О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ КАК ИНСТИТУТЕ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ КИБЕРБЕЗОПАСНОСТИ НА ПРИМЕРЕ ПРОЕКЦИИ ОТДЕЛЬНЫХ МЕЖДУНАРОДНЫХ ОРГАНИЗАЦИЙ

ГОНТАРЬ Людмила Олеговна, соискатель Института законодательства и сравнительного правоведения при Правительстве Российской Федерации, советник Департамента нормативно-правового регулирования науки и образования Министерства науки и высшего образования Российской Федерации

Россия, 117218, г. Москва, ул. Большая Черемушkinsкая, 34

E-mail: cambridge.gontar@gmail.com

В условиях развития информационных технологий актуальна проблема международной информационной кибербезопасности и поиска правовых решений для надлежащего обеспечения гарантий в создающемся информационном обществе. В статье дан анализ защиты персональных данных как ключевого института международной информационной кибербезопасности, во многом предопределяющего концептуальные начала данной подотрасли, что имеет практико-ориентированное значение, продиктованное необходимостью углубленного изучения международной информационной кибербезопасности и возможностью дальнейшей разработки теоретико-практических правовых рекомендаций по данной проблеме. Рассматривается практика Европейского суда по правам человека. Затрагивается так называемый эффект Сноудена, вызвавший бурную реакцию законодателей различных государств, а также трансформацию в международную проблему. Уяснение направления, являющегося актуальным на международном уровне в сфере реализации международной информационной кибербезопасности, отсылает к пониманию информационного общества и другим концептуальным вопросам. Проанализировано показательное дело “Big Brother Watch”, в котором более четко демонстрируется позиция Европейского суда по правам человека в отношении массовой слежки и предпринимаются попытки предложить правовые средства защиты. Данное решение отсылает к более глобальной проблеме радиоэлектронной борьбы, что придает значимость институту защиты персональных данных. В нашей статье содержится синтез теоретических и практических подходов, позволяющих утверждать о существовании и динамике института защиты персональных данных в рамках подотрасли права международной информационной кибербезопасности.

Ключевые слова: институт защиты персональных данных, Конвенция о защите физических лиц при автоматизированной обработке персональных данных (Конвенция 108), информационное общество, информационные права, Европейский суд по правам человека, эффект Сноудена.

Для цитирования: Гонтарь Л. О. О защите персональных данных как институте международной информационной кибербезопасности на примере проекции отдельных международных организаций // Журнал зарубежного законодательства и сравнительного правоведения. 2020. № 1. С. 74—86. DOI: 10.12737/jflcl.2020.002

ON PERSONAL DATA AS AN INSTITUTE OF INTERNATIONAL INFORMATION CYBERSECURITY IN THE PROJECTION OF INTERNATIONAL ORGANIZATIONS

L. O. GONTAR, Institute of Legislation and Comparative Law under the Government of the Russian Federation, Moscow 117218, Russian Federation

E-mail: cambridge.gontar@gmail.com

In the context of the development of information technologies, one often encounters the problem of international information cyber security and seeks legal solutions to ensure adequately guarantees in the emerging information society. The article proposes to analyze the protection of personal data as a key institution of international information cyber security, which will determine the concept of this sub-sector. Understanding the protection of personal data as an institution of the aforementioned sub-industry is of practical importance. It is dictated by the need to study international information cyber security and the actual possibility for further development of theoretical and practical legal recommendations. The article includes cases and theoretical and practical conclusions on them. It touches on the case of the “Snowden effect”, which marked the beginning of a violent reaction of legislators in various states to these changes, as well as its transformation into an international problem. It is important to understand in which direction it is relevant at the international level in the implementation of international information cyber security, which refers us to an understanding of the information society and other conceptual issues. In addition to this, the article analyzes the case study “Big Browser Watch”, which demonstrates more clearly the position of the European Court of Human Rights regarding mass

surveillance and attempts made to offer legal remedies. This solution also refers to the more global problem of “electronic warfare”, which in fact attaches importance to the institution of personal data protection. The article contains a synthesis of theoretical and practical approaches which allow us to argue about the existence and dynamics of the personal data protection institution within the framework of the sub-branch of international cyber information security law.

Keywords: institute for the protection of personal data, Convention 108, information society, information rights, European Court of Human Rights, Snowden effect.

For citation: Gontar L. O. On Personal Data as an Institute of International Information Cybersecurity in the Projection of International Organizations. *Zhurnal zarubezhnogo zakonodatel'stva i sravnitel'nogo pravovedeniya* = *Journal of Foreign Legislation and Comparative Law*, 2020, no. 1, pp. 74—86. DOI: 10.12737/jflcl.2020.002 (In Russ.)

«Лишение свободы, использующее механизмы надзора и наказания, действует, напротив, в соответствии с принципом относительной непрерывности. Непрерывность самих институтов, которые отсылают друг к другу (государственная помощь и сиротский дом, исправительные заведения, каторга, дисциплинарный батальон, тюрьма; школа и благотворительное общество, мастерская, дом призрения, пенитенциарный монастырь; рабочий городок, больница и тюрьма). Непрерывности критериев и механизмов наказания, которые, начиная с простого отклонения, постепенно ужесточают правила и утяжеляют наказание. Непрерывной градации органов власти, институционализированных, специализированных и компетентных (в порядке знания и порядка власти), которые, не прибегая к произволу, а в строгом соответствии с правилами, посредством констатации и оценки устанавливают иерархию, дифференцируют, санкционируют, наказывают и постепенно переходят от санкции против отклонения к наказанию преступления»¹.

Мишель Фуко

В условиях развития информационных технологий, новых технологических проектов, таких как Big Data², все более актуальным вопросом выступает информационная кибербезопасность. Данная тема обусловлена стремлением государств как можно тщательнее защитить свое информационное киберпространство, в которое входит и Интернет. Государства создают доктрины информационной кибербезопасности³, прорабатывают вопросы отдельных институтов, таких как государственная тайна, защита персональных данных (в том числе биометрических данных), защита от вирусов и вирусных программ (в ракурсе законодательных и правоприменительных средств) и т. д. Также широко обсуждается вопрос прав человека в Интернете, а именно рассматривается право на доступ к Интернету с различных точек зрения, например в контексте права на информацию и связь, гарантированного конституциями в

государствах или закрепленного в специальном законодательстве⁴.

Недавно проходила конференция на тему «Конвенция 108+: лучшие практики защиты в цифровой среде», на которой генеральный секретарь Совета Европы Турбьёрн Ягланд подчеркнул, что быть частью Конвенции 108+ не означает быть частью какого-то «клуба» по гармонизации защиты данных или обсуждения высоких стандартов в области защиты данных, это прежде всего некое «обязательство» сторон работать вместе в части соблюдения текста Конвенции и других важных опций, которые оговариваются в данном документе. Тем более что в условиях «цифрового мира» стороны должны быть готовыми к быстро развивающимся переменам информационной трансформации⁵. На наш взгляд, следует обратить пристальное внимание на данные слова, так как речь идет о некоем «живом международном обязательстве», которое обозначено крайне широко, но актуально и необходимо. Это объясняется сложным процессом взаимодействия права и технологий, становления международной информационной кибербезопасности.

Право на доступ к Интернету более подробно описывается в резолюции Парламентской ассамблеи Совета Европы 1987 г. (2014) «Право на доступ к Интер-

¹ Фуко М. Надзирать и наказывать. Рождение тюрьмы. М., 2019. С. 366. М. Фуко демонстрирует наблюдения, которые, пожалуй, любопытно перенести посредством проецирования на реально существующие правовые казусы. Посредством данной методики можно прийти к самым неочевидным выводам.

