Вестник Томского государственного университета. 2020. № 454. С. 233–243. DOI: 10.17223/15617793/454/29

УДК 341.64

Т.Д. Оганесян

МЕЖДУНАРОДНО-ПРАВОВЫЕ АСПЕКТЫ РЕАЛИЗАЦИИ ПРАВА НА ЗАЩИТУ ДАННЫХ: ПРОБЛЕМЫ И ТЕНДЕНЦИИ

Исследуются правовая природа права на защиту данных, целесообразность ее выделения в качестве самостоятельного права и проблемы ее реализации. Особое внимание уделено поиску необходимого баланса между защитой данных и свободой выражения мнения. Проведен анализ международно-правовой базы доктринальных исследований, а также правовых позиций национальных и международных судов в области защиты. Обоснован вывод о необходимости создания независимых надзорных органов в сфере защиты данных на основе стандартов, выработанных Советом Европы.

Ключевые слова: защита персональных данных; массовое наблюдение; конфиденциальность; право на уважение частной жизни; интернет; Совет Европы; Европейский Суд по правам человека; Суд Европейского Союза; Конвенция 108.

Введение

За последние десятилетия технические возможности для сбора и обработки данных существенно расширились. Цифровая революция и технологический прогресс не только изменили отношение людей к персональным данным, но и бросили вызов существующим концепциям защиты данных. Вопросы защиты персональных данных приобретают еще большее значение также в контексте развития и массового внедрения программ и методов автоматизированной обработки данных. На сегодняшний день социальные сети и мессенджеры хранят большую часть данных о своих пользователях, и в этой связи вопросы защиты данных в интернете представляются особенно актуальными.

На основе анализа прецедентной практики Европейского Суда по правам человека (далее – ЕСПЧ) в области защиты данных возможно выделить три проблемных аспекта. Во-первых, персональная информация, размещенная пользователем в интернете, как правило, может многое рассказать об интересах и деятельности данного человека. Персональные данные, размещенные на сайтах социальных сетей, а затем хранимые и индексируемые поисковыми системами, могут быть использованы третьими лицами в коммерческих целях. В этой связи крупные корпорации стремятся использовать различные программы для оценки потребительских привычек с целью персонализации рекламы, управляя огромным количеством персональных данных. Во-вторых, в настоящее время происходит поиск «идеальной» формулы сбалансирования права на свободу выражения мнения и права на защиту персональных данных. Свою лепту в решении данного вопроса вносит также воспринимаемая неоднозначно прецедентная практика ЕСПЧ последних лет. В-третьих, возникает необходимость постоянного «обновления» стандартов защиты от произвольного массового наблюдения и сбора данных на национальном и международном уровнях.

Право на уважение частной жизни и право на защиту данных: правовые основы регулирования

Связь между правом на уважение частной жизни и защитой персональных данных обусловлена эволюцией европейской системы защиты персональных данных. До начала 2000-х гг. большинство исследователей однозначно полагали, что право на уважение частной жизни включает в себя право на защиту персональных данных, рассматривая последнее как одно из «измерений» права на уважение частной жизни [1. P. 91]. Данный подход находит свое отражение и в прецедентной практике ЕСПЧ, в рамках которой право на защиту данных является следствием расширительного толкования ст. 8 Европейской конвенции по правам человека (ЕКПЧ). Однако, несмотря на то что ЕСПЧ рассматривает право на защиту данных лишь как один из элементов права на уважение частной жизни, очевидно, что модернизация Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных (далее – Конвенция 108), закрепление в ст. 8 Хартии ЕС об основных правах «права на защиту данных» в качестве отдельного права, развитие прецедентных практик национальных и субрегиональных международных судов способствуют превращению права на защиту данных в самостоятельное и «дееспособное» право.

На сегодняшний день набирает популярность идея о том, что на самом деле существуют две отдельные, но взаимосвязанные категории: с одной стороны, право на уважение частной жизни и, с другой – право на защиту персональных данных. В этой связи Г. Гонсалес Фустер ставит под сомнение идею о том, что защита персональных данных всегда вытекает из права на уважение частной жизни [2. P. 268]. При этом ряд государств – членов ЕС с самого начала не рассматривали защиту данных в качестве составляющего элемента права на уважение частной жизни. Разумеется, в некотором смысле защита персональных данных возникла как следствие толкования права на уважение частной жизни, но в то же время наблюдаются тенденции концептуализации права на защиту данных и преобразования ее в отдельное право [3. P. 62].

Следует отметить, что на сегодня Хартия ЕС об основных правах предоставляет национальным судам ЕС все необходимые инструменты для преобразования права на защиту данных в полноценное и отдельное право. В свою очередь, ЕСПЧ постоянно отмечает, что понятие «частная жизнь» является широким понятием, не поддающимся исчерпывающему определению [4. П. 87], предпочитая, в отличие от Суда Европейского

Союза (далее – Суд ЕС), рассматривать право на защиту персональных данных лишь как один из элементов права на уважение частной жизни. С данным подходом сложно не согласиться, поскольку право на защиту персональных данных нельзя в полной мере признавать в качестве полноценного и самостоятельного права. Для того чтобы соответствующее право стало полностью «дееспособным», нужно, чтобы оно обладало элементами, присущими только ему, при этом было настолько сбалансированным, что необходимости обращаться к праву на уважение частной жизни не возникало. Однако в процессе развития законодательств и правоприменительных практик европейских стран в сфере защиты данных Европейскому Суду все сложнее будет избегать вопроса о выделении права на защиту данных в качестве отдельного права, учитывая то, что Суд ЕС уже признал последнее.

На глобальном уровне наблюдается тенденция установления минимальных стандартов регулирования сбора и обработки персональных данных. Международные документы и руководящие принципы, отражающие эти изменения, включают, среди прочего: Руководящие принципы регламентации компьютеризированных картотек 1990 г., содержащих данные личного характера; Конвенцию 108 и ее обновленные версии, в которых устанавливается высокий уровень защиты на глобальном уровне; Принципы неприкосновенности частной жизни 1980 г. Организации экономического сотрудничества и развития, обновленные в 2013 г.; Конвенцию о кибербезопасности и защите личных данных Африканского союза (Конвенция Малабо); Мадридскую резолюцию Международной конференции уполномоченных по защите данных и права на неприкосновенность частной жизни; Рамки защиты частной жизни форума Азиатско-Тихоокеанского экономического сотрудничества. Эти стандарты легли в основу рамок защиты конфиденциальности данных многих государств. Во всех документах и рекомендациях, упомянутых выше, признается, что лицам, чьи данные собираются и обрабатываются, должны предоставляться определенные права. Затрагиваемые лица как минимум имеют право знать, что персональные данные были собраны и обработаны, иметь доступ к хранимым данным, исправлять неточные или устаревшие данные и исправлять данные, которые хранятся незаконно или необоснованно.

Право на неприкосновенность личной жизни является одним из основных прав человека и закреплено в ст. 12 Всеобщей декларации прав человека, ст. 17 Международного пакта о гражданских и политических правах 1966 г. (далее – МПГПП), а также во многих других международных и региональных договорах о правах человека. В контексте международно-правового регулирования защиты данных ст. 17 МПГПП устанавливает, что вмешательство в право на уважение частной жизни допускается только в соответствии с международным правом в области прав человека, если оно не является произвольным или незаконным. Комитет по правам человека ООН в свих замечаниях пояснил [5], что термин «незаконное» подразумевает, что любое вмешательство должно быть предусмотрено законом, а сам закон должен соответствовать положениям, целям и задачам МПГПП. Это означает, что любая программа наблюдения за коммуникациями должна осуществляться на основе общедоступного закона, который в свою очередь должен соответствовать собственному конституционному режиму государства и международному праву в области прав человека. Однако очевидно, что отсутствие эффективного надзора способствовало отсутствию ответственности за произвольные или незаконные посягательства на право на неприкосновенность частной жизни в цифровой среде. Внутренние гарантии без независимого внешнего мониторинга, в частности, оказались неэффективными в отношении незаконных или произвольных методов наблюдения.

