

# ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ БЕЗ СОГЛАСИЯ СУБЪЕКТА:

## ПРАКТИКА ОБЕСПЕЧЕНИЯ НАРУШЕННЫХ ПРАВ (НА ПРИМЕРЕ КАЗАХСТАНА И ВЕЛИКОБРИТАНИИ)

Статья посвящена исследованию проблемных аспектов, возникающих при обработке персональных данных гражданина без его согласия, а также защите прав такого индивида, если обработка все-таки являлась незаконной. Проанализированы правовые положения о системе защиты персональных данных в Республике Казахстан и Великобритании. Проведенный анализ дает основания полагать, что граждане Великобритании сегодня обладают более широким набором инструментов и способов, которыми они могут обеспечить свое право на защиту персональных данных. Представлены рекомендации по развитию института защиты данных в Республике Казахстан.

*Ключевые слова: персональные данные, частная жизнь, неприкосновенность, нарушение прав, права человека, Республика Казахстан, Великобритания, Европейский Союз, международное право, защита прав человека.*

### ВВЕДЕНИЕ

Сегодня в Республике Казахстан защита персональных данных приобретает особое значение. Это положение определяется тем, что с одной стороны, в Республике прилагаются усилия по созданию законодательства в данной сфере, однако существующий уровень все-таки недостаточен. Большинство процессов формализовано, общество недостаточно информировано о своих правах и возможностях защиты данных. Кроме того, большой проблемой являются исключения из норм о защите персональных данных, когда такая информация может раскрываться и обрабатываться без согласия субъекта данных.

Настоящая статья посвящена исследованию пределов ограничения права на защиту данных, а также способам защиты нарушенного права. Для сравнения рассмотрен опыт Великобритании, в которой вопросы защиты прав человека реализуются на уровне законодательства еще с 1984 года. Будут рассмотрены понятия обработки персональных данных и «согласие» на обработку персональных данных, критерии «согласия», а также основания, когда данные могут быть обработаны (собраны, проанализированы или даже раскрыты) без такового согласия. Важнейшим и завершающим разделом станет анализ инструментов эффективной защиты рассматриваемого права граждан на национальном и международном уровне как в Республике Казахстан, так и в Великобритании.



О. В. ЛОЗОВАЯ,  
старший преподаватель кафедры международного права  
Университета КАЗГЮУ, докторант Ph.D

### ПОНЯТИЕ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Обработка персональных данных понимается по-разному как в сфере нормотворчества разных государств, так и в научных работах ученых. Для примера в Директиве 95/46/ЕС Европейского парламента и Совета Европейского Союза от 24 октября 1995 г. о защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных (*далее – Директива*) указано: обработка означает любую операцию или набор операций, выполняемых над персональными данными, как автоматическими средствами, так и без таковых, такие как сбор, запись, организация, хранение, актуализация или изменение, извлечение, консультирование, использование, раскрытие посредством передачи, распространения или предоставления иного доступа, группировка, блокирование, стирание или разрушение. Закон Республики Казахстан «О персональных данных и их защите» (*далее – Закон*) дает не столь расширенное толкование понятия «обработки персональных данных»: обработка персональных данных – действия, направленные на накопление, хранение, изменение, дополнение, использование, распространение, обезличивание, блокирование и уничтожение персональных данных. Однако, в указанной статье Закона также рассмотрены понятия «блокирование», «накопление», «сбор», «уничтожение» и «обезличивание». С одной стороны, подробное раскрытие каждого действия, которое понимается как «обработка» является необходимым и весьма удачным в законодательстве Республики Казахстан. Однако, считаем не вполне рациональным наличие закрытого списка таких действий. В данном ключе удачнее рассматривать это понятие с европейской точки зрения, где принципиальную роль играет определение «любое действие». Естественно, список действий не может быть ограниченным, с каждым днем количество субъектов, способных в какой-либо мере обрабатывать персональные данные систематически растет.

Такого же мнения придерживается профессор Туринского Университета Уго Пагалло, который утверждает, что «сегодня обработка ведется не только крупными акторами, но и небольшими сетевыми приложениями, облачными хранилищами и тому подобными программами».<sup>1</sup>

Таким образом, стоит принять общую формулировку, что «обра-

ботка персональных данных» представляет собой любую операцию, которая совершается с персональными данными, начиная с момента их сбора и до момента уничтожения.