² См.: Working Paper on Big Data and Privacy principles under pressure in the age of Big Data analytics International Working Group on Data Protection in Telecommunications. 55th Meeting, 5—6 May 2014, Skopje.

³ См., например: National Cyber Strategy of the United States of America 2018; Доктрину информационной безопасности Российской Федерации, утв. Указом Президента РФ от 5 декабря 2016 г. № 646; The UK Cyber Security Strategy Protecting and promoting the UK in a digital world. 2011.

⁴ См.: Шатилина А. С. Права человека в Интернете: проблема признания права на доступ к Интернету // Прецеденты Европейского суда по правам человека. 2018. № 1 (49). С. 38.

⁵ См.: Convention 108+: better protecting us in the digital era (материалы конференции и речь Генерального секретаря). URL: <https://www.coe.int/en/web/data-protection/conference-on-convention-108> (дата обращения: 12.08.2019).

нету» от 9 апреля 2014 г.⁶ Условно можно выделить несколько важных моментов из текста резолюции:

каждый имеет право на доступ к Интернету;

право на доступ к Интернету дифференцируется на составные части: право доступа, получения и распространения информации и идей в Интернете без вмешательства со стороны публичных органов, независимо от границ и с учетом ограничений, установленных ст. 10 Европейской конвенции, ввиду важности Интернета для демократических обществ (любые такие ограничения должны быть ясно и узко определены);

провайдеры, обеспечивающие доступ к Интернету и пользование им, должны соблюдать требования к универсальным услугам, установленные ООН и Европейским Союзом;

всеобщая доступность минимального качества интернет-услуг и доступа к Интернету относится к совместной ответственности государств-членов и провайдеров услуг;

не должно существовать дискриминации при обращении с данными и трафиком Интернета, основанной на техническом обеспечении, контенте, авторе, происхождении или назначении контента, сервисе или приложении, тем самым должен обеспечиваться сетевой нейтралитет в соответствии с внутригосударственным законодательством;

государствам-членам следует обязать публичные органы предоставлять открытый доступ к своей информации и услугам через Интернет, многоязычный доступ к Интернету, насколько это возможно, должен быть публичной целью.

Резолюция затрагивает множество проблем, связанных с доступом к Интернету, и, по сути, носит универсальный характер, перечисляя по пунктам, что необходимо сделать. Бесспорно, важным моментом является разделение «права на доступ к Интернету» на элементы (т. е. конкретные виды прав, благодаря которым соответствующие отношения регулируются).

Даже на данном периоде развития информационной кибербезопасности можно выделить несколько сценариев развития:

концепция информационного общества, которая позволит Deep Web и Dark Web⁷ объединиться и стать открытыми, правовое регулирование будет сведено к минимуму, а потом наступит правовая ликвидация (т. е. отсутствие необходимости в правовом регулировании);

концепция закрытых систем, по типу ARPANET⁸ (изначально была представлена в качестве самостоя-

тельной закрытой интернет-сети, в большей мере реализующей военное снабжение);

концепция информационно-золотой середины, при которой правовое регулирование допускается на уровне Deep Web (т. е. полуоткрытое пространство Интернета, которое частично можно идентифицировать) и с большой вероятностью будет отсутствовать на уровне Dark Web (т. е. полностью закрытое интернет-пространство, проникновение в которое практически неосуществимо).

Данные сценарии развития позволяют подойти к проблеме прогностически и выработать определенную систему правовых ценностей, на которую можно опираться, например, при оценке института защиты персональных данных.

На международном уровне развитие вышеназванных институтов обеспечивается международными организациями. Практика в рамках международных организаций не является однообразной и содержит множество институтов международной информационной кибербезопасности. Например, Международный союз электросвязи (МСЭ) предлагает любопытные пути международно-правового регулирования.

Так, Группой кибербезопасности (подразделение МСЭ) был подготовлен доклад «Глобальный индекс кибербезопасности»⁹. Данный индекс представляет собой усовершенствованную эталонную модель, состоящую из конкретных показателей, целью которой является сравнение уровня обязательств государств — членов МСЭ в области кибербезопасности. Основными задачами данного индекса выступают: определение типа, уровня и эволюции обязательств в области кибербезопасности в странах; преодоление разрыва в кибербезопасности и др.

Индекс содержит собственную методологию, состоящую из 25 показателей и 157 вопросов¹⁰. Показатели вырабатываются на основании таких критериев, как актуальность; наличие и качество данных; возможность перекрестной проверки через вторичные данные. Также в документе по данному индексу приводится схема «дерева развития кибербезопасности», в результате изучения данных на этом чертеже рождаются бинарные возможности ответа. Философия документа такова, что технические факторы здесь значительно упрощаются.

Индекс является не единственным документом, который позволяет провести оценку информационной кибербезопасности.

Международный союз электросвязи и Европейский Союз запустили в декабре 2008 г. несколько проектов. Например, проект, направленный на оказание поддержки согласованной политике и законо-

⁶ См.: Прецеденты Европейского суда по правам человека. 2018. № 1 (49). С. 91—92.

⁷ См.: *Ciancaglini V., Balduzzi M., McArdle R., Rösler M.* Below the Surface: Exploring the Deep Web // Trend Micro. 2018.

⁸ См.: *Denning P. J.* The ARPANET after Twenty Years // American Scientist. 1989. Vol. 77. P. 530—535.

⁹ Global Cybersecurity Index (GCI) 2017. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf (дата обращения: 02.04.2018).

¹⁰ Там же.

дательству в области информационно-компьютерных технологий (ИКТ)¹¹. В частности, для каждого из быстроразвивающихся регионов (Африка, Карибский бассейн, Тихоокеанские острова) предусматривается индивидуальный подход, учитывающий конкретные потребности: повышение конкурентоспособности в Карибском бассейне путем гармонизации политики, законодательства и регламентации ИКТ; поддержка согласования политики в области ИКТ в странах Африки к югу от Сахары; наращивание потенциала и политика в области ИКТ; нормативные и законодательные рамки поддержки тихоокеанских островных стран. Этот проект ориентирован на информационные технологии.

С мая 2011 г. МСЭ и Управление ООН по наркотикам и преступности (ЮНОДК) сотрудничают в глобальном масштабе для оказания помощи государствам-членам в снижении рисков, связанных с киберпреступностью, с целью обеспечения безопасного использования информационных и коммуникационных технологий¹². Принятый ими совместный меморандум требует наличия экспертных знаний и ресурсов для создания правовых мер и законодательных рамок на национальном уровне в рамках принципа международного сотрудничества на благо всех стран мира. Согласно меморандуму реализуются следующие направления:

ЮНОДК/МСЭ могут предоставить странам оценку институциональных возможностей и национальных нормативных рамок, применимых в борьбе с киберпреступностью. В зависимости от характера просьбы и ситуации в соответствующей стране такие обзоры могут быть сосредоточены на конкретных аспектах (например, возможностях высокотехнологичных преступных подразделений) или проводиться в виде полного обзора, включая все соответствующие области предотвращения киберпреступлений, расследования и преследования;

ЮНОДК/МСЭ обеспечивает наращивание потенциала и подготовку кадров, связанных с различными аспектами киберпреступности для различных аудиторий и в течение ряда сроков. Тренировочные занятия могут проходить в разных формах — от двухчасовой вводной презентации о глобальной или региональной ситуации с киберпреступностью до трехнедельного углубленного учебного курса для правоохранительных органов. Такие учебные занятия должны охватывать правовые, а также технические аспекты борьбы с киберпреступностью.