Как напомнила Генеральная Ассамблея ООН в резолюции 68/167, международное право в области прав человека обеспечивает универсальные рамки, на основе которых должно оцениваться любое вмешательство в права человека на неприкосновенность частной жизни [6]. Хотя право на неприкосновенность частной жизни в соответствии с международным правом в области прав человека не является абсолютным, любой случай вмешательства должен подвергаться тщательной и критической оценке его необходимости, законности и соразмерности. В соответствии с этими принципами государства могут нарушать право на частную жизнь лишь в той степени, в какой это предусмотрено законом, и в соответствующем законодательстве должны подробно определяться конкретные обстоятельства, в которых такое вмешательство может допускаться [7. С. 3–8]. Вмешательство является незаконным и произвольным не только в том случае, если оно не допускается законом, но и тогда, когда тот или иной закон или конкретное вмешательство противоречит положениям, целям и задачам Пакта.

В последние годы ценную роль в области защиты данных играет специальный докладчик ООН по вопросу о праве на неприкосновенность частной жизни, который ежегодно в своих докладах акцентирует внимание на различных аспектах защиты данных, выдвигая также ряд рекомендаций. Так, в докладе за 2019 г. подчеркнута возрастающая роль медицинских данных, имеющих высокую коммерческую ценность. В этой связи специальный докладчик ООН Р. Канната чи предполагает, что передача любых персональных данных как внутри страны, так и за ее пределами должна подвергаться соответствующему надзору в соответствии с принципом: «если данные подлежат обмену, то они подлежат надзору» [8].

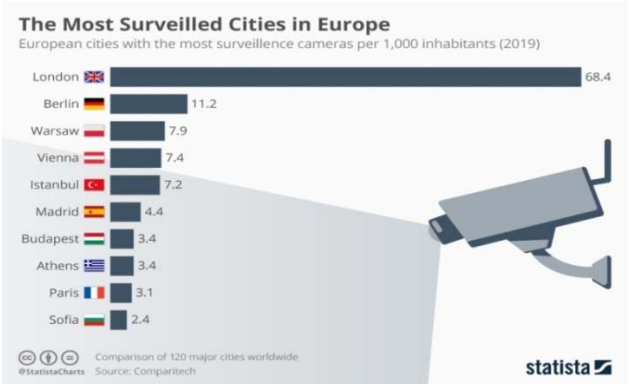
В докладе Управления Верховного комиссара ООН по правам человека отмечено, что государства часто оправдывают программы наблюдения соображениями национальной безопасности, включая борьбу с терроризмом [9]. Наблюдение по соображениям национальной безопасности или в целях предупреждения терроризма или других преступлений может быть «законной целью» для целей оценки с точки зрения ст. 17 МПГПП. Однако степень вмешательства должна оцениваться с учетом необходимости принятия мер для достижения этой цели и фактических выгод, которые она приносит для достижения этой цели.

Что касается национальных норм о защите данных, то в большинстве случаев, когда государства решались на закрепление положений об обработке данных, это осуществлялось в форме отдельных законов (например, во Франции), однако в некоторых случаях положения об автоматизированной обработке данных находили свое отражение в принятых конституциях (например, в Португалии, Испании). Например, французский закон *Loi informatique et liberté* нацелен на защиту *vie privée* (частной жизни) и связывает защиту данных с правом на уважение частной жизни [10]. Аналогичным образом австрийские конституционные положения о защите персональных данных 1978 г., закрепив впервые право на защиту данных (*datenschutz*) в качестве конституционного права, связывали защиту данных с правом на уважение частной и семейной жизни.

Риски и угрозы смарт-наблюдения

В настоящее время тематике смарт-наблюдения уделяется немало внимания, в частности, технологические компании посвящают этой тематике целые исследовательские программы и курсы, а национальные власти вносят периодично различные предложения по совершенствованию актов, регламентирующих защиту данных. В этой связи Лоуренс Лессинг, основатель доктрины интернет-права, рассуждая о праве на уважение частной жизни в контексте сбора данных о людях в киберпространстве, отмечает следующее: в реальном мире в большинстве случаев мы чаще всего замечаем или имеем возможность заметить, что за нами осуществляется наблюдение. Например, мы можем заметить видеокамеры, «не обладая какой-либо особой квалификацией, а просто представляя, как могут выглядеть такого рода устройства», или же при оплате покупки пластиковой картой на чеке отображается некоторая личная информация. Однако, по замечанию Л. Лессинга, в «киберпространстве» в большинстве случаев пользователь не сможет распознать наблюдение. В последнем случае информация передается через устройства пользователя (смартфон, смартчасы и т.д.) на сервер [11. P. 221]. Идеи профессора школы права Гарвардского университета сложно оспорить, поскольку они полностью соответствуют существующим реалиям.

Создание и внедрение систем массового наблюдения, сбора и обработки данных в последние годы привело к изменению взаимоотношений между человеком и государством. Катализатором данной трансформации стала растущая связь между «секьюритизацией» и превентивным надзором со стороны органов безопасности [12. P. 36]. Технологии наблюдения превращаются в «смарт» благодаря внедрению специальных программ. Например, камеры смарт-наблюдения начинают сбор данных в случае, если система замечает «опасный объект или опасную ситуацию». Согласно опросу, проведенному Comparitech, городами-лидерами, в которых установлено больше всего камер наблюдения на душу населения, являются Лондон (630 тыс. камер наблюдают за 9,6 млн жителей – 68,4 камеры на 1 тыс. лондонцев) и Берлин (11,2 камеры на 1 тыс. жителей) [13].



Одним из ключевых аспектов сотрудничества государств с частными компаниями (в целях создания системы всеобщего превентивного наблюдения для борьбы с терроризмом) является возложение на телекоммуникационные компании обязанности сохранять метаданные о телефонных звонках или электронной почте своих клиентов и передавать соответствующие данные государственным органам. Данная практика является довольно распространенной и применяется в странах ЕС и США. Например, в ЕС поставщики телекоммуникационных услуг обязаны хранить данные от 6 месяцев до 2 лет в отступление от положений директивы 2002/58/ЕС [14]. Кроме того, срок хранения данных может быть продлен государствами – членами ЕС, «столкнувшимися с особыми обстоятельствами, которые требуют продления» (ст. 12). Доступ к сохраненным данным имеют лишь «только компетентные национальные органы в конкретных случаях и в соответствии с национальным законодательством» (ст. 4). Однако законодательство ЕС не определяет четко, кто является компетентным органом, оставляя решение данного вопроса на усмотрение национальных властей.

Неудивительно, что у смарт-наблюдения есть и некоторые плюсы, одним из которых, по замечанию М. Вермеулена и Р. Беллановой, является отсутствие дискриминации при использовании интеллектуальных методов наблюдения, поскольку именно машина, а не человек, выбирает субъектов наблюдения, что «компенсирует человеческие предрассудки» [15. P. 309]. Действительно, дискриминация в данном случае отсутствует, поскольку человеческие предрассудки уступают место программным алгоритмам. Однако существенным вопросом является то, как собранные в результате наблюдения данные будут в последующем использованы уже не программой, а отдельными лицами или службами.

