УДК 338.242.2

Марианна СОКОЛОВА

ПЕРВЫЕ УСПЕХИ НОВОГО ЕВРОПЕЙСКОГО ОБЩЕГО РЕГЛАМЕНТА ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Аннотация. В статье автор рассматривает значение нового общеевропейского регламента General Data Protection Regulation (GDPR) (вступил в силу 23 мая 2018 г.) для эффективного регулирования в сфере защиты персональных данных в ЕС. Крупные штрафы за нарушения при обработке персональных данных, права пользователей на контроль за своими персональными данными, их удаление (право на забвение), исправление и право на переносимость данных (портабилити) сделали GDPR эффективным законодательным инструментом для европейских регуляторов. Приведены первые результаты влияния штрафных санкций GDPR на изменение политики конфиденциальности в компаниях, работающих с данными европейцев, в том числе в американских ТНК, за 2018–2019 гг. Показано, как правовые нормы Регламента повлияли на принятие аналогичных законов в других странах, особенно на калифорнийский закон “О защите данных интернет-пользователей” (California Consumer Privacy Act) (2018 г.).

Ключевые слова: персональные данные, защита и обработка персональных данных, штрафы, информационная экономика, General Data Protection Regulation.

GDPR: новый общеевропейский регулятивный инструмент по защите персональных данных

Современное общество и управление им невозможно представить без систем наблюдения, самых разных баз, в том числе биометрических, ДНК и т.д. Собираемая таким образом информация касается частной жизни граждан. Между тем ни доступа к этой информации, ни контроля над её использованием у пользователей по большей части нет.

Сегодня, когда любой маркетолог или digital-аналитик может узнать о своих клиентах абсолютно всё, опираясь на оставленный ими “цифровой след”, вопрос,

© **Соколова Марианна Евгеньевна** – кандидат философских наук, старший научный сотрудник отдела военно-политических исследований, Институт США и Канады РАН, Институт перспективных исследований Московского педагогического государственного университета. **Адрес:** 121069, Россия, Москва, Хлебный переулок 2/3. **E-mail:** mariamva@yandex.ru

DOI: <http://dx.doi.org/10.15211/soveurope220205666>

что ожидает человечество в ближайшем будущем, если не будут найдены способы и средства изменить это положение вещей, актуален как никогда. Понимание того, что человеческую цивилизацию в её развитии может ожидать сценарий Паноптикума¹, стало частью социально-философской мысли и получило отражение во многих литературных и кино-утопиях. Правда, на смену прежней модели просматриваемого сверху пространства, отдельные ячейки которого отделены друг от друга непроницаемыми стенками, пришла новая модель тотальной открытости, когда не только один “Большой брат”, но и множество более мелких “братьев” (коммерческие акторы, ИТ-бизнес, хакеры, электронные преступники и проч.) имеют доступ ко всем сторонам жизни человека, собирая, обрабатывая и продавая его личные данные [Пазюк, Соколова, 2015: 26].

Для европейской традиции защиты права человека на конфиденциальность такое положение вещей неприемлемо, что и предопределило жёсткий подход к регулированию сферы защиты персональных данных в условиях современной информационной экономики, в том числе суровое по отношению к технологическим компаниям законодательство.

История европейских законов по защите персональных данных, подвергающихся автоматической обработке, насчитывает более четырёх десятилетий и несколько поколений правовых актов. Среди ключевых документов, определявших правила соблюдения конфиденциальности – Конвенция № 108 Совета Европы о защите частных лиц при автоматизированной обработке данных личного характера 1981 г. и Дополнительный протокол к ней, принятый в 2001 г., Директива 95/46/ ЕC (“Общие положения о защите данных”), Директива 2002 г. – ePrivacy Directive (Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) и ряд других документов. Вступление в действие 25 мая 2018 г. Регламента 2016/679 Европейского парламента и Совета “О защите персональных данных и о свободном перемещении таких данных” (General Data Protection Regulation, GDPR) стало её новым этапом². На очереди стоит и новый законопроект ePrivacy Regulation, который должен заменить прежнюю европейскую Директиву 2002 г.³ Действие нового Регламента Евросоюза распространяется как на европейские, так и на зарубежные компании, работающие с персональными данными граждан и резидентов ЕС по всему миру.

