Стенограмма парламентских слушаний на тему «Неприкосновенность частной жизни в условиях цифровизации и ответственность за ее нарушение»

31 мая 2021 года

И.В. РУКАВИШНИКОВА

Уважаемые коллеги, дорогие друзья! Мы рады вас приветствовать на сегодняшних парламентских слушаниях, посвященных вопросу неприкосновенности частной жизни в условиях цифровизации и ответственности за ее нарушение.

Думаю, что лучшим вступлением к нашему мероприятию будет небольшая иллюстрация результатов социологического опроса, проведенного фондом "Общественное мнение", который состоялся в марте этого года. Напомню, что данная статистика впервые была представлена на заседании Научно-экспертного совета при Председателе Совета Федерации "Развитие цифровой среды в Российской Федерации как пространства безопасности, верховенства права и устойчивого развития". Заседание этого совета состоялось 19 апреля текущего года.

На экране появляются слайды, которые я прокомментирую.

Первый слайд. На вопрос о том, больше пользы или вреда приносят информационные технологии, почти половина опрошенных (47 процентов) положительно оценили их развитие. Мнения оставшейся аудитории разделились между ответами "затрудняюсь ответить", "польза и вред одновременно". И только 20 процентов опрошенных видят однозначный вред от применения цифровых технологий.

Далее. Интересно, что мнения варьировались в зависимости от образования (наличия высшего образования) и возраста респондентов. Превалирующее число выступающих за пользу информационных технологий наблюдается в группе от 18 до 30 лет. По мере увеличения возраста респондентов количество положительных оценок снижается. При этом интересен тот факт, что респонденты с высшим образованием чаще других видят полезные стороны развития информационных технологий.

Следующий слайд, пожалуйста, покажите.

Обратите внимание на то, что в числе наиболее полезных свойств "цифры" респонденты отмечают повышение… Здесь ответы сформулированы и расположены по степени популярности – от более популярного к менее популярному. Следующие полезные свойства: повышение доступности информации и увеличение ее объема, удобство в получении услуг, получение знаний, расширение возможностей в целом, экономия времени. И примечательно, что третий по

популярности ответ звучит следующим образом: "Развитие технологий важно для прогресса нашей страны".

Свои доводы приводят и те, кто видит в развитии информационных технологий больше вреда, нежели пользы, – в частности, увеличение объема ложной, неоднозначной информации, зависимость от гаджетов, снижение интеллектуального развития (используется даже такое слово, как "отупение"), вред экологии, здоровью людей, доступ к ненужной, лишней или аморальной информации.

Также в ходе исследования был задан вопрос об отношении к размещению персональных данных в интернете. И здесь мы видим серьезный рост обеспокоенности граждан по поводу сохранения конфиденциальности персональных данных. По сравнению с 2013 годом в два раза выросло число людей, которые переживают по поводу сохранности личной информации в сети. При этом наибольшую обеспокоенность за сохранность своих персональных данных в интернете высказали люди, входящие в возрастную группу от 30 до 45 лет, имеющие высшее образование.

Что же вызывает наибольшие опасения? Самый популярный ответ (на следующем слайде, мы сейчас его увидим) – это возможная потеря денежных средств в случае хищения данных банковской карты.

Следующий слайд нам покажите, пожалуйста.

Также чаще всего людей беспокоят возможные мошенничество и другие преступные действия, использование персональных данных во вред их обладателю – в частности, оформление кредитов на чужое имя, разглашение личных данных, вмешательство в личную жизнь, жизнь семьи. Другими словами, речь идет о том, насколько распространение и использование цифровых технологий обеспечивает соблюдение конституционных прав каждого на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени.

Как в практике цифровой трансформации реализуется конституционный принцип свободы поиска, получения, передачи, производства и распространения информации в сочетании с конституционным запретом на сбор, хранение, использование и распространение информации о частной жизни лица без его согласия?

Спасибо большое. Слайды можно уже убрать.

Очевидно, что реализация конституционных принципов через нормы отраслевых законов должна создавать понятную и непротиворечивую правоприменительную практику, основанную на балансе частных и публичных интересов. При этом правовое регулирование таких сфер, как

частная жизнь, семейная тайна, честь, доброе имя, всегда вызывало и вызывает повышенный интерес и внимание в силу сложности и многоаспектности самих категорий. Вероятно, поэтому мы видим большое количество обращений граждан в судебные органы, в том числе в Конституционный Суд Российской Федерации.

Конституционное право каждого на неприкосновенность частной жизни получило довольно подробное исследование в документах Конституционного Суда. Например, разъяснение ключевого понятия "частная жизнь". Конституционный Суд называет частной жизнью ту область жизнедеятельности человека, которая относится к отдельному лицу, касается только его и не подлежит контролю со стороны общества и государства, если она носит непротивоправный характер.

Приведенные нормы соотносятся с положениями международно-правовых договоров Российской Федерации, в том числе Конвенции о защите прав человека и основных свобод.

Европейский суд по правам человека в своих решениях указывал, что информационно-телекоммуникационная сеть Интернет ввиду ее общедоступности и способности хранить и распространять огромные объемы информации играет важную роль в расширении доступа общественности к новостям и в облегчении распространения информации вообще.

В то же время опасность того, что материалы и информация в сети Интернет могут причинить вред осуществлению прав и свобод лица, особенно права на частную жизнь, и пользованию этими правами и свободами, определенно выше, чем опасность, исходящая от печатных средств массовой информации.

Указанные фундаментальные права общепризнаны в правовых демократических государствах постольку, поскольку они защищают являющиеся одинаково значимыми интерес частного лица в обеспечении его приватности, с одной стороны, и интерес широкой общественности в доступе к информации – с другой, не находятся в состоянии главенства и подчинения и не обладают безусловным приоритетом друг перед другом. В связи с этим необходимо установить баланс между защитой частной жизни и свободой выражения мнения.

Публикации, направленные исключительно на удовлетворение любопытства определенного круга читателей относительно подробностей личной жизни лица, каким бы известным оно ни было, как правило, не могут считаться вкладом в дискуссию, представляющую общественный интерес.

В одном из определений Конституционного Суда Российской Федерации содержится разъяснение категории общественного интереса, к которому следует относить не любой интерес, проявляемый аудиторией, а, например, потребность общества в обнаружении и раскрытии угрозы демократическому правовому государству и гражданскому обществу, общественной безопасности, окружающей среде.

Конституция Российской Федерации устанавливает, что осуществление прав и свобод человека и гражданина не должно нарушать права и свободы других лиц, к числу которых относятся, в частности, право на охрану достоинства личности и право на защиту своих чести и доброго имени.

Также Конституционный Суд Российской Федерации неоднократно обращал внимание на то, что Конституция России возлагает на государство обязанность охранять достоинство личности, чем утверждается приоритет личности и ее прав, причем эта охрана должна осуществляться во всех сферах.

Правовые позиции высших судебных органов являются ориентиром и вектором законотворческой деятельности. Основные отраслевые законы, регулирующие вопросы информационного пространства, были приняты в один день – 27 июля, 15 лет назад, в 2006 году. Речь идет о Федеральном законе "О персональных данных" и о Федеральном законе "Об информации, информационных технологиях и о защите информации". И сегодня мы уверенно можем говорить о том, что созданный правовой фундамент является достаточно прочным, стабильным и эффективным. Об этом свидетельствует относительно небольшое количество поправок, внесенных в данные федеральные законы за прошедшее время.

Федеральный закон "О персональных данных" содержит ключевые принципы и условия обработки персональных данных, права субъекта персональных данных, обязанности оператора персональных данных, а также очерчивает полномочия государственных органов в сфере защиты прав субъекта персональных данных.

Закон об информации закрепляет понятие информации как объекта правоотношений, определяет случаи ограничения доступа к информации, ключевые правила использования информационно-телекоммуникационных сетей, устанавливает требования к защите информации.

Появление новых информационных технологий, несущих как преимущества, так и угрозы, обязательно формирует новые общественные отношения, нуждающиеся в правовом обеспечении. Если проследить историю поправок в законодательство, то можно увидеть, в какой

последовательности возникали те или иные новые информационные отношения. Например, в 2013 году в законе об информации был закреплен порядок ограничения доступа к информации, распространяемой с нарушением авторских или смежных прав, а также предусмотрены внесудебные меры по прекращению нарушения этих прав.

В части защиты персональных данных граждан в 2014 году в данном федеральном законе был закреплен порядок ограничения доступа к информации, обрабатываемой с нарушением законодательства Российской Федерации в области персональных данных. Была создана автоматизированная информационная система "Реестр нарушителей прав субъектов персональных данных". Целью этого реестра является ограничение доступа к информации в сети Интернет, обрабатываемой с нарушением законодательства в области персональных данных. Основанием для внесения в реестр нарушителей является решение суда о признании деятельности по распространению персональных данных, а также права субъекта персональных данных на неприкосновенность частной жизни, личную и семейную тайну.

Одновременно с этим федеральным законом о персональных данных для оператора персональных данных была установлена новая обязанность, предполагающая локализацию баз данных, содержащих персональные данные граждан Российской Федерации, на территории России. Требования о локализации персональных данных применяются и к иностранным компаниям, которые не имеют физического присутствия в России, если они осуществляют деятельность, направленную на территорию нашей страны.

С появлением новых субъектов правоотношений в информационной сфере, таких как, например, аудиовизуальные сервисы, в законодательстве появлялись нормы, устанавливающие обязанности таких субъектов с учетом особенностей их деятельности. Так, последовательно в 2014, 2015, 2017 и 2020 годах в законе об информации появлялись положения, регулирующие деятельность операторов поисковых систем, новостных агрегаторов, владельцев аудиовизуальных сервисов и, наконец, владельцев социальных сетей.

Одним из недавних изменений законодательства о защите персональных данных (напомню, это был конец прошлого года) стало обязательное получение согласия субъекта на использование его персональных данных. Кроме того, закреплены право субъекта на запрет обработки его данных и право требовать удаления информации о себе оператором персональных данных. При этом не допускается получение оператором согласия по умолчанию или бездействию субъекта персональных данных.

Важным направлением защиты интересов личности является противодействие распространению заведомо ложной и порочащей информации. Интересны в связи с этим поправки в федеральный закон о средствах массовой информации, касающиеся ответственности сотрудников СМИ. Конечно, система установленных правил и ограничений в сфере работы с информацией, затрагивающей интересы личности, была бы неэффективна без соответствующих норм, устанавливающих ответственность за нарушение указанных требований. Соответствующие статьи об ответственности содержатся в Кодексе об административных правонарушениях, а также в Уголовном кодексе. Уголовное законодательство предусматривает ответственность за нарушение неприкосновенности частной жизни, а также за клевету, то есть распространение заведомо ложных сведений, порочащих честь и достоинство другого лица или подрывающих его репутацию.

Уважаемые коллеги, сфера цифровизации общественных отношений сегодня самая динамичная. При этом законодательное регулирование новых явлений и процессов в информационном пространстве все еще происходит с опозданием, хотя за последнее время этот временной разрыв значительно сократился. Одним из катализаторов развития законодательства и научных исследований в этой области стал прошлый год, высветивший как множество новых направлений цифровизации экономики, так и существующие пробелы правового регулирования.

В идеальном варианте законодательное обеспечение должно быть синхронизировано с фиксацией новых цифровых явлений, а при необходимости работать на опережение, то есть предупреждать возможное возникновение негативных факторов в этой сфере. Думаю, что научная дискуссия о формировании отрасли цифрового права, которая в настоящее время происходит в науке, обязательно должна затронуть вопрос перспективного правового регулирования сферы применения цифровых технологий. Уверена, что формирование доктринальных подходов окажет положительное влияние не только на разработку качественных правовых норм, особенно в сфере регламентации новых информационных продуктов, но и в целом на развитие законодательства и правоприменительной практики.

Указом Президента Российской Федерации утверждена Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы. Этот документ содержит, по сути, "дорожную карту" процесса развития информационной и коммуникационной структуры, обеспечения свободного доступа граждан и организаций, органов государственной власти Российской Федерации, органов местного самоуправления к информации на всех этапах ее

создания и распространения. При этом особое внимание уделяется вопросам защиты персональных данных.

В числе первоочередных мер: совершенствование нормативно-правового регулирования в сфере обеспечения безопасной обработки информации; обеспечение баланса между своевременным внедрением современных технологий обработки данных и защитой прав граждан, включая право на личную и семейную тайну; обеспечение обработки данных на российских серверах при электронном взаимодействии лиц, находящихся на территории Российской Федерации, а также передачи таких данных с использованием сетей связи российских операторов; обеспечение государственного регулирования и координации действий при создании и ведении информационных ресурсов в Российской Федерации в целях соблюдения принципа разумной достаточности при обработке данных; проведение мероприятий по противодействию незаконным обработке и сбору сведений о гражданах, в том числе персональных данных граждан, на территории Российской Федерации.

Уважаемые коллеги! Сегодня мы будем обсуждать вопросы эффективности правового регулирования использования информации в контексте реализации конституционных прав граждан и сохранения баланса частных и публичных интересов, повышения цифровой грамотности населения. Уверена, что в ходе дискуссии будут подняты вопросы повышения качества межведомственного взаимодействия, в том числе взаимодействия с органами государственной власти субъектов Российской Федерации. Также уместно было бы коснуться проблем правоприменительной практики, анализ которой всегда дает новые законодательные импульсы.