ЮНОДК/МСЭ тесно сотрудничает с академическими учреждениями, которые предоставляют сертифицированные учебные и академические программы и др.

Таким образом, наблюдаются постепенные попытки реализации правового мониторинга, который охватывает не собственно технический прогресс, но анализ законодательств государств в сфере регламентации проблем киберинформационной безопасности.

На уровне Совета Европы данный институт закреплен в Конвенции о защите физических лиц при автоматизированной обработке персональных данных 1981 г. (ETS № 108)¹³ (далее — Конвенция 108). Конвенция рассматривает следующие важные вопросы:

1) определение понятий «персональные данные» (ст. 2) (всякая информация, используемая для идентификации и для идентифицируемых данных), «обработка персональных данных», т. е. любая операция для структурирования или передачи данных, и др.;

2) выделение специальных категорий данных (ст. 6): генетических, персональных данных, относящихся к правонарушениям, биометрических, персональных данных о расовом или этническом происхождении, политических убеждениях, членстве в профсоюзах, религиозных и иных убеждениях, сексуальной жизни;

3) определение задачи защиты данных (ст. 7) — устранение рисков неавторизованного доступа к данным и входу в систему;

4) закрепление вопроса о трансграничном потоке персональных данных (ст. 14): стороны, исходя из общих целей безопасности и защиты персональных данных, вправе запретить или установить специальное разрешение на передачу данных получателю, который находится под юрисдикцией другого государства.

Протокол о внесении изменений в Конвенцию 108 2018 г.¹⁴ внес множество поправок, в частности:

1) проведена коррекция в части статьи, где закрепляется цель Конвенции 108: «Цель настоящей Конвенции состоит в обеспечении защиты каждого физического лица, независимо от его гражданства или места жительства, при обработке его персональных данных, тем самым способствуя уважению его прав и основных свобод, в том числе права на неприкосновенность частной жизни...»;

2) в части терминологии уточняется термин «контролер базы данных», под которым понимаются «фи-

¹¹ См.: Support for the Establishment of Harmonized Policies for the ICT Market in the ACP States. 2008. URL: <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Legal-Measures.aspx> (дата обращения: 01.04.2018).

¹² См.: Memorandum of understanding ITU/UNODC. 2011. URL: <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/UNODC.aspx> (дата обращения: 07.03.2018).

¹³ Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data. 1981. URL: <https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regard-to-the-automatic-processing-of-personal-data/16808b36f1> (дата обращения: 23.06.2019).

¹⁴ Протокол о внесении изменений в Конвенцию о защите физических лиц при автоматизированной обработке персональных данных (ETS № 223) // Бюллетень Европейского суда по правам человека. 2018. № 12. С. 102—111.

зическое лицо или юридическое лицо, орган государственной власти, учреждение или любой другой орган, которые самостоятельно или совместно с другими лицами/органами обладают полномочиями на принятие решений по обработке данных»; вводятся понятия «реципиент» т. е. физическое или юридическое лицо, орган государственной власти, учреждение или любой другой орган, которым персональные данные раскрываются или предоставляются в доступ, и «процессор» — «физическое лицо или юридическое лицо, орган государственной власти, учреждение или любой другой орган, которые обрабатывают персональные данные по поручению контролера...»;

3) законность обработки персональных данных (ст. 5) рассматривается через призму следующих признаков:

- соразмерность обработки персональных данных и преследуемые законом цели, которые должны отражаться на всех стадиях обработки;

- осуществление обработки персональных данных на основе свободы, информативности при ясном согласии субъекта;

- обязанность производить обработку персональных данных исключительно по законодательству;

- адекватность и нечрезмерность обработки данных по отношению к субъекту персональных данных;

- точность и подверженность данных обновлению;

- обеспечение контролеру и, где это применимо, процессору возможности принять необходимые меры безопасности против рисков, таких как случайный или несанкционированный доступ к персональным данным, их повреждение, потеря, несанкционированное использование, изменение или раскрытие (ст. 7);

- установление важного нормативного условия (ст. 14): любая сторона исключительно в целях защиты персональных данных не запрещает и не требует получения особых разрешений для передачи таких данных реципиенту, который находится на территории другой Стороны Конвенции. Однако такая Сторона может создать ситуацию, при которой возникает риск того, что передача данных другой Стороне или от другой Стороны к государству, не являющемуся Стороной Конвенции, может привести к вероятности обхода положений Конвенции. Сторона Конвенции также может поступить подобным образом в случае, если она связана согласованными правилами защиты, разделяемыми государствами — участниками Конвенции, входящими в региональную международную организацию.

Таким образом, подобные изменения корректируют цель Конвенции 108 и позволяют с большей точностью произвести правовое измерение возможностей обеспечения защиты персональных данных, а также баланса между мерой правовой защиты и свободы в информационном пространстве.

Конвенция 108 является регулятором специального института (защиты персональных данных) и рассматривает ряд общих вопросов, механизм реализации защиты персональных данных, его задачи, а также трансграничности как свойства, которое является основным в условиях обмена данными в Интернете.

Представляется любопытной система правореализационных механизмов в отношении обеспечения защиты персональных данных. Среди них можно выделить три группы: 1) организационно-аппаратный механизм; 2) общая система международных мер, реализуемая на уровне государства; 3) судебный механизм.

Организационно-аппаратный механизм строится на функционирующем в соответствии с Конвенцией 108 Консультативном (конвенционном) комитете (ст. 22 и 23 Конвенции). К полномочиям Комитета относится:

- вынесение рекомендаций с целью эффективного применения Конвенции;

- внесение предложений о поправках в Конвенцию 108;

- выполнение исполнительных и методических функций и др.

Приведем в пример рекомендацию Комитета министров Совета Европы «О роли и ответственности интернет-посредников» 2018 г.¹⁵ Под интернет-посредниками понимается круг игроков, которые обмениваются информацией в Интернете между физическими и юридическими лицами, предлагают и выполняют различные функции. Основными функциями данных лиц являются подключение к Интернету, защита, обработка информации. Уникальность рекомендации заключается во включении практической информации из информационных кейсов, например американского кейса Shadow Brokers или Black Market Reloaded¹⁶. Так, скрытый веб-сайт “Opion” использовался для нелегальной продажи наркотиков и других запрещенных товаров (украденных кредитных карт и огнестрельного оружия). Группа людей, создавших данный сайт, была своего рода Т-командой, которая создавала и размещала рынок услуг, доступных ограниченному кругу лиц, выход на который обеспечивался предварительной договоренностью. Данные лица хотя и выступали интернет-игроками, однако поставляли нелегальную продукцию и использовали методы, подрывающие в том числе безопасное подключение к Интернету. В связи с этим рекомендация четко ставит перед игроками цель, которая заключается в эффективной защите в offline- и online-режимах.

¹⁵ Recommendation CM/Rec (2018)2 of the Committee of Ministers to member States on media pluralism and transparency of media ownership (Adopted by the Committee of Ministers on 7 March 2018 at the 1309th meeting of the Ministers' Deputies). URL: <https://rm.coe.int/1680790e13> (дата обращения: 24.06.2019).

¹⁶ См.: Buxton J., Bingham T. The Rise and Challenge of Dark Net Drug Markets. Policy Brief 7. January 2015.