¹ Идея тотального надзора, сформулированная английским философом Иеремией Бентамом в образе тюрьмы, спланированной так, что заключённые всё время остаются под надзором.

² Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (2016), *Official Journal of the European Union*, no.119, available at: <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32016R0679> (дата обращения: 10.08. 2019).

³ Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) (2017), Eur-Lex.europa.eu, available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017PC0010&from=EN> (дата обращения: 10.08. 2019).

В целом, GDPR можно назвать общеевропейским ответом на вызовы экономики Больших данных в защиту персонального, личного пространства человека на пороге эпохи тотальной прозрачности, когда объёмы самых разнообразных данных, в том числе и визуально-звуковых, биометрических, стремительно увеличиваются, интенсивно пополняя “цифровой след” и становясь источником новых правовых коллизий. В результате возможность защитить своё интимное пространство как основа неприкосновенности частной жизни за последние два десятилетия пошатнулась, и прежде всего усилиями международных технологических компаний, которых принято называть ИТ-гигантами, в большинстве своём имеющих американскую юрисдикцию. В настоящее время остаётся лишь один способ скорректировать ситуацию – вернуть человеку возможность контролировать информацию о том, что происходит с его персональными данными, решать, когда, как и в каком объёме информация о личности становится известной или сообщается другим [Пазюк, Соколова, 2015: 11].

В современном праве принято разделять представление о конфиденциальности как защите неприкосновенности, частной жизни от вторжений и понятие контроля над персональными данными и предотвращением их незаконного использования [Пазюк, Соколова, 2015: 54]. Это означает отход от тех основ, на которых базировался институт приватности с конца XIX века, прежде всего – от доктрины “права быть оставленным в покое”, положения которой зафиксированы в базовых документах о правах человека, в том числе во Всеобщей декларации прав человека [Дмитрик, 2018: 56]. Современные законодательные инструменты направлены именно на регулирование контроля за персональными данными.

Одним из таких инструментов является General Data Protection Regulation – современный нормативный акт, который существенно расширяет права физических лиц по контролю за своими персональными данными и их обработкой, ужесточает требования к ИТ-компаниям, обрабатывающим персональные данные, и расширяет перечень санкций, в частности, устанавливает более высокие штрафы за нарушения в этой сфере. Среди основных принципов: обработка персональных данных на законной, справедливой и прозрачной основе; информирование о целях использования данных в максимально доступной и простой форме; сбор данных исключительно в целях, заявленных компанией; запрет собирать личные данные в большем объёме, чем это необходимо для целей обработки; точность личных данных, возможность их удалить и исправить по требованию пользователя; хранение данных в форме, которая позволяет идентифицировать субъекты данных на срок не более, чем это необходимо для целей обработки; защита данных при обработке от несанкционированного или незаконного доступа, уничтожения и повреждения. Персональные данные по GDPR – это любая информация, по которой можно определить субъекта данных, в том числе его имя, местоположение, IP-адрес, онлайн-идентификатор, данные о физической, физиологической, генетической, умственной, экономической, культурной или социальной идентичностях.

Необходимы немалые усилия, чтобы создать соответствующую новым технологическим и экономическим условиям систему защиты персональных данных в условиях, когда экономика, бизнес, система управления основаны на сборе, обработке и многократном использовании данных.

“Укрощение строптивых”: европейские регуляторы против ИТ-гигантов

Европейские регуляторы смогли сосредоточить усилия на продвижении общественных ценностей – защите интересов и прав интернет-пользователей, достижении этических целей, главным образом благодаря тому, что в ЕС не так много, как в США, крупных ИТ-компаний, неограниченно лоббирующих свои интересы [Курбалая, 2018: 351]. Именно поэтому GDPR ориентирован прежде всего на такую жёсткую для бизнеса меру как значительные денежные штрафы за нарушения при обработке персональных данных – до 200 тыс. евро или 4% годового дохода в случае, если об этом не будет сообщено регулятору в течение 72 часов.