Напомню, что названная тематика является приоритетной в рабочей повестке Совета по развитию цифровой экономики, который возглавляет первый заместитель Председателя Совета Федерации Андрей Анатольевич Турчак. И именно поэтому все предложения, озвученные в рамках парламентских слушаний, пройдут серьезную проработку на предмет формирования возможных законодательных инициатив.

Уважаемые коллеги, достаточно большое количество участников сегодня было заявлено на наше мероприятие. Как показывает практика, работа в течение двух часов, если не соблюдать регламент, не позволяет высказаться всем, поэтому заранее прошу прощения у тех, до кого сегодня слово, возможно, и не дойдет. Сразу предупреждаю о том, что все ваши предложения, которые будут высказаны, которые у вас имеются, должны быть направлены в наш адрес, и в

течение этой и следующей недель мы их ждем от вас, для того чтобы включить в итоговый документ, который будет принят по итогам сегодняшнего мероприятия – парламентских слушаний.

Уважаемые коллеги, прежде чем мы перейдем непосредственно к докладам, я бы хотела представить моих коллег, которые сегодня здесь, в Совете Федерации, принимают участие в нашей работе, – это Дина Ивановна Оюн и Харлов Вадим Борисович, сенаторы Российской Федерации, коллеги и активные участники сегодняшнего мероприятия.

Дорогие друзья! Я бы хотела предоставить возможность выступить сейчас Вагнеру Милошу Эдуардовичу, заместителю руководителя Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций.

Милош Эдуардович, пожалуйста.

М.Э. ВАГНЕР

Здравствуйте, коллеги! Здравствуйте, Ирина Валерьевна! Спасибо за возможность поучаствовать в этом мероприятии.

Действительно, неприкосновенность частной жизни – один из наиболее часто встречающихся предметов для общественной дискуссии по поводу обработки персональных данных, потому что бóльшая часть сведений о частной жизни – действительно персональные данные. И, как Вы уже сказали, законодательство в этой сфере развивается, развивается поступательно.

В частности, за последний год принят закон, который позволяет любому гражданину требовать удаления своих персональных данных из общего доступа. Внесены изменения в Кодекс об административных правонарушениях, которыми увеличены срок давности по делам об административных правонарушениях в области персональных данных с трех месяцев до одного года, размер санкций за такие нарушения.

Тематика обращений в Роскомнадзор, связанных с персональными данными, достаточно различна – это и обработка данных в рамках различных гражданских договоров, и законность обработки персональных данных при взыскании задолженности, и вопросы хранения персональных данных, и в том числе обработка биометрических персональных данных, включая использование систем видеонаблюдения.

И, вы знаете, такой анализ схож с данными, которые Вы в начале озвучили, опроса ВЦИОМ. Людей беспокоит обработка их персональных данных и риски, которые несет такая обработка прямо здесь и сейчас, то есть сейчас возможно мошенничество, сейчас возможно

вмешательство в частную жизнь. При этом запроса и оценки рисков со стороны граждан о том, какие риски будут от такой неконтролируемой обработки персональных данных через три года, пять, 10 лет, не прослеживается, то есть всех беспокоит, что именно сейчас происходит с обработкой этих персональных данных. И, возможно, действительно требуется какой-то, как Вы сказали, научный комплексный анализ изменившегося информационного ландшафта с учетом развития технологий, с учетом того, что сейчас обработка персональных данных происходит преимущественно в сети Интернет и с помощью новых технологий, которые находятся далеко вне контроля самого человека.

Если говорить о возможных предложениях с точки зрения изменения текущего законодательства, что мы наблюдаем? У нас есть административная ответственность за обработку персональных данных в случаях, не предусмотренных законодательством. Однако зачастую оператор, пользуясь законодательно установленными правами, обрабатывает персональные данные, при этом нарушая требование конфиденциальности. В этом случае нарушение законодательства есть, однако административную ответственность установить не получается.

И второе, возможно, изменение в законодательство – чтобы операторы персональных данных в случае возникновения у них каких-то инцидентов с обработкой персональных данных информировали уполномоченные органы, в том числе Роскомнадзор, о произошедшем, чтобы мы могли принять какие-то превентивные меры для восстановления нарушенных прав, в частности, например, в рамках ведения Реестра нарушителей прав субъектов персональных данных выявить сайты, где такие данные уже размещаются, либо подать исковые заявления об ограничении доступа к таким ресурсам, либо уже в рамках действующих полномочий направить требование об удалении этих персональных данных.

Вот, наверное, буквально два слова, которые по сегодняшней теме хотелось бы сказать. Спасибо.

И.В. РУКАВИШНИКОВА

Милош Эдуардович, спасибо большое.

Я позволю себе немножко отойти от нашего регламента, поскольку уж очень краткое выступление у Вас получилось. У меня вопрос тогда к Вам такой по поводу этого реестра: насколько он активно пополняется? Может быть, Вы чуть более широко по этому поводу скажете? И какие Вы видите проблемы на сегодняшний день в правоприменительной практике?

Мы начали говорить, в общем-то, с того, что законодательство достаточно широкий спектр мер предоставляет гражданам для защиты нарушенных прав и возможности реагирования. Но насколько часто граждане используют этот механизм, насколько он доступен для простоты понимания и использования? Есть ли по этому поводу какая-то статистика? Потому что пока по крайней мере в информационном пространстве, к сожалению, мы сталкиваемся с информацией об утечках, о нарушениях прав (об этом сегодня тоже будем говорить). Вот насколько эффективно идет противодействие в правовом пространстве? Насколько активно граждане инициируют эти процессы, те граждане, чьи права нарушены (если есть такая статистика)? Спасибо.

М.Э. ВАГНЕР

Если говорить относительно применения статьи 15.5 (о ней идет речь) закона об информации и информационных технологиях, мы действительно ведем Реестр нарушителей прав субъектов персональных данных. Однако по закону единственным правовым основанием для включения каких-то доменных имен или указателей страниц в этот реестр является судебное решение. То есть, до того как требовать от оператора удаления персональных данных на основании сведений из реестра или передавать операторам связи для ограничения доступа к каким-то указателям страниц информацию, нужно получить судебное решение. Судебное решение, как все мы прекрасно понимаем, – это дело не одного-двух-трех дней, речь идет о месяцах. Как правило, за такими судебными решениями обращается Роскомнадзор и в тех случаях, когда понимает, что в рамках иных полномочий добиться прекращения распространения персональных данных и нарушения прав субъекта персональных данных не получается, то есть когда мы понимаем, что речь идет об умышленном размещении копий баз данных, телефонных справочников и так далее.

Если говорить о статистике, то за прошлый год включено 726 интернет-ресурсов в этот реестр. При этом в большинстве случаев после получения судебного решения операторы таких интернет-сайтов удаляют противоправную информацию, но при этом все еще порядка 400 с лишним ресурсов остаются заблокированными на основании сведений из этого реестра. То есть Реестр нарушителей прав субъектов персональных данных – это уже крайняя мера, когда владелец сайта не реагирует на требования Роскомнадзора, когда не реагирует на законные требования субъектов персональных данных. То есть это крайняя мера, в общем-то. Спасибо.

И.В. РУКАВИШНИКОВА

Насколько часто граждане обращаются в Роскомнадзор за защитой своих прав, используя административные механизмы?

М.Э. ВАГНЕР

У нас порядка 40 тысяч обращений граждан в год, большинство из них – это действительно жалобы. Обращений за разъяснением законодательства достаточно небольшое количество. Тематику обращений я обозначил. В основном жалуются на деятельность управляющих компаний, на деятельность организаций кредитной сферы, на деятельность организаций, взыскивающих задолженность, то есть, по сути, речь идет о правомерности и законности обработки персональных данных.

Иногда возникают вопросы о том, насколько правомерно заводили ту или иную персональную информацию такие операторы. В данном случае тогда речь идет о нарушении условий конфиденциальности. Но таких обращений не так много по сравнению с общим количеством – порядка 350–400 случаев в год, когда происходит нарушение конфиденциальности, когда граждане чувствуют, что что-то произошло, и действительно в рамках законной деятельности оператор передал персональные данные тому, кому он не должен был их передавать.

И.В. РУКАВИШНИКОВА

Спасибо большое.

Но мне кажется, что действительно очень небольшое количество обращений объясняется пока тем, что, во-первых, эта сфера еще не совсем изучена, исследована и понята до конца, тем, что законодательство относительно "молодое", и тем, что, возможно, граждане просто не понимают, каким образом правильно действовать, не имеют четкого понимания и алгоритма действий в том случае, когда их права нарушены. И здесь, естественно, мы опять возвращаемся к постоянной нашей теме, к разъяснительной работе, просветительской работе, которую ведут все государственные органы, и опять адресуем вам такую просьбу. Я думаю, что запрос на постоянные разъяснения, на консультации, конечно, очень высок.

Милош Эдуардович, большое Вам спасибо за то, что Вы нашли возможность выступить. Но я все-таки хочу попросить Вас побыть с нами до конца по возможности, для того чтобы в завершение еще тоже какие-то итоги вместе с нами подвести. Спасибо большое.

Уважаемые коллеги, передаю микрофон Виталию Григорьевичу Колесникову, заместителю руководителя Федеральной налоговой службы.

Виталий Григорьевич, пожалуйста.

В.Г. КОЛЕСНИКОВ

Добрый день, уважаемая Ирина Валерьевна! Спасибо большое за предоставленную возможность сказать о нашем статусе исполнения закона № 168 о едином регистре, содержащем сведения о населении Российской Федерации. И одновременно я хотел бы поднять вопрос, как мы предполагаем в контексте нашего совещания защищать персональные данные, те сведения, которые будут у нас в реестре.

Пожалуйста, поставьте сначала первую презентацию, которая называется "Создание ЕРН". У меня все зависло.

Меня слышно?

И.В. РУКАВИШНИКОВА

Да, Вас слышно, но у нас почему-то…

В.Г. КОЛЕСНИКОВ

Меня слышно?

И.В. РУКАВИШНИКОВА

Да-да, Виталий Григорьевич, мы Вас слышим и видим, но мы можем представить только ту Вашу презентацию, которую Вы нам передали.

С МЕСТА

Вторую – формат не позволяет.

И.В. РУКАВИШНИКОВА

А вторую Вы передали в каком-то формате, который…

В.Г. КОЛЕСНИКОВ

Включите, пожалуйста, первую презентацию, которая…

И.В. РУКАВИШНИКОВА

Первую презентацию, пожалуйста, включите. *(Оживление в зале.)*

В.Г. КОЛЕСНИКОВ

А есть еще первая презентация? EXE-файл исполнимый, пожалуйста, запустите.

И.В. РУКАВИШНИКОВА

Виталий Григорьевич, это все, что у нас есть. Все остальное не было передано от ваших сотрудников. Вот все, что есть, мы можем запускать.

В.Г. КОЛЕСНИКОВ

Давайте тогда так сделаем. Я сначала скажу о статусе нашего закона, а потом перейду к информационной безопасности.

Закон № 168 мы исполняем, и, как Вы помните, Ирина Валерьевна, вы, как Совет Федерации, брали под контроль в том числе издание подзаконных нормативных актов, которые регулируют точное исполнение тех или иных правил, которые в законе определены в общем порядке.

Соответственно, было издано распоряжение правительства, точнее – план-график, который утвержден заместителем председателя правительства Григоренко, об издании 19 подзаконных актов. Сроки заканчиваются по одному акту в 2022 году, по шести актам – в 2020–2021 годах. Хочу доложить, что все, что было необходимо сделать в 2020 году, мы выполнили. В том числе были приняты первые шесть актов, критически важных для создания системы.

Напоминаю, что система у нас начинает функционировать уже с 1 января 2022 года, а сведения она будет выдавать с 1 января 2023 года. Соответственно, приняты постановления правительства о формировании записи и номера записи, о направлении поставщиками сведений в ЕРН (в том числе для целей первоначального наполнения ЕРН, чем мы будем заниматься уже в этом году), о проверке поставщиками сведений на полноту, актуальность и достоверность перед направлением в ЕРН, использование УКЭП при ведении ЕРН. Остальные пункты плана-графика находятся уже в проектах на согласовании в федеральных органах исполнительной власти. И у нас нет особых сомнений в том, что они будут приняты в указанные в плане-графике правительства сроки.

Что еще я хочу сказать? Мы уже приступили фактически к практической апробации представленных сведений. Напоминаю, что в регистр населения будут предоставляться сведения 12 поставщиками (всего 34 вида таких сведений), и основные сведения – это, безусловно, из ЕГР ЗАГС, оператором которого также является Федеральная налоговая служба, и из МВД России. Мы очень надеемся, что МВД России предоставит сведения в уже согласованных нами форматах из новой системы, которую они создают фактически в этом году. И соответственно мы запускам наш регистр в следующем году и начинаем его уже проверять, наполнять и готовиться к предоставлению сведений другими поставщиками.

В части опытной эксплуатации могу сказать, что сегодня по сведениям, которые мы уже имеем в АИС "Налог-3", в том числе это косвенные сведения, которые нам предоставило МВД в

рамках статьи 85 Налогового кодекса, мы уже сформировали профили примерно 136 миллионов физических лиц нашей страны и отрабатываем их на консистентность, непротиворечивость, достоверность и соответствие всем другим сведениям, которые мы получаем от поставщиков, уже в рамках апробации и первоначальной выгрузки сведений.

Соответственно, мы в графике по внедрению регистра населения, это у нас такая большая проектная работа. И в целом на сегодня мы не видим каких-то критических позиций, которые заставляли бы нас усомниться в том, что мы вовремя не введем его в промышленную эксплуатацию. Опять-таки очень надеюсь, что органы МВД начиная с октября по графику нам начнут предоставлять уже реальные сведения для первоначального наполнения ФГИС ЕРН.

