас наиболее обсуждаемым вопросом в области телекоммуникаций. Одним из самых сложных вопросов является вопрос выделения частот для развертывания сетей связи 5G.

Наиболее распространенным частотным диапазоном для внедрения сетей 5G по всему миру является диапазон 3400-3800 МГц. Это объясняется тем, что в большинстве стран в этом диапазоне есть достаточно широкие свободные полосы частот – около 100 МГц на оператора, которые могут быть использованы для передачи растущих объемов трафика. Широкая доступность этого диапазона во многих странах делает его приоритетным при разработке пользовательских устройств: в первую очередь смартфонов.

Еще одна область частот, которая используется для развития сетей 5G в мире, – это диапазоны частот свыше 26 ГГц. Сегодня в этих диапазонах работают только операторы в США. В перспективе к ним присоединятся и другие страны, в первую очередь Европа (ожидается в 2021 году) и Южная Корея.

В Российской Федерации наиболее перспективный диапазон (3400-3800 МГц) занят в основном военными и спутниковыми системами связи, которые не планируется переводить на другие частоты в ближайшее время. Операторы и производители оборудования ожидают от регулятора решения вопроса выделения/расчистки частот как можно скорее, иначе Россия может существенно отстать во внедрении и развитии нового поколения связи от остального мира.

ЧЛЕНЫ КОМИТЕТА

ABB • Accenture • AIG Insurance Company JSC • ALRUD Law Firm • Antal Russia • Atos • Baker Botts • Baker McKenzie • Bayer • Beiten Burkhardt • Brother • Capital Legal Services • CMS Russia • Coleman Services UK • Credit Agricole • Dassault Systems • Deloitte • Dentons • Egorov Puginsky Afanasiev & Partners • Ericsson • EY • General Electric • Google Russia • HSBC Bank • JTI • Morgan Lewis • Noerr • Nokia Solutions & Networks • Orange Business Services • PwC • Pepeliaev Group • Philips • PwC • Sanofi • SAP C.I.S • SCHNEIDER GROUP • Siemens LLC • TeliaSonera International Carrier • Tieto • VEGAS LEX Advocate Bureau • Zurich Reliable Insurance.

IT & TELECOM COMMITTEE

Chairman:
Edgars Puzo, Atos

Deputy Chairpersons:
Vadim Perevalov, Baker McKenzie; **Aleksandra Shmigirilova**, Ericsson;
Gleb Vershinin, SAP CIS

Committee Coordinator: **Svetlana Lomidze** (svetlana.lomidze@aebrus.ru)

PROSPECTS FOR THE DEVELOPMENT OF THE REGULATION OF TELECOMMUNICATIONS AND INFORMATION TECHNOLOGIES IN RUSSIA

INTRODUCTION

In 2020 the coronavirus pandemic led to an increased demand for various IT solutions, significantly speeding the pace of digital transformation of the Russian economy. Broad support of the Government's efforts from Russian and international telecommunications and IT companies, many of which have provided expanded access to their infrastructure and services, became the foundation for the stability of the Russian economy during the self-isolation period.

Digital transformation and the achievement of 'digital maturity' in key economic sectors and the social sphere were first included in the updated development goals in accordance with the Decree on the National Development Goals of the Russian Federation for the Period up to 2030 signed by the President of the Russian Federation on 21 July 2020. The Government of the Russian Federation is developing indicators of the level of digital maturity and appropriate adjustments to national projects, including the Digital Economy Programme. The import phase-out policy has been implemented intensively owing to broad support measures for Russian IT companies, stimulating government demand for domestic products as well as due to the restriction of competition.

The experience of other European countries shows that restrictive measures aimed at protecting the internal market do not lead to the creation of competitive world-class products in the long term. However, a reverse effect is possible if similar restrictions are imposed on Russian products in foreign markets.

RUSSIAN LEGISLATION ON PERSONAL DATA

On 10 October 2018 the Russian Federation signed a protocol amending the 1981 Convention of the Council of Europe for the Protection of Individuals with Regard to Automatic Processing of Personal Data, which will help align the legislation of the Russian Federation and the European Union related to the processing of personal data.