### ПОНЯТИЕ СОГЛАСИЯ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ И СПОСОБЫ ЕГО ВЫРАЖЕНИЯ

Что касается определения, что же такое «согласие» на обработку персональных данных и каким образом оно получается, то следует отметить глубокий интерес к данному понятию со стороны научного сообщества.

По общему правилу лицо вправе давать или не давать согласие на обработку своих персональных данных тому или иному оператору. Субъект персональных данных имеет также право свое согласие отозвать.<sup>2</sup> Следовательно, наличие согласия является краеугольным камнем в определении легитимности работы с персональными данными в принципе.

В Законе Республики Казахстан нет определения понятия согласия на сбор и обработку персональных данных, однако удачно разработана статья, касающаяся предоставления и отзыва согласия на обработку данных. В частности, установлено, что субъект дает или отзывает свое согласие в письменной форме или путем подачи электронного документа. Позднее в статью 8 Закона был добавлен пункт о том, что дача согласия в портале электронного правительства также возможна через sms-подтверждение.<sup>3</sup>

Менее удачной является формулировка в Директиве 95/46/ЕС: «согласие субъекта данных» означает любое свободно данное конкретное и сознательное указание о своей воле, которым субъект данных оповещает о своем согласии на обработку касающихся его персональных данных.<sup>4</sup> Из указанного определения следует, что согласие может быть устным. Думается, что такое положение не является идеальным. Получение устного согласия достаточно сложно доказать или опровергнуть в случае возникновения спора. Кроме того, насколько контролер, работающий с данными, может быть уверен в действительном понимании субъектом данных всех рисков процесса обработки его данных? В случае же письменного или иного защищенного согласия субъект берет на себя ответственность за полноценное осознание тех пунктов об обработке его персональных данных, которые указаны в подписываемом документе.

Эдгар Уитли утверждает, что основной характеристикой согласия является информированность, иначе можно утверждать, что согласие не имеет смысла, так как индивид не достаточно осведомлен о том, на что такое согласие дается. Таким образом еще раз подтверждается тезис о том, что письменное согласие может быть наиболее эффективным, так как в таком случае можно точно утверждать, была ли информированность достаточной для утверждения, что субъект понимает предупреждения обо всех манипуляциях с информацией о нем.<sup>5</sup>

<sup>2</sup>Петрыкина Н.И. Правовое регулирование оборота персональных данных. Теория и практика. М.: «Статус», 2011. С. 28.

<sup>3</sup>Ст. 8, п. 1 Закона Республики Казахстан от 21 мая 2013 года № 94-V «О персональных данных и их защите». [http://online.zakon.kz/Document/?doc\\_id=31396226#pos=134;-231](http://online.zakon.kz/Document/?doc_id=31396226#pos=134;-231) (03.10.2016 г.).

<sup>4</sup>Ст. 2, п. h Директивы 95/46/ЕС Европейского парламента и Совета Европейского Союза от 24 октября 1995 года о защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных. <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3A114012> (03.10.2016 г.).

<sup>5</sup>Whitley E.A. Informational privacy, consent and the “control” of personal data // Computer law & Security Review, №14, 2009. P. 157.

Если обратиться к практике Российской Федерации, то стоит обратить внимание на мнение видного ученого в сфере защиты персональных данных Д.А. Скрипника, который утверждает, что «оператор персональных данных обязан предоставить доказательство получения согласия субъекта персональных данных на обработку его персональных данных, а в случае обработки общедоступных персональных данных на него возлагается обязанность доказать, что обрабатываемые персональные данные являются общедоступными».<sup>6</sup> Данный тезис является еще одним доказательством того, что письменное согласие на обработку данных является более эффективным инструментом в данных правоотношениях.