Одним из самых главных критериев, необходимых для принятия в промышленную эксплуатацию нашего реестра, будет, естественно, его готовность с точки зрения защиты данных, моделей угроз и аттестации системы как таковой. Система эта у нас отдельная. У нас, собственно говоря, в ФНС России всего четыре информационных системы, как ни странно, они все раздельные – это система налогового администрирования АИС "Налог-3", система ЕГР ЗАГС, о которой я говорил, система ФИАС (это государственный адресный реестр) и система регистра населения. Почему я это говорю? Я хочу сказать, что они отдельные, обособленные, каждая вращается на своих отдельных физических контурах и отдельно администрируется, поэтому там нет пересечения внутри (но я об этом чуть позже скажу).

Теперь приступаю к моему докладу по презентации, которая у вас на экране.

Пожалуйста, следующий слайд.

Здесь вы видите правовые основы нашей работы по защите данных в ЕРН. Мы прекрасно понимаем, что государственный регистр сведений о населении является фактически беспрецедентным источником и базой данных, тех сведений, которые в статье 7 закона прямо поименованы и которые мы собираем, и поэтому вопросам безопасности мы придаем большое значение. Не буду перечислять правовые основы, вы их видите на экране.

Пожалуйста, следующий слайд.

Это те задачи информационной безопасности, которые мы решаем при создании регистра населения. Соответственно, мы предотвращаем хищение данных, исключаем их модификацию, потому что они должны быть достоверны, и обеспечиваем доступность данных. Я хочу сказать, что абсолютно все эти задачи решаются в рамках соответствующих статей (особенно статей 8, 9 и

10) закона о регистре населения, где четко и абсолютно конкретно прописаны обязанности оператора регистра населения, которым является ФНС России.

Пожалуйста, следующий слайд.

Переходя к конкретным аспектам, как мы это делаем, хочу сказать, что регистр населения создается в ЦОД Минфина и ФНС России, в тех ЦОД, в которых, собственно говоря, происходит налоговое администрирование. У нас их два – в Дубне и в Городце. Мы обеспечиваем физическую охрану объектов. Время реагирования вы видите. Мы сегментируем зоны, то есть то, о чем я говорил, и, соответственно, все, что касается персональных данных, у нас обрабатывается в так называемом красном сегменте, защищенном. Это как бы ЦОД в ЦОД, куда имеет доступ только считаное количество обслуживающего персонала и где ведется непрерывный видео- и аудиоконтроль в периметре всей рабочей зоны.

Наши ЦОД аттестованы по уровню надежности международного института Tier III. Вы видите, что всего лишь на полтора часа в год они могут быть остановлены по различным причинам, то есть уровень надежности очень высокий. Все системы имеют двойное обеспечение, такие как электропитание, каналы связи, охлаждения и так далее.

Следующий слайд, пожалуйста.

Если рассматривать угрозы с точки зрения нарушителей, то нас особенно волнуют (и это показывает опыт и других наших коллег) внутренние нарушители, потому что против внешних мы более-менее научились бороться. Внутренние нарушители – это те люди, которые имеют официальные права доступа либо к обработке данных, либо к обслуживанию этих данных. Какие меры мы принимаем? Мы их ограничиваем по физическому доступу, о чем я говорил. Все копии мы шифруем (а копии, естественно, мы делаем). Мы обеспечиваем контроль несанкционированного доступа, в том числе привилегированных пользователей, которыми являются представители оператора, которые имеют право на постановку методологических задач, над данными. И, естественно, у нас четко прописаны ролевые модели – кто что и когда делает.

Естественно, у нас журналируются любые операции, которые производятся непосредственно с данными в ЦОД, и мы всегда, в любой момент можем посмотреть, кто когда и на основании каких данных, под каким именем и с какой электронной подписью внес изменения в запись о гражданине Российской Федерации в нашем ЦОД, в нашей системе.

Следующий слайд, пожалуйста.

Я уже говорил, что мы обрабатываем ЕРН в отдельном контуре – это ЦОД в ЦОД. Все обслуживание производится аттестованными сотрудниками нашего подведомственного казенного учреждения – ФКУ "Налог-Сервис". При этом инженерный состав, естественно, не имеет доступа к персональным данным. И хочу сказать, что как ЕГР ЗАГС, так и регистр населения мы строим целиком на отечественном ПО, отечественном оборудовании и соответствующих реестрах Минцифры России. И в этом плане я надеюсь и уверен, что у нас нет опасности, опасений, что кто-либо извне когда-нибудь сможет вмешаться в управление нашими данными, которые внутри регистра населения.

Следующий слайд, пожалуйста.

Хочу сказать, что, как оператор, естественно, мы создаем регистр населения не для того, чтобы он был как таковой, а чтобы он использовался в рамках оказания госуслуг (напомню цели основные закона № 168) посредством гармонизации данных других реестров с регистром населения, а также для представления сведений отдельным категориям, таким как правоохранительные органы, нотариусы, избирательные комиссии. И, соответственно, всё мы организуем в доверенной среде электронного правительства под управлением Минцифры в системе межведомственного электронного взаимодействия и выводим все виды сведений исключительно на площадку СМЭВ, где они регистрируются по установленным Минцифры правилам. Но это примерно то же самое, как мы делали и по АИС "Налог-3", и по ЕГР ЗАГС. Здесь не буду останавливаться.

Следующий слайд, пожалуйста.

Хочу сказать, что есть еще отдельная категория сведений в регистре населения, которая предполагает особую защиту – выделение в обособленный, физически разделенный сегмент данных, которые касаются защищаемых лиц: защита свидетелей, защита отдельных категорий государственных служащих – всех тех, кто подпадает под такую защиту.

Сейчас компетентными органами разрабатываются соответствующие нормативные акты, которые указаны в законе, по тому, как обращаться с этими сведениями. Но напоминаю, что закон уже содержит требование – в случае если лицо стало защищаемым, сведения о нем физически изымаются из регистра населения и помещаются в физически обособленный сегмент, у которого еще особая категория доступа к ним. Это фактически режимно-секретный объект, а не просто ЦОД ФНС России. Соответственно, при миновании надобности закрытия сведений об этих защищаемых лицах они на съемном (вот здесь изображена флешка) физическом носителе (не

через каналы связи, не через СМЭВ, не через какие-то сервисы, а исключительно на съемном носителе) возвращаются в регистр населения. То есть это так называемый воздушный зазор, который мы запланировали.

В целом мы готовимся к аттестации системы в конце года, плотно работаем с коллегами из регулирующих органов и будем представлять нашу систему, соответствующую аттестации, что является необходимым условием для ее ввода в промышленную эксплуатацию с 1 января 2022 года.

Мой доклад окончен. Извините за то, что не смогли продемонстрировать первую презентацию, но мы ее вам обязательно в материалах представим в нормальной и удобной форме. Спасибо.

И.В. РУКАВИШНИКОВА

Спасибо большое, Виталий Григорьевич, за такое подробное разъяснение и за презентацию.

Я думаю, что в начале следующей, осенней сессии, возможно, необходимо будет провести какое-то отдельное мероприятие, которое будет посвящено исключительно работе этого единого реестра. Тем более что есть такое поручение по мониторингу, а также мы понимаем, что с каждым днем вы продвигаетесь все дальше, и будет возможность более подробно, наверное, эту проблематику обсудить.

В.Г. КОЛЕСНИКОВ

Да. Будем готовиться, Ирина Валерьевна.

И.В. РУКАВИШНИКОВА

Спасибо большое.

Запланируем тогда совместное мероприятие.

Один вопрос. Конечно, Вы абсолютно правильно расставили риски и угрозы, и, наверное, легче защищаться от внешних угроз, чем от внутренних. Есть такое понятие, как человеческий фактор, который невозможно исключить ни в каком виде. Вы действительно рассказали нам о тех способах противодействия внутренним угрозам, которые могут быть (как я поняла; возможно, я Вас неправильно поняла, я бы хотела, чтобы Вы все-таки уточнили). Речь идет о возможности несанкционированного использования этой информации, ну, путем перекачивания с одного ресурса на другой, на флешку. Флешки вы тоже ставите под жесткий контроль и так далее. Но самый простой вариант – когда на экран выводится информация, человек имеет к ней доступ по

закону, он просто ее переписывает от руки либо фотографирует и потом использует ее, дает возможность ей утечь несанкционированно. Это нарушение конфиденциальности (то, о чем говорил Милош Эдуардович).

Как Вы считаете, насколько защищен будет реестр от такого рода действий сотрудников, которые будут допущены к его обслуживанию? И поддерживаете ли Вы предложение Милоша Эдуардовича о необходимости доработки законодательства об административной ответственности в части защиты конфиденциальности и использования конфиденциальной информации? Пожалуйста.

В.Г. КОЛЕСНИКОВ

По поводу внешних и внутренних нарушителей. Мы действительно особое внимание уделяем внутренним нарушителям. Почему? Потому что это наши сотрудники (ну, потенциально), которые могут в рамках своих различных каких-то интересов нарушать неприкосновенность персональных данных и, более того, ими пользоваться в других целях.

Соответственно, это может быть только либо персонал, который обслуживает ЦОД (а персонал, который обслуживает ЦОД, не имеет доступа к персональным данным, просто не имеет, то есть он обслуживает инженерные системы), либо это могут быть пользователи информационных систем, которые занимаются методологией или оценкой инцидентов. Под инцидентами мы понимаем любое несоответствие полученных сведений о человеке уже имеющимся сведениям в нашей системе. Вы помните, что, так как мы эталонная система, мы обязаны класть к нам в рамках обогащения профиля физического лица только то, в чем мы точно уверены. Соответственно, здесь у нас жесткая ролевая модель, жесткое журналирование и логирование операций. И сотрудники, которые являются методологами системы, работают на специально отведенных рабочих местах под постоянным видеоконтролем.

Всегда нужно, конечно, в рамках информационной безопасности быть очень аккуратными в прогнозировании будущего, но пока что (стучу по дереву) на сегодня у нас нет каких-либо существенных утечек, слава богу, связанных именно с внутренними нарушителями, утечек, которые были бы именно в рамках сегментов информационных баз как таковых. Поэтому в этом плане мы работаем, как и над всеми другими нашими системами.

Я хочу сказать, что ЕГР ЗАГС, оператором которого мы являемся, обладает еще и другими сведениями – сведениями, составляющими медицинскую тайну, сведениями о рождении и смерти. Уже три года скоро будет, как мы являемся оператором этой системы, и пока (тоже

стучу по дереву) в рамках всех принятых нами мер противодействия никаких нарушений мы не зафиксировали.

Что касается предложения Роскомнадзора, да, мы поддерживаем наших коллег и, конечно, готовы тоже включаться в эту работу, считаем это абсолютно правильным.

И.В. РУКАВИШНИКОВА

Большое спасибо. Тогда мы постараемся и ваше предложение, и предложение Роскомнадзора погрузить в итоговое решение по сегодняшним слушаниям.

Спасибо большое, Виталий Григорьевич. Я надеюсь, что Вы тоже с нами останетесь до завершения мероприятия. Возможно, будут вопросы еще у участников. Спасибо большое.

Уважаемые коллеги! Реуцкий Дмитрий Владимирович, временно исполняющий обязанности директора Департамента информационной безопасности Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации.

Дмитрий Владимирович, прошу Вас.

Д.В. РЕУЦКИЙ

Добрый день, Ирина Валерьевна! Добрый день, коллеги! Сейчас хотел бы кратко рассказать о том, какие проекты, направленные на защиту персональных данных, в министерстве на сегодняшний день есть.

Первый проект – это уже небезызвестный законопроект, в рамках которого мы вносим изменения в закон о персональных данных. Он готовится ко второму чтению. Сегодня по нему должно пройти заседание КЗД в правительстве. Мы, правда, не знаем сейчас оперативные данные, уже прошло заседание комиссии или нет, но сегодня он вынесен туда под пунктом 15.

Это законопроект, который мы уже освещали, направленный на установление ряда новшеств в отношении обработки персональных данных, в частности следующего. Предусматривается возможность предоставления согласия на обработку персональных данных в письменной форме одновременно на несколько целей. Мы сокращаем количество бумажной работы для операторов и граждан, которые уже реально не помнят, кто кому и сколько согласий дал. А в случае возникновения необходимости обработки персональных данных для дополнительных целей также не требуем собирать повторно эти данные и сокращаем количество хранимой информации у операторов.

Дальше. При уничтожении персональных данных по достижении цели обработки данным законопроектом предусматривается использовать средства защиты информации, в составе которых есть функция уничтожения информации, прошедшая оценку соответствия, скажем так.

Дополнительно подготовлен проект поправок к этому законопроекту, в котором устанавливается порядок обработки персональных данных, полученных в результате обезличивания. Сегодня у нас есть одна отсылочная норма к этому, данным законопроектом устанавливается такой порядок. Данный проект поправок, как я сказал, находится в Правительстве Российской Федерации и сегодня должен быть рассмотрен на заседании Комиссии по законопроектной деятельности.

Из совсем свежего. Сегодня мы работаем над новым постановлением правительства о государственном контроле (надзоре) и муниципальном контроле в Российской Федерации в соответствии с законом № 248-ФЗ. В нем, скажем так, реализован риск-ориентированный подход, который диктует нам закон № 248-ФЗ. В соответствии с положениями проектируемого постановления определены критерии отнесения к категориям риска и классам опасности, оказывающим влияние на периодичность проведения плановых контрольных (надзорных) мероприятий в отношении объектов контроля. Сейчас проект находится на regulation.gov.ru, опубликован 20 мая 2021 года. В ближайшее время будет завершено его общественное обсуждение, после чего он будет внесен в Правительство Российской Федерации.

