На вопросы редакции журнала «ЗАКОН» отвечает соучредитель и член правления *Russian Privacy Professionals Association*
Алексей Витальевич МУНТЯН

МЫ ВСТУПИЛИ В ЭПОХУ ЦИФРОВОГО ОГОРАЖИВАНИЯ И НАЦИОНАЛИЗАЦИИ (ПЕРСОНАЛЬНЫХ) ДАННЫХ

Основатель и CEO в компании *Privacy Advocates*, соучредитель и член правления *Russian Privacy Professionals Association*. Внешний *Data Protection Officer* в двух транснациональных холдингах, член Совета Торгово-промышленной палаты РФ по развитию антикоррупционного комплаенса и деловой этики. Эксперт *Privacy & Legal Tech* кластера РАЭК, участник комитета по безопасности данных партнеров и пользователей при Консультативном совете по развитию экосистемы «Яндекса».

— Как получилось, что Вы выбрали такую область специализации, как персональные данные?

— К этой профессии я пришел не случайно, а осознанно. В 2003 году поступил в МИФИ на факультет правового обеспечения информационной безопасности. Сейчас этого факультета, к сожалению, уже нет в институте. В 2008 году устроился работать в Управление комиссара по правам человека ООН в Восточно-Африканском региональном офисе в Эфиопии. Здесь я проработал год специалистом по информационной безопасности. Моей главной задачей была защита персональных данных лиц, которые обращались в Управление с жалобами на нарушение прав человека. Так как были попытки несанкционированного доступа к этим данным, я в течение года занимался тем, что пересматривал и улучшал те подходы к обеспечению защиты персональных данных, которые применялись ранее. Увы, более подробно рассказать не смогу, так как связан бессрочными обязательствами по *NDA*.

Потом я окончил магистратуру в Колледже королевы Марии при Лондонском университете по специализации в области права *IT/IP*, телекоммуникационного права. Кроме того, был опыт работы в компании, которая занималась администрированием портала персональных данных Роскомнадзора; в компании — системном интеграторе, где оказывал консультационные услуги по защите персональных данных, коммерческой тайны. Еще работал менеджером по защите персональных данных в ряде крупных российских и международных компаний. Сейчас я также занимаюсь общественной деятельностью в области приватности данных и выступаю в качестве внешнего консультанта по вопросам в данной области.

— А кто сейчас готовит специалистов в сфере защиты персональных данных в России?

— Есть определенные программы в МГУ, НИУ ВШЭ, но это не специализированная подготовка, а, скорее, организационно-юридическая специализация в рамках *IT/IP*. Такого комплексного образования, как было в МИФИ, сейчас нет. В МИФИ мы изучали и технические вопросы, и экономику информационной безопасности, психологические аспекты информационного противоборства. Сегодня в нашей стране я не знаю ни одной аналогичной по содержанию полноценной программы высшего образования в этой сфере. Но проводятся курсы повышения квалификации и тренинги по *Data privacy*. Мы, *RPPA.ru*, совместно с МГУ запустили свой учебный курс повышения квалификации. Я думаю, что в ближайшее время появятся и полноценные программы обучения в сфере защиты персональных данных.

— Что сейчас понимается под персональными данными? Изменяется ли содержание этого понятия со временем?

— Последние годы мы наблюдаем рецепцию именно европейского подхода к трактовке понятия «персональные данные». Хочу обратить внимание, что само регулирование в сфере информационной приватности, защиты персональных данных в нашей стране появилось благодаря европейской правовой традиции, после присоединения России в 2005 году к Конвенции № 108[1]. И как раз в рамках взятых нами на себя обязательств был принят Закон № 152[2] в 2006 году.