Рекомендация Комитета министров Совета Европы «О защите данных, связанных со здоровьем» 2019 г.¹⁷ охватывает принципы обработки персональных данных, связанных со здоровьем, с целью обеспечения гарантий уважения прав и основных свобод каждого человека в части права на неприкосновенность частной жизни и защиту персональных данных о состоянии здоровья по мере необходимости. К вышеуказанным персональным данным рекомендация относит: данные о нерожденных детях; генетические данные; обмен данными, связанными со здоровьем, в целях предоставления и управления медицинским обслуживанием. Безусловно, данная информация является важной для учета в работе и формирования карточек гражданина в системе здравоохранения. Однако это не исключает правовые риск-факторы хранения данной информации.

В 2011 г. Комитет министров Совета Европы принял декларацию «О защите свободы выражения мнения и свободы объединения в связи с деятельностью частных интернет-платформ и провайдеров интернет-услуг»¹⁸, где справедливо отметил, что нарушение ст. 10 и 11 Конвенции 108 может быть вызвано политически мотивированным давлением, оказываемым на частные интернет-платформы и интернет-провайдеров, а также другими нападениями на интернет-сайты независимых средств массовой информации, правозащитников, диссидентов, информаторов и новых медийных акторов. В декларации отмечается, что вмешательство в контент, который создается для общественного достояния с помощью интернет-средств, или попытки сделать интернет-сайты недоступными должны рассматриваться в соответствии с международными стандартами, призванными обеспечить защиту свободы мнения и права на распространение и получение информации, в частности с положением ст. 10 Конвенции 108 и отнесимой прецедентной практикой ЕСПЧ.

Комитетом министров Совета Европы 30 марта 2016 г. принята стратегия СМ(2016)10 «Управление Интернетом» на 2016—2019 гг.¹⁹, которую условно можно разделить на следующие части:

1) вопросы построения демократии в Интернете (где рассматриваются такие вопросы, как электронная демократия и голосование, электронное правосудие и правосудие, отмечаются условия построения электронной демократии и, в частности, доступ к устойчивой цифровой культуре и подлинному цифровому контенту, к документам и информации публичного характера и т. д.);

2) защита основных прав человека в цифровом мире (риск-факторы при использовании интернет-пространства, средства защиты и анонимность, включая шифрование);

3) партнерство и взаимодействие (укрепление сотрудничества Совета Европы с заинтересованными сторонами — Европейским Союзом, Организацией по безопасности и сотрудничеству в Европе, Организацией экономического сотрудничества и развития и др.);

4) планирование, реализация и оценка Стратегии (подчеркивается, что главными акторами в ходе реализации данных действий будут соответствующие конвенционные и руководящие комитеты Совета Европы, а сети и платформы будут вспомогательным средством).

В Стратегии следует отметить уникальный термин — «цифровая гражданственность», под которой понимается осуществление и защита (охрана) демократических прав и обязанностей в цифровом пространстве (киберпространстве). Если анализировать данный термин с точки зрения концепции прав человека, то можно сделать вывод, что Стратегия постепенно выводит и новую доктрину прав человека — киберинформационные права.

Также следует обратить внимание на рекомендацию Комитета министров Совета Европы государствам-членам «О соблюдении, защите и осуществлении прав детей в цифровой среде» 2018 г.²⁰, основной целью которой является поиск баланса между гарантиями правовой защиты ребенка в цифровой среде, а также реализации его прав и свобод. Так, в документе подчеркивается, что в правовом регулировании следует уделить внимание «наилучшим интересам ребенка», которые являются точкой соприкосновения между «защитой» и «реализацией» прав ребенка в цифровой среде. Термин «цифровая среда» включает информационные и коммуникационные техноло-

¹⁷ Recommendation CM/Rec(2019)2 of the Committee of Ministers to member States on the protection of health-related data (Adopted by the Committee of Ministers on 27 March 2019 at the 1342nd meeting of the Ministers' Deputies). URL: https://www.apda.ad/sites/default/files/2019-03/CM_Rec%282019%292E_EN.pdf (дата обращения: 20.06.2019).

¹⁸ Декларация Комитета министров Совета Европы «О защите свободы выражения мнения и свободы объединения в связи с деятельностью частных интернет-платформ и провайдеров интернет-услуг» принята 7 декабря 2011 г. на 1129-м заседании // Прецеденты Европейского суда по правам человека. 2018. № 1. С. 93—94.

¹⁹ Прецеденты Европейского суда по правам человека. 2018. № 1. С. 95.

²⁰ Recommendation CM/Rec(2018)7 of the Committee of Ministers to member States on Guidelines to respect, protect and fulfil the rights of the child in the digital environment (Adopted by the Committee of Ministers on 4 July 2018 at the 1321 meeting of the Ministers' Deputies). URL: https://violenceagainstchildren.un.org/sites/violenceagainstchildren.un.org/files/documents/political_declarations/recomendation_of_the_committee_of_ministers_of_the_council_of_europe_to_member_states_on_guidelines_to_respect_protect_and_fulfil_the_rights_of_the_child_in_the_digital_environment.pdf (дата обращения: 19.06.2019).

гии, в том числе Интернет, мобильные и связанные с ними технологии и устройства, а также цифровые сети, базы данных, контент и услуги (раздел 1).

Основными правами ребенка в соответствии с рекомендацией являются:

право на доступ к цифровой среде и ее использование;

право на свободу выражения мнения и распространения информации;

право на представительство и на участие в играх, а также право на свободу собраний и ассоциаций (например, право на представительство через социальную сеть, средства массовой информации);

неприкосновенность частной жизни и защита данных;

право на образование (цифровая грамотность, образовательные программы и ресурсы);

право на защиту и безопасность (в связи с возможностями сексуальной эксплуатации и насилия, унижительного и стереотипного изображения, в частности чрезмерной сексуализации женщин и детей; издевательств, притеснений и иных форм домогательств; чрезмерного использования, лишения сна и причинения физического вреда в цифровой сфере), которое подразделяется на блоки:

меры по устранению рисков в цифровой среде;

меры по повышению уровня осведомленности;

меры, касающиеся материалов, связанных с сексуальным насилием в отношении детей, и др.

В рекомендации подчеркивается международный и национальный способы реализации мер защиты. Это в определенной степени позволяет гармонизировать подходы и осуществлять как защиту прав в цифровой среде, так и реализацию прав и основных свобод в цифровой среде.

Таким образом, на органы власти ложится обязанность информационного обмена, обеспечения защиты, в том числе от злоупотребления информацией. Данный механизм нацелен на процессуально-организационное обеспечение реализации Конвенции 108, что позволяет говорить о возможности дальнейшего процесса имплементации ее норм.

Вторым механизмом является общая система международных мер, реализуемая на уровне государств. Она подразделяется на следующие правоприменительные операции (ст. 16 Конвенции 108):

взаимный обмен между национальными органами различных государств;

помощь субъекту персональных данных вне зависимости от гражданства;

надзор органов за применением данных при запросе от собственного имени.

Помимо механизмов, предлагаемых Конвенцией 108, существует судебный механизм. Такой механизм обеспечивается Европейским судом по правам человека посредством применения на практике ст. 8 и 13 Европейской конвенции о защите прав че-

ловека и основных свобод 1950 г. (далее — Европейская конвенция).

Роль ЕСПЧ в решении вопросов относительно прав человека невозможно переоценить, так как он является органом международного правосудия и на протяжении долгих лет рассматривает дела относительно нарушений прав человека, закрепленных в Европейской конвенции. Как правильно отмечает профессор А. И. Ковлер: «Даже краткий экскурс в историю позволяет убедиться в том, что концепция органа международного правосудия формировалась столетиями и получила отклик в отечественной правовой науке, по крайней мере в умах масштабно мыслящих ее представителей»²¹.

Итак, остановимся подробно на судебном механизме защиты в ракурсе института защиты персональных данных.