Кроме данных инициатив у нас есть инициатива по вопросам административной ответственности за нарушение законодательства Российской Федерации в области персональных данных. В целях повышения эффективности механизмов защиты прав субъектов персональных данных федеральным законом от 24 февраля 2021 года № 19 внесены изменения в Кодекс Российской Федерации об административных правонарушениях, предусматривающие в том числе повышение штрафных санкций за правонарушения в сфере обработки персональных данных.

Также принятие проекта федерального закона, о котором я уже говорил, потребует внесения изменения, мы считаем, в часть 7 статьи 13.11 КоАП, направленного на расширение именно субъектного состава административных правонарушений. Указанной частью сегодня предусмотрена ответственность только для операторов, являющихся госорганами или муниципальными органами. Все-таки мы считаем, что эта ответственность должна быть расширена абсолютно на весь субъектный состав.

Также считаем целесообразным дополнить КоАП новым составом административного правонарушения – за невыполнение оператором или иным лицом, получившим доступ к персональным данным, обязанности по соблюдению требования конфиденциальности персональных данных, о чем уже Милош Эдуардович говорил в начале. Согласованная с нами позиция абсолютно, то есть мы разрабатывали эти проекты совместно.

Соответствующие предложения в настоящее время прорабатываются совместно с Минюстом для включения в проект нового КоАП.

Четвертая инициатива, также длящаяся, о которой мы уже неоднократно говорили, – это подготовка к ратификации Протокола о внесении изменений в Конвенцию Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, подписанного от имени Российской Федерации в Страсбурге 10 октября 2018 года. Законопроект подготовлен совместно с заинтересованными ФОИВ, такими как Минюст России, Роскомнадзор, ФСБ России, ФСТЭК России и МИД России. В законопроекте содержится заявление, предусматривающее, что Российская Федерация может относить отдельные категории персональных данных к сведениям, составляющим государственную тайну. Кроме того, в соответствии с требованиями модернизированной Конвенции, устанавливающими обязанность учредить один или несколько надзорных органов, несущих ответственность за ее выполнение, законопроектом данные полномочия возлагаются на Роскомнадзор, как уполномоченный орган по защите прав субъектов персональных данных. Протокол содержит иные правила, чем предусмотрены законодательством Российской Федерации сейчас. И осуществляется корректировка некоторых вопросов, таких как уточнение понятийного аппарата, уточнение положений, касающихся трансграничной передачи персональных данных и закрепления обязанности операторов по уведомлению уполномоченных органов об утечках персональных данных.

В целом, наверное, вкратце у меня все. Спасибо за внимание.

И.В. РУКАВИШНИКОВА

Спасибо большое, Дмитрий Владимирович.

Мы бы хотели от Вас тоже получить предложения по формированию нашего итогового документа и, возможно, тем самым каким-то образом ускорить решение законодательных проблем, о которых в том числе Вы говорили.

Д.В. РЕУЦКИЙ

Обязательно.

И.В. РУКАВИШНИКОВА

Спасибо большое.

Уважаемые коллеги, Иван Валерьевич Осколков, управляющий директор – директор центра GR Сбербанка.

Иван Валерьевич, пожалуйста.

И.В. ОСКОЛКОВ

Здравствуйте, Ирина Валерьевна! Добрый день, уважаемые коллеги! Я хотел бы, может быть, немножко даже тональность обсуждения поменять. Начну с тезиса о том, что, к сожалению, персональные данные граждан, и в том числе, и особенно, относимые к банковской тайне, стали на сегодняшний день товаром, обращаются в том числе на черном рынке и используются мошенниками в криминальных целях. Страдают граждане, страдает общество, и с этим нужно что-то делать. Вот хотелось бы поговорить о предложениях.

Чуть-чуть официальной статистики для начала. По данным Банка России, потери граждан только за 2020 год составили порядка 10 млрд рублей, прирост в 1,5 раза по сравнению с 2019 годом. Это достаточно существенные цифры. Кредитные организации (банки, другие кредитные организации) фиксируют лавину жалоб от граждан. Только у нас в Сбербанке (вдумайтесь!) за 2020 год было получено 3,7 миллиона жалоб на подобные инциденты с некорректным обращением и с использованием мошенниками сведений, составляющих банковскую тайну, в состав которых входят и персональные данные.

Ну а что у нас с наказанием? На сегодняшний день наказание за незаконные получение и распространение сведений, составляющих банковскую тайну, конечно, несоизмеримо с возможным ущербом и для банковского бизнеса, и, главное, конечно, для клиентов, для общества. Конечно, преступники у нас принимают в расчет те нормы и те меры, которые против них могут быть применены, но на сегодняшний день они оценивают угрозу уголовного преследования как не вызывающую беспокойства в общем и целом (то, с чем мы живем, что называется).

Ну и есть официальная статистика судебного департамента. За период с 2018 года по первое полугодие 2020 года по нашей профильной статье 183 Уголовного кодекса привлечено к уголовной ответственности всего несколько десятков преступников, из них реального лишения свободы никто не получил, то есть ни одного приговора о реальном лишении свободы. В общем-то, это не что иное, как отношение сегодняшнего общества к таким правонарушениям. И мы считаем, что надо это менять, надо это корректировать.

Вот мы здесь говорим (коллеги передо мной очень подробно говорили и еще, наверное, будут говорить) о том, что мы предлагаем, какие меры государство предлагает для добросовестных обработчиков данных. И я могу сказать, что Сбербанк, как добросовестный обработчик персональных данных, постоянно сталкивается с увеличением нагрузки как раз на добросовестную обработку данных. То есть те, кто живет по закону, все время получают то в одном месте дополнительные согласия, необходимость их брать, то в другом месте (вот коллега Реуцкий сказал сейчас). При уничтожении персональных данных каждый обработчик данных вынужден будет (вот сейчас закон примут) пользоваться сертифицированными средствами. Это такая очень неслабая нагрузка. Но мы же говорим о добросовестных обработчиках. Вот недобросовестные обработчики и мошенники ничего этого, конечно, не чувствуют, и для них все сейчас проходит очень легко.

В чем проблема состоит на сегодняшний день? Наказание по упомянутой статье 183 Уголовного кодекса за незаконное разглашение или использование сведений, составляющих банковскую тайну, на сегодняшний день касается только лиц, которым соответствующая тайна была доверена или стала известна по службе или работе. То есть, даже если человек работает в банке или у сотового оператора и он эту тайну не получил в рамках должностных инструкций, мы его привлечь никаким образом не можем, он может свободно скачивать эти данные и потом торговать ими.

Отсутствует специальный уголовно-правовой механизм наказания за такие преступления, как распространение баз персональных данных (участившиеся случаи). То есть тоже на сегодняшний день у нас можно распространять это относительно свободно. И понятно, что, если кто-то, некто – мошенник и цели у него мошеннические, преступные, никаких согласий ему не нужно, у него затраты – ноль, грубо говоря, а деньги он за это получает существенные. В общем-то, это проблема на сегодняшний день.

Подобные преступления не относятся к категориям тяжких и даже средней тяжести на сегодняшний день. И при их расследовании правоохранительные органы не могут применять оперативно-розыскные мероприятия в необходимом объеме. Это все, что вытекает из того, что у нас так статья сформулирована на сегодняшний день.

Ну и, наконец, квалифицирующий признак – совершение преступления группой лиц – в статье 183 тоже отсутствует. Тоже, получается, соразмерное содеянному наказание нельзя применить.

Мы считаем, что надо пересмотреть, усилить ответственность за подобного рода преступления. И здесь, вы извините (может быть, это будет выглядеть немного даже неформально), рыночный закон: необходимо цену повысить, чтобы снизить спрос на такого рода деяния.

Преступный интерес к банковской тайне на сегодняшний день у нас несопоставим (я думаю, все это понимают) по ценности с налоговой и коммерческой тайной, а, к сожалению, в статье 183 эти виды тайны через запятую перечислены, то есть там и налоговая, и коммерческая, и банковская тайна. И именно незаконные распространение и использование банковской тайны и влекут ощутимый ущерб. То есть это не налоговая и не коммерческая тайна, а именно банковская.

И банковское сообщество, в том числе Сбербанк, разработало проект федерального закона о внесении изменений и дополнений в Уголовный кодекс. И что мы предлагаем?

Первое – выделить преступления, связанные с банковской тайной, в отдельную статью (например, это может быть статья 183.1, как мы предлагаем). Мы там расширим круг привлекаемых к ответственности лиц. Нам нужно покрыть как можно большее количество преступлений, связанных с банковской тайной, чем сегодня вмещает статья 183.

Второе – описать границу разделения ответственности за преступления и административные проступки. Понятно, что тяжесть и последствия могут быть разными.

Третье – описать, что такое на сегодняшний день неправомерный доступ к банковской тайне. На сегодняшний день, к сожалению, это не сформулировано.

Четвертое – конкретизировать, что понимается под незаконным способом собирания сведений. Собирание сведений на сегодняшний день никоим образом не регулируется, грубо говоря, можно посмотреть в одном месте, посмотреть в другом (подсмотреть, я бы так сказал), потом дальше воспроизвести – и ничего вам за это не будет.

Дальше – точно указать, в каких случаях лицо не подлежит ответственности. Это некая компенсационная тема, обязательно нужно это учесть.

Дальше. Мы предлагаем увеличить санкции и обязательно добавить квалифицирующий признак по группе лиц.

Понятно, что все это нужно делать соразмерно, все это нужно продумывать, просчитывать.

Мы наши предложения направили и в ведомства, и в Государственной Думе они есть, и на заседании соответствующей межфракционной группы у Александра Евсеевича Хинштейна мы об этом доложили. На сегодняшний день все рассматривают. Первую порцию замечаний мы

получили – будем, безусловно, дорабатывать. Мы не оставим эту тему. Это волнует не столько нас, как банк, сколько наших клиентов, а через это, через их ощущение безопасности, это волнует и все банковское сообщество.

Но тем не менее очень просим вас, Ирина Валерьевна, коллеги, помочь, поддержать. Если будет возможность, может быть, и на заседании совета у Турчака рассмотреть соответствующую тему. Мы дадим все материалы, дадим формулировки в итоговый документ парламентских слушаний. Всё. Спасибо большое.

И.В. РУКАВИШНИКОВА

Иван Валерьевич, спасибо большое за предельно конкретное выступление, предельно конкретные предложения. Готовы вас поддержать. Ждем от Вас материалы.

И, наверное, Ваше выступление абсолютно коррелирует с итогами опроса, с которого мы начали. Потому что самый большой страх, который сейчас есть, психологическая такая нервозность, которая есть у населения, связаны как раз с утерей имущества, в том числе вследствие мошеннических действий с банковскими картами, с банковскими счетами и так далее, с нарушением как раз таки в части информации, которая входит в понятие "банковская тайна".

Спасибо большое. Принимаем в работу, ждем конкретных материалов.

Уважаемые коллеги, доклады, которые были запланированы, завершились. Теперь мы переходим к выступлениям. Я напоминаю, что по регламенту выступления наши – не более пяти минут. Давайте я буду предоставлять слово и сразу называть следующего выступающего, чтобы было время подготовиться.

Сейчас слово предоставляется Ашманову Игорю Станиславовичу, члену Совета при Президенте Российской Федерации по развитию гражданского общества и правам человека.

Подготовиться Орехович Александре Владимировне.

Пожалуйста, Игорь Станиславович.

И.С. АШМАНОВ

Добрый день! Я буду краток.

На мой взгляд, то, что мы услышали, говорит о том, что в государственных органах, особенно там, где серьезно относятся к безопасности, персональные данные граждан, в общем, достаточно хорошо защищены. Хотелось бы также надеяться, что и люди, которые их защищают, – в основном это люди в погонах и под присягой, ну, или хотя бы под очень строгим соглашением о неразглашении.

Но нужно сказать, что серьезные нарушения прав человека в части конфиденциальности персональных данных и приватности на самом деле происходят в основном в коммерческой области сейчас, причем это происходящие нарушения, а не потенциальные. То есть огромное количество частных игроков, к которым относятся интернет-платформы, а также мобильные операторы, видеосервисы и так далее, собирают данные в совершенно чудовищных количествах и вовсю их используют в абсолютно серой зоне. Я никогда не слышал, чтобы кого-то из них наказали за разглашение персональных данных или какое-то другое их использование.

Я приведу пример (я где-то его уже приводил). Служба продаж компании "МТС" просто веером рассылает по рекламным агентствам письма, где предлагает покупать персональные данные или давать доступ к телефонам, к звонкам своих клиентов и обещает такие данные о своих клиентах, как посещение магазинов, других мест, география, покупки и так далее. То есть клиенты, лояльные клиенты компании "МТС" (и это на самом деле так со всеми мобильными операторами), заплатили этой компании уже за связь, подписали с ней, естественно, соглашение и считают, что на этом их сотрудничество заканчивается. В то же самое время компания просто берет и получает дополнительную прибыль или пытается ее получить (я не знаю, насколько этот бизнес успешен), продавая еще и данные об их поисковых запросах, географии, посещении магазинов и так далее, на что никто из пользователей согласия не давал.