Согласно европейскому подходу, персональные данные — это любая информация, которая прямо или косвенно относится к определенному или определяемому физическому лицу. В нашей стране в первоначальной редакции Закона была попытка перечислить некоторые категории персональных данных (ФИО, паспортные данные и т.п.). Но в 2011 г. были внесены изменения и примеры исключили из определения, так как это порождало много толкований, сужая сферу применения Закона. Сейчас в нем содержится гармонизированное определение персональных данных, соответствующее Конвенции № 108 и *GDPR*[3]. Поэтому в целом на сегодня мы находимся в едином понятийном поле с европейским регулированием. Но на практике до сих пор встречается непоследовательный подход и толкование содержания понятия «персональные данные». Например, в нашей стране в отношении номера телефона или государственного номера автомобиля еще идут споры, потому что Роскомнадзор официально не считает их персональными данными. Но в отдельных случаях есть возможность в конечном счете установить персональные данные лица, которое допущено к управлению автомобилем, и идентифицировать его, — и тогда с точки зрения европейского понимания это в чистейшем виде персональные данные. При отнесении тех или иных данных к персональным большое значение имеет контекст, и у нас только-только появляется понимание некоторых вопросов.

Другой пример: когда вы включаете новый ноутбук, заходите в Сеть и вводите поисковый запрос в любой поисковой системе, при этом еще нигде не зарегистрировавшись, данные о ваших запросах и предполагаемых интересах фиксируются поставщиками интернет-рекламы. То есть не обязательно знать, кто вы такой, вы можете быть определенным или определяемым лицом. Но вас можно выделить по техническим данным среди другой массы людей и с вами можно будет взаимодействовать прямо или косвенно (например, таргетировать в Интернете и показывать нацеленную на ваши интересы рекламу). Это говорит о том, что технических данных

[1] Конвенция о защите физических лиц при автоматизированной обработке персональных данных (заключена в г. Страсбурге 28.01.1981). URL: http://www.consultant.ru/document/cons_doc_LAW_121499/ (дата обращения: 15.03.2022).

[2] Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

[3] Общий регламент защиты персональных данных, принятый постановлением Европейского союза 2016/679.

вашего компьютера, браузера и т.п. достаточно, чтобы вступить с вами во взаимоотношения в части демонстрации рекламы.

— Тогда где пределы определения содержания понятия «персональные данные» с точки зрения права?

— С точки зрения права это любая информация, которая прямо или косвенно относится к определяемому или определенному лицу. Понимание персональных данных давно сложилось в судебной практике и идет по пути расширительного толкования как раз в сторону европейского подхода. В 2016 году был целый ряд громких кейсов: дело МГТС, дело «Сумма телеком» — где суд прямо указал, что хеш-сумма пользовательских данных, *IP*-адрес являются персональными данными. И странной выглядит ситуация, когда кто-то из надзорных органов или регуляторов занимает позицию, что номер телефона — это не персональные данные, а, например, всего лишь номер персонального устройства. В Европе такая позиция была бы невозможна, так как этот номер абонентского устройства принадлежит какому-то конкретному пользователю. При этом надо различать персональные и личные данные как часть персональных данных. Личные данные — это данные, принадлежащие определенной личности как социальному отражению индивида. Личность — это то, что формируется в процессе взаимодействия с обществом. Персональные данные кроме данных о личности включают еще и наши нативные характеристики, биологические, генетические и т.п.

— Чтобы нащупать границы этого понятия, давайте уточним: рекламный звонок по моему телефону без моего согласия — это нарушение персональных данных, а если мне бросают рекламу в почтовый ящик — это разве не то же самое?

— Разносчик рекламы по почтовым ящикам не знает, что этот ящик принадлежит именно вам, не знает, что именно вы живете в определенной квартире. С одной стороны, звонок сам по себе — это вторжение в личное пространство человека, что, конечно, является в некоторой степени вопросом субъективной оценки. С другой стороны, часто подобного рода звонки носят мошеннический характер и номер телефона может быть использован, чтобы записать образец вашего голоса, который в условиях технологий голосовой идентификации является ценнейшей информацией. Например, вам звонит автоинформатор, который просит отвечать на вопросы в форме «да» или «нет». Ваши ответы записываются, а потом запись используется для обхода систем биометрической идентификации в банках. Поэтому, отвечая на входящий звонок с неизвестного номера, лучше первым не заговаривать.