Системы смарт-наблюдения способны также извлекать необходимую информацию из имеющейся для последующего применения при принятии автоматизированных решений [16. P. 347]. Ключевой особенностью смарт-наблюдения является также то, что они используются для наблюдения в общественных местах. Рабочая группа ЕС по защите персональных данных признала, что при смарт-наблюдении лицо должно рассчитывать на меньшую степень конфиденциальности [17. С. 5]. ЕСПЧ, в свою очередь, указал, что наблюдение за действиями человека в общественном месте с помощью фотооборудования, которое не

фиксирует визуальные данные, само по себе не приводит к вмешательству в частную жизнь человека [18. P. 38], а само вмешательство в право на уважение частной жизни происходит лишь в том случае, если данные, полученные с помощью смарт-наблюдения, предаются гласности.

Смартфоны, ноутбуки и быстрый межсетевой доступ стирают временные и пространственные границы между трудовой и домашней жизнью, а также между работой и домом. Как отмечает К. Джервис, становится все труднее различать, в каком качестве человек действует в тот или иной момент времени [19. P. 443]. В этой связи естественным образом актуализируется вопрос, связанный с осуществлением наблюдения на рабочем месте. Европейский Суд рассмотрел целую группу подобных дел, среди которых ключевым является постановление Большой Палаты по делу «*Barbulescu v. Romania»,* в котором было констатировано отсутствие европейского консенсуса по вопросу об осуществлении наблюдения на рабочем месте, а также пределов свободы усмотрения государств в данном случае [20. П. 121].

Одним из ключевых дел, рассмотренных ЕСПЧ в 2019 г., является постановление по делу *«López Ribalda and Others v. Spain»*, в котором Большая Палата не признала нарушения ст. 8 Конвенции вследствие скрытого видеонаблюдения за сотрудниками магазина. Суд, в частности, установил, что испанские суды сбалансировали права заявителей – сотрудников супермаркета, подозреваемых в краже, и права работодателя, проведя тщательную проверку соразмерности применения видеонаблюдения.

Наглядным примером того, что правовые позиции ЕСПЧ в области наблюдения не категоричны, является то обстоятельство, что Палата ЕСПЧ из 7 судей в постановлении в январе 2018 г. по данному делу единогласно пришла к обратному выводу о нарушении ст. 8 Конвенции. Большая Палата ЕСПЧ перенесла принципы, изложенные в деле «*Barbulescu v. Romania»*, касающиеся контроля работодателем за учетной записью электронной почты сотрудника, на данный случай, отметив, что национальные суды не превысили пределов усмотрения. Приняв во внимание, что наблюдение длилось всего 10 дней, а записи просмотрело ограниченное число людей, Суд счел, что вторжение в частную жизнь заявителей не достигло высокой степени серьезности. Важным обстоятельством является также цель наблюдения: видеозаписи не использовались ни для каких-либо других целей, кроме как для отслеживания лиц, ответственных за убытки, и что не было никакой другой меры, которая могла бы удовлетворить преследуемую законную цель.

Примечательно, что судьи Й. Грозев, А. Юдковская и В.А. Де Гаэтано, не согласившиеся с мнением большинства судей, в особом мнении отметили, что Суд, не обнаружив нарушения ст. 8 Конвенции, разрешил неограниченное использование скрытого видеонаблюдения на рабочем месте без предоставления достаточных правовых гарантий тем, чьи личные данные будут собираться и использоваться в неизвестных целях. Трудно не согласиться с мнением судей ЕСПЧ, оказавшихся в меньшинстве при разрешении данного дела, поскольку даже наличие «разумных подозрений в совершении правонарушения» не должно являться достаточным основанием для осуществления скрытого наблюдения. В этой связи при отсутствии в национальных законодательствах четких процессуальных гарантий подобные наблюдения будут массово применяться.

Защита данных в интернете

Непрерывное распространение персональных данных в интернете способствует несанкционированному доступу к данным миллионов пользователей, в связи с чем опасения по поводу незаконной обработки данных выглядят более чем реальными. И. Гюрсель отмечает, что как только мы появляемся в интернете, все наши действия оставляют «цифровые следы про нашу личную жизнь» [21. P. 39]. Уязвимость персональных данных и отсутствие гарантий защиты служат основными причинами для сотрудничества государств и международных организаций в целях выработки единых стандартов для защиты данных.

Одной из многих работ, посвященных массовому наблюдению и дающих понимание того, что современная проблема обеспечения конфиденциальности и защиты данных не такая уж современная, является эссе американского инженера Пола Бэрана (Paul Baran) «Будущая компьютерная утилита» (The future computer utility). В своей работе американский исследователь предполагал, что когда-нибудь несколько больших централизованных компьютеров обеспечат обработку информации: «домашний компьютер будет использоваться для отправки и получения сообщений. Мы могли бы проверить, есть ли в наличии на складе рекламируемая рубашка нужного цвета и размера. Мы могли бы спросить, когда будет осуществлена доставка... Сам компьютер мог бы напоминать нам о предстоящей годовщине и спасти нас от катастрофических последствий забывчивости» [22. P. 78]. При всех плюсах компьютеризации П. Бэран также предполагал существование механизма, который мог бы «предложить максимальную защиту права на неприкосновенность частной информации от потенциального подслушивающего устройства» [22. P. 79].

На сегодняшний день коммерческие интересы технологических компаний и политические интересы правительственных учреждений в интернете во многом похожи: обе стороны заинтересованы в сборе и быстром анализе пользовательских данных. Исследования показывают, что данные, представленные на страницах пользователей социальных сетей, могут быть использованы для получения так называемых «чувствительных» данных. Например, Facebook может определить сексуальную ориентацию посредством анализа онлайн-поведения пользователя и его «друзей» [23], политические взгляды [24], а также определить склонность к суициду [25]. Microsoft, в свою очередь, на основе данных пользователей может предсказать болезнь Паркинсона и болезнь Альцгеймера. А голосовой помощник Amazon Alexa может определять состояние здоровья на основе моделей

речи [26]. Несмотря на то что ни одно из этих приложений не позволяет осуществлять прогнозы с абсолютной уверенностью, тем не менее, с помощью данных программ крупные корпорации хранят и обрабатывают данные своих пользователей для различных целей.

Исходя из широких возможностей крупных компаний осуществлять сбор и хранение больших данных, представляется возможным выделить два проблемных аспекта. Во-первых, персональные данные, размещенные пользователем в интернете, как правило, могут многое рассказать об интересах и деятельности этого человека. Персональные данные, опубликованные на сайтах социальных сетей, а затем хранимые и индексируемые поисковыми системами, могут быть произвольно использованы третьими лицами в коммерческих целях. В этой связи крупные корпорации стремятся использовать более «умные» и бесконтрольные технологии (алгоритмы) для оценки потребительских привычек с целью персонализации рекламы, управляя огромным количеством персональных данных.

Во-вторых, стоит задуматься о том, все ли персональные данные в интернете подлежат защите. Как отмечает британский судья ЕСПЧ Тим Эйке, вполне очевидно, что не все лайки и смайлы заслуживают защиты [27]. Суд вряд ли будет предлагать высокий уровень защиты данных пользователей социальных сетей, если речь идет о том, что «автор ел или носил» [28], поскольку соответствующие данные не обладают особой информативной ценностью. Очевидно, что многое из того, что пользователи «твитят» и публикуют, не может в конечном итоге требовать защиты, однако даже такие данные находится в «сфере действия» ст. 8 ЕКПЧ, чтобы при необходимости обеспечить защиту данных в соответствии с требуемыми стандартами ЕСПЧ.

На основе анализа правовых позиций Суда ЕС по делу *Google Spain* можно утверждать об увеличении случаев нарушения права на защиту данных вследствие распространения интернета и поисковых систем в современном обществе, которые делают данные «вездесущими» [29. П. 80]. Это значительно затрудняет возможность требовать удаления или стирания личной информации из интернета, т.е. так называемого «right to be forgotten» («право быть забытым» или «права на забвение»). Определенный вклад в укрепление европейской онлайн-безопасности, как представляется, вносят вступившие в силу в июне 2019 г. новые правила безопасности в интернете для компаний и отдельных интернет-пользователей, получившие закрепление в законе о кибербезопасности ЕС (EU Cybersecurity Act), согласно которым страны ЕС теперь должны следить за тем, чтобы зарегистрированные на их территории онлайн-ресурсы были безопасными и не распространяли дезинформацию [30]. Предлагаемая общеевропейская система сертификации предполагает выдачу Европейским агентством кибербезопасности (ENISA) сертификатов, свидетельствующих о соответствии товаров и услуг требованиям кибербезопасности.