Для еще более надежной защиты права субъекта данных на безопасность их обработки, стоит обратить внимание на практику Испании. Данное государство не только исполняет общие минимальные европейские требования по защите данных, но и усиливает их положения. Например, важно, что если процедура получения согласия субъекта данных соблюдена, контроллер данных, тем не менее, не может использовать их снова для подобной обработки и для тех же целей, если с момента получения согласия прошло более одного года.<sup>7</sup> Видится логичным включение подобной нормы в законодательство государств, которые стремятся совершенствовать свою систему защиты прав человека в рассматриваемом секторе.

Таким образом, можно сделать следующие выводы:

- согласие субъекта персональных данных – это волеизъявление субъекта в письменной форме, которым субъект данных выражает разрешение на обработку его персональных данных;
- письменная форма согласия является единственно верной и эффективной в целях обеспечения информированности субъекта, а также возможности удостовериться в том, что согласие было действительно получено контролером;
- субъект данных имеет право как давать, так и не давать или отзывать свое согласие на обработку персональных данных. Данные, согласие на обработку которых не получено или отозвано, не могут подлежать обработке по общему правилу.

### ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ БЕЗ СОГЛАСИЯ СУБЪЕКТА

Сфера защиты персональных данных, как и любая другая, имеет ряд исключений. Ограничение права на защиту персональных данных может происходить по ряду причин, которые будут более подробно рассмотрены ниже. Однако уже сейчас стоит отметить, что многие основания для ограничения этого права носят достаточно широкий или оценочный характер. Ущемление этого права происходит параллельно с обеспечением какого-либо другого права зачастую другого субъекта. Таким образом, всегда возникает правовая коллизия, которая должна в итоге разрешаться правоприменителем или судом в случае возникновения спора.

Юридическим основанием для такого ограничения должен быть реальный конфликт частного интереса сохранения тайны неприкосновенности частной жизни и более значимых публичных интересов государственной безопасности, общественной безопасности (общественного спокойствия), экономической безопасности госу-

<sup>6</sup>Скрипник Д.А. Обеспечение безопасности персональных данных. Курс лекций. С. 14. <http://www.twirpx.com/file/637521/> (03.10.2016 г.).

<sup>7</sup>Vilasau M. Legal grounds to process personal data under Spanish legislation after the ECJ Judgment of 24 November 2011 (the ASNEF and FECEMD case) // Computer law & Security Review, № 28, 2012. С. 42.

дарства (экономического благосостояния страны), предотвращения беспорядков, предотвращения преступлений, охраны здоровья или нравственности, защиты прав и свобод других лиц.<sup>8</sup> Таким образом, задачей законодателя должно было стать формирование единого подхода к отграничению того круга правовых отношений, защита которых стояла бы выше защиты персональных данных.

Вместе с тем «применять исключения необходимо с «должной степенью осмотительности», так как на оператора возлагается обязанность доказывания того, что обрабатываемые персональные данные являются общедоступными».<sup>9</sup>

Стоит обратиться к тем основным основаниям обработки данных без согласия субъекта, которые вызывают сомнения при их применении.

**Обработка персональных данных без согласия субъекта в случаях осуществления деятельности правоохранительных органов и судов.**<sup>10</sup>

Данное положение по очередности поставлено законодателем на первое место и это неслучайно. В международной практике существует ряд прецедентов, когда в обеспечение справедливого и полного судебного разбирательства раскрывались персональные данные.

Для наглядного рассмотрения такого положения мы обратились к практике Европейского Суда по правам человека, который неоднократно сталкивался с подобной проблемой. Стоит рассмотреть дело *К.Ю. против Финляндии* (Постановление от 2 декабря 2008 г.).<sup>11</sup>

В 1999 г. неизвестное лицо поместило объявление сексуального характера на сайте знакомств в Интернете от имени заявителя, которому было двенадцать лет, и без его ведома. Объявление содержало информацию о возрасте, годе рождения и физических характеристиках заявителя и указывало, что он искал интимных отношений с женщиной. Оно также включало ссылку на страницу в Интернете, где можно было найти его фотографию и номер телефона. Заявитель узнал об объявлении, когда получил сообщение по электронной почте от мужчины, предлагавшего ему встретиться. Была подана жалоба в полицию, но поставщик услуг отказался раскрыть личность поместившего объявление человека, поскольку считал себя обязанным соблюдать правила о конфиденциальности.