Выбор способа коммуникации с субъектом персональных данных имеет значение. В *GDPR* предусмотрен такой механизм, как *DPIA* (*Data Privacy Impact Assessment*), т.е., когда мы хотим использовать персональные данные для той или иной цели, мы должны заблаговременно продумать, какие риски это может нести для субъекта персональных данных, насколько будет соответствовать его разумным ожиданиям. Например, в рамках маркетинговых коммуникаций большинство людей преимущественно выбирают вариант связи посредством электронной почты и мало кто выберет связь по телефону. И многие раздражаются, когда компании звонят или используют номер телефона для коммуникаций в мессенджерах. У людей есть разумные ожидания в отношении коммуникации, и по статистике надзорных органов, наших и европейских, больше половины жалоб — это жалобы на маркетинговую коммуникацию.

— Мы сами оставляем огромное количество данных о себе, выкладывая ролики в социальных сетях, которые, получается, можно использовать в нарушение наших интересов?

— Действительно, чем больше материала, аудио-, видеороликов вы оставляете о себе в Сети, тем больше возможностей для создания соответствующих моделей, которые будут на очень хорошем уровне вас имитировать. Есть технология *Puppet Master* («Кукловод»), с помощью которой можно полностью создать иллюзию вашего лица и дать возможность другому человеку, используя видеосигнал, полностью подделать вас в видео. И тут опасно даже не то, что кто-то может разместить какой-то порочащий вас ролик с вашим лицом, а в большинстве случаев злоумышленники будут использовать такие технологии, чтобы обойти системы биометрической аутентификации (удостоверения личности).

— Если с помощью технологий можно так качественно подделать видеоизображение человека, то, может быть, понятие компромата скоро станет неактуальным?

— Данный вопрос обсуждается давно. Как только появилась фотография, появился фотомонтаж, фотошоп.

Вспомним, к примеру, истории с видеороликами с человеком, похожим на генерального прокурора, и т.п., в 90-х годах. Уже тогда говорили о том, что современная технология позволяет лицо одного человека «посадить» на лицо другого человека. Сейчас технологии очень быстро развиваются, порог получения доступа к продвинутым технологиям все ниже, и если сейчас создание качественных дипфейков еще достаточно дорого, то скоро этот процесс, думаю, станет проще и дешевле. Например, в Китае проблема создания и использования дипфейков уже регулируется. Это вопрос права на личность.

— Наши данные уже широко распространены в Сети: записи лекций, фотографии, видеоролики. Мы знаем о рисках, а регулирования соответствующего нет, притом что само государство интенсивно внедряет технологии идентификации, например с помощью биометрических данных. Почему, на Ваш взгляд, не развивается соответствующее регулирование?

— Обычно в начале развиваются технологии, в данном случае технологии создания дипфейков. Потом в отношении этой технологии складываются определенные общественные отношения, которые могут иметь явные признаки общественной опасности. После чего появляется адекватное правовое регулирование, когда государство начинает, например, требовать обозначения материалов, созданных с помощью такой технологии, указанием, что это дипфейк. При этом использование изображения другого человека также должно регулироваться. И создание дипфейков без таких меток станет административным правонарушением как минимум.

— Получается, что само государство интенсивно внедряет эти технологии вне регулирования?

— Редко бывает обратный порядок, когда в начале появляется регулирование, а потом технология. Пока само явление и его масштаб не вызывают общественного резонанса. Десять лет назад мало кто знал закон о персональных данных, мало кто специализировался в этой сфере, а сейчас с персональными данными сталкиваются все, в связи с чем к этой сфере очень повысилось внимание. Сами персональные данные появились, конечно, не в 2006 году, они всегда существовали, но регулирование появилось только тогда, когда существующие возможности, которые были на рубеже 60–70-х годах прошлого века, уже позволяли получать огромную власть и возможности через автоматизированную, а потом и автоматическую обработку данных. И самое потенциально опасное для обладателя персональных данных состоит не в самом объеме данных, которые о нем могут собрать и систематизировать, а в возможности выявления тех знаний о нас и моделей нашего поведения тем, кто сможет соответствующим образом наши данные обработать. Есть данные достоверные и актуальные, а есть данные предполагаемого характера, о нашем предполагаемом поведении в той или иной ситуации, например данные о прогнозе развития болезни, информация о его привычках, образе жизни, частоте полетов на самолете и т.п. Такая предиктивная аналитика позволит управлять нашим с вами поведением, поскольку, используя подобные технологии и понимая, как устроено поведение человека, можно непосредственно влиять на него.