Субъекты персональных прав в странах ЕС, будь то граждане Евросоюза или лица, временно пребывающие на его территории, имеют право, согласно Регламенту, запросить у компании подтверждение факта обработки их данных, а также уточнить, кому и какая информация передаётся, узнать источник получения данных, потребовать прекращения их обработки. Право на забвение позволяет удалять свои личные данные по запросу во избежание их распространения или передачи третьим лицам, если эта информация не представляет собой общественного интереса или это не влияет на свободу слова и не противоречит интересам общества или иным фундаментальным правам.

При выявлении нарушений в процессе обработки и хранения персональных данных граждане ЕС могут обратиться в национальные регуляторные органы для расследования. Согласие на обработку персональных данных должно быть выражено в форме утверждения и активных действий пользователя, а не по умолчанию или с уже поставленной галочкой. В GDPR введено новое право на переносимость данных – портабилити (right to data portability): по требованию субъекта данные компании обязаны предоставлять бесплатно электронную копию персональных данных для другой, выбранной пользователем компании, хотя на практике этим пока зачастую трудно воспользоваться из-за технических различий между информационными системами и отсутствия функционала для этого.

В целом же, хотя новые требования к обработке данных в GDPR очень жёсткие, все заинтересованные стороны – регуляторы, бизнес, пользователи – согласны в том, что европейский Регламент задаёт новый вектор развития цифрового общества. Правда, подготовиться к выполнению требований Регламента было не так просто не только для мелкого и среднего бизнеса, но и для гораздо более крупных компаний, которым пришлось потратить значительные суммы на приведение своих рабочих процессов, интерфейсов продуктов и политик конфиденциальности в соответствие с требованиями GDPR. Приложенные усилия не смягчили европейских регуляторов, которые, получив в руки новый законодательный инструмент, продолжили стратегию “укрощения строптивых”. Речь идёт о борьбе с нарушениями при использовании персональных данных, которые допускают ИТ-гиганты на рынке и ЕС и обрабатывают данные европейских пользователей. Политики Европейского союза, представители регулирующих органов зарабатывают немалый репутационный, карьерный и политический капитал на обличении крупных технологических компаний.

Для крупного, прежде всего для американского ИТ-бизнеса, европейский рынок – это 500 млн человек с высоким уровнем использования интернет-услуг (79,3% по состоянию на 2015 г.) и высокой покупательной способностью. Соответственно, большая часть нарушений в области защиты персональных данных приходится именно на долю американских ТНК. Например, европейские регуляторы высказывают много претензий к Google, который контролирует более 90 % рынка интернет-поиска в Европейской экономической зоне [Курбалайя, 2018: 351]. В США в последние годы вскрывается всё больше нарушений при обращении с персональными данными пользователей.

После того как вере в демократические основы избирательного процесса был нанесён значительный ущерб, во-многом, за счёт использования в предвыборных кампаниях Х. Клинтон и Д. Трампа информационных сервисов Google и Facebook [Роговский, 2017: 56], последовали расследования, вынесение огромных штрафов, обличающие публикации, выступления законодателей, политиков, медиа-активистов и представителей правоохранительных органов против IT-гигантов. Так, Facebook был оштрафован Федеральной торговой комиссией США на 5 млрд долл. за скандал с компанией Cambridge Analytica, которой был предоставлен несанкционированный доступ к данным 87 млн пользователей, не дававших согласия на их использование в подобных целях.

Европейские пользователи всё активнее используют свои новые права по контролю за обработкой персональных данных. Так, по данным на февраль 2019 г. Европейского совета по защите данных (European Data Protection Board) за 2018 – начало 2019 гг. около половины дел о нарушении безопасности персональных данных (94 622) были возбуждены европейскими регуляторными органами на основании жалоб граждан о нарушении их прав как потребителей и субъектов персональных данных и их утечки. Вдвое – с 21 до 41 тыс. – увеличилось количество обращений граждан, зарегистрированных британским регулятором¹.