Статья 8 Европейской конвенции гласит, что каждый имеет право на уважение его личной и семейной жизни, его жилища и его корреспонденции. Не допускается вмешательство со стороны публичных властей в осуществление этого права, за исключением случаев, когда такое вмешательство предусмотрено законом и необходимо в демократическом обществе в интересах национальной безопасности и общественного порядка, экономического благосостояния страны, в целях предотвращения беспорядков или преступлений, для охраны здоровья или нравственности, или защиты прав и свобод других лиц. В статье 13 говорится, что каждый, чьи права и свободы, признанные в Европейской конвенции, нарушены, имеет право на эффективное средство правовой защиты в государственном органе, даже если это нарушение было совершено лицами, действовавшими в официальном качестве.

Комбинация ст. 8 и 13 либо только ст. 8 Европейской конвенции используется для обоснования позиции: было совершено правонарушение в отношении персональных данных либо нет. Это подтверждается практикой рассмотрения дел в Европейском суде по правам человека²².

Так, дело «Роман Захаров против Российской Федерации»²³ касалось реализации секретного перехвата мобильной связи в России. Заявитель жаловался на то, что операторы сотовой связи в Российской Федерации в рамках закона устанавливают специальное оборудование, позволяющее правоохранитель-

²¹ Ковлер А. И. Европейская Конвенция в международной системе защиты прав человека. М., 2019. С. 232.

²² В конце статьи будет приводиться еще одно дело, в котором фигурирует ст. 10 Европейской конвенции, и это позволяет утверждать, что комбинации статей в области института защиты персональных данных могут быть различными. Однако это можно назвать «неклассической комбинацией» исходя из смысла, транслируемого в данной статье.

²³ Жалоба № 47143/06, 04.12.2015.

ным органам проводить соответствующие оперативно-розыскные мероприятия. ЕСПЧ пришел к выводу, что в нормативно-правовой базе имеются недостатки и мера государственного принуждения не может быть законной ввиду отсутствия каких-либо объективных фактов для ее применения. ЕСПЧ признал нарушение ст. 8 Европейской конвенции.

В деле *«Мустафа Танрикулу против Турции»*²⁴ заявитель жаловался на решение национального суда 2005 г., которым был узаконен перехват любой информации у любого лица в Турции, включая заявителя. По мнению ЕСПЧ, мера перехвата как форма государственного принуждения на тот момент являлась злоупотреблением со стороны органов власти. В дополнение к этому был установлен факт отказа в эффективном средстве судебной защиты. Таким образом, было признано нарушение ст. 8 и 13 Европейской конвенции.

В деле *«Вебер и Саравия против Германии»*²⁵ заявительница Г. Вебер (Уругвай) являлась независимым журналистом и расследовала вопросы, которые находятся в компетенции Федеральной разведывательной службы (новое вооружение, незаконный оборот наркотиков и т. д.). Второй заявитель С. Р. Саравия (Уругвай) работал сотрудником в городском совете Монтевидео, он отслеживал телефонные сообщения для Вебер, когда последняя выполняла задания, а затем отправлял ей. Заявители утверждали, что некоторые положения Закона «О борьбе с преступностью» нарушают их права, в частности право на тайную переписку, право на свободу слова и др. В этом решении ЕСПЧ проверил соответствие Европейской конвенции законодательства о «стратегическом мониторинге», позволявшего перехватывать телекоммуникации для целей выявления и предотвращения таких рисков, как, например, вооруженное нападение на ФРГ или террористический акт. В данном деле ЕСПЧ оценивал факт слежки как общую меру принуждения со стороны государства. И хотя Суд и не признал это «массовой слежкой», которая может нарушать ст. 8 Европейской конвенции, и признал жалобу явно необоснованной, тем не менее он суммировал некоторые критерии. Данные критерии могут применяться для оценки предсказуемости правовой базы, задачей которой является регулирование «тайной слежки».

В деле *«Либерти и другие против Соединенного королевства»*²⁶ рассматривался аналогичный случай, связанный с осуществлением Министерством обороны в 1990-е гг. массовых перехватов телефонных сообщений, факсимильных сообщений и электронной почты, которые передавались с помощью ра-

диосигналов между двумя станциями «Бритиш Телеком». ЕСПЧ признал, что право заявителей, закрепленное ст. 8 Европейской конвенции, было нарушено ввиду того, что власти Великобритании позволили неоправданно широко трактовать закон в части возможности перехвата тех или иных сообщений.

Дело *«"Биг Бразер Вотч" и другие против Великобритании»*²⁷ было следствием «откровения Эдварда Сноудена» о секретных службах, которые использовали информацию о персональных данных с целью реализации «эффективной» системы безопасности. Жалоба в ЕСПЧ была на массовый перехват сообщений, обмен разведывательными данными, получение данных связи от поставщиков услуг связи.

В деле рассматривались три различных типа наблюдения: массовый перехват сообщений; обмен разведанными данными и получение данных связи; отслеживание людей через GPS и запись разговоров. Отметим, что Суд опирался на дело Вебер и Саравия, при этом исключив из совокупности общих критериев, применимых к режиму массовой слежки, критерии о природе правонарушения и категории лиц, чьи сообщения могут перехватываться. В деле были рассмотрены оставшиеся четыре критерия: ограничение продолжительности перехвата данных; процедура, которая должна использоваться для проверки, использования и хранения полученных данных; меры предосторожности, которые должны быть приняты при передаче данных другим сторонам; обстоятельства, при которых перехваченные данные должны быть стерты или уничтожены.

Однако новеллой в решении стало расширение круга информации, перехватывание которой может составлять посягательство на ст. 8 Европейской конвенции, начиная с содержания сообщений до их метаданных. Конкретно это распространяется на картографирование социальных сетей, отслеживание местоположения, а также истории использования интернет-браузера, выявления паттернов коммуникации, равно как и инсайда о том, с кем происходило общение. Вывод ЕСПЧ о допустимости массовой слежки базировался на позиции Венецианской комиссии, признающей существенным вторжением в право на защиту частной жизни не сбор, а доступ и последующую работу с перехваченными данными. Суд признал позицию, изложенную Венецианской комиссией в докладе «О демократическом контроле за службами безопасности»²⁸, о радиоэлектронной разведке и возможности ее воздействия на права человека. Так, в докладе Комиссии было отмечено, что радиоэлектронная сфера недостаточно урегулирова-

²⁷ ECHR, Big Brother Watch and others v. the United Kingdom, 13.09.2018.

²⁸ Report on the Democratic oversight of the Security Services adopted by the Venice Commission at its 71st Plenary Session (Venice, 1—2 June 2007) CDL-AD(2007)016-e.

²⁴ ECHR, Mustafa Sezgin Tanrikulu v. Turkey, 18.07.2017.

²⁵ ECHR, Gabriele WEBER and Cesar Richard Saravia v. Germany, 29.06.2006.

²⁶ ECHR, Liberty and Others v. United Kingdom, 01.07.2008.

на правом, это неумолимо влечет ограничение права частной жизни и другого комплекса прав (которые подпадают под сферу наблюдения), поэтому государства — члены Совета Европы не должны ограничиваться исключительно выполнением стандартов, которые может устанавливать ЕСПЧ посредством выводов в кейсах.

Безусловно, термин «радиоэлектронная борьба» может толковаться широко, однако не следует забывать о том, что «золотая середина» в отношении баланса прав человека и пределов обеспечения государством безопасности в данной связи так и не достигнута. То есть, с одной стороны, вопросы должны быть конкретизированы, а с другой — достижение этой конкретизации становится невозможным. Это объясняется тем, что массовый перехват сообщений в каждой конкретной ситуации будет иметь индивидуальные свойства, которые будут влиять на пределы усмотрения государства, степень информационных киберрисков и ограничения основных прав и свобод граждан того или иного государства.