Защита персональных данных и свобода выражения мнения: поиск необходимого баланса

Безусловно, экспансия интернета преобразила многие сферы общественной жизни, в том числе и правовую, затронув в первую очередь права человека. В этой связи концептуальными вопросами стали вопросы, связанные с поиском оптимальной формулы балансирования права на защиту данных и права на свободу выражения мнения. Актуальной представляется прецедентная практика ЕСПЧ, которая выработала ряд правовых позиций по данному вопросу. В частности, в постановлении по делу «*Delfi AS v. Estonia»* Европейский Суд прямо указал, что «Интернет, предоставляя своим пользователям возможность активно себя реализовывать, является уникальной платформой для реализации свободы выражения мнения» [31. П. 110]. Вместе с тем ЕСПЧ отметил, что наряду с положительными аспектами интернета имеют место и определенные риски, одним из которых выступает «напряженность» между свободой выражения мнения и защитой персональных данных [32. С. 29].

В доктрине международного права по вопросу регулирования интернета преобладают две точки зрения. Согласно первой позиции государства, крупные информационно-коммуникационные сети должны воздерживаться от любых форм и попыток регулирования интернет-пространства. Сторонники данной точки зрения тем самым выступают за неограниченную свободу пользователей в интернете без какого-либо вмешательства со стороны в первую очередь государственных служб. Визави-оппоненты данной точки зрения считают, что правовое регулирование должно также касаться интернета без исключения, чтобы не допускать возникновения правового вакуума.

Представляется, что определенную ясность в исследовании данного вопроса может внести прецедентная практика ЕСЧП, которая уделяет особое внимание делам, связанным с ответственностью информационного посредника за недопустимые комментарии онлайн-пользователей в контексте стандартов Конвенции. В постановлениях по делам «*Delfi AS v. Estonia», «Magyar T.E. and Index.hu Zrt. V. Hungary»* ЕСПЧ впервые попытался конкретизировать допустимые пределы в отношении режимов ответственности интернет-посредника за комментарии анонимных онлайн-пользователей, а также факторы, которые подлежат оценке при установлении баланса между правами интернет-посредника на свободу выражения мнения (ст. 10 ЕКПЧ) и правами лиц, затронутых недопустимыми комментариями пользователей, на защиту репутации (ст. 8). Дело касалось обязанностей и ответственности новостных интернет-порталов, которые на коммерческой основе предоставляли платформу для комментариев пользователей к ранее опубликованному контенту. Компания-заявитель Delfi AS, управлявшая новостным порталом, жаловалась, что была привлечена к ответственности национальными судами за оскорбительные комментарии на вебстранице, размещенные ее читателями ниже одной из своих новостных статей о паромной компании. По просьбе адвокатов владельца паромной компании

Delfi удалила оскорбительные комментарии примерно через шесть недель после их публикации.

В указанном деле ЕСПЧ впервые сформулировал общие принципы для оценки свободы усмотрения государств в контексте ст. 10 ЕКПЧ в отношении привлечения к ответственности интернет-посредников. Вопрос, стоявший перед Большой Палатой ЕСПЧ, заключался не в том, была ли нарушена свобода выражения мнений авторов комментариев, а в том, было ли привлечение Delfi к ответственности за комментарии, опубликованные третьими сторонами, нарушением ее свободы распространять информацию, гарантированной ст. 10 ЕКПЧ.

Большая Палата не признала нарушения ст. 10 Конвенции и пришла к выводу, что эстонские суды обоснованно и пропорционально ограничили право портала на свободу выражения мнения, в частности, потому, что комментарии, о которых идет речь, были диффамационными и размещены в ответ на статью, опубликованную Delfi на своем профессионально управляемом новостном портале. Тем самым Суд оставил на усмотрение государств – участников Конвенции выбор режима ответственности посредника на внутригосударственном уровне. Исландский судья ЕСПЧ Р. Спано в особом мнении отметил, что Суд занял среднюю позицию между двумя диаметрально противоположными точками зрения на регулирование интернета – защищающей интернет-пространство, свободное от ограничений онлайн-поведения, и выступающей за регулируемый интернет, в котором должны применяться одни и те же правовые принципы – как онлайн, так и офлайн [32. С. 28].

Данное постановление ЕСПЧ подверглось критике со стороны тех, кто считает, что оно ограничивает свободу слова в интернете, позволяя национальным властям привлекать к ответственности посредников, дающим частным пользователям возможность свободно обсуждать те или иные новости, и что онлайн-порталы обязаны обеспечивать определенный мониторинг [33]. Предложенный в данном деле подход ЕСПЧ в определенной степени можно понять, учитывая сложные поиски «золотой середины» между защитой свободы выражения мнения и защитой права на частную жизнь.

Другое дело «*Magyar T.E. and Index.hu Zrt. v. Hungary»* касалось ответственности саморегулируемого органа интернет-провайдеров контента и новостного интернет-портала за вульгарные и оскорбительные онлайн-комментарии, размещенные на их сайтах. Компания MTE (Magyar Tartalomszolgáltatók Egyesülete) и новостной портал (Index.hu Zrt) жаловались на то, что они были привлечены к ответственности национальными судами за онлайн-комментарии, опубликованные их читателями после публикации мнения, критикующего методы ведения бизнеса двух сайтов по торговле недвижимостью.

Европейский Суд вновь заявил, что хотя интернет-новостные порталы и не являются издателями комментариев в традиционном смысле этого слова, но они несут ответственность. Суд признал нарушение ст. 10 Конвенции, указав главным образом на то, что венгерские суды, принимая решение по понятию ответственности в деле заявителей, не обеспечили должного баланса между соответствующими конкурирующими правами, а именно между правом заявителей на свободу выражения мнений и правом веб-сайтов по недвижимости на защиту деловой репутации.

Следует отметить, что последнее дело в некоторых аспектах отличалось от дела, рассмотренного ранее ЕСПЧ дела Delfi AS v. Estonia, поскольку было лишено ключевых элементов «языка вражды». Оценивая прецедентное значение постановления по делу Delfi AS, нужно учитывать, что это первое постановление по делу подобного рода, рассмотренного ЕСПЧ. Как отмечает судья ЕСПЧ Р. Спано, данное дело носит в известной степени уникальный характер и может служить основой для интерпретаций за рамками фактов данного конкретного дела [32. С. 37]. Очевидно, что эти два постановления обогащают судебную практику ЕСПЧ и дополняют ее новыми элементами, проводя разграничение между ситуациями, когда государства могут свободно устанавливать ответственность новостных порталов за онлайн-комментарии пользователей.

Правила обработки данных: независимость контролирующих органов и национальная безопасность

Согласно общим правилам, установленным в Конвенции 108, персональные данные должны обрабатываться только на основе принципов, включающих требование о том, чтобы сбор был соразмерен осуществляемым целям [34]. В свою очередь законодательство ЕС запрещает обработку персональных данных в случае, если пользователи данных не были проинформированы о сборе и не имели право получать доступ к данным. Основываясь на этих простых правилах, ЕСПЧ и Суд ЕС за последние несколько лет существенно обогатили свои прецедентные практики в области защиты данных. Тем не менее режим защиты данных в Европе содержит ряд недостатков и отступлений, которые ослабляют способность защищать право на уважение частной жизни. Одним из таких отступлений является то обстоятельство, что сложившаяся система защиты данных в странах ЕС позволяет государствам ограничивать право на защиту данных по широким соображениям национальной безопасности и правопорядка. Например, парламент Франции, сразу же после терактов ноября 2015 г., утвердил новое законодательство, расширяющее полномочия правительства по осуществлению наблюдения в целях борьбы с терроризмом [35].