<sup>8</sup>Лоскутов И.Ю. Альтернативный Национальный план действий в области прав человека в Республике Казахстанна 2015-2020 гг. Раздел 8: Право на частную жизнь и защиту персональных данных. <http://www.zakon.kz/4685815-pravona-chastnuju-zhizn-i-zashhitu.html> (14.09.2016 г.).

<sup>9</sup>Баймакова И., Новиков А., Рогачев А., Хыдыров А. Обеспечение защиты персональных данных. Методическое пособие. 3-е изд. М.: ООО «1С-Пабблишинг». С. 88.

<sup>10</sup>П. 1, ст. 9 Закона Республики Казахстан от 21 мая 2013 года № 94-V «О персональных данных и их защите»

<sup>11</sup>Решение Европейского Суда по правам человека. <http://hudoc.echr.coe.int/eng/?i=001-89964#i=001-89964> (03.09.2016 г.).

Европейский Суд считал необходимым подчеркнуть воздействие на частную жизнь заявителя, учитывая потенциальную угрозу физическому и душевному благополучию заявителя и его беззащитный возраст. Таким образом, государство не выполнило обязательств по защите неприкосновенности частной жизни заявителя путем признания приоритета требования о конфиденциальности над физическим и душевным состоянием заявителя.

Невозможно представить мотивы логики, нравственности или права, которыми мог руководствоваться контролер данных в этом случае. При столкновении столь значимого личного интереса субъекта данных, учитывая его особую незащищенность как несовершеннолетнего лица, контролер должен был предпринять все возможные усилия по установлению, являются ли эти данные законными. Кроме того, при возникновении коллизии прав разных субъектов не стоит радикально или однобоко рассматривать приоритет одного из субъектов.

**Обработка персональных данных без согласия субъекта в случаях осуществления государственной статистической деятельности и в случаях использования государственными органами персональных данных для статистических целей с обязательным условием их обезличивания.**<sup>12</sup>

На наш взгляд вопросы статистики также особенно щепетильны. Например, возникает серьезный вопрос относительно национальности. Статистические данные о национальном составе государства чрезвычайно важны, на основании этого у государства появляется возможность наиболее эффективно защищать права представителей всех национальностей. Однако, как широко известно, в Республике Казахстан сегодня граждане не обязаны сообщать свою национальность включая этапы оформления паспорта и других документов. Таким образом, почему тот же гражданин должен сообщать свою национальность для целей статистики? С другой стороны, статистика, собранная с исключениями, будет отражать данные, не соответствующие реальности. На наш взгляд в данном контексте законодатель должен четко определить, каких именно данных касаются указанные вопросы статистики. Представляется, что при условии обеспечения полной анонимности, данные о национальности, все-таки, могут собираться и обрабатываться.

**Обработка персональных данных без согласия субъекта в случаях защиты конституционных прав и свобод человека и гражданина, если получение согласия субъекта или его законного представителя невозможно.**<sup>13</sup>

<sup>12</sup>Пп. 2, 3 ст. 9 Закона Республики Казахстан от 21 мая 2013 года № 94-V «О персональных данных и их защите».

<sup>13</sup>П. 10, ст. 9 Закона Республики Казахстан от 21 мая 2013 года № 94-V «О персональных данных и их защите».





Ярким примером для подобной обработки данных может быть случай, когда лицо поступает в медицинское учреждение, находясь в бессознательном состоянии. В таком случае, персонал может обратиться к документам, которые при нем имеются, для получения сведений о его личности, физическом состоянии, каких-либо специфических медицинских показаниях и т.д. В таком случае действия медицинских работников не будут являться нарушением прав на сохранность персональных данных, так как реализуется конституционное право человека на жизнь.<sup>14</sup>

Однако пример с медицинской также не универсален. Например, в практике Великобритании рассмотрено дело *Сулук против Соединенного Королевства* (Постановление от 2 июня 2009 г.).<sup>15</sup> Заявитель перенес мозговое кровоизлияние, после чего попал в тюрьму на длительный срок. Во время пребывания в тюрьме он вел переписку с лечащим врачом, которая систематически вскрывалась и изучалась охраной с целью контроля за его физическим состоянием. Европейский Суд по правам человека постановил, что такое чтение может препятствовать получению адекватной медицинской помощи и серьезно вмешивается в личную жизнь заявителя.