— Как защитить персональные данные от самого государства?

— Сам по себе правовой институт защиты персональных данных появился как ответ на социальные волнения, произошедшие в Европе в 60-х годах XX века, и реакцию правительств, в том числе и в Европе, которые очень серьезно усилили роль спецслужб. Европейский союз в 60–70-е годы только как поколение назад прошел через опыт оккупации в ходе Второй мировой войны, когда данные архивов использовались, чтобы выявлять людей еврейской и других национальностей[4]. Местное население испугалось, что усиление роли спецслужб угрожает демократическому обществу и что накопление данных о гражданах может быть использовано против них самих.

— Эти опасения сегодня только усилились.

— Тогда технологии обработки информации были в начале развития, достаточно быстро в 80-е годы в аккумулировании и создании массивов персональных данных стала расти роль бизнеса и особенно транснациональных корпораций, возможности которых стали превосходить возможности государств.

— Но у этих корпораций все же нет политической власти.

— Да, но у них есть мягкая власть, *soft power*, и есть много исследований, которые подтверждают, что эти корпо-

[4] См., напр.: Нюрнбергские расовые законы от 1935 года.

рации воздействуют на людей и их мнение, в частности в рамках избирательных кампаний.

Понятно, что государства не откажутся от технологии, например биометрической идентификации/аутентификации. Однако в Европейском союзе идет работа по ограничению использования технологий распознавания лиц и о запрете использования технологий искусственного интеллекта для этой цели.

— Может, это разумно?

— Каждое общество выбирает свой путь. С одной стороны, разумно, когда мы говорим, что каждый имеет право на приватность и безопасное выражение своей общественной позиции. С другой стороны, здесь проходит тонкая грань, ведь на общественных мероприятиях и политических акциях могут быть провокаторы, например как во время манифестаций «желтых жилетов» во Франции. Поэтому в реальности большинство государств, хотя бы нелегально, не откажутся от использования этих технологий.

— При таком обширном характере распространения наших персональных данных насколько мы реально можем обеспечить их безопасность?

— Под защитой персональных данных надо понимать не столько техническую защиту, сколько применение мер по соблюдению принципов обработки данных. Например, в рамках соблюдения права на частную жизнь вы имеете право запрещать доступ чужим лицам к частной информации и защищать это право посредством обращения в суд и правоохранительные органы при его нарушении, т.е. в данном случае используется метод запрета. А есть институт защиты персональных данных *(data protection)*, в соответствии с которым применяется следующий подход: ваше право на личную и семейную жизнь и информационную приватность признается, но без обработки ваших персональных данных функционирование современного общества и экономики невозможно. Поэтому вы даете согласие обрабатывать ваши данные, но с соблюдением определенных принципов: законности, справедливости, пропорциональности, соблюдения цели обработки и т.д. Дьявол, конечно, кроется в деталях. У нас в стране инструментарий пока недостаточно развит для соблюдения этого подхода. В Европе государство не диктует, как тебе технически защищать персональные данные, а предоставляет право выбора способов соблюдения установленных принципов. Но если что-то пойдет не так, то применяется оборотный штраф. У нас традиционно все более бюрократизировано. Если в Европе больше смотрят на содержание мер защиты персональных данных, то в России больше смотрят на форму. В конце прошлого года у нас была утечка данных в одной очень крупной компании, ей выписали штраф в размере 30 000 рублей. Естественно, в такой ситуации никакого экономического стимула защищать персональные данные не возникает. Например, в Китае был принят закон, который позволяет государству противодействовать утечкам данных, их противоправному раскрытию, также посредством установления оборотного штрафа до 5%. И должностные лица, которые персонально ответственны за утечку, фактически получают волчий билет от государства — они могут попрощаться со своей карьерой. Я думаю, что надо изменить меры ответственности и акцентировать внимание на компании, которая допустила утечку, нужно стигматизировать именно ее, обязывая указывать информацию о том, что компания допустила утечку персональных данных. Или вносить такие компании в специальный реестр нарушителей, т.е. воздействовать на них не только финансово, но и через репутационные риски.

— Хватит ли у нас мощностей в масштабах страны, учитывая количество компаний, ресурсов, чтобы контролировать и расследовать факты таких утечек?