Та же самая история и с другими цифровыми платформами, часть из которых вообще, как мы знаем, иностранная. Здесь упоминалось о том, что закон требует локализации персональных данных, но этого же не произошло. На самом деле единственный успешный эпизод предъявления такой претензии западным платформам свелся к тому, что компания LinkedIn просто покинула наше пространство, объявила, что перестала здесь работать, потому что ей неудобно переносить данные и она решила просто не связываться. Все остальные – Facebook, Google и так далее – работают и данные никуда не переносят, то есть они просто "не слушаются".

То есть, с моей точки зрения, в коммерческой области данные воруются массово, и там применение норм закона № 152-ФЗ, да и других норм, вообще говоря, не происходит. То есть правоприменительная практика там негодная, с моей точки зрения. Это, в частности, происходит потому, что у того же регулятора – Роскомнадзора в реальности мало инструментов. Ведь Роскомнадзор может проверять, условно говоря, регламенты хранения, то есть бумаги, или работать по жалобам.

Как мы уже слышали (сегодня уже говорилось), жалоб может быть мало не потому, что мало инцидентов, а потому, что граждане просто не понимают, что происходит, просто они не осведомлены. В этом смысле их, конечно, нужно учить цифровой гигиене начиная со школьного возраста. Но было бы хорошо, если бы регулятор имел возможность проверять, например, потоки данных, то есть не происходит ли на всей цепочке передачи данных кому-то нарушение конституционных прав граждан.

Я приведу условный пример. Я сейчас объясню, зачем я его приведу, и закончу. Я его уже приводил как-то, мы его использовали на встрече Владимира Владимировича Путина с членами СПЧ в декабре.

Представим себе, что некая девушка в каком-то поисковике, например "Яндексе" или Google, вводила запросы о товарах для беременных. Поисковик эти запросы, естественно, распознает и классифицирует. Он поставил себе где-то заметку о том, что, возможно, здесь имеется беременность. Дальше эти данные могли как-то попасть к клиенту поисковика, точнее, к тому, кто с ним обменивается данными, например, к службе занятости, которая размещает у себя резюме. Затем один из многих тысяч корпоративных клиентов, какой-то кадровик из какой-то корпорации, зашел посмотреть это резюме, увидел пометку о беременности и выкинул его в корзину, условно говоря. По сути, по всей цепочке никто не виноват, все просто работают, все просто занимаются обработкой больших данных, а все вместе против лояльного своего пользователя совершили уголовное преступление по статье 145 Уголовного кодекса – отказали в работе на основании беременности.

И это не значит, что они так делают. Я говорю о другом – о том, что, если мы их спросим, делают они так или нет, они все горячо будут отрицать. Но проверить, происходят ли подобные вещи, может быть, не с беременными, а с раковыми больными, мы не можем, потому что нет инструмента, нет сейчас института экспертизы потоков данных, экспертизы обработки, инструментальных средств. У того же Роскомнадзора нет права инструментальной проверки того, что на самом деле происходит с данными, а не бумаг. Я считаю, что это очень важно и такую возможность регулятору нужно дать.

Вообще, нужно каким-то образом по-другому начать относиться к персональным данным. Здесь прозвучало тоже такое предложение (насколько я его понял) – что часть этих персональных данных вообще нужно объявить тайной и наказывать за ее разглашение совершенно другим способом. Потому что сейчас надо понимать, что во всех этих коммерческих компаниях, где

происходит хищение этих данных, этим занимаются просто обычные программисты, сисадмины и цифровые клерки. Они вообще ничем не ограничены и ничего не боятся. Это такой новый цифровой класс, который считает, что ему все можно. Спасибо. Я закончил.

И.В. РУКАВИШНИКОВА

Игорь Станиславович, спасибо большое.

Мы бы хотели конкретные предложения получить, в частности касающиеся добавления инструментальных возможностей Роскомнадзору. Это очень интересное предложение. Мы неоднократно по этому поводу тоже общались и с Роскомнадзором, и с нашими коллегами. Но требуются ли в данном случае какие-то законодательные изменения или требуется уже технологическая оснащенность? Это тогда уже другой вопрос, он лежит в другой плоскости.

И.С. АШМАНОВ

Мне кажется, что нужны законодательные изменения в смысле мандата Роскомнадзора, но об этом лучше поговорить с ними или как-то совместно.

И второе. Мне кажется, что нужно подумать о создании механизма какой-то независимой экспертизы, которая в других отраслях существует. То есть у нас нет независимой экспертизы ни по поводу обработки больших данных, ни по поводу того, как работают системы искусственного интеллекта. Сейчас это все и для пользователей, и для операторов, да даже для разработчиков – в общем, черный ящик. Здесь нужно какой-то такой сегмент рынка создавать независимого аудита и экспертизы.

И.В. РУКАВИШНИКОВА

Да, вопрос только в том, насколько они будут допущены к этим данным, чтобы не переборщить.

И.С. АШМАНОВ

Конечно. На то, чтобы всерьез открыть алгоритмы, рассчитывать нельзя. Это безусловно. Но тем не менее обнаруживать, что данные где-то всплыли, и требовать показать путь, каким образом они туда попали, – кто-то должен получить такое право, с моей точки зрения.

И.В. РУКАВИШНИКОВА

Ну, возможно. Очень разумное предложение. Тем более что действительно население, которое является основным источником поставки этих персональных данных, в общей своей массе, конечно, на самом деле действительно не понимает масштабов бедствия, если это можно так

назвать. И многие из нас не понимают, каким образом можно противодействовать этому. Здесь, конечно, оказание профессиональной помощи сообществом было бы очень уместно.

Спасибо большое за предложения.

И.С. АШМАНОВ

Извините, я еще приведу пример. Вы помните, что в прошлом году было несколько утечек данных, в том числе из госорганов. В частности, данные о больных COVID утекали из мэрии Москвы, из ДИТ.

Вообще говоря, эти истории как-то ничем не заканчиваются. Здесь несколько раз говорили о том, что ответственность не наступает, то есть этого просто не происходит. Понятно, что в случае этих утечек возникает два вопроса – о надежности хранения и о том, почему данные не удалили, как было обещано и положено по закону № 152-ФЗ. Но, вообще, самый основной вопрос – а что произошло дальше, почему никто не ответил? Вот эта правоприменительная практика должна измениться, с моей точки зрения. На самом деле у нас почти никого не наказывают по закону № 152-ФЗ, кроме как за бумажки. Спасибо.

И.В. РУКАВИШНИКОВА

Игорь Станиславович, спасибо большое. Ждем Ваших предложений тогда в письменном виде. Хотя, я напоминаю, у нас ведется стенограмма, но нам удобнее будет работать уже с конкретными предложениями. Спасибо большое.

Передаю слово Александре Владимировне Орехович, директору по правовым инициативам Фонда развития интернет-инициатив.

И подготовиться Юлии Сергеевне Алфёровой.

Пожалуйста.

А.В. ОРЕХОВИЧ

Спасибо большое.

Коллеги, скажите, слышно меня хорошо? Потому что у меня периодически прерывается связь.

И.В. РУКАВИШНИКОВА

Мы Вас хорошо слышим и видим. Пожалуйста.

А.В. ОРЕХОВИЧ

Спасибо большое.

Знаете, я бы хотела вернуться к словам Ивана Валерьевича Осколкова относительно того, что сейчас получается так, что данные стали товаром на черном рынке. Я бы скорректировала даже слова Ивана Валерьевича, сказав о том, что данные сейчас являются товаром на рынке – и точка. В принципе товар на черном или не на черном рынке – вопрос на самом деле большой, потому что не всегда на черном рынке, а, мне кажется, зачастую на сером. И вся статистика, которую и Ирина Валерьевна приводила в самом начале, и вся та статистика, которая говорит о доверии граждан, как раз говорит именно о том, что зачастую та самая торговля данными происходит на рынке сером и на относительно законных основаниях.

Вот последняя статистика Google, которую они привели: 81 процент пользователей не пожертвует своими персональными данными даже в рамках и ради получения услуг. 81 процент пользователей! Наша статистика чуть более щадящая: РАЭК подсчитала, что более 70 процентов пользователей не считают, что их данные в безопасности.

О чем это говорит? На самом деле пользователи уже доведены до предела и всеми историями, конечно же, утечек (если мы говорим о черном рынке), и всеми историями спама, и очень сильно обеспокоены всеми историями относительно того, что зачастую интернет-площадки знают о пользователях гораздо больше, чем хотелось бы им самим.

Какие в связи с этим проблемы вскрываются? Они немного противоречивые, и их надо каким-то образом уравновесить.

Первая проблема. Очевидно, доступ к данным, в том числе бизнесу, необходим. Это действительно так, это непреложная истина, и это уже понимают регуляторы везде. Если мы берем международное сообщество, даже Европейский союз, у которого, казалось бы, самое жесткое регулирование в этом плане, склоняется к необходимости обеспечения доступа к данным для развития экономики, для развития цифровой экономики, для того самого пресловутого искусственного интеллекта.

В то же время важно не потерять доверие пользователей, не забывая, как Вы правильно говорите, Ирина Валерьевна, о том, кто является источником данных. Без источника данных не будет самих данных. Потеряв доверие пользователей, уже невозможно будет нарастить тот самый объем данных, который необходим и для развития цифровой экономики, и для развития искусственного интеллекта, и так далее.

Какие шаги в связи с этим предпринимаются в части законодательства для решения первой проблемы (доступ к данным необходим)? Что сейчас происходит? Вот Дмитрий

Владимирович упомянул очень важную инициативу – законопроект, тот самый, как я понимаю, который сегодня рассматривается на заседании КЗД. Это законопроект, который в СМИ окрестили законопроектом об обезличении данных.

Я не видела окончательной редакции, но, я так понимаю, судя по сообщениям СМИ (на самом деле это очень важно), в нем содержатся очень важные поправки относительно того, что обезличивание может производиться оператором без согласия пользователей, ну и затем могут передаваться третьим лицам эти самые обезличенные данные, если при этом им передается дополнительная информация, позволяющая обезличить данные. Если это так опять-таки, то, конечно, здесь необходимо с большой осторожностью относиться к тому, что будет пониматься под методом и технологиями обезличивания, поскольку, конечно, обезличивание данных сейчас позволяет в любой момент, в общем-то, любым операторам эти данные обезличить, даже если ему не была передана дополнительная информация. Поэтому здесь, конечно, нужно будет с очень большой осторожностью относиться к разработке подзаконных актов.

И второе, на что хотела бы обратить внимание в рамках решения проблемы доступа к данным. Многие юрисдикции (огромное количество юрисдикций – и США, и Европейский союз, и Австралия, и Сингапур) сейчас идут по пути обеспечения доступа к данным, идут по пути повторного использования данных. Что есть повторное использование данных? Это, условно говоря, возможность доступа к ГИС, получение информации в том числе о персональных данных через livestream – посредством четкого, жесткого регулирования относительного того, кто может получить эту информацию, при каких условиях, каким образом должны соблюдаться эти условия.

На мой взгляд, это хороший опыт, который по крайней мере следует изучить, дабы предоставлять тот самый доступ к данным, который так сейчас необходим для развития цифровой экономики, и при этом предоставлять этот доступ вбелую, то есть иметь возможность четко следить за тем, кто при каких обстоятельствах и при каких условиях может эти данные обрабатывать.

И вторая проблема, которую я сейчас подняла помимо необходимости доступа к данным, – это не потерять доверие пользователей. Ирина Валерьевна очень правильно сказала такую фразу: пользователи не понимают масштабов бедствия. Это правда, пользователи действительно не понимают масштабов бедствия. И цифровая гигиена – это, конечно, прекрасно. Однако сейчас (и, вообще, это признается не только в Российской Федерации, эта проблема актуальна не только у нас) даже Европейский союз в своем отчете о соблюдении GDPR признал, что согласие на

обработку персональных данных – это не что иное, как способ манипуляции пользователями, и операторами используется как способ манипуляции пользователями.

Эта проблема у нас – в полный рост. Согласие – это действительно способ манипуляции пользователями. Цифровая гигиена – это хорошо, но даже лично я, являясь юристом и понимая, что я подписываю, не всегда могу исключить каких-то операторов из согласия, которое меня, можно сказать, обязывают подписывать. И не всегда я понимаю даже, где находятся и куда будут переданы мои данные после того, как я подпишу это согласие, и не всегда я могу вычеркнуть каких-то операторов, относительно которых я не понимаю, зачем им нужно будет мое согласие.

Так вот, на мой взгляд (продолжая, кстати, мысль, которую Игорь Станиславович Ашманов начал), прежде всего нужно дать субъектам персональных данных, самим пользователям возможность понять масштабы бедствия, возможность хотя бы получить доступ в простой, понятной, четкой форме относительно того, где, зачем их данные находятся, куда они передаются, для этого же – возможность четко отозвать точечно эти данные, если пользователь не понимает и не видит ценности в передаче какому-либо оператору персональных данных. И уже как корреспондирующая норма, которая будет вытекать из этого, – возможность добавления тех самых инструментальных возможностей для контроля за оборотом, можно сказать, этих персональных данных у операторов.

Из моих предложений всё. Спасибо большое за внимание.

И.В. РУКАВИШНИКОВА

Спасибо большое, Александра Владимировна.

Я бы Вас, наверное, дополнила. Очень внимательно мы Вас слушаем, всегда Вы активно участвуете, поскольку являетесь одним из экспертов, членом экспертно-консультативного совета при комитете по конституционному законодательству.