**Обработка персональных данных без согласия субъекта в случаях осуществления законной профессиональной деятельности журналиста и (или) деятельности средства массовой информации либо научной, литературной или иной творческой деятельности при условии соблюдения требований законодательства Республики Казахстан по обеспечению прав и свобод человека и гражданина.**<sup>16</sup>

Развитие института свободы слова и право на получение информации создают такую обстановку, что удовлетворение публичного интереса приобретает все больший вес в современном обществе.

Широко известно дело *Фон Ганновер против Германии*.<sup>17</sup> Данное дело представляет собой многолетний спор в отношении заявления старшей дочери князя Монако Ренья III. В частности, она обвиняла газеты Германии в том, что они без получения ее согласия публикуют фотографии, где изображены картины ее частной жизни. По данному делу суд провел экспертизу каждого фото в отдельности, определяя, является ли обстановка на них частью частной жизни, или они представляют публичную ее сторону и могут быть доступны общественности. В итоге некоторые из фотографий были признаны незаконно опубликованными, а некоторые признаны публикацией в обеспечении публичного интереса.

Несмотря на то, что практика Европейского суда по правам человека непосредственно не применима в Республике Казахстан, однако ее можно исследовать как пример эффективно работающих норм в сфере защиты персональных данных. Таким образом, видно, что осуществление деятельности СМИ не всегда может быть основанием для сбора и тем более обработки (в виде публикации) персональных данных без согласия субъекта этих данных. С другой стороны, четкие критерии для разграничения выработать невозможно, поэтому считаем, что формулировка, выработанная законодателем Республики Казахстан, достаточно успешно обобщает положение о том, что такая обра-

ботка без согласия не должна идти в разрез с «требованиями законодательства Республики Казахстан по обеспечению прав и свобод человека и гражданина». Таким образом, баланс будет обеспечиваться на практике или, при возникновении спора, судом.

В целом, исходя из исследованного раздела, можно сделать следующие выводы:

- персональные данные могут собираться и обрабатываться без согласия субъекта данных;
- основания для подобной обработки должны быть четко отражены в законодательстве;
- споры относительно приоритета при столкновении права субъекта на защиту персональных данных и другого законного права человека решает суд.

### **ЭФФЕКТИВНАЯ ПРАВОВАЯ ЗАЩИТА НАРУШЕННОГО ПРАВА НА РАБОТУ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ (НА ПРИМЕРЕ РЕСПУБЛИКИ КАЗАХСТАН И ВЕЛИКОБРИТАНИИ).**

Споры относительно защиты персональных данных в любом случае должны возникать в логично развивающемся государстве. Информированность граждан о своих правах растет, сведения о информационном контроле постоянно тиражируются СМИ. Для обеспечения защиты этого права в государстве должна существовать четкая система органов с разграниченной компетенцией.

В Законе Республики Казахстан определена работа в сфере защиты персональных данных относительно некоторых государственных органов: Правительства (в сфере разработки политики и общих направлений защиты данных), а также органов прокуратуры (в сфере надзора за исполнением соответствующего законодательства).<sup>18</sup>

Менее конкретизирован вопрос относительно рассмотрения споров или защиты нарушенного права (хотя он и является особенно принципиальным для гражданина, ведь именно в защиту его права и создан Закон). В частности относительно обращений граждан указано, что «Государственные органы в пределах своей компетенции <...> 2) рассматривают обращения физических и (или) юридических лиц по вопросам персональных данных и их защиты; 3) принимают меры по привлечению лиц, допустивших нарушения законодательства Республики Казахстан о персональных данных и их защите, к ответственности, установленной законами Республики Казахстан».<sup>19</sup>

Исходя из смысла п. 2) неясно, в какой все-таки орган стоит обращаться. Все, что известно об этом органе – это то, что такие вопросы должны входить в его компетенцию. Однако, это слишком широкое понятие, лицо, которое не близко знакомо с порядком работы государственных органов, скорее всего не сможет самостоятельно определить адресата для своего обращения. Какого-либо специализированного органа в Республике сегодня не создано.