Несмотря на наличие минимальных общих правил обработки данных, установленных в прецедентной практике ЕСПЧ, тем не менее, национальные правила существенно различаются, причем некоторые государства обеспечивают более фундаментальную защиту данных, в то время как другие заметно отстают. Например, ФРГ имеет более регламентированное национальное законодательство и устоявшуюся практику в области защиты данных. Это в определенной степени позволяет германским властям прибегать и к некоторому «активизму». Так, Федеральный Консти-

туционный суд Германии последовательно ввел право на информационное самоопределение (the right to informational self-determination), которое стало основополагающим правом, защищаемым в соответствии с основным законодательством [36. P. 87].

Как отмечают Д. Коул и Ф. Фабринни, ни европейское законодательство, ни конвенционные стандарты в нынешнем толковании ЕСПЧ не способны фактически ограничить наблюдение европейских государств за иностранными гражданами за пределами их юрисдикций [37. P. 224]. В этой связи, рассуждая о необходимости создания контрольных (надзорных) органов в области защиты данных, не следует также забывать об их независимости. В рамках обсуждений по вопросу характера независимости соответствующего органа по защите данных Европейская комиссия отметила, что полная независимость предполагает свободу от любого влияния, будь то со стороны других государственных органов или извне [38. П. 15]. Данная идея выдвигалась в деле «European Commission v. Federal Republic of Germany» представителями ФРГ, предложившими более узкий, функциональный подход, в соответствии с которым контролирующие органы должны быть просто независимы от органов, находящихся под их контролем, а не независимы от других государственных органов. Однако Суд ЕС в 2011 г. отверг узкое толкование независимости, выдвинутое германским правительством, постановив, что независимость касается не только «отношений между контролирующими органами и органами, подлежащими такому надзору» [38. П. 19]. По мнению Суда ЕС, «простого риска того, что контролирующие органы могут оказывать политическое влияние на решения контролирующих органов, достаточно для того, чтобы препятствовать данным органам независимо выполнять свои задачи» [38. П. 36].

Изучению независимости контрольных органов в сфере защиты данных посвящена работа профессора Лондонской школы экономики и политических наук О. Лински. В своем исследовании О. Лински выделяет горизонтальную и вертикальную независимости надзорных органов в сфере защиты данных: независимость на национальном уровне (горизонтальная независимость) или независимость от институтов и учреждений ЕС (вертикальная независимость). Горизонтальная независимость может быть далее подразделена на две части для определения того, являются ли контролирующие органы независимыми от государственных органов или физических и юридических лиц [39. P. 257].

На сегодняшний день основным действующим органом европейского механизма защиты данных является созданный Европейский Совет по защите данных (European Data Protection Board), способствующий последовательному применению правил защиты данных во всем ЕС и содействующий сотрудничеству между органами ЕС по защите данных. Представляется целесообразным в качестве меры рекомендовать государствам – членам Совета Европы учреждать соответствующие органы, которые бы осуществляли внесудебный и независимый контроль за защитой данных в рамках национальных правовых систем, основываясь на требованиях, изложенных в модернизированной Конвенции 108.

При создании национального органа контроля в области защиты данных должное внимание следует уделять вопросу национальной безопасности. Право на защиту данных не является абсолютным правом, поскольку в целях обеспечения национальной безопасности, обороны и общественной безопасности право на защиту данных может быть ограничено. В этой связи одним из ключевых документов в сфере информационной безопасности в рамках СНГ является Концепция информационной безопасности государств – участников СНГ в военной сфере 2013 г. (далее – Концепция), которая представляет собой официально принятую государствами – участниками Содружества систему взглядов на цели, задачи и принципы обеспечения информационной безопасности. Например, в качестве угрозы информационной безопасности государств – участников Содружества отмечено нарушение установленных регламентов сбора, обработки и передачи информации, а также отсутствие необходимой нормативно-правовой базы, регулирующей межгосударственные отношения в информационной сфере [40]. В указанной Концепции информационной безопасности отражен в основном технический аспект информационной безопасности, подразумевающий технические средства обработки информации. Представляется, что ряд мер, предложенных в Концепции, действительно могут повысить уровень защиты данных в государствах – членах СНГ. К числу таких мер относятся: разработка и внедрение механизмов реализации и согласования правовых норм, регулирующих межгосударственные отношения в информационной сфере; создание Межгосударственного консультативного совета по информационной безопасности государств – участников Содружества.

Другим важным актом, определяющим векторы сотрудничества в области защиты данных в рамках СНГ, является Соглашение о сотрудничестве государств – участников СНГ в области обеспечения информационной безопасности (далее – Соглашение). Принимая во внимание важное значение информационной безопасности для реализации права на защиту данных, Соглашение предусматривает взаимодействие и сотрудничество по разработке нормативных правовых актов и стандартов в информационном пространстве, направленных на обеспечение информационной безопасности в государствах – членах СНГ [41]. В рамках других международных организаций также наблюдаются ограничения права на защиту данных в связи с соображениями борьбы с терроризмом. Например, в рамках Шанхайской организации сотрудничества также существует соглашение [42], которое в качестве основания ограничения защиты данных предусматривает борьбу с «информационным терроризмом». Что касается Евразийского экономического союза, то в рекомендациях Коллегии Евразийской экономической комиссии содержится также ряд стандартов в области защиты персональных данных: обработка персональных данных ограничивается достижением конкретных, зара-

нее определенных и законных целей; ответственность за раскрытие и распространение персональных данных без согласия субъекта персональных данных возлагается на операторов персональных данных и иных лиц, получивших доступ к этим персональным данным; последующая передача персональных данных, в том числе трансграничная передача персональных данных, осуществляется только при наличии соответствующего согласия субъекта персональных данных и в соответствии с законодательством государства-члена [43].

Таким образом, одной из тенденций сегодняшнего времени является принятие государствами законов, предусматривающих возможности ограничения права на защиту данных «в целях борьбы с терроризмом». Не стала исключением и российская нормативная база в области защиты данных, которая в 2016 г. обязала сотовых операторов и организаторов распространения информации в интернете хранить в течение года не только сами факты приема, передачи, доставки или обработки информации, но и их содержимое в течение шести месяцев [44]. Приведенные выше примеры соглашений в рамках региональных международных организаций также являются свидетельством ограничения права на защиту данных, что в свою очередь вызвано распространением так называемого информационного терроризма и соображениями национальной безопасности. Международные суды, рассматривая в последнее время дела, связанные с защитой персональных данных частных лиц, все более охотно принимают во внимание дискреционные полномочия государства в области защиты национальной безопасности, особенно с учетом современных угроз глобального терроризма и серьезных трансграничных преступлений.

Заключение

Необходимость защиты данных обусловлена растущим влиянием и контролем технологий, осуществляющих сбор и обработку личных данных миллионов людей в повседневной деятельности. Будучи «живым инструментом», Конвенция и ЕСПЧ должны не только признать влияние современных технологий, но и разработать более адекватные правовые гарантии для обеспечения надлежащей защиты данных. Новые технологии резко изменили легкость, с которой видеонаблюдение может осуществляться, что значительно увеличивает потенциальную возможность нарушения прав на неприкосновенность частной жизни в соответствии со ст. 8 Конвенции. Именно по этой причине на национальном уровне необходимо, чтобы законодательная база была ясной и предсказуемой в отношении дел, касающихся электронного наблюдения.