— Утечка утечкам рознь. Например, с этого года должна быть запущена система выявления утечек баз с персональными данными, работа в эту сторону идет. Безусловно, учитывая, что у нас несколько миллионов субъектов малого и среднего бизнеса, это непростая проблема, но в данной ситуации нам требуется дифференцированное регулирование. Если большая компания может нанять и консультанта, и технические условия обеспечить, то малому бизнесу это не по карману. В Европе, например, есть поблажки для малого бизнеса. В Германии в компаниях с менее чем 20 сотрудниками можно не назначать отдельное лицо, ответственное за защиту персональных данных *(Data Protection Officer)*. Считается, что даже если утечка или иное нарушение безопасности обработки персональных данных произойдет в таких компаниях, то это не создаст такого общественного резонанса, как в огромных корпорациях.

— Как быть с депривацией персональных данных, когда они обрабатываются без нашего согласия

и создаются новые данные о нас, а мы об этом не знаем? Нужно ли запретить такую обработку или регулировать ее особым образом?

— Данная проблема возникает в результате того, что мы взаимодействуем с огромным количеством сервисов и компаний, которым нужны наши персональные данные. С одной стороны, закон дает возможность запрашивать у любой компании подтверждение факта обработки ваших персональных данных с выяснением, какие данные, с какими целями обрабатываются, кому передавались. С другой стороны, какого-то тотального и полного контроля возможности управлять этими данными у субъекта нет. Следует сразу определиться, что полная и абсолютная приватность — это миф. Например, вы оплатили в интернет-магазине товар, а после этого просите магазин уничтожить ваши персональные данные. В этом случае вы получите ответ, что все данные уничтожить невозможно, потому что есть обязательства в соответствии с правилами бухгалтерского и налогового учета хранить определенную информацию о покупателях. Поэтому абсолютизировать право на информационную приватность не стоит — могут быть нарушены права и интересы других лиц, например интересы компании на ведение деятельности законным способом. Другой вопрос, что сейчас много разговоров о создании неких систем, через которые субъект может давать разрешения на обработку своих персональных данных всем заинтересованным лицам. Например, предлагается использование государственной ЕСИА[5] для целей получения гражданами РФ сервисов и услуг в Интернете. Покупая что-то в интернет-магазине, вы в нем регистрируетесь через учетную запись ЕСИА и предоставляете возможность магазину получить ваши данные. Учитывая, что наши с вами действия и действия в отношении нас с вами порождают новые данные, создание некоего единого хранилища персональных данных проблему защиты данных не решит, потому что фактически данные появляются не в этой системе, а являются результатом кропотливой работы по их сбору и аналитике.

Есть другие аспекты использования персональных данных. Например, возникает вопрос, можно ли платить своими персональными данными за те или иные услуги и товары. С одной стороны, есть европейский подход, согласно которому персональные данные не могут быть товаром. Человек не может отказаться от своего естественного права на защиту собственных персональных данных, и любая сделка об обратном будет ничтожна. С другой стороны, у любого субъекта есть право на управление своими персональными данными и распоряжение ими. В рамках европейских норм и судебной практики транслируется устоявшаяся позиция, что в принципе субъект может заплатить своим согласием на обработку персональных данных той или иной компании, если он получает в качестве встречного предоставления какие-то блага, например бесплатное участие в лотерее, возможность скачать бесплатно приложение, которым можно пользоваться при условии предоставления организации — собственнику приложения возможности отслеживать геолокацию такого субъекта. Согласие можно в любой момент отозвать, но при этом будет утрачена возможность пользоваться этим сервисом. Вопрос гражданского оборота персональных данных очень дискуссионный, и в ближайшее время дискуссия будет продолжаться.

— Если обеспечить контроль за своими персональными данными и их защиту так сложно, может, надо искать иные инструменты идентификации человека для совершения юридически значимых действий? Может быть, ввести какие-то персонифицированные чипы?

— Я считаю, что это решение не найдет поддержки в обществе. Всегда будут люди, которые против использования каких-то технологических новшеств. К тому же, на мой взгляд, использование таких инструментов не соответствует демократическим принципам общественного устройства.

> Скорее, зная о проблеме обработки персональных данных, люди станут внимательнее относиться к ним и соблюдать так называемую информационную гигиену.