Что касается защиты нарушенного права в суде, то здесь для граждан Республики предусмотрен тот же путь, что возникает при нарушении других прав человека: судебные органы государства до Верховного суда и, в случае дальнейшей борьбы, обращение в комитет по правам человека. Международный пакт о гражданских и политических правах 1966 года (ратифицированный Республикой Казахстан в 2005 г.) содержит положения о защите права на частную жизнь. Понятие «персональных данных» часто приравнено с категорией «частная жизнь», однако не всегда.

<sup>14</sup> Кроме того, интересным для изучения материалом может являться статья: Жаппарова А.С. Правовые аспекты биоэтики // «Право и государство», № 2 (59), 2013. С. 50-53.

<sup>15</sup> Решение Европейского Суда по правам человека. <http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-92767>. (27.09.2016 г.).

<sup>16</sup> П. 6, ст. 9 Закона Республики Казахстан от 21 мая 2013 года № 94-V «О персональных данных и их защите»

<sup>17</sup> Решение Европейского Суда по правам человека. <http://hudoc.echr.coe.int/eng?i=001-61853#i=001-61853> и <http://hudoc.echr.coe.int/eng?i=001-109029#i=001-109029>. (03.09.2016 г.).

<sup>18</sup> Ст. 28, 28 Закона Республики Казахстан от 21 мая 2013 года № 94-V «О персональных данных и их защите».

<sup>19</sup> П. 2 ст. 27 Закона Республики Казахстан от 21 мая 2013 года № 94-V «О персональных данных и их защите».

«Понятие «персональные данные» более узко, потому что оно имеет дело только с обработкой личных данных, в то время как объем частной жизни шире (он охватывает также мысли, чувства и так далее – прим. автора). Но она и шире, потому что относится и к обработке персональных данных, даже если последние не касаются частной жизни (записи о рабочем времени, банковские счета и т.д. – прим. автора).»<sup>20</sup>

Соответственно, для гражданина Казахстана может просто не оказаться эффективного инструмента защиты его права на международном уровне.

Сегодня в ООН ведутся разработки по созданию правовой базы касательно персональных данных. Однако, в отличие от таких фундаментальных прав, как право на жизнь, свободу слова и других, право на защиту персональных данных не так развито на уровне ООН.<sup>21</sup> Существует ряд разработок на уровне Генеральной Ассамблеи и Управления Верховного Комиссара по правам человека, однако, это лишь намерения, специализированного документа до сих пор нет.

Более показателен и эффективен опыт Великобритании в вопросе защиты права на обработку персональных данных. Отметим несколько важных и позитивных аспектов и правовых инструментов, которыми гражданин Великобритании может воспользоваться в случае нарушения его права.

1) Первый Закон о защите данных в Великобритании был принят в 1984 г. В 1998 г. Закон был модернизирован в соответствии с правовыми реалиями. Следовательно, уже с 1984 г. у граждан Великобритании была возможность защищать подобные права в национальных судах.

2) Великобритания является участником Конвенции о защите физических лиц при автоматизированной обработке персональных данных 1981 года (Конвенция 108). Конвенцией создается Консультативный Комитет, который в случае спорной ситуации «может выразить мнение по определенному положению договора. Логичен вывод, что данный правовой инструмент также может быть применен

в рассмотрении спора и помочь в реализации права на защиту персональных данных».<sup>22</sup>

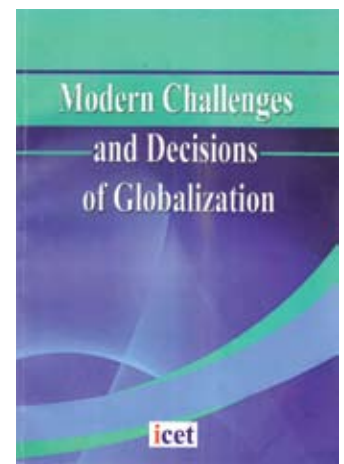
3) Великобритания, как и все европейские государства, подчиняется действию упомянутой ранее Директивы 95/46/ЕС. Как известно, Директивы имеют законодательный характер, а также указанные в них положения должны быть внедрены в национальное законодательство. Однако, стоит учесть, что даже если государство не провело соответствующие изменения в своей правовой системе, Директива тем не менее имеет силу и нарушение ее положений может быть обжаловано в Суде Европейского Союза. Таким образом, в случае нарушения права на защиту персональных данных, гражданин Великобритании с 1995 г. имеет возможность защищать свои права в Суде ЕС.<sup>23</sup>