Особое внимание также следует уделить вопросу о создании единой системы независимых органов среди всех государств – членов Совета Европы для проведения эффективного надзора за любой деятельностью, нарушающей неприкосновенность частной жизни, в отношении разведывательных служб и правоохранительных органов. В этой связи, рассуждая о необходимости создания контрольных (надзорных) органов в области защиты данных, не следует также забывать об их независимости. Хотя исчерпывающего перечня требований к независимости контролирующих органов в области защиты данных не существует, из судебной практики ЕСПЧ можно выделить ряд критериев. Во-первых, не должно быть никакого прямого или косвенного внешнего влияния на контролирующий орган. На практике это означает, что решения и другие действия надзорного органа не могут быть приняты с предварительного одобрения или отменены (за исключением отмены на основе судебного решения). Во-вторых, контролирующий орган должен обладать организационной независимостью (например, отдельной правосубъектностью, чтобы не быть юридически частью другого государственного органа); независимыми сотрудниками (которые не работают в других государственных органах); финансовыми и информационными ресурсами.

На сегодняшний день стандарты Совета Европы являются той минимальной ступенью, от которой государствам следует отталкиваться при установлении стандартов защиты данных на национальных уровнях. В качестве рекомендации государствам для повышения стандартов национальной правовой системы и установления достаточных гарантий в области защиты данных рекомендуется ратифицировать и имплементировать новые положения Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных.

ЛИТЕРАТУРА

1. Benyekhlef K. Les normes internationales de protection des données personnelles et l'autoroute de l'information. In Les Journées Maximilien-Caron: Le respect de la vie privée dans l'entreprise. Thémis, 1996. P. 65–105.
2. Gonzalez Fuster G. The Emergence of Personal Data Protection as a Fundamental Right of the EU. Springer International Publishing, 2016. 274 p.
3. Hustinx P.J. Data protection in the European Union // Privacy & Informatie. 2005. P. 62–65.
4. ECtHR, López Ribalda and Others v. Spain (applications nos. 1874/13 and 8567/13). 17.10.2019.
5. UN Human Rights Committee (HRC), CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, 8 April 1988, HRI/GEN/1/Rev.9 (Vol. I). URL: https://www.globalhealthrights.org/wp-content/uploads/2013/10/General-Comment-16-of-the-Human-Rights-Committee.pdf (дата обращения: 10.01.2020).
6. Резолюция 68/167, принятая Генеральной Ассамблеей 18 декабря 2013 года. Право на неприкосновенность частной жизни в цифровую эпоху. URL: https://undocs.org/A/RES/68/167 (дата обращения: 10.01.2020).
7. Замечание общего порядка № 16 Комитета по правам человека о праве на личную жизнь, пункты 3 и 8. 1988. URL: https://www.globalhealthrights.org/wp-content/uploads/2013/10/General-Comment-16-of-the-Human-Rights-Committee.pdf (дата обращения: 10.01.2020).
8. Доклад за 2019 год Специального докладчика ООН по праву на неприкосновенность частной жизни. URL: https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/AnnualReports.aspx (дата обращения: 10.01.2020).

9. Доклад Управления Верховного комиссара ООН по правам человека по вопросу о праве на неприкосновенность частной жизни в цифровой век (A/HRC/27/37). 2014. URL: https://www.ohchr.org/RU/Issues/DigitalAge/Pages/ReportDigitalAge.aspx (дата обращения: 10.01.2020).
10. Закон Франции № 78-17 от 6 января 1978 года об обработке данных, файлах и свободах (Loi № 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés). URL: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006068624& dateTexte=vig (дата обращения: 12.09.2019).
11. Lessig L. Code: Version 2.0. New York : Basic Books, 2006. 350 p.
12. Mitsilegas V. The Transformation of Privacy in an Era of Pre-emptive Surveillance // Tilburg law review. 2015. Vol. 20. P. 35–37.
13. Statista. The most surveilled city in Europe. URL: https://www.statista.com/chart/19268/most-surveilled-cities-in-europe/ (дата обращения: 01.11.2019).
14. Council Directive 2006/24/ec of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/ec Art. 3 (1).
15. Vermeulen M., Bellanova R. European 'smart' surveillance: What's at stake for data protection, privacy and non-discrimination? // Security and Human Rights. 2013. Vol. 4. P. 297–311.
16. Wright D. Sorting out Smart Surveillance // Computer Law & Security Review. 2010. Vol. 26, № 4. P. 342–361.
17. Доклад рабочей группы ЕС по защите персональных данных. 2004. URL: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2004/wp101_en.pdf (дата обращения: 01.11.2019).
18. ECtHR. Perry vs United Kingdom. 17 July 2003.
19. Jervis C. Barbulescu v Romania: Why There is no Room for Complacency When it Comes to Privacy Rights in the Workplace // Industrial Law Journal. 2018. P. 440–453.
20. ECtHR. Barbulescu v. Romania. 05.09.2017.
21. Gursel I. Protection of Personal Data in International Law and the General Aspects of the Turkish Data Protection Law // Dokuz Eylul Universitesi Hukuk Fakultesi Dergisi. 2016. Vol. 18. P. 33–62.
22. Baran P. The future computer utility. 1967. P. 75–87.
23. Jernigan C., Mistre B.F. Gaydar: Facebook Friendships Expose Sexual Orientation // FIRSTMONDAY.ORG. 2009. Oct. 5. URL: https://firstmonday.org/ojs//index.php/fm/article/view/2611 (дата обращения: 01.11.2019).
24. Merrill J. Liberal, Moderate or Conservative? See How Facebook Labels You // N.Y. TIMES. 2016. Aug. 23. URL: https://www.nytimes.com/2016/08/24/us/politics/facebook-ads-politics.html (дата обращения: 01.11.2019).
25. Constine J. Facebook Rolls Out AI to Detect Suicidal Posts Before They're Reported // TECHCRUNCH. 2017. Nov. 27. URL: https://techcrunch.com/2017/11/27/facebook-ai-suicide- prevention/?guccounter=1 (дата обращения: 01.11.2019).
26. Cook J. Amazon Patents New Alexa Feature That Knows When You're Ill and Offers You Medicine // TELEGRAPH. 2018. Oct. 9. URL: https://www.telegraph.co.uk/technology/2018/10/09/amazon-patents-new- alexa-feature-knows-offers-medicine/ (дата обращения: 01.11.2019).
27. Eicke T. 'Big Data': The ECtHR as facilitator or guardian? Lecture 2018 – Lincoln's Inn, 29 November 2018. § 15–16.
28. Woods L. 'Social media: it is not just about Article 10 // UNSPECIFIED Edward Elgar / eds. by D. Mangan, L.E. Gillies. 2017. 154 p.
29. Case C-131/12 Google Spain SL, Googl eInc. V Agencia Espahiolade Protecci6n de Datos (Aepd), M. Costeja Gonzdlez (European Court of Justice Grand Chamber 13 May 2014).
30. EU Cybersecurity Act. URL: http://europa.eu/rapid/press-release_IP-17-3193_en.htm (дата обращения: 01.11.2019).
31. ECtHR. Delfi AS v. Estonia, 64569/09, 16/06/2015.
32. Спано Р. Ответственность информационного посредника за комментарии онлайн-пользователя в контексте Европейской Конвенции по правам человека // Международное правосудие. 2017. № 2 (22). С. 28–41.
33. Woods L. Delfi v Estonia: Curtailing online freedom of expression? 2015. URL: http://eulawanalysis.blogspot.com/2015/06/delfi-v-estonia-curtailing-online.html (дата обращения: 01.11.2019).
34. Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных (принята в г. Страсбурге 28.01.1981). URL: https://www.coe.int/ru/web/conventions/full-list/-/conventions/treaty/108 (дата обращения: 01.11.2019).
35. LOI n 2015-912 du 24 juillet 2015 relative au renseignement. URL: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000030933629&dateTexte=20180930 (дата обращения: 01.11.2019).
36. Hornung G., Schnabel C. Data Protection in Germany I: The Population Census Decision and the Right to Informational Self-Determination // Computer Law & Security Review. 2009. Vol. 25. P. 84–88.
37. Cole D., Fabbrini F. Bridging the transatlantic divide? The United States, the European Union, and the protection of privacy across borders // International Journal of Constitutional Law. 2016. Vol. 14. P. 220–237.
38. European Commission v Federal Republic of Germany, C-518/07, EU:C:2010:125.
39. Lynskey O. The 'Europeanisation' of Data Protection Law // Cambridge Yearbook of European Legal Studies. 2017. Vol. 19. P. 252–286.
40. Решение Совета глав правительств СНГ «О Концепции информационной безопасности государств – участников Содружества Независимых Государств в военной сфере» (Принято в г. Минске 04.06.1999). URL: https://www.lawmix.ru/abrolaw/8896
41. Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в области обеспечения информационной безопасности от 20 ноября 2013 года. URL: http://docs.cntd.ru/document/420278452 (дата обращения: 10.01.2020).
42. Соглашение между правительствами государств – членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности от 16 июня 2009 года. URL: http://docs.cntd.ru/document/902289626 (дата обращения: 10.01.2020).
43. Рекомендация Коллегии Евразийской экономической комиссии от 21.11.2017 № 27 «Об Общих подходах к проведению государствами – членами Евразийского экономического союза согласованной политики в сфере защиты прав потребителей при реализации товаров (работ, услуг) дистанционным способом» // СПС КонсультантПлюс.
44. Федеральный закон от 6 июля 2016 г. № 374-ФЗ «О внесении изменений в ФЗ "О противодействии терроризму" и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» // Российская газета. 2016. 8 июля (№ 149).