On 2 December 2019 a law came into force introducing significant fines for non-compliance with requirements for the localization of databases containing personal data. The fines range from 1 to 18 million roubles for companies and from 100,000 to 800,000 roubles for CEOs and other top managers. The court has already imposed fines in the amount of 4 million roubles on Twitter and Facebook.

On 21 July 2020 the Russian Government submitted a draft law to the State Duma (https://sozd.duma.gov.ru/bill/992331-7) on the procedure for depersonalizing personal data; the requirements and methods for depersonalizing such data will be approved by the Federal Service for Supervision of Communications, Information Technology and Mass Media. For the purpose of personal data erasure in IT systems, the draft law prescribes using only security products that have been certified by the Federal Service for Technical and Export Control (FSTEC) or the Federal Security Service (FSS), which will create additional difficulties for the data controller in fulfilling the legal requirement for the timely erasure of personal data.

EUROPEAN LEGISLATION ON PERSONAL DATA

On 25 May 2018 the EU General Data Protection Regulation entered into force. The GDPR is extraterritorial in nature and is applicable to a number of Russian companies, which, if they do not comply with it, may be subject to significant financial liability (for example, a fine in the amount of 20 million euros).

After the Court of Justice of the European Union issued the judgement in case C-311/18 (Schrems II) on 16 July 2020, uncertainty has emerged in the European legislation whether it is permissible to transfer personal data from the EU to Russia. We believe that to solve this problem, more active cooperation between state authorities of Russia and the EU is needed.

RESTRICTING ACCESS TO INFORMATION ON THE INTERNET

Recently, the Federal Service for Supervision of Communications, Information Technology and Mass Media has repeatedly pointed out the ineffectiveness of the mechanism for blocking information resources (for example, websites and mobile applications) that violate data protection legislation.

On 18 June 2020 the Federal Service for Supervision of Communications, Information Technology and Mass Media, in agreement with the General Prosecutor's Office of the Russian Federation, removed the

restrictions on access to Telegram. The decision taken by the Federal Service for Supervision of Communications, Information Technology and Mass Media suggests that a website or a mobile application may be unblocked out of court if the company has taken the necessary measures to comply with Russian legislation. We believe that it is advisable to apply this practice to other resources.

STORING USER MESSAGES AND USER DATA

There is still some uncertainty regarding the implementation of the Yarovaya package, in particular, regarding the obligations of telecom operators and organizers of information dissemination to store text messages, voice information, images, sounds, video and other messages of communication services users. Effective 1 July 2018, the above data must be stored for up to 6 months from the end of their collection, transmission, delivery and/or processing.

Due to the COVID-19 pandemic, telecom operators and the business community count on the relaxing of/changes in some of the legal requirements.

SECURITY OF CRITICAL INFORMATION INFRASTRUCTURE

On 1 January 2018 the Federal Law on the Security of the Critical Information Infrastructure of the Russian Federation came into force.

At the end of May, the Ministry for Digital Development, Communications and Mass Media of Russia proposed making a transition to the 'preferential use' of Russian software and equipment at CII facilities. In accordance with this proposal, the owners of CII facilities will be obliged to switch to the preferential use of software registered in the Russian register and the EAEU (Eurasian Economic Union) Software Register by 1 January 2021 and to the preferential use of Russian equipment by 1 January 2022.

Acceptance of the proposed requirements in their current version may lead to a failure of the IT systems supporting the operation of CII facilities, and CII entities will have to bear significant unreasonable costs for the purchase of new equipment and software when the life cycle of their already installed equipment and software has not yet expired. In addition, there is a risk of violation of WTO agreements if instruments are adopted restricting the purchase of foreign products by CII entities, many of which are privately owned.