Наверное, когда человек дает свое согласие на обработку персональных данных, действительно не всегда понимает, зачем и куда он их отдает. Мне кажется, и тот, кто собирает в этот момент, тот, кто предлагает передать такое согласие, тоже не до конца понимает, для чего он это собирает (возможно, не все злоумышленники и не все собирают с какими-то темными целями), исполняя норму закона. Вот у меня есть абсолютно стойкое такое бытовое, наверное, убеждение, что очень часто люди, которые собирают эти данные, потом не знают, что с ними делать. Чаще всего эти согласия… не чаще всего, а зачастую это все происходит на бумажном носителе, то есть мы оставляем свою подпись, реже в цифровом варианте согласия такие передаем. Вот куда потом

деваются все эти документы, каким образом они утилизируются, хранятся, используются – это тоже очень большой вопрос на самом деле. И здесь я абсолютно согласна и с Вами, и с предыдущим докладчиком в том, что необходимо, конечно, эту сферу мониторить более активно и привлекать сюда больше заинтересованных субъектов.

Спасибо большое. Ждем также Ваших предложений в наш адрес в письменном виде.

Юлия Сергеевна Алфёрова, еще один наш эксперт, генеральный директор АНО "Национальное агентство развития предпринимательства".

И подготовиться Дмитрию Александровичу Алимову.

Пожалуйста, Юлия Сергеевна.

Ю.С. АЛФЁРОВА

Уважаемая Ирина Валерьевна, уважаемые коллеги, добрый день! И в рамках продолжения предыдущих наших мероприятий вопрос, касающийся работы с персональными данными, на данных парламентских слушаниях отдельно поднимается. Но с учетом той актуальности, которая на сегодняшний момент у нас имеется, важно говорить как о внесении изменений в верхнеуровневые документы стратегического планирования, так и непосредственно о конкретных быстрых шагах.

Маленькую ремарку вставлю. Я сама на сегодняшний момент являюсь тем человеком, который за последние полтора года… Буквально на прошлой неделе (я посчитала) лично ко мне поступило более 15 звонков от телефонных мошенников, которые используют мои данные, представляясь сотрудниками Сбербанка. Соответственно, на 15-й звонок я уже отработала скрипт, каким образом я призываю к совести звонившего человека. Но это так, для информации.

То есть, для того чтобы я идентифицировала этого звонящего как мошенника (а я занимаюсь цифровой трансформацией несколько лет)… Я при первых же секундах могу идентифицировать комментарии звонящего. И призыв человека открыть договор, попытка сказать: "Вы там сможете увидеть телефон, с которого мы звоним, поэтому мы реально служба безопасности", – на 15-й звонок, с учетом того что я отрабатываю на них скрипты, уже не срабатывают. Но сколько нас таких из тех, кто получает эти звонки, с большой осведомленностью о происходящем процессе, о том, что происходит сейчас, с возможностью иметь информацию о том, где потенциально (во ФСИН или не во ФСИН) находятся звонящие, и так далее? Мы видим большую работу, которая в этом направлении сейчас ведется. Мы понимаем, что граждане в таком контексте находятся, что манипуляции звонящих… Последний звонок реально даже меня смог

практически выбить из колеи, потому что девушка на другом конце провода, представившись сотрудником Сбербанка, кричала уже в мой адрес (она просто первая бросила трубку, то есть она не выдержала моего напора), что она подаст на меня в суд за то, что я оскорбляю сотрудника Сбербанка. Вот это была наша последняя дискуссия.

Представьте себе любого гражданина, вообще не осведомленного, которому звонят, вводят в этот психологический мандраж, соответственно вытягивая эти данные. Но для этого нам не всегда достаточно информации, новостей, которые, допустим, у нас быстро… И я считаю, что был абсолютно правильный инструмент реагирования при манипуляциях со SWIFT. Когда у нас пошла информация о том, что нас могут отключить, тут же начали звонить мошенники и на фоне этого "нагреваться". И тут же по федеральным каналам пошла информация о том, чтобы на это не реагировать, это манипуляции.

Но те системные вопросы, которые мы сегодня озвучили, безусловно, в полном объеме также, я согласна, должны стекаться. И пока мы видим оператора – Роскомнадзор, который может разъяснять. И мы сейчас понимаем, что, если вдруг завтра мы по всем информационным каналам сообщим и направим туда граждан за разъяснениями, мне кажется, Роскомнадзор рухнет. А мы понимаем, что разъяснение – это ключевой момент, за которым нужно обратиться как гражданину, так и юридическому лицу. Так как у нас очень много стейкхолдеров, у нас должно быть большое количество синхронизированных направлений, которые как помогают бизнесу сохранить себя…

Вот после выступления Михаила Владимировича на прошлой неделе по внесению в Кодекс об административных правонарушениях поправок о штрафах за сбор тех или иных персональных данных мы неделю пытаемся выяснить, каким образом сейчас субъектам предпринимательства, по сообществам и деловым объединениям (мы сейчас готовим юридические справки), разъяснить, что можно завтра собирать на продающих лендингах, – а это микробизнес, то есть это самозанятые. У нас у многих предпринимателей бизнес встает, потому что они начинают в большей степени бояться, нежели дальше запускать те или иные бизнес-процессы. И сейчас мы увидели большое количество направлений, но не увидели синхронизации. С учетом этого есть предложение – от верхнеуровневых до нижнеуровневых.

Так как у нас в настоящий момент стратегия национальной безопасности выходит на свою финальную редакцию, есть два ключевых раздела, которые касаются национальных интересов и стратегических национальных приоритетов. В связи с этим по этим документам основное предложение – включить в национальные интересы обеспечение цифрового суверенитета, где у

нас персональные данные граждан внутри, будут входить в понятие, а в стратегические национальные приоритеты добавить обеспечение охраны и защиты персональных данных граждан. Там у нас есть культура, здравоохранение…

Мы все помним заседание коллегии ФСБ в феврале, на котором президент говорил о необходимости с учетом геополитической обстановки защищать наши данные, потому что это инструмент манипуляций. То есть каким образом можно воздействовать сейчас на нашу страну? Это как раз закупка или дестабилизация через манипуляцию. То есть сейчас можно закупить, по сути, всё. То есть если у нас внутри это оборачивается, то что говорить о внешней истории? То есть мы в большей степени становимся доступными.

Дальше, соответственно, по декомпозиции документов стратегического планирования. После обновления стратегии национальной безопасности, получается, должно идти обновление и доктрины информационной безопасности, и концепции общественной безопасности, так как эти два документа у нас также на подходе.

Если мы говорим о финансовом и материальном обеспечении данного направления, то, конечно же, это и госпрограммы, это стратегия социально-экономического развития до 2030 года, которая сейчас верстается. И непосредственно та канва… и бюджет, который зашит, должен быть зашит в "Цифровой экономике".

Если мы посмотрим на текущие федеральные проекты, то мы поймем, что нам просто жизненно необходим целый комплексный проект по защите персональных данных. То есть мы его не можем рассовывать по текущим проектам, и таким образом мы спускаемся от документов верхнеуровневых до исполнения. А там мы уже можем расширять мандат на Роскомнадзор, сформировать новую институциональную сущность, потому что мы, по сути, поймем, что нам не хватает организационно-методологического оператора, кто будет реализовывать этот федеральный проект. То есть, мы понимаем, чтобы завтра со всеми взаимодействовать, у нас с ходу нет такой, условно, организационно-правовой структуры в системе. В связи с этим данное направление является приоритетным с точки зрения национальной безопасности.

В моем понимании, Ирина Валерьевна, сейчас очень горячая пора, когда есть необходимость, опять же с учетом статуса Совета Федерации, данное направление усилить. Потому что основная задача – не просто оставить в верхнеуровневых документах упоминание, основная задача – завтра очень быстро начать помогать гражданам.

И финальное предложение, по которому в принципе с учетом саморегулирования необходимо работать и взаимодействовать уже завтра. Буквально на прошлой неделе Минэкономразвития (Департамент развития цифровой экономики) опубликовало документ о концепции регулирования экосистем. То есть это очень хорошая декомпозиция относительно того законопроекта, который в Государственную Думу был внесен, видна очень профессиональная работа. И здесь очень важно включить платформу (а там даются определения, что такое "цифровая платформа", что такое "экосистема"), включить добровольную трансляцию информации о работе с персональными данными. Буквально сегодня была новость о том, что Google использовал (там было признание, судебное решение), специально зашивал данные о геолокации, для того чтобы пользователи не смогли найти.

То есть у нас есть четкое понимание, что мы с вами, чтобы дотянуться до той галочки, чтобы убрать какую-то информацию, должны дойти. Нам, наоборот, должны компании транслировать эту открытость, от методичек до роликов, то есть они прежде всего должны свою конкурентоспособность показывать именно своей открытой политикой. То есть, по сути, мы должны ввести практику открытой демонстрации работы с персональными данными на примере инфографики и мини-, микророликов.

Если кратко, предложения такие. Развернутые мы, как обычно, отправим, Ирина Валерьевна.

И.В. РУКАВИШНИКОВА

Спасибо большое, Юлия Сергеевна. Понимаю, что Вы абсолютно правильно говорите с позиции профессионала, с позиции человека, который так часто общается с мошенниками, к сожалению. И, наверное (масштабы бедствия, если возвращаться к этой конфигурации), пока лично каждого эта проблема не коснется, ничто не заставит изучать законодательство, ничто не заставит более внимательно относиться к процессу передачи персональных данных и смотреть те ролики, о которых Вы говорите, даже если они и будут в наглядном варианте. Как правило (давайте будем честными), среднестатистический пользователь интернета, конечно, эти ролики просто проматывает в лучшем случае, закрывает просто их, быстро соглашаясь, передавая, и быстро переходит к контенту, который его интересует. Редко кто на самом деле вчитывается, глубоко осознает и так далее.

Возможно, сейчас сама эта информация представлена не в выигрышном варианте для чтения. Лонгрид, возможно, многих отталкивает. Но тем не менее, давайте будем честными (мы

понимаем, что здесь инициатива должна, конечно, быть с двух сторон), прежде всего в сохранении своих персональных данных от несанкционированного использования должен быть заинтересован, конечно, сам носитель этих персональных данных. Вот здесь очень важно в психологии поменять что-то путем постоянных разъяснений, обучения, начиная действительно с детского сада, и, в общем-то, на протяжении всей жизни необходимо об этом напоминать. Цифровая гигиена в чистом виде.

Спасибо большое. Принимаются все Ваши предложения, очень интересные предложения, касающиеся стратегических документов. Ждем от Вас документов. Спасибо большое.

Дмитрий Александрович Алимов, доцент кафедры конституционного и муниципального права Ростовского государственного экономического университета (РИНХ). Город Ростов сейчас подключится к нам.

И потом мы передадим слово Лукашевичу Василию Александровичу.

Пожалуйста, Дмитрий Александрович.

Д.А. АЛИМОВ

По ходу дискуссии можно говорить, что основная проблема, которая волнует собравшихся, – это защита именно персональных данных, в частности, отдельные проблемы – банковская тайна, утечка персональных данных и так далее. Я хотел бы кратко выступить.

Во-первых, рано или поздно мошенники дозваниваются до каждого из нас. Так случилось и со мной буквально на прошлой неделе. Там была очень сложная конструкция, оговаривался какой-то единый денежный счет, который у меня есть. Да, такая конструкция, конечно, проходит тяжело, но так или иначе…

Совершенно верно сегодня подметили, что утечка персональных данных – это все-таки в большей степени проблема не государственных структур или каких-то органов публичной власти, которые контролируют те или иные информационные системы, – в большей степени это все-таки проблема частных организаций, в том числе в IT-сфере, в том числе в банковской сфере.

Вот один из актуальных вопросов, который я сегодня не услышал (он не был озвучен): почему многие банковские организации?.. Со мной такого еще не было, но товарищи по работе в том числе часто говорят. Это не дополнительная услуга по стороны банка. Когда ты подписываешь пакет документов, допустим, на потребительский кредит, тебе подкладывают на подпись бумажку о том, что банк берет твое разрешение передавать эту информацию (твою личную, конфиденциальную) третьим лицам. Это не запрещено, кстати, Гражданским кодексом

Российской Федерации. Но вот каковы, собственно, правовые основания предлагать гражданину, берущему потребительский кредит, такое дополнительное условие? Вы знаете, как у нас работают частные банки. Формально они не могут тебе отказать на основании того, что ты не подпишешь, допустим, какую-то дополнительную бумагу, но на деле обычно так и происходит.

Вот одна из актуальных проблем, которую я сегодня просто не услышал, – дополнительная бумага, которую мы подписываем, которая передает бог знает каким юридическим лицам твои конфиденциальные данные. И как потом найти вот эти концы, кому я передал свои данные? С кем мне обсуждать вопрос о прекращении их использования? Это уже достаточно тяжело.

Поэтому еще одна прозвучавшая сегодня идея, безусловно, заслуживающая внимания, но близкая к излишне фантастичной, – это общий реестр физического лица, в котором он может проследить, проконтролировать все виды разрешений на распространение своих персональных данных, начиная от школы, учебного учреждения, места работы. Ну и наиболее актуальна, конечно, проблема банковских данных, потому что они наиболее полные, наиболее охотно ими пользуются мошенники и так далее.

В средствах массовой информации сегодня прошел новый тезис – что есть уже проект федерального закона (я не понял, сегодня о нем нам сказали или нет) о том, что новая административная ответственность вводится в части навязывания определенных услуг в сфере торговли при условии получения дополнительных данных, в том числе конфиденциального характера, в том числе в части персональной информации. Вот это нужно только исключительно приветствовать.