Например, среди молодых людей все чаще становится популярным не иметь собственные аккаунты в социальных сетях и минимизировать информацию о себе в Сети. Они создают небольшие виртуальные площадки, на которых общаются. Возможно, в ближайшее время вернется интерес к интернет-форумам или чему-то похожему, но на новом технологическом уровне, а социальные сети все больше и больше будут ограничиваться регулированием.

[5] Единая система идентификации и аутентификации.

— Создает ли использование *QR*-кодов в рамках борьбы с распространением коронавирусной инфекции угрозу безопасности персональным данным?

— Один из чиновников Роскомнадзора по Санкт-Петербургскому управлению заявил, что это вообще не персональные данные. К сожалению, в целях достижения текущих целей государство может либерально подходить к толкованию содержания персональных данных, считая, что номер телефона и *QR*-код не являются персональными данными, хотя *QR*-код может содержать в кодированном виде и инициалы, и паспортные данные человека. В ЕС даже сомнений бы не возникло, что это, конечно, персональные данные. Сама по себе технология создания и использование *QR*-кодов, посредством которых можно получить информацию о том, что его предъявитель вакцинирован или переболел, хорошая, но то, как часто ее используют и как трактуют, вызывает определенную озабоченность. Непоследовательность в этом вопросе создает много проблем в правоприменении. Даже безотносительно того, насколько подходы соответствуют мировой практике, хочется просто стабильного правоприменения.

— Не идем ли мы в данном случае по китайскому пути?

— Да, в Китае есть система социального рейтинга, причем она имеет двойную природу. Одна система касается физических лиц, другая — юридических. И последняя вызывает даже большую обеспокоенность международных компаний, которые работают на китайском рынке. Но модель Китая в целом специфичная, связанная с культурным кодом, своими представлениями о демократии, правах человека, построении общества и государства. В то же время мы в целом находимся в эпохе цифрового огораживания, национализации данных, когда все крупные страны пытаются оградить персональные данные граждан от конкурентов. В России приняты Закон о локализации персональных данных[6], «пакет Яровой»[7] и другие меры, которые приводят к повышению издержек бизнеса в связи с обработкой и хранением персональных данных. Но такие акты есть не только у нас. Гораздо раньше подобное регулирование появилось, например, в Германии. В 2020 г. Европейским судом было принято решение по делу Максимилиана Шремса *(Max Schrems)*[8], которое как раз очень существенно ограничило право передачи персональных данных из Европы в США в связи с негативной оценкой американского законодательства в части возможности слежки за гражданами и получения данных о них. После этого решения европейский бизнес, который в основном использовал американские системы, приложения для обработки персональных данных и аналитики, получил неофициальные рекомендации пользоваться отечественными платформами, провайдерами и т.п. Прямой запрет не установили, но были созданы все условия, чтобы максимально ограничить использование европейским бизнесом зарубежных сервисов, в первую очередь сервисов США, так как этот рынок составляет около 1 трлн евро в год.

— Мы же не можем полностью избежать того, чтобы не передавать свои персональные данные за рубеж, и не можем полностью контролировать процесс их обработки. В чем тогда цель защиты персональных данных?

— Никто и не призывает это делать. Вопрос состоит в возможности контроля за объемом передачи данных и их использования. Вопрос защиты персональных данных, информационной приватности — это именно тот элемент, который склоняет чашу весов в сторону защиты более слабого субъекта: работник — работодатель, потребитель — производитель. И, на мой взгляд, такой подход будет усиливаться. Сейчас в публичном поле РФ обсуждается законопроект о регулировании рекомендательных сервисов. Это аналитические алгоритмы, которые анализируют ваше поведение и предлагают вам приобрести тот или иной товар или услугу. И есть существенный риск или угроза, что через данные сервисы можно регулировать ваше поведение. Например, эти алгоритмы используются в социальных

[6] Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

[7] Федеральный закон от 06.07.2016 № 374-ФЗ «О внесении изменений в Федеральный закон „О противодействии терроризму“ и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности»; Федеральный закон от 06.07.2016 № 375-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности».