Каких же успехов удалось добиться европейским регуляторам с помощью штрафных санкций за время, прошедшее с момента вступления в силу GDPR в 2018–2019 гг.?

На первом этапе в 2018 г., согласно отчёту Европейского совета по защите данных, штрафы были невысокими, хотя летом 2019 г. произошла крупная утечка персональных данных клиентов на сайте британской компании British Airways. Только через год британский регулятор – Управление комиссара по информации (Information Commissioner's Office, ICO) – направил извещение о штрафе в 183 млн ф. ст. (примерно 230 млн долл.), что составляет, согласно правилам GDPR, 1,5% от её глобального оборота за 2017 г.

Общая сумма взысканий в 2018–2019 гг. составила почти 56 млн евро, возбуждено около 206 тыс. дел о нарушении безопасности персональных данных. Ещё 64

¹ First overview on the implementation of the GDPR and the roles and means of the national supervisory authorities (2017), *European Parliament*, available at: www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2019/02-25/9_EDPB_report_EN.pdf (дата обращения: 10.08. 2019).

864 дела открыли по уведомлению об утечке данных от компаний-виновников¹. Самый крупный штраф из общей суммы взысканий – в 50 млн евро – за непрозрачность, недостаточное информирование пользователей, а также отсутствие адекватной формы для получения согласия пользователей на персонализацию рекламы по отношению к другим целям обработки данных был вынесен компании Google в январе 2019 г. французским регулятором – Национальной комиссией по защите данных CNIL. Против Microsoft были выдвинуты обвинения в нарушениях при хранении данных пользователей и получении их согласия на обработку. Осенью 2019 г. комиссар по защите персональных данных Хелен Диксон заявила о расследованиях в отношении 17 технологических ТНК, среди которых и такие американские гиганты как WhatsApp, Google, LinkedIn, Instagram and Twitter².

Facebook постарался подготовиться к исполнению новых требований общеевропейского законодательства, перестроив свои технологические процессы обработки персональных данных пользователей и внося изменения в политику конфиденциальности и интерфейс. Однако этой компании грозит штраф в 4 млрд долл. со стороны ирландской Комиссии по защите данных. В сентябре 2018 г. от взлома сети пострадали 50 млн пользователей Facebook, 5 млн из которых оказались гражданами ЕС.

Можно привести примеры и меньших штрафов в отношении менее крупных компаний. Так, осенью 2018 г. регуляторный орган немецкого региона Баден – Вюртемберг (LfDI) вынес первый штраф в размере 20 тыс. евро согласно требованиям GDPR чат-приложению для знакомств Knuddels, где логины и пароли клиентов хранились в незашифрованном виде. Португальская комиссия по защите данных (CNPd) в сентябре 2018 г. наложила штраф в 300-400 тыс. евро за уязвимость в системе хранения персональных данных пациентов на португальскую больницу Barreiro Hospital. Небольшое кафе в Австрии оштрафовали на 5280 евро за незаконное видеонаблюдение³.

Из-за сложностей выполнения всех требований GDPR ряд компаний вынуждены были закрыться, например, ряд сервисов онлайн-игр, биржи, которые занимались размещением рекламы по технологии программатик, сервис проверки биографических данных PICOPS (своеобразное цифровое удостоверение личности), приложение CoinTouch (связывало друзей для обмена криптовалютой) и др. С 2019 г. количество штрафов и их размер увеличиваются. Готовятся новые штрафные санкции и против крупных американских компаний. Многие из последних выбрали тактику отказа от европейского трафика, чтобы не нарушить GDPR и не получить де-

¹ First overview on the implementation of the GDPR and the roles and means of the national supervisory authorities (2017), *European Parliament*, available at: www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2019/02-25/9_EDPB_report_EN.pdf (дата обращения: 10.08. 2019)

² Lynch S. Data protection commissioner opens investigations into 17 tech multinationals // *The Irish Times*. 2019. May 2, available at: <https://www.irishtimes.com/business/health-pharma/data-protection-commissioner-opens-investigations-into-17-tech-multinationals-1.3877850> (дата обращения: 15.12. 2019).