Вообще, расширение административной ответственности можно приветствовать. Сегодня мы уже говорили: у нас есть законы о персональных данных, об информации, информационных технологиях и о защите информации – огромные, полноценные законы, в которых прослеживается единая линия, четко очерченная сфера общественных отношений. А если мы открываем, собственно, Уголовный кодекс и Кодекс об административных правонарушениях, чтобы реально посмотреть ответственность за данные виды преступлений и правонарушений, у нас там информации не так много. В частности, это касается Уголовного кодекса тоже. Это проблема, которая сегодня в большей степени обсуждается.

Вторая часть проблемы. Я напомню, что у нас тема сегодня широко была заявлена – неприкосновенность частной жизни, ну и, в частности, проблема соотношения частных и

публичных интересов. Напомню, что личные права и свободы в том числе гарантированы Конституцией Российской Федерации (статья 23). Они давно уже перестали восприниматься в науке исключительно как характеризующие негативный аспект свободы. С одной стороны, человек старается предупредить, не допустить излишнее вмешательство государства в свою жизнь, с другой стороны – он требует уже положительных действий от государства, когда хочет, чтобы государство защитило его от вмешательства в его жизнь других лиц. Данный аспект темы сегодня особо не рассматривался. Я просто хочу подчеркнуть, что в этой области также есть много больших проблем, которые требуют своего законодательного регулирования.

В частности, актуальная проблема у нас сегодня, если почитать научную литературу, посмотреть правоприменительную практику, – это проблема биометрических персональных данных. Два закона у нас есть (я сегодня их уже озвучил), в которых данный вопрос рассматривается, однако вот такого общего, систематизированного понимания биометрических данных на уровне федерального законодательства у нас пока не существует. У нас федеральный законодатель отнес основной блок вопросов для разработки на уровень федерального органа исполнительной власти. Не знаю, насколько это хорошо или плохо, но пока вот так. Рассмотрение проблемы в зачаточном состоянии на самом деле и на уровне международного законодательства, и на уровне международного правоприменения.

И производная проблема от проблемы биометрических данных (это актуальная сейчас проблема) – так называемые умные камеры слежения. Если раньше были просто камеры и по ним были даже решения ЕСПЧ, по камерам, работающим в общественных местах (проблема – где заканчивается частное пространство человека, где начинается публичное), то с появлением камер распознавания лиц актуализировалась проблема перехода частных интересов человека в том числе в публичные места. Вот по этому вопросу у нас не только нет нормальной правоприменительной практики внутри страны, но и на уровне международного права, на уровне внутригосударственного права других стран. Проблема сводится к тому, что люди не представляют себе алгоритмов работы данных "умных", интеллектуальных устройств.

Если раньше камера просто записывала – сейчас она может, соответственно, на уровне использования искусственного интеллекта принимать какие-то иные облики, разрабатываются какие-то иные способы контроля за людьми. Безусловно, это здóрово и для оперативно-розыскной деятельности, и для правоохранительной деятельности в целом. Но общая тенденция в мире сейчас – достаточно аккуратное отношение к этим "умным" механизмам. И хотелось бы

законодательного урегулирования в данной области также, потому что алгоритм работы камер по распознаванию лиц никому на самом деле до сих пор не понятен. У нас было два судебных решения в этой части на уровне Москвы: гражданка обращалась и была недовольна тем, что алгоритм распознавания лиц использовался для привлечения ее к административной ответственности. У нас будет решение ЕСПЧ рано или поздно по этому поводу, там можно будет посмотреть (в большей степени интересно) общетеоретическую часть. Еще раз скажу, по этому поводу решения Европейского суда по правам человека у нас в наличии до сих пор нет.

Но можно было бы уже сейчас подумать (не дожидаясь того момента, когда, допустим, что-то в решениях Европейского суда по правам человека появится, что-то не понравится в нашей правоприменительной практике) о разработке на уровне федерального законодательства как раз основы для использования не просто камер видеослежения, но и камер видеослежения, оснащенных искусственным интеллектом, нацеленных на распознавание лиц в частности. Возможно ли распознавание лиц задним числом? То есть что у нас сейчас обычно происходит? Закладывается часть каких-то фотографических изображений – и камеры в процессе работы на улицах сразу выделяют лиц, скажем так, неблагонадежных, скрывающихся от правосудия и так далее. Возможно ли это задним числом делать? Обязательно ли это? Как соотносится работа этих камер с едиными реестрами биометрической информации и так далее? Вот эту, собственно, проблему я хотел бы сегодня поднять.

Она, еще раз скажем, проработана в основном на уровне подзаконных актов исполнительной власти федерального уровня. Хотелось бы и надлежащего законодательного урегулирования в данной сфере на федеральном уровне. Потому что общемировые тенденции не понятно, куда нас ведут. Допустим, американская судебная практика говорит о постепенном запрете использования камер с технологией распознавания лиц в различных городах, различных штатах. Спасибо большое за внимание.

И.В. РУКАВИШНИКОВА

Спасибо большое, Дмитрий Александрович. Действительно, очень интересную проблематику Вы сейчас осветили. Мы исходим из того, что (и мы начали, в общем-то, наше мероприятие с этого), что информационные технологии развиваются стремительно. Они, конечно, опережают и мысль законодателя, естественно, и законодательные документы. Но в своем вступительном слове я не зря сделала акцент на необходимости глубоких научных разработок в этой сфере, поскольку всегда ученые, которые работают над какой-то тематикой, в какой-то

степени, наверное, и футурологи, и провидцы, потому что научная мысль, в общем-то, всегда идет немножко впереди законодательства. И это очень правильно – когда законодательство основывается на имеющихся доктринальных разработках.

Знаю, что Вы занимаетесь этой проблематикой. Знаю, что рядом с Вами мои коллеги из Ростовской области, города Ростова-на-Дону, представляющие школу конституционного и административного права. Будем очень рады продолжению нашего сотрудничества. И ждем от Вас в том числе и научных предложений, касающихся такого формализованного, может быть, использования, уже в контексте разработки понятий, категорий, в том числе того, на чем Вы заострили внимание. Спасибо большое.

Я передаю своему родному городу Ростову-на-Дону большой привет.

Прошу нас переместить сейчас в город Страсбург. И хочу попросить выступить Василия Александровича Лукашевича, несудебного докладчика Европейского суда по правам человека, старшего юриста Секретариата ЕСПЧ, эксперта в сфере сравнительного права и публичной политики.

Подготовиться к выступлению Кутейникову Дмитрию Леонидовичу.

Василий Александрович, пожалуйста.

В.А. ЛУКАШЕВИЧ

Коллеги, здравствуйте! Я надеюсь, что меня хорошо слышно.

Во-первых, я хотел бы поблагодарить Ирину Валерьевну за более чем лестное и интересное предложение поучаствовать в этих слушаниях. А во-вторых, сразу хочу оговориться, что, поскольку я работаю в европейском суде, важно сказать, что сказанное мною сегодня не обязательно отражает позицию европейского суда. Поэтому не надо это воспринимать как мое выступление в профессиональном качестве – это мое выступление в качестве эксперта, в личном качестве.

Хочу сказать сразу, что вообще тема неприкосновенности частной жизни, и в том числе защиты персональных данных, на удивление актуальна, она на удивление актуальна уже на протяжении последних, я бы сказал, 15–20 лет. Не далее чем вчера я по французскому телевидению смотрел очень большую передачу о том, как утекают данные французских граждан в руки зловредных корпораций, которые собирают эти данные, а потом используют в своих коммерческих целях. То есть эта проблематика – не чисто российская проблематика, это действительно общемировая проблематика. И в связи с этим мне кажется, что стоит опираться при

решении этих вопросов и на опыт других стран и обращать внимание на удачи, и в том числе на ошибки, совершенные в других юрисдикциях.

Но я сегодня хотел бы подчеркнуть такую базовую мысль, которая недостаточно прозвучала, некоторые коллеги в своих выступлениях, как мне кажется, не обратили на нее достаточного внимания. Я бы задал базовый вопрос для начала: кому принадлежат эти данные и кто имеет право распоряжаться этими данными? Это самый первый вопрос, который надо задать. Второй вопрос, который надо задать себе: а чье это право и какое право мы защищаем?

И не надо забывать, что частные данные и неприкосновенность частной жизни – это не некий абстрактный политический, общественный либо государственный интерес. Частные данные принадлежат тому лицу, которое, собственно говоря, является носителем этих данных, – это прежде всего. И это право, право неприкосновенности частной жизни, и право на защиту этих данных – это права конкретного индивидуального лица. И, мне кажется, это должно быть отправной точкой для любой дискуссии на данную тему.

Какие у этого есть конкретные практические последствия? Во-первых, нам надо разграничивать, и, мне кажется, в нашей дискуссии представители особенно государственных органов очень хорошо это отразили в своих выступлениях, – что есть разные операторы данных и что абсолютно разные органы государства, а также частные лица собирают данные. В том случае, когда мы говорим о государстве, мы говорим о сборе данных помимо воли самого человека. То есть государство собирает данные о своих налогоплательщиках, о должниках в базе данных, неплательщиках алиментов, тех людях, которые не исполняют судебные решения,– государство собирает эти данные помимо воли человека. И поэтому основными вопросами здесь, безусловно, являются безопасность и сохранение этих данных, а также кто имеет к ним доступ. И наши коллеги из Роскомнадзора, из Федеральной налоговой службы очень хорошо это осветили и подчеркнули эти моменты, и мне кажется, что здесь идет весьма достойная работа.

Когда речь заходит о частных операторах данных, о тех самых злобных корпорациях, которые собирают наши данные, а потом начинают их продавать, то тут мы говорим о совершенно другом контексте. Если эти корпорации не нарушают закон, если они получают данные от конкретных индивидуальных лиц, то они их получают, как правило, законным способом. Частные лица передают этим корпорациям свои данные.

И здесь у нас возникает несколько практических вопросов. Во-первых, надо подчеркнуть (и я вновь это подчеркну), что любой из нас может передать свои частные данные любой

корпорации. И когда мы подписываем эти бесконечно длинные договоры с мелким шрифтом внизу… Знаменитый мелкий шрифт, кстати, появился не в эпоху интернета. Если вы почитаете романы XVIII века, мелким шрифтом на последней странице длинного договора… – вот там-то все ловушки и находятся, они там находятся многие-многие столетия, это совершенно не современная проблема. Но у этой проблемы, особенно с развитием технических форм и с развитием технологий, форм взаимодействия между компаниями и индивидуальными лицами, есть вполне конкретные и четкие решения. Приведу пример того, как можно получать, так скажем, информированное согласие на сбор и распространение данных.

Хорошим примером, допустим, является Франция, в которой в случае сбора данных медицинского характера уведомление о сборе подобных данных всегда должно быть отдельным уведомлением, как правило, на отдельной странице, если это страница в интернете, или отдельном экране в приложении, где простым, понятым языком, коротким текстом написано о том, что эти данные могут быть переданы данному оператору и могут им использоваться и распространяться. То есть для этих вопросов существуют определенные процедуры и способы решения.

Но при этом, мне кажется, было бы ошибочным ожидать от государства… И это совершенно для государства несвойственная функция и неподъемная функция, я сразу скажу, – мониторить передачу всех данных об индивидуальной жизни всем частным операторам, мониторинг всех возможных алгоритмов обработки этих данных, а также установление... Поймите, у нас государство превратится в того самого Большого Брата, если мы ему поручим наблюдать за всем бизнесом и за всеми транзакциями между частными лицами, чтобы, не дай бог, в ходе этих транзакций не были нарушены права отдельных лиц.

В первую очередь (я все же согласен и с Ириной Валерьевной, которая сказала это в самом начале, и некоторые другие выступающие подчеркивали) самое важное – это та самая цифровая гигиена, это то самое образование граждан. Граждане должны понимать, что они делают со своими персональными данными. И они не столь наивны, как мы думаем иногда. Потому что если вы подойдете к человеку на остановке и попросите его дать номер телефона в обмен на какую-нибудь красивую открытку, то он вам, конечно, никогда его не даст. Но, скачивая приложение с какой-нибудь совершенно дурацкой игрой, где он будет разбивать конфетки, он с радостью передаст свой номер телефона. И это будет тот же самый человек.

И, мне кажется, поэтому нам не стоит недооценивать именно необходимость образования граждан. И, к сожалению, дискуссию о необходимости образования граждан я слышу последние

10–15 лет, но, как говорится, воз и ныне там. О необходимости государственной программы повышения цифровой грамотности, интернет-грамотности я тоже слышу уже очень много лет, но я не знаю, насколько эта программа как-либо практически реализуется. Но, мне кажется, это именно тот момент, на который надо обращать внимание, потому что именно сам гражданин должен защищать в первую очередь свои права. Государство должно ему помочь. И, естественно, обратившись в Роскомнадзор, допустим, он может потребовать, чтобы данные этого гражданина были удалены с какого-то сайта (и это нормально), ровно так же, как мы обращаемся в суд, когда нам не нравится, как ведут себя наши соседи. Когда сосед сверху вас заливает и не хочет вам платить компенсацию, вы не говорите, что у ЖЭКа или, не дай бог, у Министерства внутренних дел должно быть полномочие по мониторингу всех протечек во всех квартирах с целью того, чтобы платились компенсации за ремонт. Нет, существуют стандартные гражданско-правовые средства для решения подобных вопросов.