Статья представлена научной редакцией «Право» 13 февраля 2020 г.

International Legal Issues of Realization of the Right to Data Protection: Problems and Trends

Vestnik Tomskogo gosudarstvennogo universiteta – Tomsk State University Journal, 2020, 454, 233–243.
DOI: 10.17223/15617793/454/29

Tigran D. Oganesian, Institute of Legislation and Comparative Law Under the Government of the Russian Federation (Moscow, Russian Federation). E-mail: t.oganesian@mail.ru

Keywords: protection of personal data; mass surveillance; confidentiality; right to respect for privacy; Internet; Council of Europe; European Court of Human Rights; Court of Justice of the European Union; Convention 108.

There is a particular need to rethink the nature of the right to data protection and to develop new standards of international protection against relevant abuses in connection with the use of new information and communication technologies. The article aims to analyze the different approaches to the study of the nature of the right to data protection in the context of the right to respect for private life; to identify the appropriateness of allocation of the right to data protection as an independent and separate right; to determine trends in the development of case law and the current legal position of some national courts, the European Court of Human Rights, and the Court of Justice of the European Union in the field of data protection. The analysis of the international legal framework of doctrinal research and of the legal positions of national and international courts on data protection showed that the importance of data protection in terms of Internet development and the new transnational ways of data collecting and processing that the entire international community has not yet had to face dictate the need for continued development and improvement of international and national standards of data protection. Here, the ECHR and the CJEU are of particular importance as they play a leading role in the progressive development of European case law in this area. At the same time, based on the analysis of the ECHR case law, it can be concluded that the ECHR, in its decisions of recent years, departs from a rigid approach, giving more freedom to states in the implementation of mass surveillance. It is concluded that today the right to protection of personal data is in an intermediate state: it can no longer be fully considered either as part of the right to respect for private life, or as a full and independent right. As a matter of urgency, states should review their own national laws, policies and practices to ensure that they fully comply with the data protection standards developed by the Council of Europe and the EU. In order to improve the standards of the national legal system and establish sufficient safeguards in the field of data protection, it is recommended that the new provisions of Convention 108+ be ratified and implemented. It is noted that the current system of data protection in the EU allows states to limit the right to data protection for broad reasons of national security and law enforcement. Particular attention should also be paid to the establishment of a single system of independent bodies among all the Council of Europe member states to effectively oversee any activities of the intelligence services and law enforcement agencies that violate privacy.

REFERENCES

1. Benyekhlef, K. (1996) Les normes internationales de protection des données personnelles et l'autoroute de l'information. In: *Les Journées Maximilien-Caron: Le respect de la vie privée dans l'entreprise*. Thémis. pp. 65–105.
2. Gonzalez Fuster, G. (2016) *The Emergence of Personal Data Protection as a Fundamental Right of the EU*. Springer International Publishing.
3. Hustinx, P.J. (2005) Data protection in the European Union. *Privacy & Informatie*. pp. 62–65.
4. ECtHR. (2019) *López Ribalda and Others v. Spain (applications nos. 1874/13 and 8567/13*). 17.10.2019.
5. UN Human Rights Committee. (2013) *CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation.* 8 April 1988, HRI/GEN/1/Rev.9 (Vol. I). [Online] Available from: https://www.globalhealthrights.org/wp-content/uploads/2013/10/General-Comment-16-of-the-Human-Rights-Committee.pdf. (Accessed: 10.01.2020).
6. UN. (2013) *Rezolyutsiya 68/167, prinyataya General'noy Assambleey 18 dekabrya 2013 goda. Pravo na neprikosnovennost' chastnoy zhizni v tsifrovuyu epokhu* [The Right to Privacy in the Digital Age: Resolution 68/167 Adopted by the General Assembly on 18 December 2013]. [Online] Available from: https://undocs.org/A/RES/68/167. (Accessed: 10.01.2020).
7. UN Human Rights Committee. (2013) *General Comment No. 16 Article 17 (The right to respect of privacy, family, home and correspondence, and protection of honour and reputation) (No. 3 & 8)*. [Online] Available from: https://www.globalhealthrights.org/wp-content/uploads/2013/10/General-Comment-16-of-the-Human-Rights-Committee.pdf. (Accessed: 10.01.2020).
8. UN Human Rights Committee. (2020) *Doklad za 2019 god Spetsial'nogo dokladchika OON po pravu na neprikosnovennost' chastnoy zhizni* [UN Special Rapporteur on the right to privacy: An annual report]. [Online] Available from: https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/AnnualReports.aspx. (Accessed: 10.01.2020).
9. UN Human Rights Committee. (2014) *Doklad Upravleniya Verkhovnogo komissara OON po pravam cheloveka po voprosu o prave na neprikosnovennost' chastnoy zhizni v tsifrovoy vek (A/HRC/27/37)* [Report of the Office of the United Nations High Commissioner for Human Rights: The Right to Privacy in the Digital Age (A/HRC/27/37)]. [Online] Available from: https://www.ohchr.org/RU/Issues/DigitalAge/Pages/ ReportDigitalAge.aspx. (Accessed: 10.01.2020).
10. Legifrance. (2020) *Loi № 78-17 du 6 janvier 1978 relative à l'inform atique, aux fichiers et aux libertés*. [Online] Available from: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006068624& dateTexte=vig. (Accessed: 12.09.2019).
11. Lessig, L. (2006) *Code: Version 2.0*. New York: Basic Books.
12. Mitsilegas, V. (2015) The Transformation of Privacy in an Era of Pre-emptive Surveillance. *Tilburg Law Review*. 20. pp. 35–37.
13. Statista. (2019) *The most surveilled city in Europe.* [Online] Available from: https://www.statista.com/chart/19268/most-surveilled-cities-in-europe/. (Accessed: 01.11.2019).
14. EC. (2006) *Council Directive 2006/24/ec of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/ec Art. 3 (1)*.
15. Vermeulen, M. & Bellanova, R. (2013) European 'smart' surveillance: What's at stake for data protection, privacy and non-discrimination? *Security and Human Rights*. 4. pp. 297–311.
16. Wright, D. (2010) Sorting out Smart Surveillance. *Computer Law & Security Review*. 26, (4). pp. 342–361.
17. EU. (2004) *Article 29 Data Protection Working Party. Declaration of the Article 29 Working Party on Enforcement*. [Online] Available from: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2004/wp101_en.pdf. (Accessed: 01.11.2019).
18. ECtHR. (2003) *Perry vs United Kingdom*. 17 July 2003.
19. Jervis, C. (2018) Barbulescu v Romania: Why There is No Room for Complacency When it Comes to Privacy Rights in the Workplace. *Industrial Law Journal*. 47 (3). pp. 440–453.
20. ECtHR. (2017) *Barbulescu v. Romania*. 05 September 2017.
21. Gursel, I. (2016) Protection of Personal Data in International Law and the General Aspects of the Turkish Data Protection Law. *Dokuz Eylul Universitesi Hukuk Fakultesi Dergisi.* 18. pp. 33–62.
22. Baran, P. (1967) The Future Computer Utility. *National Affairs*. 43. pp. 75–87.
23. Jernigan, C. & Mistre, B.F. (2009) *Gaydar: Facebook Friendships Expose Sexual Orientation*. Oct. 5. [Online] Available from: https://firstmonday.org/ojs//index.php/fm/article/view/2611. (Accessed: 01.11.2019).
24. Merrill, J. (2016) Liberal, Moderate or Conservative? See How Facebook Labels You. *N.Y. TIMES*. Aug. 23. [Online] Available from: https://www.nytimes.com/2016/08/24/us/politics/facebook-ads-politics.html. (Accessed: 01.11.2019).
25. Constine, J. (2017) *Facebook Rolls Out AI to Detect Suicidal Posts Before They're Reported*. Nov. 27. [Online] Available from: https://techcrunch.com/2017/11/27/facebook-ai-suicide- prevention/?guccounter=1. (Accessed: 01.11.2019).
26. Cook, J. (2018) Amazon Patents New Alexa Feature That Knows When You're Ill and Offers You Medicine. *TELEGRAPH*. Oct. 9. [Online] Available from: https://www.telegraph.co.uk/technology/2018/10/09/amazon-patents-new-alexa-feature-knows-offers-medicine/. (Accessed: 01.11.2019).