³ 56 миллионов евро штрафов – итоги года с GDPR // *Навр*. 2019. 23 марта. URL: <https://habr.com/ru/company/it-grad/blog/444968> (дата обращения: 10.08. 2019).

нежных взысканий. Не стоит забывать, что после того, как штраф по итогам проверки или жалобы, вынесен регулятором, компания-оператор имеет право на его обжалование и может добиться значительного снижения суммы выплаты.

Оценивая эффективность штрафов по GDPR, важно учитывать не только статистические показатели, но и конкретные примеры, которые показывают, насколько тщательно европейские регуляторы оценивают исполнение норм нового закона. Например, самый крупный штраф в Венгрии был вынесен организаторам SZIGET и VOLT фестивалей за упущения в организации безопасности его участников. Регулятор счёл, что для использования ручных браслетов с чипами для идентификации при проходе на территорию фестиваля, было выбрано неверное правовое основание. Другой пример – руководство одной из шведских школ было оштрафовано за то, что согласие студентов на использование технологии распознавания лиц для учёта посещаемости было дано не в свободной форме¹. В этой связи небезынтересно сравнить этот подход с некоторыми российскими примерами.

В частности, осенью 2019 г. общественный деятель Алена Попова подала в Савеловский суд г. Москвы иск к столичной полиции, а также Департаменту информационных технологий Москвы (ДИЦ) о признании незаконным использования технологий распознавания лиц в городской системе видеонаблюдения. В иске Поповой утверждалось, что использование камер без согласия гражданина противоречит Конституции РФ и закону “О защите персональных данных” и не регулируется действующим законодательством. В октябре 2019 г. суд, однако, отказался признать использование этих технологий незаконным². В конце 2019 г. Рособннадзор объявил о планах использовать в 2020 г. систему распознавания лиц во время проведения Единого государственного экзамена (ЕГЭ) для идентификации учащихся, предотвращения подмены личности и минимизации бюджетных расходов в регионах. Правда, эксперты уже поставили вопрос о правовой экспертизе этих планов. Было бы полезно учитывать опыт ЕС при правовом решении всех возможных коллизий с персональными данными учащихся³.

Что касается европейского регулирования использования файлов cookie, которые согласно GDPR приобретают статус персональных данных, поскольку могут быть использованы для создания информационного профиля пользователя и его идентификации, то в 2019 г. вступил в силу новый законопроект по электронной конфиденциальности – ePrivacy Regulation, который должен ужесточить правила работы с cookies и получения согласия на их обработку, причём штрафы за несоблюдение требований составляют от двух до четырёх процентов годового дохода

¹ Боровикова К. GDPR в цифрах: обзор по штрафам и утечкам // X Международная конференция “Защита персональных данных”. 2019. 7 ноября. URL: <https://zpd-forum.com/> (дата обращения: 15.12.2019).

² Корня А. Москвичка просит суд запретить распознавание лиц городской системой видеонаблюдения // “Ведомости”. 2019. 6 октября. URL: <https://www.vedomosti.ru/politics/articles/2019/10/06/812955-moskvichka-prosit-sud> (дата обращения: 11.12.2019).

³ Рособннадзор анонсировал внедрение нейросетей на ЕГЭ //РБК. 2019. 25 декабря. URL: <https://www.rbc.ru/society/25/12/2019/5e0371569a7947829c5a3f01> (дата обращения: 15.12.2019).

компаний-виновницы или десять миллионов евро. Законе регулирует и передачу данных между устройствами Интернета вещей¹.