4) В Великобритании действует независимый орган – Комиссариат по защите информации (ICO). Данный орган занимается такими важными аспектами, как регистрация организаций, имеющих отношение к обработке данных, а также прием и рассмотрение жалоб от частных лиц касательно нарушения соответствующего права. Решения и консультативные заключения этого органа обычно принимаются во внимание компаниями и органами. То есть у гражд-

участвовать в правоотношениях по поводу защиты данных на определенных условиях могут, тем не менее, взять на себя аналогичные обязательства. Например, государства, которые имеют тесные связи с европейскими государствами и желающие избежать постоянной проверки адекватности уровня защиты персональных данных в своих государствах, имеют возможность присоединиться к Конвенции 108, имплементировать ее положения в свое законодательство и значительно упростить процедуру обмена данными с ранее подписавшими государствами (см. также некоторые аспекты «глобализации» Конвенции 108: Greenleaf G. "Modernising" data protection Convention 108: A safe basis for a global privacy treaty? // Computer law & Security Review, № 29, 2013. P. 430-436).

<sup>23</sup> Стоит, безусловно, учесть, что летом 2016 г. в Великобритании был проведен референдум о выходе из состава Европейского Союза. В случае фактического выхода положения данной Директивы более не будут распространяться на Великобританию, а, следовательно, граждане не смогут отстаивать свои права в Суде Европейского Союза. Однако, невозможно недооценивать значение данной Директивы для уже проведенных реформ британского законодательства, основанных в том числе на ее положениях.

<sup>24</sup> Создание именно независимого органа, который бы занимался исключительно вопросами защиты персональных данных крайне важно. Например, в Российской Федерации вопросами защиты данных занимается Роскомнадзор, в ведение которого помимо этого входит анализ работы СМИ, массовых коммуникаций и связи. Такой широкий спектр вопросов не позволяет органу сосредоточиться на одном правовом аспекте, учитывая тот факт, что защита персональных данных при кажущейся узости предмета является достаточно обширным институтом в международной и национальной практике. Более того, количество контролеров персональных данных, а также лиц, чьи данные собираются и обрабатываются, невероятно велико, оно исчисляется сотнями тысяч физических и юридических лиц в случае контролера и практически всем населением в случае субъекта данных. Для охвата такой глобальной «сети» правоотношений необходим специализированный орган.



<sup>20</sup>Gellert R, Gutwirth S. The legal construction of privacy and data protection. // Computer law & Security Review, № 29, 2013. P. 526. В деле «Дюрант против Органа финансовых услуг» (Великобритания) Апелляционный суд постановил, что данные должны касаться частной жизни человека для того, чтобы соответствовать критерию «относительности» к индивиду и, таким образом, рассматриваться как персональные данные в соответствии с Законом о защите данных 1998 г. Такое положение до сих пор вызывает споры в научном сообществе. (см. Cumbley R., Church P. What is personal data? The House of Lords identifies the issues. // Computer law & Security Review, № 24, 2008. P. 565).

<sup>21</sup>См., например, Резолюцию Генеральной Ассамблеи ООН №68/167 «Право на неприкосновенность личной жизни в цифровой век», принятую 18.12.2013 г.

<sup>22</sup>Интересно отметить, что данная Конвенция 108 является открытой для подписания не только европейскими, но и любыми изъявившими желание государствами. Таким образом, даже государства, которые изначально не должны

дан есть также возможность защитить свои права в независимом и беспристрастном органе.<sup>24</sup>

Исходя из проведенного анализа можно выделить следующие положения:

– на сегодняшний день в Республике Казахстан существуют некоторые правовые инструменты для защиты прав, касающихся персональных данных граждан, однако, этих инструментов недостаточно для уверенного обеспечения данного права и эффективного рассмотрения возникающих споров. В частности: отсутствует специализированный орган по вопросам защиты данных; нет международного инструмента, направленного непосредственно на защиту данных, а не частной жизни, который бы распространял свое действие для Республики.