RECOMMENDATIONS

- To involve experts from international and professional associations to participate in working groups and expert councils of the executive and legislative authorities in the development of a legal regime comprising concepts that are relevant for the modern digital economy (big data, Internet of Things etc).
- To develop a balanced approach to the distribution of costs between business and the state with regard to the implementation of the Yarovaya package.
- To develop an official position on the GDPR, the possibility of cross-border transfer of personal data from the EU to Russia and vice versa and approaches that would make it possible to effectively implement the changes provided for by the revised Convention of the Council of Europe in Russian legislation on personal data.
- To issue official explanations and create conditions for broader practical application by data controllers of clause 7 of part 1 of article 6 of 152-FZ (processing of personal data is necessary to exercise the rights and legitimate interests of the data controller or third parties) for the purpose of justifying personal data processing.
- To issue official explanations on the following matters:
  (a) application of the Federal Law 'On the Security of the Critical Information Infrastructure of the Russian Federation' to companies;
  (b) the mechanism for assessment and decision-making in accordance with the Federal Law 'On the Security of the Critical Information Infrastructure of the Russian Federation'.
- To decline to adopt regulatory instruments instructing private companies to switch to the 'preferential use' of Russian software and equipment at critical information infrastructure facilities.
- To accelerate adoption of a legal framework for new technologies in order to not lag behind the global high-tech market.

STATE AND DEVELOPMENT TRENDS IN THE RUSSIAN TELECOMMUNICATIONS MARKET

The Russian telecommunications market remains highly consolidated.

The number of phones, smartphones, tablets and modems connected to the mobile internet (the main driver of operators' revenue growth) in Russia is about 100 million.

Innovations stimulate the development of a society fully connected to the internet. A promising market segment is developing – the Internet of Things (IoT), which involves connecting various objects to the network. Already today, M2M connections in the world demonstrate an annual growth of 40%. With the emergence of the IoT, this segment is expected to explode.

At the moment, the transport industry is a leader in terms of the volume of the enterprise market of the Internet of Things among Russian industries – 13.1 billion roubles. This amount is largely generated by vehicle telematics systems (they account for about 44% of the current number of all M2M connections).

Data security is another popular segment of the corporate ICT market. According to the IDC forecast, the average annual growth rate of the corporate cybersecurity service market will amount to 3.9% by 2022. This is facilitated by the growing number of cyberthreats – the development of the Internet of Things alone in the coming years will provoke an avalanche-like increase in the number of devices connected to the global network. The presence of threats from so many unmanaged or poorly managed devices will lead to a need to protect both existing online services and newly connected objects.

The next generation of 5G mobile communications is currently the most debated issue in the telecommunications industry. One of the most difficult issues is the issue of frequency allocation for the deployment of 5G communication networks.

The most common frequency range for 5G networks worldwide is 3,400–3,800 MHz. This is due to the fact that this range has quite wide free frequency bands in most countries – about 100 MHz per operator, which can be used to transmit growing traffic volumes. The wide availability of this range in many countries makes it a priority in the development of consumer devices, primarily, smartphones.

Another frequency area used for the development of 5G networks in the world is the frequency ranges above 26 GHz. Only US operators currently work on these bands. In the future, other countries will join them, primarily, Europe (expected in 2021) and South Korea.

As to the Russian Federation, the most promising range (3,400–3,800 MHz) is occupied mainly by military and satellite communication systems, which are not planned to be transferred to other frequencies in the near future. Operators and equipment manufacturers expect the regulator to resolve the issue of allocating/clearing frequencies as soon as possible; otherwise Russia may significantly lag behind the rest of the world in the implementation and development of the new generation of communications.

COMMITTEE MEMBERS

ABB • Accenture • AIG Insurance Company JSC • ALRUD Law Firm • Antal Russia • Atos • Baker Botts • Baker McKenzie • Bayer • Beiten Burkhardt • Brother • Capital Legal Services • CMS Russia • Coleman Services UK • Credit Agricole • Dassault Systems • Deloitte • Dentons • Egorov Puginsky Afanasiev & Partners • Ericsson • EY • General Electric • Google Russia • HSBC Bank • JTI • Morgan Lewis • Noerr • Nokia Solutions & Networks • Orange Business Services • PwC • Pepeliaev Group • Philips • PwC • Sanofi • SAP C.I.S • SCHNEIDER GROUP • Siemens LLC • TeliaSonera International Carrier • Tieto • VEGAS LEX Advocate Bureau • Zurich Reliable Insurance.