Международное влияние GDPR

С момента вступления в силу GDPR доказал свою эффективность как регулятивный инструмент для защиты персональных данных, основанный на крупных штрафах. Эксперты единогласно признают значение Регламента как комплексного, системного законодательного эталона в нынешней ситуации, на который равняется законодательство многих стран. Появление этого нормативного акта говорит о твёрдой решимости европейских законодателей и регуляторов продолжать нынешний жёсткий курс “конфиденциальности по умолчанию”, когда необходимые технические и организационные меры должны быть приняты заблаговременно всеми лицами, обрабатывающими данные пользователей. Принципы и нормы GDPR получили преломление во многих национальных правовых системах. Прежде всего это касается таких стран как США, Канада Китай, Индия, Сингапур, Аргентина, Бразилия и Австралия.

В этой связи примечательно, с какой оперативностью отреагировали на появление GDPR два глобальных конкурента с развитыми цифровыми экономиками – Вашингтон и Пекин.

Ряд принципов GDPR, в частности, штрафные санкции как средство регулирования защиты персональных данных, отражены в недавно принятом в Калифорнии (США) законе “О защите данных интернет-пользователей” (California Consumer Privacy Act) (2018 г.), вступившем в силу в 2020 г. Согласно калифорнийскому закону, пользователи получили право запрашивать у компаний, какие именно персональные данные о них были собраны, как и почему они используются, список третьих лиц, которым эта информация стала известна, цели сбора персональных данных и их источники. Пользователь может потребовать удалить информацию о себе с серверов компании и третьих лиц и запретить им продажу этой информации, имеет право запрашивать денежную компенсацию и подать иск в суд на организацию, которая неправомерно воспользовалась его персональными данными, допустила утечку информации или не выполнила какой-либо из его запросов в срок². Он может получить до 750 долл. компенсации, а на компанию может быть наложен штраф до 7,5 тыс. долл. за нарушения при обработке персональных данных.

В то время как GDPR защищает права очень широкого круга физических лиц на территории ЕС на основании прямого согласия пользователей на обработку персональных данных, CCPA направлен на защиту прав граждан Калифорнии, и распространяется только на компании, соответствующие ряду критериев, среди которых:

¹ Интернет вещей – концепция вычислительной сети физических предметов (“вещей”), оснащённых встроенными технологиями для взаимодействия друг с другом или с внешней средой. The new EU ePrivacy Regulation: what you need to know, [Online], available at: <https://www.i-scoop.eu/gdpr/eu-eprivacy-regulation/> (дата обращения: 10.08. 2019).

² AB-375 Privacy: personal information: businesses (2017–2018) (2018), *California Legislative Information*, available at: http://leginfo.legislature.ca.gov/faces/billCompareClient.xhtml?bill_id=201720180AB375 (дата обращения: 10.08. 2019).

годовой оборот более 25 млн долл., обработка данных более чем 50 тыс. клиентов, устройств или домохозяйств, а также более половины дохода от продажи персональных данных. При этом компании не обязаны раскрывать какие-либо факты нарушения без соответствующего запроса граждан.

В целом же, в отличие от GDPR, ССРА прежде всего предусматривает практическое выполнение компаниями ряда функций, среди которых вывешивание на сайте политики конфиденциальности и предоставление пользователям опции запрета передачи данных другим лицам за вознаграждение.

GDPR повлиял и на новый китайский государственный стандарт защиты персональных данных, принятый в 2018 г., который, в частности, содержит положения, нацеленные на повышение контроля пользователей над своей персональной информацией¹. Китайские эксперты, однако, предупреждают, что копирование европейских регулятивных норм невозможно в условиях развитой цифровой экономики КНР² [Cao Yin, 2019b]. Аналитики из других стран в свою очередь не устают напоминать об отличном от западного понимании прав человека в китайском обществе, отсутствии в законодательстве Китая ряда важных фундаментальных кодифицированных правовых документов, что предопределяет особенности юридической практики в этой стране [Трощинский, 2018: 110]. Национальные регуляторы в Китае с января 2019 г. начали проверять, как работают с персональными данными пользователей популярные приложения для смартфонов, сервисы доставки еды, такси и навигаторов³ [Cao Yin, 2019a].