По делу Big Brother Watch ЕСПЧ признал нарушение ст. 8 Европейской конвенции, однако дело передано в Большую палату, соответственно, заявленные выводы можно рассматривать как промежуточные, которые могут быть полезными для научного анализа темы защиты персональных данных.

Дело Big Brother Watch затрагивает весьма важные проблемы международной информационной киберсвободы и некоторые вопросы ее реализации на национальном уровне. Собственно, вопрос об ограничении государством данных прав, в том числе права защиты персональных данных, не является новым, но следует относиться к нему с должным вниманием ввиду постоянной динамики цифровой среды.

Это отсылает нас к делу Эдварда Сноудена, используемому в образовательных целях, где раскрывается проблема соотношения публичных и частных интересов (так называемый эффект Сноудена). В США наметилась тенденция противоречия (столкновения) двух режимов — гражданских свобод и обеспечения национальной безопасности. Допускается вторжение в осуществление гражданских прав, преимущественно права на частную жизнь, тайну переписки и т. д., а также пренебрежение гражданскими свободами под предлогом необходимости национальной безопасности, которой угрожают внешние враги. В данном случае показательно заявление президента Б. Обамы²⁹: должны уважаться принципы, заложенные в Конституции США, и также работа информационных агентств. Информационные агентства призваны создавать условия для соблюдения баланса между избираемыми политическими лидерами и гражданскими свободами (например, избирательные права).

Необходимо предоставить все правовые средства для реализации компетенций данными агентствами.

Эдвард Сноуден — сотрудник американских спецслужб — передал СМИ секретные сведения о массовой слежке со стороны органов власти. В этом и проявился «эффект Сноудена»³⁰ — создались предпосылки для постановки личных прав и свобод выше национальной безопасности. Собственно, национальная безопасность в данном случае была скорее предлогом для оправдания не ограниченных правовыми лимитами действий спецслужб США.

Данный эффект проявился и в том, что массовое мнение относительно многих информационных процессов в обществе изменилось, доверие к IT-компаниям было подорвано. Транснациональные корпорации также оказывают влияние на общественное мнение и собственно восприятие той или иной информации, касающейся в том числе правовых лимитов в отношении информационной массовой слежки.

На наш взгляд, дело не дает конкретного ответа на вопрос, к какому правовому решению следует прийти, но приводит объективные юридические факты относительно массовой слежки.

Не менее интересно дело *«Хелили против Швейцарии»*³¹. Заявительница жаловалась, что полиция неправомерно внесла ее в свои записи, указав в графе «профессия» информацию о том, что она является проституткой. Это произошло вследствие обработки полицией визитных карточек заявительницы, в которых было указано, что она «хотела бы встретить мужчину, с которым можно выпить или выбираться куда-нибудь время от времени». Заявительница обосновывала нарушение ст. 8 Европейской конвенции тем, что обработка предположительно ложных данных, касающихся ее личной жизни, нарушила ее право на уважение к личной жизни. ЕСПЧ пришел к выводу, что было нарушение ст. 8 Европейской конвенции. Суд мотивировал это тем, что подобная обработка данных может подорвать нормальные условия повседневной жизни заявителя и к тому же эти данные могут быть переданы властям, что является не менее важным, потому как персональные данные подлежат автоматической обработке, что делает данные легко распространяемыми на различные носители.

Дело *«Кэтт против Соединенного Королевства»*³² касалось сбора и хранения личных данных заявителя (который являлся активистом) в одной из баз данных полиции под названием «внутренние экстремисты». ЕСПЧ признал нарушение ст. 8 Европейской

²⁹ См.: *Obama B.* Security and Privacy: In search of balance // Vital speeches of the day. 2014. 80 (30). P. 102—107.

³⁰ Подробнее см.: *Gurnow M.* The Edward Snowden Affair: Exposing the Politics and Media Behind the NSA Scandal. Indianapolis, 2014; *Greenwald G.* No place to hide: Edward Snowden, NSA, and the U. S. Surveillance State. New York, 2014.

³¹ ECHR, *Khelili v. Switzerland*, 18.10.2011.

³² ECHR, *Catt v. the United Kingdom*, 24.01.2019.

конвенции. Аргументация Суда заслуживает особого внимания, так как он подходит к вопросу оценки обстоятельств с позиции различных критериев. Так, материалы, собранные и включенные в базу, касались политических взглядов заявителя, а следовательно, относились к категории политических прав (в части выражения политических взглядов и собственно права придерживаться их). Также был учтен возраст заявителя (94 года) и тот факт, что не было предшествующих фактических обстоятельств, касающихся совершения насилия.

В деле *«Лопез Рибальда и другие против Испании»*³³ рассматривается проблема, связанная с осуществлением работодателем скрытой видеосъемки на рабочем месте сотрудниц супермаркета и использованием полученных видеозаписей в суде в качестве доказательства их вины. Пять заявительниц по делу работали кассирами в супермаркете в Испании. Работодатель ввиду недостатков заподозрил кражи в супермаркете и в связи с этим установил камеры, предназначенные для слежки за покупателями, а также скрытые — направленные на кассовые столы, в целях наблюдения за сотрудниками. Ни сотрудники, ни комитет сотрудников компании о скрытых камерах уведомлены не были. Соответственно, камеры зафиксировали кражи некоторыми из заявительниц, а также пособничество в кражах покупателям и сотрудникам с их стороны, что они признали после предъявления им видеозаписи. В итоге всем заявительницам была вменена санкция в виде увольнения.

Национальными судами дело было разрешено в пользу работодателя, в дальнейшем заявительницы обратились в ЕСПЧ.

ЕСПЧ вынес решение, в котором было признано, что видеонаблюдение за работниками без их предварительного уведомления составляет нарушение ст. 8 Европейской конвенции, а использование в суде видеозаписей, сделанных с нарушением данной статьи, равно как и всех доказательств, полученных в результате использования видеозаписи, составляет нарушение п. 1 ст. 6 Европейской конвенции. Суд привел общие принципы, которыми руководствовался при принятии данного решения:

средства, предназначенные для обеспечения соблюдения ст. 8 Европейской конвенции, находятся в рамках пределов усмотрения государства, соответственно, характер обязательств государства будет зависеть от конкретных аспектов частной жизни, которые рассматриваются в деле;

понятие частной жизни распространяется на такие аспекты ее идентичности, как имя или изображение;

право на уважение частной жизни затрагивается в том случае, если запись информации носит систематический или постоянный характер;

важно понимать, было ли целью наблюдения конкретное лицо и была ли личная информация обработана или использована таким образом, что это являлось вмешательством в право на уважение частной жизни;

скрытое видеонаблюдение за работником на рабочем месте должно расцениваться как значительное вмешательство в его частную жизнь;

необходимо установить, был ли соблюден государством в контексте своих позитивных обязательств по ст. 8 справедливый баланс между правом заявительниц на уважение частной жизни и интересом работодателя в части защиты его организационных и управленческих прав в отношении прав собственности, а также публичных интересов в надлежащем отправлении правосудия.

Данные выводы тоже следует воспринимать как промежуточные, так как дело передано в Большую палату. В действительности следует обратить внимание на вывод о праве на уважение частной жизни — оно затрагивается только в случае систематического и постоянного наблюдения. Важно понимать, как формулировать данный критерий и в случае, если способы наблюдения изменятся, каким образом вышеназванные критерии будут применяться и насколько практичным будет их видоизменение.