Я, коллеги, вас призываю не пренебрегать уже наработанным опытом, столетиями наработанным опытом и десятилетиями в различных правовых системах. Все эти вопросы решаемы. Безусловно, для того чтобы решать эти вопросы в новом контексте – контексте цифровизации, новой информационной реальности, нам нужны новые процедуры, нам нужны новые алгоритмы действия, нам нужны новые подходы. Но нам не нужно изобретать велосипед, велосипед давно изобретен, может быть, нужно просто на него поставить другой подшипник, у которого будет больше скоростей.

Традиционный пример, который мне кажется очень показательным в плане вариативности, наличия множественных вариантов действия, – допустим, извечный вопрос блокировки сайтов. И наш коллега из Роскомнадзора наверняка знает, что, что бы его агентство ни сделало, их будут критиковать: не заблокировали, не попросили заблокировать – плохо, заблокировали – тоже плохо, медленно блокируют – плохо, быстро блокируют – тоже плохо. В любом случае это будет плохо, потому что это действия государства. Всегда будет кто-нибудь недоволен.

Но действительно доступ к сети Интернет существенно облегчен по сравнению с газетами. И информацию с какого-либо сайта можно получить гораздо легче. И, естественно, процедура похода в суд и получения окончательного решения занимает время. Но существуют в том числе промежуточные способы. И, допустим, у наших коллег из Соединенных Штатов вполне себе действуют процедуры, в рамках которых блокировать могут сразу в рамках предварительных обеспечительных мер даже по административному иску.

Эти меры могут быть оспорены, но если они не будут оспорены, то блокировка останется. Если тот человек, который разместил частную информацию, не против того, что заблокирован его сайт с частной информацией, так она там и останется. То есть мне кажется, что в первую очередь средства должны быть гибкими. Гибкость и вариативность средств – это очень важно, потому что, мне кажется, они в наибольшей степени отражают именно суть той самой цифровой эпохи, в которую мы живем.

Если позволите, коллеги, я вступлю немного в дискуссию с парой наших предыдущих спикеров, и я буду готов с ними продолжить дискуссию в любом другом формате.

Во-первых, я хотел бы сказать нашему коллеге из Сбербанка, что уповать на уголовную ответственность – по-моему, это худшая из всех возможных надежд. Уголовное право известно своей неэффективностью. Действительно, есть превентивная функция у уголовного права, но с помощью только уголовного судопроизводства проблему кражи банковских данных и их нелегальной продажи не решишь.

И в связи с тем выступлением в первую очередь у меня возник вопрос: а откуда, собственно говоря, те самые бесчестные мошенники взяли банковские данные? Эти банковские данные очевидным образом утекли из баз данных тех самых банков. Поэтому в первую очередь нашему коллеге из Сбербанка, мне кажется, надо обратиться к вопросу о том, каким образом (не конкретно Сбербанк, я не имею в виду, что Сбербанк что-то плохо хранит) банковская сфера может улучшить способы хранения данных, как сделать хранение более безопасным. Мне кажется, наши коллеги из налоговой службы могут иногда и некоторым банкам рассказать, как обезопасить данные конкретных граждан.

Административная ответственность – это наиболее популярное решение в современном мире для большинства из таких вопросов, плюс гражданская ответственность. И мне кажется, что именно оперативность средств административного воздействия и гибкость средств гражданско-правового воздействия в наибольшей степени отвечают данной проблематике. И в первую очередь, мне кажется, проблема распространения данных зачастую в конечном счете сводится не к тому, что кто-то не хотел передавать свои данные, их собрали и начали потом перепродавать, а к той процедуре, благодаря которой эти данные начинают утекать. Важно отслеживать именно эти процедуры, важно регулировать доступ к данной информации.

Само по себе хранение данных не есть проблема. Проблематичным может быть использование данных данных (прошу прощения за некую тавтологию), а также проблема в том,

насколько безопасно эти данные хранятся и кому они могут быть переданы. Но для всего этого есть вполне устоявшиеся решения в мировой практике. Мне кажется, что российские законодатели в том числе вполне могут на нее опереться и придумать, безусловно, свои новые и абсолютно адекватные решения.

Конкретные предложения я передам в письменном виде. Спасибо.

И.В. РУКАВИШНИКОВА

Василий Александрович, спасибо большое за интересное выступление, за то, что нашли возможность присоединиться сегодня к нашему обсуждению.

Я хотела бы поддержать Ваше предложение по рассмотрению гибкой системы защиты, это очень интересное направление. На самом деле, возможно, именно этого сейчас не хватает в оперативности реагирования на нарушения в том числе и конституционных прав граждан.

И буквально одна реплика по поводу образовательных технологий и того, что уже достаточно давно ведется дискуссия о необходимости повышения цифровой грамотности. Действительно, это так. Я думаю, что еще не один год эта дискуссия будет вестись, и это абсолютно правильно, потому что сама по себе дискуссия уже привлекает внимание к проблеме и заставляет человека интересоваться возможными способами ее решения.

И в качестве серьезного направления деятельности… Совершенно недавно в абсолютно все образовательные стандарты, которые используются на территории Российской Федерации, были включены нормы, касающиеся обязательного изучения в учебных заведениях вопросов цифровизации в рамках как профессиональной деятельности, так и общеобразовательной. И, на мой взгляд, это очень серьезный шаг, который на сегодняшний день для определенной части населения (естественно, я имею в виду студентов, школьников, обучающихся) эту проблему решит. Другое дело – что есть вопросы, касающиеся просвещения более взрослой аудитории. Мы видели по статистике, что аудитория после 45 (45+) начинает испытывать определенные трудности, и вот здесь, конечно, вопросы просвещения очень актуальны.

Спасибо большое.

Уважаемые коллеги, я хочу попросить выступить Дмитрия Леонидовича Кутейникова. И это будет завершающее выступление, потому что, конечно, по времени мы уже перебрали.

Дмитрий Леонидович, пожалуйста, с учетом регламента.

Д.Л. КУТЕЙНИКОВ

Добрый день, уважаемые коллеги! Меня слышно хорошо?

И.В. РУКАВИШНИКОВА

Да-да, мы Вас слышим, продолжайте.

Д.Л. КУТЕЙНИКОВ

Я очень коротко, в двух словах постараюсь остановиться на своих конкретных предложениях.

Тема моего доклада касалась удаленной биометрической идентификации в основном, ну и в целом применения технологий искусственного интеллекта и того, как это отражается на реализации конституционного права граждан на неприкосновенность частной жизни.

Во-первых, я хотел бы дополнить коллегу, который начал выступать по этой теме, тем, что сейчас действительно в Российской Федерации нет специального регулирования данной проблемы. У нас регулирование основывается на Конституции Российской Федерации, отдельных нормах Гражданского кодекса, законе о персональных данных.

В других странах регулирование действительно начинает появляться. О США коллега говорил – что оно фрагментированное, разрозненное, в отдельных местностях технология распознавания лиц либо полностью запрещается, либо вводится мораторий до создания необходимого регулирования. На федеральном уровне есть предложения, но они не приняты пока. Также рассматривается вопрос алгоритмической подотчетности и прозрачности.

Что касается Европейского союза, здесь я как раз хотел бы коротко изложить интересный опыт, потому что буквально в этом месяце был опубликован проект регламента Европейского союза о гармонизированных правилах в отношении искусственного интеллекта. И как раз таки в этом акте использовался риск-ориентированный подход для использования систем искусственного интеллекта, и, собственно, предлагается запретить полностью удаленную биометрическую идентификацию физических лиц в режиме реального времени в общедоступных пространствах в целях охраны общественного порядка.

Устанавливаются всего три случая, когда может вестись такая слежка за людьми: во-первых – в случае поиска потенциальных жертв преступлений, включая пропавших детей; во-вторых – в случае угрозы жизни или безопасности человека, а также в случаях террористических атак, и в-третьих – для обнаружения, локализации, идентификации и преследования лиц, совершивших (или подозреваемых в совершении) преступления по конкретно определенным составам. Там определено 32 состава уголовных правонарушений со сроком лишения свободы не менее трех лет, если иное не установлено законодательством конкретного государства.

Таким образом, на мой взгляд, необходимо дополнительно законодательно урегулировать вопрос относительно процедуры и конкретных случаев использования систем искусственного интеллекта для удаленной идентификации личности. Представляется, что, несмотря на то что в части 3 статьи 55 Конституции предусмотрено ограничение прав и свобод федеральным законом, однако для данного конкретного случая следует руководствоваться смыслом главы 2 Конституции, которая предусматривает, что ограничение ряда личных прав возможно лишь на основании судебного решения в данном случае.

Также хотел бы остановиться на использовании комбинаций нескольких технологий внутри искусственного интеллекта. Помимо распознавания лиц, помимо машинного зрения это еще и технология машинного обучения. И при использовании этих двух технологий, в том числе для анализа больших массивов данных, создаются и используются в отдельных странах так называемые системы социального рейтингования (не буду останавливаться на том, что это). Также хотелось бы указать на то, что данные системы социального рейтингования, по сути дела, противоречат как букве, так и духу самой Конституции Российской Федерации, и отдельно законодательно необходимо не допустить возможность создания и применения социальных рейтингов в каком-либо выражении как на общегосударственном уровне, так и на уровне отдельных территориальных единиц либо сфер общественной жизни.

И последний мой пункт, который не прозвучал у коллег. Мы сегодня много говорили о деперсонализированных данных и процедуре деперсонализации. Однако в законодательстве других государств, в том числе в Европейском союзе, есть процедура анонимизации данных, то есть вывода, по сути дела, этих данных из категории персональных, для того чтобы на этих данных тренировать нейронные сети. Собственно, процедуру анонимизации данных было бы неплохо тоже отразить в российском законодательстве, это позволило бы создать вот этот пресловутый баланс между интересами личности и при этом развитием бизнеса.

Спасибо. Насколько смог, кратко изложил свои тезисы.

И.В. РУКАВИШНИКОВА

Дмитрий Леонидович, спасибо большое. Я прекрасно понимаю, что эти тезисы можно развивать и каждый из них может быть предметом отдельной дискуссии. Большое спасибо Вам за участие в этой дискуссии.

Согласна с Вами, что самое главное, наверное, в правовом регулировании этой сферы – это действительно все время держать баланс между соотношением частных и публичных

интересов, а это, как показывает практика, самое сложное на сегодняшний день. И без помощи научных исследований, без экспертного сообщества, конечно, в этой сфере пока законодателю достаточно проблематично принимать эффективные нормы, без опоры на уже имеющиеся разработки, предложения и так далее.

Именно поэтому, коллеги, наша дискуссия, мне кажется, очень полезна, очень интересна, очень важна и для освещения этой проблематики, и в принципе для очередного этапа опубличивания этих отношений, поскольку у нас идет трансляция сейчас в интернете и будет опубликована стенограмма, и для практических действий, и ее, я думаю, мои коллеги и здесь, в Совете Федерации, и в исполнительных органах власти, безусловно, примут в качестве рекомендаций к действию.

И я бы хотела сейчас еще раз предоставить слово Милошу Эдуардовичу Вагнеру, поскольку сегодня было очень много апелляций к Вам.

Милош Эдуардович, пожалуйста, прокомментируйте. И будем завершать мероприятие.

М.Э. ВАГНЕР

Вы знаете, из сегодняшних выступлений очень-очень ясно, понятно стало, что действительно нужно искать баланс, и не только баланс между частным и общественным, частным и публичным, но и баланс между интересами и правами отдельных лиц. Например, когда мы говорим о том, что нужно предоставить доступ бизнесу к данным, получается, права граждан, чьи данные предоставляются, каким-то образом тоже должны затрагиваться. Или, когда мы говорим о том, что необходимо усиливать контроль за обработкой персональных данных, мы, получается, вторгаемся в ту область регулирования, которая обеспечивает права организаций при их проверках и так далее.

Мне очень понравилась мысль, которую Василий Александрович Лукашевич обозначил, о том, что правовые инструменты должны быть гибкими и позволять реагировать сегодня и прямо сейчас, а не быть какими-то правилами, которым, один раз написав, нужно будет следовать. Например, тот самый инструмент предварительных обеспечительных мер – действительно очень хороший, эффективный, и его можно применять на деле при защите прав субъектов персональных данных достаточно эффективно, главное – этим заниматься.

Сегодня было очень много интересных мыслей. Нужно будет некоторые взять и прорабатывать вместе с Вами, Ирина Валерьевна. Спасибо большое.

И.В. РУКАВИШНИКОВА

Спасибо Вам большое.

Коллеги, еще раз хочу поблагодарить всех за состоявшуюся дискуссию. Очень важно, что наша дискуссия носила не только теоретический характер, а в большей части прикладной. Возможно, это от того, что многие (как раз представители науки), кто хотел выступить… Просто не уложились мы по времени, я прошу прощения, но, к сожалению, нет возможности продлить наше мероприятие. Но я обращаюсь к вам, уважаемые коллеги: мы ждем ваших предложений в письменном виде.

И напоминаю о том, что регулярно на площадке Совета Федерации эти вопросы поднимаются, обсуждаются в различных форматах, это не только формат, как сегодня, парламентских слушаний – это и "круглые столы", и совещания. И я прошу вас принять участие. Буквально через несколько дней мы опять вернемся к обсуждению этой тематики. На официальном сайте Совета Федерации информация обо всех мероприятиях размещена. Просьба регистрироваться и принимать активное участие.

Поверьте, что все высказанные предложения будут очень внимательно проработаны, изучены, и я надеюсь, что большинство из них будет реализовано.

Большое спасибо, уважаемые коллеги. Парламентские слушания завершены.

_____