Гармонизирован с европейским регламентом и индийский закон о защите персональных Personal Data Protection Bill (2018 г.). Во многом, это связано с потребностью регулирования глобальных аутсорсинговых IT-услуг. Согласно индийскому закону, пользователи имеют аналогичные GDPR права, а штрафы за несоблюдение его требований так же высоки, как и в европейском регламенте, например, операторам персональных данных за нарушения грозит взыскание до 2 млн долларов (или 4% от годового оборота)⁴. Особое внимание уделено здесь локализации персональных данных, по крайней мере, одна служебная копия которых должна храниться на сервере или в центре обработки данных, расположенном в Индии.

Европейский опыт крупных штрафов и ряд других положений законодательства ЕС по обработке персональных данных, выполнение требований максимальной

¹ Есть вещи посильнее GDPR. Китайский закон о конфиденциальности // Computerworld. 2018. 26 июня. URL: <https://www.computerworld.ru/articles/Est-veschi-posilnee-GDPR-Kitayskiy-zakon-o-konfidentsialnosti> (дата обращения: 26.07.2019).

² Cao Yin (2019b) Lawmakers, political advisers focus on personal data protection, *China Daily Global* [Electronic], available at: <http://global.chinadaily.com.cn/a/201903/20/WS5c9187e4a3104842260b1788.html> (дата обращения: 10.08.2019).

³ Cao Yin (2019a) Illegal data collection by apps targeted, *China Daily Global* [Electronic], available at: <http://www.chinadaily.com.cn/a/201901/26/WS5c4ba316a3106c65c34e69ea.html> (дата обращения: 11.08.2019).

⁴ В Индии представлен новый законопроект о защите ПД — ещё один аналог GDPR? // Habr. 2018. 5 августа. URL: <https://habr.com/ru/company/it-grad/blog/419257/> (дата обращения: 20.08.2019).

прозрачности процессов обработки данных, организация надзорной деятельности и перестройка компаниями бизнес-процессов вызывают большой интерес и в РФ, где штрафы могли бы заменить блокировки сайтов. Российские компании также подпадают под компетенцию деятельности GDPR. На основе диалога бизнеса и государства в нашей стране готовятся новые правовые решения в этой области, разработка отраслевых кодексов, стандартов и административных мер для обеспечения защиты прав граждан и безопасности их данных.

Безусловно, крупные штрафы были бы разорительны и для отечественного бизнеса, и для государственных органов. В то же время недавно был опубликован законопроект, который предусматривает введение достаточно небольшого на фоне сумм взысканий в ЕС и США административного штрафа в 18 млн рублей за нарушение новых правил обработки персональных данных.

Перед российскими компаниями возникает вопрос, переходить ли им на единый интерфейс для регулирования работы с персональными данными или дифференцировать различные потоки данных в соответствии с требованиями конкретных национальных законодательств.

Оценивая эффективность и влияние GDPR на мировое законодательство, эксперты считают, что цели и технологии современной экономики, основанной на Больших данных, несовместимы с принципами, лежащими в основе современного законодательства о персональных данных: соответствие целей обработки персональных данных целям, заранее определённым и заявленным при их сборе, ограничение объёма собираемых и обрабатываемых данных минимально необходимым объёмом, обработка данных на основе информированного согласия, не говоря уже о возможностях деобезличивания даже обезличенных индустриальных данных. Соответственно, ряд законодательных требований на практике трудноисполнимы, например, требование объяснить пользователю, как именно алгоритмически обрабатываются его персональные данные. Ведь даже сам создатель алгоритма, интеллектуальной системы не имеет возможности заглянуть внутрь “чёрного ящика” [Савельев, 2015: 62].

Как дальше будет эволюционировать “право эпохи калькуляторов” в эпоху компьютеров, остаётся дискуссионным. Попытка посредством крупных денежных санкций поставить барьер нарушениям при обработке персональных данных вряд ли сможет решить все проблемы технологического развития. Сегодня, безусловно, можно констатировать тенденцию гармонизации мировых стандартов регулирования технологий обработки данных в законодательстве по защите персональных данных. При этом третьи страны не просто копируют нормы GDPR в своих национальных законодательствах, а, скорее, идут в едином фарватере увеличения штрафных санкций. В свою очередь мировой IT-бизнес всё больше осознаёт, что в нынешних условиях конкурентоспособность компаний неразрывно связана с их клиентоориентированностью как частью стратегии трансформации процессов обработки персональных данных.