В деле *«Барбулеску против Румынии»*³⁴ ЕСПЧ также признал нарушение ст. 8 Европейской конвенции. Гражданин Барбулеску использовал оборудованный на рабочем месте компьютер для личной переписки, впоследствии был уволен. В данном казусе румынские суды не смогли установить справедливый баланс между правом на уважение частной жизни (право на переписку) и правом работодателя на эффективный производственный результат в работе. ЕСПЧ установил, что румынские суды не смогли определить, получал ли гражданин предварительное уведомление от своего работодателя о возможности мониторинга его сообщений. В толковании не обошлось без рассмотрения вопросов публичной власти и пределов ее вмешательства, было подчеркнуто, что государство может использовать режим массового перехвата, если оно считает это необходимым в интересах национальной безопасности. Однако государство должно четко указывать характер преступлений, которые могут повлечь судебное постановление о перехвате, категорий людей, которые могут входить в зону перехвата, процедуру, применяемую для изучения и использования полученных данных, продолжительность перехвата полученных данных, меры предосторожности, которые должны быть приняты, и т. д. Так, было признано нарушение ст. 8 Европейской конвенции ввиду необоснованности решения о доступе к частной переписке.

³³ ECHR, *López Ribalda and Others v. Spain*, 09.01.2018.

³⁴ ECHR, *Bărbulescu v. Romania*, 05.09.2017.

В деле *«Антовиц и Миркович против Черногории»*³⁵ заявителями выступили два гражданина Черногории — Н. Антовиц и Й. Миркович, которые утверждали, что незаконные установка и использование оборудования видеонаблюдения в университетских аудиториях, где они проводили занятия, нарушили их право на уважение частной жизни. В данном деле ЕСПЧ установил нарушение ст. 8 Конвенции в отличие от национальных судов. Суд констатировал, что понятие «частная жизнь» может включать профессиональную деятельность или деятельность, осуществляемую в публичном контексте. Скрытое видеонаблюдение за работником на рабочем месте должно рассматриваться как серьезное вмешательство в его личную жизнь. Любое вмешательство может быть оправдано по смыслу ст. 8 (2), если оно соответствует закону, преследует одну из более законных целей, а также необходимо в демократическом обществе для достижения любой такой цели. ЕСПЧ признал данный вид вмешательства в частную жизнь не соответствующим закону, а следовательно, нарушение ст. 8 Европейской конвенции.

В деле *«С. и Марпер против Соединенного королевства»*³⁶ ЕСПЧ постановил, что хранение образцов ДНК лиц, которые арестованы, но позднее оправданы или обвинения против них сняты, является нарушением права на неприкосновенность частной жизни в соответствии со ст. 8 Европейской конвенции.

В деле *«Мохамед Бен Файза против Франции»*³⁷ рассматривался вопрос о пределах использования информационных технологий при ведении уголовного расследования, при этом преступление касалось незаконного оборота наркотиков. При помощи GPS-устройства правоохранительным органам удалось зафиксировать геолокацию в режиме реального времени. ЕСПЧ отметил, что французское законодательство с недостаточной ясностью указывало на то, в какой степени и как власти имели право использовать свои дискреционные полномочия; постановление суда, переданное телефонному оператору, также представляло собой акт вмешательства в личную жизнь заявителя. Это является нарушением ст. 8 Европейской конвенции.

В деле *«Пек против Великобритании»*³⁸ заявитель пытался предпринять попытку суицида, что было зафиксировано на видеозаписи. Со стороны полиции попытка заявителя нанести себе вред была пресечена. В дальнейшем видеозапись была выпущена для прессы. Заявитель утверждал, что его право на частную жизнь было нарушено (ст. 8 Европейской конвенции) в результате разглашения видеозаписи, а также жаловался на нарушение права на эффектив-

ное средство правовой защиты (ст. 13 Европейской конвенции). ЕСПЧ установил, что имелось нарушение ст. 8 Европейской конвенции и не было никаких достаточных оснований для опубликования данной видеозаписи в прессе. Также ЕСПЧ установил нарушение ст. 13 Европейской конвенции и, соответственно, признал отсутствие эффективных средств правовой защиты заявителя в связи с нарушением права, предоставляемого ст. 8 Европейской конвенции.

Обстоятельства дела *«Годелли против Италии»*³⁹ касались конфиденциальной информации о рождении ребенка и невозможности получить данную информацию из медицинского учреждения. Заявительница утверждала, что хотела получить информацию о том, кто ее мать, и в этом ей было отказано как на уровне медицинского учреждения, так и на судебном уровне. Заявительница утверждала, что ей был причинен серьезный ущерб в результате непредоставления данной информации и истории о ее кровной линии. ЕСПЧ постановил, что действительно имело место нарушение ст. 8 Европейской конвенции, учитывая, в частности, что справедливый баланс между позицией законодателя относительно конфиденциальной информации о рождении ребенка и возможности получения заявителем хотя бы частичной информации о своих родственных корнях, безусловно, должен решаться в пользу последнего (заявителя).

По делу *«Ротару против Румынии»*⁴⁰ заявитель утверждал, что правовые средства не позволяли ему опровергнуть информацию, хранимую в румынской разведывательной службе, о том, что он был приговорен в 1948 г. к году лишения свободы за то, что выразил критику в отношении коммунистического режима. ЕСПЧ постановил, что имело место нарушение ст. 8 Европейской конвенции и дал разъяснение, что хранение и использование информации о личной жизни заявителя было незаконно. Общественная информация систематически собирается и хранится в системных файлах органов государственной власти. Однако законодательство не устанавливает конкретный тип информации, которая может храниться, также и не устанавливает сроки хранения информации. Это, безусловно, расширяет возможности сбора абсолютно всей информации, в том числе о частной жизни, что создает невозможность защиты субъектов правовыми средствами, предоставляемыми законодателем.

В практике ЕСПЧ интерес представляет дело *«Компания “Мадьяр Йети Зрт” против Венгрии»*⁴¹, которое, по нашему мнению, косвенно связано с за-

³⁵ ECHR, *Antović and Mirković v. Montenegro*, 28.11.2017.

³⁶ ECHR, *S. and Marper v. the United Kingdom*, 04.12.2008.

³⁷ ECHR, *Ben Faiza v. France*, 08.02.2018.

³⁸ ECHR, *Peck v. the United Kingdom*, 28.01.2003.

³⁹ ECHR, *Godelli v. Italy*, 25.09.2012.

⁴⁰ ECHR, *Rotaru v. Romania*, 04.05.2000.

⁴¹ Бюллетень Европейского суда по правам человека. 2019. № 6. С. 29—31.

щитой персональных данных. Фабула дела заключалась в том, что названная компания управляла популярным новостным онлайн-порталом и, соответственно, выполняла роль информационной платформы. На своей новостной платформе компания опубликовала статью об инциденте, и эта новость содержала гиперссылку на видео с канала Youtube. Видео содержало интервью главы местного самоуправления румынского меньшинства, который прокомментировал инцидент с футбольными фанатами, которые, находясь в состоянии алкогольного опьянения, выкрикивали расистские высказывания, угрожали ученикам школы, где учились преимущественно румыны. При этом в интервью было подчеркнуто, что болельщики, возможно, являлись членами ультраправой националистической политической партии «Йоббик». Жалоба на данную компанию состояла в том, что она распространяет сведения, которые порочили честь, достоинство и деловую репутацию ультраправой партии «Йоббик».