– полезным для рассмотрения является опыт Великобритании, граждане которой, опираясь на действующее право, могут обратиться с вопросами защиты именно персональных данных в следующие органы: Комиссариат по защите информации (ICO); Государственные суды; Суд Европейского Союза; Европейский Суд по правам человека.

### ЗАКЛЮЧЕНИЕ

Стоит подчеркнуть уже достаточно серьезную проделанную работу по обеспечению права на защиту персональных данных в Республике Казахстан в виде принятия Закона «О персональных данных и их защите», наделения соответствующими полномочиями Правительства и Прокуратуры. Однако все еще актуальны дополнения. Уточнения и развития требуют аспекты обработки данных без согласия субъекта, а также возникающие в связи с этим споры и способы защиты нарушенных прав.

По анализу и выводам в данной статье нами могут быть сформулированы некоторые предложения, рассмотренные на примере Великобритании, которые могли бы быть полезными в практике Республики Казахстан, а именно:

– подписание международного договора, касающегося непосредственно защиты персональных данных (Одним из примеров такого договора может быть Проект Конвенции о защите персональных данных для государств-участников ЕАЭС, разработанный в рамках диссертационного исследования на соискание степени Ph.D автором настоящей статьи);

– создание специализированного независимого органа по вопросам защиты персональных данных, в ведение которого входило бы как консультирование по возникающим вопросам, так и разрешение

споров с последующим контролем за исполнением решений;

– дальнейшее совершенствование законодательства Республики Казахстан, основанное на существующих и устоявшихся международных стандартах;

– осуществление политики по ликвидации правового нигилизма в сфере защиты данных среди населения, для создания прецедентной практики в судах Республики Казахстан относительно толкования некоторых положений Закона.

### **О.В. Лозовая: Субъектінің келісімінсіз жеке мәліметтерді өңдеу: бұзылған құқықтарды қамтамасыз етудің тәжірибесі (Қазақстан Республикасы мен Ұлыбритания мысалында).**

Мақала азаматтың жеке деректерін оның келісімінсіз өңдеу кезінде және осы өңдеу заңсыз жүргізілсе, азаматтың құқықтарын қорғауда туындайтын проблемалық аспектілерді зерттеуге арналған. Қазақстан Республикасы мен Ұлыбританияның жеке деректерді қорғау жүйелері туралы құқықтық ережелерге талдау жасалған. Жүргізілген талдау нәтижелері бойынша Ұлыбритания азаматтары өзінің жеке деректерін қорғауда құралдар мен әдістердің көбірек жиынтығын қолдана алатыны анықталды. Мақала соңында Қазақстан Республикасында жеке деректерді қорғау институтын дамытуға бағытталған ұсыныстар жасалған.

*Түйінді сөздер:* жеке деректер, жеке өмір, қолсұқпаушылық, құқықты бұзу, адам құқықтары, Қазақстан Республикасы, Ұлыбритания, еуропалық одақ, халықаралық құқық, адам құқықтарын қорғау.

### **O. Lozovaya: Processing of personal data without the consent of the subject: the practice of provision and restoration of violated rights (by the example of the Republic of Kazakhstan and the United Kingdom).**

The article investigates the problematic areas encountered in the processing of personal data of citizen without his consent, as well as the protection of the rights of an individual, if the treatment is still illegal. The comparison of the provisions of the personal data protection system in the Republic of Kazakhstan and the UK is conducted for a more in depth analysis. The analysis gives a reason to believe that British citizens now have a broader set of tools and ways to protect their right of protection of personal data. At the end the article reflects main recommendations for the development of the institute of data protection in the Republic of Kazakhstan.

*Keywords:* personal data, privacy, integrity, violation of rights, human rights, Kazakhstan, United Kingdom, European Union, international law, human rights protection.