В этом контексте современная европейская законодательная модель защиты персональных данных вызывает всеобщий интерес и продолжает оказывать решающее влияние на глобальную практику распространения информации и национальные правовые модели других стран.

Список литературы

- Дмитрик Н.А. (2018) Пределы правового регулирования в цифровую эпоху. *Информационное общество*. № 3, с. 47–58.
- Курбалийя Й. (2018) Управление Интернетом. DiploFoundation, Москва, Россия.
- Пазюк А., Соколова М. (2015) Защита персональных данных: введение в проблематику: учебное пособие. Центр правовой информации. Минск, Белоруссия.
- Роговский Е.А. (2017) Выборы в США: триумф цифровой демократии? *США: экономика, политика, культура*. № 4. с. 5–19.
- Савельев А.И. (2015) Проблемы применения законодательства о персональных данных в эпоху “больших данных” (big data). *Право*. № 1, с. 33–66.
- Трошинский П.В. (2018) Эволюция правовой системы Китайской Народной Республики (1949–2018 гг.). Историко-правовой аспект. ВКН, Москва, Россия.

References

- Dmitrik, N.A. (2018), Limits of legal regulation in the digital age, *Information society*, no.3, pp. 47–58.
- Kurbalijja, J. (2018), *Upravlenie Internetom* [Internet governance], DiploFoundation, Moscow, Russia, 391 p.
- Pazjuk, A. and Sokolova, M. (2015), *Zashhita personal'nyh dannyh: vvedenie v problematiku: uchebnoe posobie* [Protection of personal data: introduction to the subject: tutorial], Centr pravovoj informacii, Minsk, Belorussia, 116 p.
- Rogovskij E.A. (2017) US election: the triumph of digital democracy? *SSHA: ekonomika, politika, kul'tura*, no.4, pp. 5–19.
- Savel'ev, A.I. (2015), Problems of application of personal data legislation in the era of “big data”, *Pravo*, no.1, pp. 43–66.
- Troshchinskij P.V. (2018) Evolyuciya pravovoj sistemy Kitajskoj Narodnoj Respubliki (1949–2018 gg.). Istoriko-pravovoj aspekt. [Evolution of the legal system of the people's Republic of China (1949–2018 gg.). Historical and legal aspect], VKN, Moscow, Russia, 181 p.

First successes of the new pan-European General Data Protection Regulation

Author: Sokolova M., Candidate of Sciences (Filosofy), Senior Researcher, Department of military-political research, Institute for US and Canadian Studies, Russian Academy of Sciences. The Russian Institute for Advanced Study (RIAS), Moscow Pedagogical State University. **Address:** 2/3, Khlebnyy per., Moscow, Russia, 121069. **E-mail:** mariamva@yandex.ru

Abstract. The article explores the importance of the new pan-European General Data Protection Regulation (GDPR) (effective May 23, 2018) for regulation of personal data protection in the EU. Large fines for violation of personal data envisaged, the rights of users to control their personal data (including the data deletion, i.e. “a right to be forgotten”), correction and portability have made GDPR an effective legislative tool for European regulators. The immediate results of the impact of GDPR penalties on the change of privacy policy among companies working with data of Europeans, especially American TNCs, for 2018–2019 are presented. It is shown how the legal norms, laid down in the Regulation influenced the emergence of similar legislation in third countries such as the California law California Consumer Privacy Act (CCPA) (2018). In this context the modern European legislative model for the protection of personal data has a general interest and continues to have a decisive influence on the global practice of disseminating information and on the national legal models of other countries.

Keywords: personal data, personal data protection, fines, information economy, General Data Protection Regulation, personal data.

DOI: <http://dx.doi.org/10.15211/soveurope220205666>