Казалось бы, в деле нет ничего относящегося к информационной безопасности и к персональным данным и в действительности применяется ст. 10 Европейской конвенции. Однако речь шла о гиперссылке, благодаря размещению которой и стало доступно интервью. Гиперссылка была приравнена к значимому юридическому факту, поскольку по сути является способом передачи определенной информации и лишь направляет пользователя Интернета на определенные ресурсы и тем самым не подтверждает истинность данной информации. Размещение такой информации является реализацией права, закрепленного в ст. 10 Европейской конвенции. Но при этом возникает вопрос, может ли размещение гиперссылки повлечь ответственность за размещение информации, порочащей честь, достоинство и деловую репутацию. ЕСПЧ указал, что в каждом конкретном случае следует проводить оценку по субъекту, который распространяет информацию (журналист к примеру), и рассматривать ситуацию по таким критериям, как: поместил ли журналист гиперссылку на контент (не одобряя и не повторяя его), знал ли журналист или должен был знать о том, что оспариваемый контент был порочащим или иным образом незаконным, и т. д.

ЕСПЧ признал нарушение ст. 10 Европейской конвенции.

В связи с этим полагаем важным обратить внимание на осложненность отношений по передаче информации гиперссылкой (информационно-технологическим элементом). Данный вид отношений по персонификации, утверждению или изменению информации постепенно начинает вырабатывать собственную структуру.

Такой вид постепенно развивающихся отношений придает текущим социальным отношениям но-

вые элементы, которые важно учитывать при оценке обстоятельств, анализе юридических фактов и т. д.

Судебный механизм, существующий в настоящее время, развивает применение правовых норм о защите персональных данных, при этом затрагиваются отдельные вопросы правоприменения. Это постепенно обеспечивает развитие института защиты персональных данных именно в ракурсе международной информационной кибербезопасности. Такая модель правового регулирования позволяет сформулировать определенные начала теоретико-прикладного инструментария для данного института, а также отдельные аспекты его применения. В связи с этим наблюдается необходимость в теоретическом обобщении накопленного опыта и более четких формулировках для правоприменительной и международной нормотворческой практики.

В принципе, если анализировать всю систему вновь образующихся прав человека, то, как правильно отмечает А. И. Ковлер⁴², классические права человека подвергаются новым испытаниям, после того как их удалось «отбить» у тоталитарных режимов, а именно в связи с навязыванием стереотипов сознания, поведения и потребления, тотальной слежкой за передвижениями граждан и фиксацией их действий, подменой социальной системой M2M (межмашинного взаимодействия). Отчуждение личности приобретает новые формы. Автор совершенно обоснованно делает вывод, что время покажет, насколько эффективными окажутся предлагаемые меры, если они, конечно, найдут воплощение в соответствующих международных конвенциях и национальных законодательствах⁴³.

Вопрос о персональных данных в ракурсе международной информационной кибербезопасности не является новым. Он лишь доказывает правоту относительно возможности изменения концепции прав человека на международном уровне под воздействием данных «революционных» и быстроразвивающихся изменений. Однако остается нерешенным вопрос, по какому вектору развития будет двигаться данная тенденция.

Степень важности теоретического понимания проблемы нельзя отрицать и необходимо выработать единую концепцию, которая будет служить настольной книгой для того же законодателя. Тема института защиты персональных данных носит двоякий характер, так как по своей природе состоит из подлинно юридического содержания и технического. Нужно постепенно исследовать междисциплинарный вопрос взаимодействия технического и юридического критериев, что будет опорным пунктом в об-

⁴² См.: Ковлер А. И. Права человека в цифровую эпоху // Бюллетень Европейского суда по правам человека. 2019. № 6. С. 146—150.

⁴³ Там же.

щей теории международной информационной кибербезопасности.

Полагаем, важно задать определенный вектор концепции информационной кибербезопасности для понимания и обеспечения внедрения единых критериев института персональных данных. Вместе с тем предлагается несколько теоретических концепций:

1) концепция закрытой информационной кибербезопасности, в которой институт персональных данных постоянно находится на контроле какого-то конкретного государства, при этом обмен между государствами информацией затруднен;

2) концепция открытой информационной кибербезопасности, при которой институт персональных данных сохраняет гарантии от незаконной обработки данных и их использования (даже с целью обеспечения национальной безопасности).

Возможно ли в данный период времени признать защиту персональных данных институтом международной информационной кибербезопасности и

создать теоретико-практические рекомендации для юриспруденции в области защиты персональных данных? Только при ответе на вопрос о доктрине информационной кибербезопасности можно задать конкретное направление практической юриспруденции в сфере защиты персональных данных (в том числе на международном уровне) в целях наполнения качественной содержательной частью института персональных данных и установления конкретных гарантий защиты персональных данных.

Обобщая вышеизложенное, можно сделать вывод о формировании института информационной кибербезопасности — института защиты персональных данных и необходимости теоретической доработки полученных результатов, их обобщения и, возможно, закрепления в практических руководствах международных организаций, а также постановки вопроса об имплементации их материала государствами — участниками организаций.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

- Ciancaglini V., Balduzzi M., McArdle R., Rösler M. Below the Surface: Exploring the Deep Web // *Trend Micro*. 2018.
- Convention 108+: better protecting us in the digital era (материалы конференции и речь Генерального секретаря). URL: <https://www.coe.int/en/web/data-protection/conference-on-convention-108> (дата обращения: 12.08.2019).
- Denning P. J. The ARPANET after Twenty Years // *American Scientist*. 1989. Vol. 77.
- Greenwald G. No place to hide: Edward Snowden, NSA, and the U. S. Surveillance State. New York, 2014.
- Gurnow M. The Edward Snowden Affair: Exposing the Politics and Media Behind the NSA Scandal. Indianapolis, 2014.
- Obama B. Security and Privacy: In search of balance // *Vital speeches of the day*. 2014. 80 (30).
- Ковлер А. И. Европейская Конвенция в международной системе защиты прав человека. М., 2019.
- Ковлер А. И. Права человека в цифровую эпоху // *Бюллетень Европейского суда по правам человека*. 2019. № 6.
- Шатилина А. С. Права человека в интернете: проблема признания права на доступ к Интернету // *Преценденты Европейского суда по правам человека*. 2018. № 1 (49).

REFERENCES

- Ciancaglini V., Balduzzi M., McArdle R., Rösler M. Below the Surface: Exploring the Deep Web. *Trend Micro*, 2018. 47 p.
- Convention 108+: better protecting us in the digital era. Available at: <https://www.coe.int/en/web/data-protection/conference-on-convention-108> (accessed 12.08.2019).
- Denning P. J. The ARPANET after Twenty Years. *American Scientist*, 1989, vol. 77, pp. 530—535.
- Greenwald G. No place to hide: Edward Snowden, NSA, and the U. S. Surveillance State. New York, 2014. 300 p.
- Gurnow M. The Edward Snowden Affair: Exposing the Politics and Media Behind the NSA Scandal. Indianapolis, 2014. 384 p.
- Kovler A. I. European Convention in the International System of Human Rights Protection. Moscow, 2019. 304 p. (In Russ.)
- Kovler A. I. Human Rights in the Digital Age. *Bulletin of the European Court of Human Rights*, 2019, no. 6, pp. 146—148. (In Russ.)
- Obama B. Security and Privacy: In search of balance. *Vital Speeches of the Day*, 2014, 80 (30), pp. 102—107.
- Shatilina A. S. Human Rights on the Internet: The Problem of Recognizing Internet Access Rights. *Pretsedenty Evropeyskogo suda po pravam cheloveka*, 2018, no. 1 (49), pp. 38—46. (In Russ.)