27. Eicke, T. (2018) *'Big Data': The ECtHR as facilitator or guardian?* Lecture 2018 – Lincoln's Inn, 29 November 2018. § 15–16.
28. Woods, L. (2017) Social media: it is not just about Article 10. In: Mangan, D. & Gillies, L.E. (eds) *The Legal Challenges of Social Media*. Edward Elgar. pp. 104–124.
29. European Court of Justice Grand Chamber. (2014) *Case C-131/12 Google Spain SL, Googl eInc. V Agencia Espahiolade Proteccion de Datos (Aepd), M. Costeja Gonzdlez.* 13 May 2014.
30. EU. (2017) *EU Cybersecurity Act*. [Online] Available from: http://europa.eu/rapid/press-release_IP-17-3193_en.htm. (Accessed: 01.11.2019).
31. ECtHR. *Delfi AS v. Estonia, 64569/09.* 16 June 2015.
32. Spano, R. (2017) Otvetstvennost' informatsionnogo posrednika za kommentarii onlayn-pol'zovatelya v kontekste Evropeyskoy Konventsii po pravam cheloveka [Responsibility of the Information Intermediary for the Comments of the Online User in the Context of the European Convention on Human Rights]. *Mezhdunarodnoe pravosudie*. 2 (22). pp. 28–41.
33. Woods, L. (2015) *Delfi v Estonia: Curtailing online freedom of expression?* [Online] Available from: http://eulawanalysis.blogspot.com/2015/06/delfi-v-estonia-curtailing-online.html. (Accessed: 01.11.2019).
34. Council of Europe. (1981) *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.* [Online] Available from: https://www.coe.int/ru/web/conventions/full-list/-/conventions/treaty/108. (Accessed: 01.11.2019). (In Russian).
35. Legifrance. (2015) *Loi n 2015-912 du 24 juillet 2015 relative au renseignement.* [Online] Available from: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte= LEGITEXT000030933629&dateTexte=20180930. (Accessed: 01.11.2019).
36. Hornung, G. & Schnabel, C. (2009) Data Protection in Germany I: The Population Census Decision and the Right to Informational Self-Determination. *Computer Law & Security Review*. 25. pp. 84–88.
37. Cole, D. & Fabbrini, F. (2016) Bridging the transatlantic divide? The United States, the European Union, and the protection of privacy across borders. *International Journal of Constitutional Law*. 14. pp. 220–237.
38. Grand Chamber. (2010) *European Commission v Federal Republic of Germany, C-518/07, EU:C:2010:125*.
39. Lynskey, O. (2017) The 'Europeanisation' of Data Protection Law. *Cambridge Yearbook of European Legal Studies*. 19. pp. 252–286.
40. Lawmix.ru. (1999) *Reshenie Soveta glav pravitel'stv SNG "O Kontseptsii informatsionnoy bezopasnosti gosudarstv – uchastnikov Sodruzhestva Nezavisimykh Gosudarstv v voennoy sfere" (Prinyato v g. Minske 04.06.1999)* [Decision of the Council of the Heads of Government of the CIS "On the Concept of Information Security of the Member States of the Commonwealth of Independent States in the Military Sphere" (Adopted in Minsk on 04.06.1999)]. [Online] Available from: https://www.lawmix.ru/abrolaw/8896.
41. Docs.cntd.ru. (2013) *Soglashenie o sotrudnichestve gosudarstv – uchastnikov Sodruzhestva Nezavisimykh Gosudarstv v oblasti obespecheniya informatsionnoy bezopasnosti ot 20 noyabrya 2013 goda* [Treaty on Cooperation of the Member States of the Commonwealth of Independent States in the Field of Information Security of November 20, 2013]. [Online] Available from: http://docs.cntd.ru/document/420278452. (Accessed: 10.01.2020).
42. Docs.cntd.ru. (2009) *Soglashenie mezhdu pravitel'stvami gosudarstv – chlenov Shankhayskoy organizatsii sotrudnichestva o sotrudnichestve v oblasti obespecheniya mezhdunarodnoy informatsionnoy bezopasnosti ot 16 iyunya 2009 goda* [Treaty Between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security of June 16, 2009]. [Online] Available from: http://docs.cntd.ru/document/902289626. (Accessed: 10.01.2020).
43. Consultant Plus. (2017) *Recommendation of the Board of the Eurasian Economic Commission No. 27 of November 21, 2017, "On General Approaches to the Implementation by the Member States of the Eurasian Economic Union of a Consolidated Policy in the Sphere of Consumer Rights Protection in the Realization of Goods (Work, Services) Remotely"*. [Online] Available from: http://www.consultant.ru/document/cons_doc_LAW_283378/. (In Russian).
44. *Rossiyskaya gazeta.* (2016) Federal'nyy zakon ot 6 iyulya 2016 g. № 374-FZ "O vnesenii izmeneniy v FZ "O protivodeystvii terrorizmu" i otdel'nye zakonodatel'nye akty Rossiyskoy Federatsii v chasti ustanovleniya dopolnitel'nykh mer protivodeystviya terrorizmu i obespecheniya obshchestvennoy bezopasnosti" [Federal Law No. 374-FZ of July 6, 2016, "On Amendments to the Federal Law 'On Countering Terrorism' and Certain Legislative Acts of the Russian Federation Regarding the Establishment of Additional Counter-Terrorism Measures and Ensuring Public Safety"]. 8 July. 149.

Received: 13 February 2020