[8] URL: https://curia.europa.eu/juris/document/document.jsf?docid=228677&doclang=EN (дата обращения: 15.03.2022).

сетях, когда в зависимости от сети друзей, высказываний и предпочтений людей пользователю предлагается информация и построение сети контактов исходя из его взглядов. Таким образом при помощи алгоритмов люди разводятся по своим идейным нишам, варятся в своем бульоне, они не учатся взаимодействовать друг с другом и с людьми отличающихся взглядов. Другой пример применения подобных технологий — дело «Кембридж Аналитики»[9], которую обвиняли уже в более жестком манипулировании, когда аудитории подаются только определенные новости, фейк-ньюз. Когда мы говорим о потребительском поведении, то существует много разных способов подсунуть вам любой товар, привлечь ваше внимание. Собственно, то, как эти рекомендательные сервисы выстраивают свои алгоритмы, почему они решают вам показать то или иное сообщение сейчас или в другой момент времени — это большая коммерческая тайна. Но нужно, чтобы такие данные раскрывались, чтобы не допускалось манипулирование поведением потребителей. Например, у любого крупного банка достаточно информации о человеке, чтобы стимулировать его совершить определенную крупную покупку, приводить в правильное расположение духа. Потенциал у этих технологий огромный.

— Насколько безопасно расширение применения технологий с использованием биометрических данных человека?

— Сейчас обработка биометрических данных начала регулироваться в рамках Закона № 479[10]. Этот Закон фактически открыл новую главу в регулировании обработки биометрических данных, которая сейчас у нас серьезно ограничена. Только очень крупные организации, *IT*-компании смогут позволить себе обрабатывать биометрические данные с соблюдением всех новых требований. Государство четко разделило биометрию для целей идентификации (установление, определение личности) и аутентификации (удостоверение личности). Теперь регулируется процесс сбора и создания библиотек биометрических данных, но в Законе большое количество пробелов, например в Единой биометрической системе (ЕБС) предусмотрено хранение информации только о лице и голосе. Притом что есть и другие биометрические персональные данные, статические (например, генотип, отпечатки пальцев) и динамические (походка, голос). Еще одна из самых больших проблем в том, что у нас не регулируются некоторые вопросы, например точность применяемой технологии. Что делать, если происходит положительное срабатывание в несоответствующем случае (ложноположительное срабатывание, когда система принимает одно лицо за другое) или, наоборот, система не может распознать человека? А это создает затруднения и для внедрения технологий, и для доверия к результатам использования этих технологий с юридической точки зрения.

— Вы организовали *Russian Privacy Professionals Association* — Сообщество профессионалов в области приватности. Расскажите о нем, пожалуйста. В чем цель его создания?

— Наше сообщество существует больше двух лет, объединяет около 750 участников — физических лиц. Бóльшая часть из них — это корпоративные юристы, также много коллег, которые являются консультантами в области защиты персональных данных, сотрудниками Роскомнадзора, коллеги из академической сферы. Мы защищаем в первую очередь интересы профессионалов, понимаем трудности бизнеса, консультантов, проблемы защиты персональных данных. В последние полтора года мы активно проводим мероприятия информационного, просветительского характера, семинары, конференции. В прошлом году у нас была большая международная конференция «Евразийский конгресс по защите данных», в которой участвовали представители из разных стран, например руководитель Европейского инспектора по защите данных. Также мы являемся сообществом, которое уже два года подряд выбирает и награждает компании и физических лиц, которые смогли проявить себя на поле защиты персональных данных, в рамках премии *Russian Privacy Awards*. Основная цель сообщества — построение взаимодействия между профессионалами, так как мы работаем в непрозрачной и непредсказуемой регуляторной среде. В рамках сообщества мы общаемся, обмениваемся опытом, информацией, принимаем участие в законотворческой деятельности. Мы считаем, что развитие данной отрасли и регулирование персональных данных должны идти по пути человекоцентричности, постановки во главу угла прав и законных интересов человека.

[9] *Громов А.* Как Cambridge Analytica «взламывала выборы» по всему миру https://tass.ru/mezhdunarodnaya-panorama/5048632 // ТАСС. 2018. 5 апр. (дата обращения: 15.03.2022).

[10] Федеральный закон от 29.12.2020 № 479-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации».