DOI 10.52390/2078404X_2021_12_154
УДК 341.18
ББК 67.9

С.Е. Фомина,
Санкт-Петербургский государственный университет, магистрант

ПРАВА ЧЕЛОВЕКА В ИНФОРМАЦИОННОМ ОБЩЕСТВЕ[1]

Аннотация. Предметом настоящего исследования является реализация прав человека в современном информационном обществе. Права человека – неизменная фундаментальная ценность любого демократического общества, соблюдение, уважение и защита которых является первостепенной обязанностью государств. Автор обосновывает вывод о том, что государство обязано устанавливать баланс между конкурирующими публичными и частными интересами, между правом на неприкосновенность частной жизни и интересами национальной безопасности, а также анализирует критерии для определения такого баланса.

Ключевые слова: права человека, право на свободу выражения мнения, Интернет, персональные данные, право на уважение частной и семейной жизни.

S. Fomina
Saint Petersburg State University, Master's student

HUMAN RIGHTS IN THE INFORMATION SOCIETY

Abstract. The subject of the article is the implementation of human rights in a modern information society. Human rights are an invariable fundamental value of any democratic society, the observance, respect and protection of which is the primary responsibility of states. The author concludes that the state is obliged to strike a balance between competing public and private interests, between privacy and national security interests, and also provides criteria for such a balance.

***Keywords*:** human rights, the right to freedom of expression, the Internet, personal data, the right to respect for private and family life.

На сегодняшний день человечество совершило огромный прорыв в создании и развитии различных технологий, которые не только упростили нашу жизнь, но и стали ее неотъемлемой частью. Однако государство как главный субъект обеспечения и защиты прав человека находит все больше рычагов для произвольного вмешательства в осуществление лицами их фундаментальных прав. Целями настоящей работы являются определение критериев для установления баланса между конкурирующими публичными и частными интересами, между правом на неприкосновенность частной жизни и интересами национальной безопасности, а также анализ ситуации, касающейся реализации прав человека в международном и национальном правопорядках в условиях современного информационного общества.

1. Правовое регулирование персональных данных: сбор, передача и хранение

1.1. Информационное самоопределение

Всеобщая декларация прав человека и Конвенция о защите прав человека и основных свобод (далее – Конвенция) были приняты задолго до появления компьютеров и Интернета, а также формирования информационного общества. Хотя эти технологии и принесли значительную пользу как отдельным людям, так и обществу в целом, улучшив качество жизни, эффективность и производительность труда, в то же время они создают новые риски для права на уважение частной жизни. В ответ на необходимость установления конкретных правил, регулирующих сбор и использование персональных данных, возникла новая концепция конфиденциальности, известная в некоторых юрисдикциях как «право на информационное самоопределение»[2], что привело к разработке специальных правовых норм, обеспечивающих защиту персональных данных.

Данная концепция является относительно новой и распространена в основном в континентальной Европе, особенно часто она используется Конституционным судом Германии[3]. Информационное самоопределение означает право человека контролировать или иметь какую-то «власть» в отношении того, какая информация о нем становится общедоступной, как такая информация хранится и к какой информации у государства

[1] Автор – победитель шестого Всероссийского молодежного конкурса работ по праву информационных технологий и интеллектуальной собственности – IP&IT LAW – 2021 в номинации, учрежденной издательским домом «Развитие правовых систем».

[2] См.: Постановление Большой Палаты Европейского Суда по делу «Компании "Сатакуннан Марккинапёрсси Ой" и "Сатамедиа Ой" против Финляндии» (Satakunnan Markkinaporssi Oy and Satamedia Oy v. Finland) от 27 июня 2017 г., жалоба № 931/13, § 137 // Прецеденты Европейского Суда по правам человека. Специальный выпуск. 2018. № 2.

[3] См.: The German Federal Constitutional Court (Bundesverfassungsgericht), 1 BvR 209/83, 1 BvR 484/83, 1 BvR 420/83, 1 BvR 362/83, 1 BvR 269/83, 1 BvR 440/83 (Volkszählungsurteil), 15 December 1983 // https://web.archive.org/web/20101116085553/http://zensus2011.de/fileadmin/material/pdf/gesetze/volkszaehlungsurteil_1983.pdf.

может быть доступ[1]. В Германии давно высказываются опасения относительно того, что государство, если ему придется собирать массу информации различного характера о каждом гражданине, не должно делать всю информацию, которой оно располагает о каком-либо конкретном человеке, доступной для всех, в том числе для любого государственного учреждения[2]. Аналогичное мнение высказал Конституционный суд Венгрии и принял еще в 1991 году решение, касающееся использования PIN-кодов (личных идентификационных номеров)[3]. В этом решении Конституционный суд Венгрии запретил государственным органам группировать все данные о физическом лице под одним идентификатором.

С точки зрения эффективного управления концепция конфиденциальности может вызывать вопрос: почему, если гражданин не планирует совершить что-либо незаконное, он должен возражать против того, чтобы все государственные учреждения могли просматривать любую информацию, которая правомерно хранится у другого учреждения/государственного органа? Частично эта проблема связана с доверием граждан к своему государству, но следует признать, что в наши дни совокупность информации, полученной о каждом гражданине, настолько огромна, что даже небольшое недоверие граждан к государству может оправдать разумность теории информационного самоопределения.

Существуют взаимосвязанные аспекты этого вопроса, которые уже получили широкое признание в различных правовых системах. Наиболее важным из них является вся область защиты данных, как видно на примере Закона Соединенного Королевства о защите данных[4]. Его главная суть и аналогичного законодательства заключается в том, что однажды собранная информация должна использоваться только для целей, которые изначально легитимировали ее сбор, и предоставляться только тем, у кого есть соответствующее этой цели основание «знать» ее[5].

1.2. Конвенция о защите прав человека и основных свобод

Современные общества становятся все более цифровыми. Темпы развития технологий и способы обработки персональных данных влияют на каждого из нас ежедневно. Конвенция прямо не предусматривает права, связанные с персональными данными и их защитой. Однако ее динамичное и «живое» толкование, которое осуществляет Европейский Суд по правам человека (далее – Европейский Суд), придает Конвенции силу и способствует тому, чтобы ее положения отвечали реалиям времени[6]. В своей прецедентной практике Европейский Суд расширил права, закрепленные в Конвенции, таким образом, что ее положения применяются сегодня к ситуациям, которые было невозможно представить в то время, когда Конвенция была принята, включая вопросы, связанные с новыми технологиями.

В соответствии со статьей 8 Конвенции право человека на защиту в отношении обработки персональных данных является частью права на уважение частной и семейной жизни, жилища и корреспонденции. Согласно законодательству Европейского союза (далее – ЕС), защита персональных данных признается отдельным основным правом[7], что подтверждается в пункте 1 статьи 16 Договора о функционировании ЕС (TFEU)[8], а также в пункте 1 статьи 8 Хартии ЕС об основных правах[9].

1.3. Персональные данные и право на уважение частной жизни лица

Сбор и хранение персональных данных являются вмешательством в право на уважение частной жизни лица. Данное вмешательство допустимо, только если оно соответствует критериям, установленным в статье 8 Конвенции. Европейский Суд часто анализирует вопрос о том, насколько правомерным является вмешательство, если в отноше-

[1] См.: *Kodde Claudia*. Germany's «Right to be forgotten» – between the freedom of expression and the right to informational self-determination // International Review of Law, Computers and Technology. Vol. 30. 2016. P. 18.

[2] См.: *Hornung Gerrit*. Christoph Schnabel, Data protection in Germany I: The population census decision and the right to informational self-determination // Computer Law and Security Review. 2009. Vol. 25. Issue 1. P. 87.

[3] См.: Решение Конституционного суда Венгрии от 4 сентября 1991 г. № 15/1991 (IV. 13) «Об использовании персональных данных и личного идентификационного номера» // http://public.mkab.hu/dev/dontesek.nsf/0/1ce263a376458f27c1258382003c412c/$file/en_0015_1991.pdf.

[4] См.: Data Protection Act, UK Government, 2018 // https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted.

[5] См.: *Carey Peter*. Data protection: A practical guide to UK and EU law. Oxford: Oxford University Press, 2009. P. 130.

[6] См.: Постановление Европейского Суда по делу «Тайрер против Соединенного Королевства» (Tyrer v. United Kingdom) от 25 апреля 1978 г., жалоба № 5856/72, § 31 // http://hudoc.echr.coe.int/spa?i=001-57587.

[7] См.: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) № L 119, 04.05.2016 // https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[8] См.: Consolidated version of the Treaty on the Functioning of the European Union // Official Journal C 326, 26/10/2012 P. 0001-0390 // https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT.

[9] См.: Charter of Fundamental Rights of the European Union, 2000/C 364/01 // Official Journal of the European Communities, 18.12.2000 // https://www.europarl.europa.eu/charter/pdf/text_en.pdf.

нии лица осуществляется уголовное преследование или если же такое преследование уже прекращено.

В деле «S. и Марпер против Соединенного Королевства»[1] рассматривалась жалоба на бессрочное хранение в базе данных отпечатков пальцев заявителей, их образцов клеток и ДНК после того, как уголовное дело против них было прекращено. Европейский Суд постановил, что имело место нарушение права на уважение частной жизни заявителей, поскольку использование современных научных методов в системе уголовного правосудия не может быть разрешено «при любых обстоятельствах» и без установления баланса между потенциальными преимуществами использования этих методов и важными интересами частной жизни. Любое государство, претендующее на пальму первенства в разработке новых технологий, несет особую ответственность за «установление правильного баланса». В данном деле Европейский Суд пришел к выводу, что общий и неизбирательный характер полномочий по хранению отпечатков пальцев, образцов клеток и профилей ДНК лиц, подозреваемых, но не признанных виновными в совершении правонарушений, применительно к данному конкретному делу, не смог обеспечить справедливый баланс между конкурирующими публичными и частными интересами.

Напротив, в делах «B.B. против Франции»[2], «Гардель против Франции»[3], «M.B. против Франции»[4] трое заявителей, осужденных за изнасилование, жаловались на их включение в национальную базу данных сексуальных преступников. Европейский Суд постановил, что в указанных делах не было допущено нарушения статьи 8 Конвенции (право на уважение частной жизни). Он отметил, что продолжительность хранения данных (максимум 30 лет) не является непропорциональной мерой по отношению к преследуемой цели, предотвращению преступности, путем сохранения такой информации. Кроме того, при ознакомлении с указанными данными судом, полицией и административными органами соблюдалась полная конфиденциальность.

Дело «Шимоволос против Российской Федерации» касалось регистрации правозащитника в базе данных Министерства внутренних дел, в которой фиксировалась и хранилась информация о его передвижениях по России, а также о его задержаниях[5]. Европейский Суд пришел к выводу о нарушении статьи 8 Конвенции, поскольку создание, функционирование базы данных и порядок ее работы регулировались приказом Министерства внутренних дел, который никогда не публиковался или иным образом не доводился до сведения общественности. В связи с этим Европейский Суд отметил, что законодательство Российской Федерации не предусматривает с достаточной ясностью объем и способ осуществления дискреционных полномочий, предоставленных национальным властям для сбора и хранения в базе данных информации о частной жизни людей. В частности, в соответствующем приказе не содержались в доступной для общественности форме какие-либо указания на минимальные гарантии против злоупотреблений.

В похожем деле, «Брунэ против Франции»[6], заявитель жаловался, в частности, на вмешательство в его частную жизнь в результате включения информации о нем в полицейскую базу данных уже после прекращения уголовного дела против него. Европейский Суд установил, что власти Франции вышли за пределы своей свободы усмотрения и допустили нарушение прав заявителя, поскольку у него не было реальной возможности добиваться удаления из этой базы касающейся его информации. Более того, нарушение было также и в том, что срок хранения этих данных (20 лет) можно было сократить.

В то же время Европейский Суд отмечал, что, если лицо подозревается в совершении тяжких преступлений, например, террористического характера, то наблюдение за ним со стороны властей посредством использования GPS-систем будет соразмерным и не будет являться нарушением права на уважение частной жизни[7].

По мнению Европейского Суда, нарушением права на уважение частной жизни будет являться отсутствие дифференцированного срока хранения персональных данных в зависимости от характера и тяжести совершенных правонарушений[8]. В некоторых делах он указывал, что при оценке того, было ли вмешательство со стороны государства пропорциональным, решающее значение имеет не столько срок хранения данных, сколько отсутствие

[1] См.: Постановление Большой Палаты Европейского Суда по делу «S. и Марпер против Соединенного Королевства» (S. and Marper v. United Kingdom) от 4 декабря 2008 г., жалобы №№ 30562/04 и 30566/04 // http://hudoc.echr.coe.int/rus?i=001-90051.

[2] См.: Постановление Европейского Суда по делу «B.B. против Франции» (B.B. v. France) от 17 декабря 2009 г., жалоба № 5335/06 // http://hudoc.echr.coe.int/rus?i=001-96361.

[3] См.: Постановление Европейского Суда по делу «Гардель против Франции» (Gardel v. France) от 17 декабря 2009 г., жалоба № 16428/05 // http://hudoc.echr.coe.int/eng?i=001-96457.

[4] См.: Постановление Европейского Суда по делу «M.B. против Франции» (M.B. v. France) от 17 декабря 2009 г., жалоба № 22115/06 // http://hudoc.echr.coe.int/eng?i=001-96363.

[5] См.: Постановление Европейского Суда по делу «Шимоволос против Российской Федерации» (Shimovolos v. Russia) от 21 июня 2011 г., жалоба № 30194/09 // Бюллетень Европейского Суда по правам человека. 2012. № 1.

[6] См.: Постановление Европейского Суда по делу «Брунэ против Франции» (Brunet v. France) от 18 сентября 2014 г., жалоба № 21010/10 // http://hudoc.echr.coe.int/eng?i=001-146389.

[7] См.: Постановление Европейского Суда по делу «Узун против Германии» (Uzun v. Germany) от 2 сентября 2010 г., жалоба № 35623/05 // Прецеденты Европейского Суда по правам человека. 2015. № 6.

[8] См.: Постановление Европейского Суда по делу «Айкагуэр против Франции» (Aycaguer v. France) от 22 июня 2017 г., жалоба № 8806/12 // http://hudoc.echr.coe.int/eng?i=001-175007.

определенных гарантий[1]. Таким образом, государство может осуществлять вмешательство в право на неприкосновенность частной жизни, однако данное вмешательство должно быть не только предусмотрено законом (а закон отвечать «качествам закона»), но и обеспечивать достаточные гарантии против произвола властей.

1.3.1. Сбор персональных данных в интересах национальной безопасности

Вмешательство в право, предусмотренное статьей 8 Конвенции, посредством использования различных скрытых методов (например, тайного прослушивания и наблюдения) главным образом обосновывается интересами национальной безопасности, в том числе борьбой с терроризмом. Европейский Суд также отмечал широкие пределы усмотрения государств по защите национальной безопасности, особенно с учетом современных угроз глобального терроризма и совершения серьезных трансграничных преступлений[2]. Этот вывод подтверждается Постановлением Европейского Суда по делу «Big Brother Watch и другие против Соединенного Королевства», в котором он установил, что режим массового прослушивания нарушает право на уважение частной жизни, поскольку надзор со стороны властей как за выбором соответствующих субъектов, так и за фильтрацией, поиском и отбором перехваченных сообщений для проверки был недостаточным[3].

В свою очередь, в деле «Сабо и Виши против Венгрии»[4] Европейский Суд признал, что современный терроризм принимает множество форм и власти вынуждены прибегать к передовым технологиям, включая массовый мониторинг коммуникаций, для предотвращения подобных инцидентов. Однако, по мнению Европейского Суда, законодательство Венгрии не обеспечивало достаточных гарантий, позволяющих избежать злоупотреблений. Более того, под наблюдением мог оказаться практически любой человек в Венгрии, а распоряжение о принятии этих мер принималось исключительно органами исполнительной власти и без оценки того, был ли перехват сообщений строго необходимым, и не обеспечивалось какими-либо эффективными средствами правовой защиты, в том числе судебными.

Дело «Кэтт против Соединенного Королевства» касалось жалобы заявителя на сбор и хранение его персональных данных в полицейской базе «экстремистов»[5]. Европейский Суд постановил, что имело место нарушение права на уважение частной жизни. Он, в частности, указал, что данные о заявителе касались его политических взглядов и что эта информация требовала особой защиты. Европейский Суд также принял во внимание возраст заявителя (94 года) и тот факт, что отсутствовала какая-либо угроза совершения им актов насилия. По мнению ЕСПЧ, хотя сбор информации о заявителе был оправдан, ее хранение – нет, в частности, из-за отсутствия каких-либо гарантий, к которым относятся, например, временные ограничения.

В сфере прав человека основная обязанность государства в отношении сбора и хранения персональных данных заключается в том, чтобы установить справедливый баланс между конкурирующими государственными (публичными) и частными интересами. Режим массового прослушивания сам по себе не нарушает Конвенцию, но он должен соответствовать критериям, выработанным в прецедентной практике Европейского Суда. Так, режим массового прослушивания может нарушать статью 10 Конвенции (право на свободу выражения мнения), если не существует достаточных гарантий применительно к конфиденциальным журналистским материалам[6]. Например, Большая Палата Европейского Суда относительно шведской национальной системы массового перехвата электронных сигналов решила, что эта система обеспечивает адекватные и достаточные гарантии против произвола властей, что снижает риск злоупотреблений[7].

Что касается ситуации в нашей стране, то в деле «Роман Захаров против Российской Федерации»[8] Европейский Суд указал, что российские правовые нормы, регулирующие перехват сообщений, не предусматривают адекватных и эффективных гарантий против произвола и риска злоупотребления особенно с учетом того, что специальные службы и поли-

---

[1] См.: Постановление Европейского Суда по делу «Гаугран против Соединенного Королевства» (Gaughran v. United Kingdom) от 13 февраля 2020, жалоба № 45245/15 // http://hudoc.echr.coe.int/rus?i=001-200817.

[2] См.: там же.

[3] См.: Постановление Европейского Суда по делу «Big Brother Watch и другие против Соединенного Королевства» (Big Brother Watch and Others v. United Kingdom) от 13 сентября 2018 г., жалобы №№ 58170/13, 62322/14 и 24960/15 // http://hudoc.echr.coe.int/eng?i=001-210077.

[4] См.: Постановление Европейского Суда по делу «Сабо и Виши против Венгрии» (Szabó and Vissy v. Hungary) от 12 января 2016 г., жалоба № 37138/14 // Прецеденты Европейского Суда по правам человека. 2016. № 7.

[5] См.: Постановление Европейского Суда по делу «Кэтт против Соединенного Королевства» (Catt v. United Kingdom) от 24 января 2019 г., жалоба № 43514/15 // http://hudoc.echr.coe.int/eng?i=001-189424.

[6] См.: упомянутое выше Постановление Европейского Суда по делу «Big Brother Watch и другие против Соединенного Королевства».

[7] См.: Постановление Большой Палаты Европейского Суда по делу «Компания Centrum För Rättvisa против Швеции» (Centrum För Rättvisa v. Sweden) от 25 мая 2021 г., жалоба № 35252/08 // http://hudoc.echr.coe.int/eng?i=001-210078.

[8] См.: Постановление Европейского Суда по делу «Роман Захаров против Российской Федерации» (Roman Zakharov v. Russia) от 4 декабря 2015 г., жалоба № 47143/06 // Бюллетень Европейского Суда по правам человека. 2016. № 6.

ция имеют прямой доступ с помощью технических средств ко всем средствам мобильной телефонной связи. В частности, Европейский Суд выявил недостатки правового регулирования, касающиеся обстоятельств, при которых органы власти имеют право прибегать к мерам тайного наблюдения; продолжительности применения таких мер, особенно условий, при которых они должны быть прекращены; процедур санкционирования перехвата, а также хранения и уничтожения перехваченных данных; контроля за мерами по перехвату сообщений. Кроме того, он отметил, что оспаривание перехвата сообщений доступно только лицам, которые могут представить доказательства такого перехвата, а получение соответствующих доказательств невозможно в отсутствие какой-либо системы уведомления или возможности получения доступа к информации о перехвате. Данный факт не позволяет говорить о наличии эффективных средств правовой защиты.

Европейский Суд также приходил к выводу, что законодательство Российской Федерации не отвечает критериям «качества закона» и «неспособно ограничить» применение негласных методов наблюдения (прослушивание телефонных переговоров) только тогда, когда это «необходимо в демократическом обществе»[1].

В связи с многочисленными постановлениями, вынесенными Европейским Судом против Российской Федерации, уполномоченными российскими органами был проработан вопрос о необходимости внесения изменений в законодательство и правоприменительную практику и подготовлен соответствующий доклад[2]. Однако они сочли нецелесообразным вносить изменения в том числе в отношении функционирования системы технических средств по обеспечению функций оперативно-разыскных мероприятий с учетом уже принятых мер. При этом власти ссылались на постановления Конституционного Суда Российской Федерации и на постановления Пленума Верховного Суда Российской Федерации как на обоснование отсутствия необходимости внесения изменений в законодательство[3]. Так, они отметили, что в Постановлении Конституционного Суда Российской Федерации от 9 июня 2011 г. № 12-П[4], а также в его Определении от 22 января 2014 г. № 114-О[5] прямо указано, что органы, осуществляющие оперативно-разыскную деятельность, запрашивая разрешение на проведение негласных оперативно-разыскных мероприятий, должны предоставить суду надлежащие обоснования и материалы и опираться не только на предположения о наличии признаков противоправного деяния, но и на конкретные фактические обстоятельства, подтверждающие обоснованность таких предположений. В Определении от 28 марта 2017 г. № 568-О Конституционный Суд Российской Федерации разъяснил, что проведение без предварительного судебного решения (на основании части 3 статьи 8 Федерального закона от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности») в случаях, не терпящих отлагательств, оперативно-разыскных мероприятий, ограничивающих конституционное право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, предполагает не только обязательное уведомление об этом суда, но и разрешение судом вопроса об обоснованности ограничения прав граждан при их проведении[6]. В Определении Конституционного Суда Российской Федерации от 22 ноября 2012 г. № 2046-О обращено внимание на необходимость прекращения оперативно-разыскных мероприятий, в том числе прослушивания телефонных переговоров, в случаях, когда необходимость в них отпадает, что позволяет проверяемому лицу истребовать сведения о полученной о нем информации, а в случае отказа — обжаловать его в суд[7]. Однако власти Российской Федерации не уточнили, как лицо, в отношении которого производилось прослушивание телефонных разговоров, узнает об этом.

Кроме того, в своем докладе власти Российской Федерации сослались на тот факт, что, согласно

[1] См.: Постановление Европейского Суда по делу «Москалев против Российской Федерации» (Moskalev v. Russia) от 5 марта 2018 г., жалоба № 44045/05 // Бюллетень Европейского Суда по правам человека. 2018. № 5; Постановление Европейского Суда по делу «Раджаб Магомедов против Российской Федерации» (Radzhab Magomedov v. Russia) от 20 марта 2017 г., жалоба № 20933/08 // Бюллетень Европейского Суда по правам человека. 2018. № 4.

[2] См.: Доклад о результатах мониторинга правоприменения в Российской Федерации за 2019 год // https://minjust.gov.ru/uploaded/files/doklad_qcmZYtl.pdf

[3] См.: там же. С. 71–79.

[4] См.: Постановление Конституционного Суда РФ от 9 июня 2011 г. № 12-П «По делу о проверке конституционности положений пункта 7 статьи 16 Закона Российской Федерации "О статусе судей в Российской Федерации» и части первой статьи 9 Федерального закона "Об оперативно-розыскной деятельности" в связи с жалобой гражданина И.В. Аносова» // Российская газета. 22 июня 2011 г.

[5] См.: Определение Конституционного Суда РФ от 22 января 2014 г. № 114-О «Об отказе в принятии к рассмотрению жалобы гражданина Новичкова Дмитрия Ивановича на нарушение его конституционных прав положениями статей 5, 7, 8 и 9 Федерального закона "Об оперативно-розыскной деятельности"» // Документ опубликован не был. – Источник СПС «КонсультантПлюс».

[6] См.: Определение Конституционного Суда РФ от 28 марта 2017 г. № 568-О «Об отказе в принятии к рассмотрению жалобы гражданки Побединской Александры Юрьевны на нарушение ее конституционных прав частью третьей статьи 8 Федерального закона "Об оперативно-розыскной деятельности"» // Документ опубликован не был. – Источник СПС «КонсультантПлюс».

[7] См.: Определение Конституционного Суда РФ от 22 ноября 2012 г. № 2046-О «Об отказе в принятии к рассмотрению жалобы гражданина Чудова Сергея Васильевича на нарушение его конституционных прав частью четвертой статьи 5 Федерального закона "Об оперативно-розыскной деятельности"» // СПС «КонсультантПлюс».

пунктам 69 и 70 Плана организации законопроектных работ Минюста России на 2020 год, Минюстом России дорабатываются проекты федерального закона «О внесении изменений в статью 9 Федерального закона “Об оперативно-розыскной деятельности”» (в части совершенствования гарантий прав и свобод человека при санкционировании проведения и обжаловании оперативно-разыскных мероприятий)». Однако представляется, что все меры, принятые на сегодняшний день российскими властями, не являются достаточными для того, чтобы считаться исполнением решений Европейского Суда. Он указывал на системную проблему, связанную с тем, что законодательство России в отношении использования систем тайного наблюдения не обладает «качеством закона», то есть характеризуется отсутствием правовой определенности, предсказуемости и надлежащих гарантий.

1.3.2. Права работников на неприкосновенность частной жизни

По мнению многих работодателей, установление наблюдения за работниками необходимо для того, чтобы выяснить, не злоупотребляет ли работник доверием работодателя, не использует ли противоправно его имущество и т.п. Европейский Суд неоднократно отмечал, что телефонные звонки из служебных помещений *prima facie* охватываются понятиями «частная жизнь» и «переписка». Из этого следует, что электронные письма, отправленные с работы, должны быть так же защищены, как и информация, полученная в результате личного использования Интернета на работе. В практике Европейского Суда сбор и хранение личной информации, касающиеся использования работниками телефона, электронной почты и Интернета, без ведома такого лица, рассматриваются как вмешательство в право на уважение его частной жизни[1].

В делах об отслеживании, например, электронных сообщений работника со стороны работодателя Европейский Суд анализирует следующие аспекты: 1) получило ли такое лицо предварительное уведомление от своего работодателя о возможности того, что его сообщения могут быть проверены; 2) был ли работник проинформирован о характере или масштабе наблюдения или степени вмешательства в его личную жизнь и корреспонденцию. Более того, государство должно указать конкретные причины, оправдывающие введение мер мониторинга, и пояснить, мог ли работодатель использовать меры, влекущие за собой меньшее вмешательство в личную жизнь и корреспонденцию работника[2].

[1] См.: Постановление Европейского Суда по делу «Копланд против Соединенного Королевства» (Copland v. United Kingdom) от 3 апреля 2007 г., жалоба № 62617/00 // Прецеденты Европейского Суда по правам человека. 2016. № 7.

[2] См.: Постановление Европейского Суда по делу «Бэрбулеску против Румынии» (Barbulescu v. Romania) от 5 сентября 2017 г., жалоба № 61496/08 // Бюллетень Европейского Суда по правам человека. 2017. № 10.

2. Право на информацию

Конвенция прямо не закрепляет право на информацию. Это право включает право на свободу получения информации и на ее распространение. В настоящее время Интернет стал одним из основных средств, с помощью которых каждый человек может осуществлять свое право на свободу получать и распространять информацию и идеи. Интернет предоставляет необходимые инструменты для участия в обсуждениях, касающихся политических тем и вопросов, представляющих публичный интерес. Интернет играет важную роль в расширении доступа общественности к новостям и содействует распространению информации в целом[3].

Европейский Суд уже приходил к выводу, что совместное использование или разрешение другим лицам делиться различными файлами в Интернете, даже материалами, защищенными авторским правом, и в целях получения прибыли, подпадает под действие права «получать и распространять информацию» в соответствии со статьей 10 Конвенции (право на свободу выражения мнений)[4]. Однако в подобных делах национальные суды должны устанавливать надлежащий баланс, то есть уравновешивать конкурирующие интересы, поставленные на карту: право одних лиц получать и распространять информацию и необходимость защиты авторских прав других лиц.

Учитывая, что Интернет играет важную роль в повседневной жизни огромного количества людей, Европейский Суд отмечал относительно, например, сервиса YouTube, что он является одной из платформ, которые позволяют распространять информацию, представляющую особый интерес, в частности, по политическим и социальным вопросам, и создавать гражданскую журналистику[5].

Европейский Суд не раз констатировал, что Договаривающиеся Государства не обязаны предоставлять заключенным доступ в Интернет или к конкретным интернет-сайтам. Однако если государство предусматривает возможность предоставления заключенным такого доступа, оно должно указать причины отказа в доступе к определенным сайтам[6].

[3] См.: Постановление Европейского Суда по делу «Дженгиз и другие против Турции» (Cengiz and Others v. Turkey) от 1 марта 2016 г., жалобы №№ 48226/10 и 14027/11, §§ 49, 52 // http://hudoc.echr.coe.int/eng?i=001-159188.

[4] См.: Решение Европейского Суда по делу «Фредрик Ней и Петер Сунде Колмисоппи против Швеции» (Fredrik Neij and Sunde Kolmisoppi v. Sweden) от 19 февраля 2013 г., жалоба № 40397/12 // Прецеденты Европейского Суда по правам человека. 2016. № 6.

[5] См.: упомянутое выше Постановление Европейского Суда по делу «Дженгиз и другие против Турции», § 52.

[6] См.: Постановление Европейского Суда по делу «Янковскис против Литвы» (Jankovskis v. Lithuania) от 17 января 2017 г.,

Если, например, власти отказывают в предоставлении доступа к сайтам, содержащим правовую информацию, то без разумного обоснования необходимости данного ограничения может иметь место нарушение права на свободу выражения мнения[1].

Европейский Суд не раз подчеркивал в своей практике значимость Интернета как жизненно важного инструмента в реализации права на свободу выражения мнения. В отношении России он рассматривал дела относительно различных видов блокировок веб-сайтов и устанавливал нарушение права на свободу выражения мнения. Среди прочего, он устанавливал, что положения Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», используемые для блокировки вебсайтов, имели чрезмерные и произвольные последствия и не обеспечивали надлежащих гарантий против злоупотреблений[2].

В некоторых делах Европейский Суд анализировал вопрос о том, может ли размещение гиперссылки привести к какому-либо виду юридической ответственности. По его мнению, в каждом случае необходима индивидуальная оценка. Однако прямая и строгая ответственность (без анализа обстоятельств конкретного дела) за использование гиперссылки может подорвать поток информации в Интернете, оказывая на авторов статей и издателей «сдерживающий эффект» в отношении использования таких ссылок, что отрицательно скажется на свободе выражения мнения в Интернете[3].

3. Право на забвение

Эффективность реализации правовых норм в целом и прав субъектов данных в частности в значительной степени зависит от наличия соответствующих механизмов. В эпоху цифровых технологий обработка персональных данных становится повсеместной, и все труднее бывает ее понимать и регулировать. Предоставление субъектам данных права на удаление их собственных данных особенно важно для эффективной реализации принципов защиты данных и, в частности, принципа минимизации данных (то есть личные данные и их обработка/использование должны быть ограничены теми целями, для которых они обрабатываются).

Право на удаление (англ. *right to erasure*) представляет собой расширенный вариант так называемого права на забвение. Данное право было признано Решением Суда Европейского союза в деле «Компании “Гугл Спейн СЛ” и “Гугл Инк.” против Испанского агентства по защите данных (AEPD) и Марио Костехи Гонсалеса » 2014 года[4].

В настоящее время право на удаление содержится в правовых документах Совета Европы и ЕС. Так, например, пункт 2 статьи 8 Хартии об основных правах закрепляет право на доступ к собственным данным и право на исправление в них ошибок. Общий регламент ЕС по защите данных[5] наделяет субъектов персональных данных правами, предоставляя им права в отношении контролеров данных. Помимо прав на доступ и исправление информации, в указанном Регламенте признается ряд других прав, например право на удаление («право быть забытым»), право возражать против обработки данных или ограничивать ее.

Аналогичные гарантии, позволяющие субъектам персональных данных осуществлять над ними эффективный контроль, также включены в измененную Конвенцию о защите физических лиц при автоматизированной обработке персональных данных № 108, которая прямо устанавливает, что каждый человек имеет право на удаление неточных, ложных или незаконно обработанных данных[6]. Договаривающиеся Стороны должны обеспечивать, чтобы эти права были доступны каждому субъекту данных в пределах их юрисдикции и сопровождались эффективными правовыми и практическими средствами, позволяющими субъектам данных осуществлять их.

жалоба № 21575/08 // Прецеденты Европейского Суда по правам человека. 2018. № 1.

[1] См.: Постановление Европейского Суда по делу «Калда против Эстонии» (Kalda v. Estonia) от 19 января 2016 г., жалоба № 17429/10 // Бюллетень Европейского Суда по правам человека. 2016. № 11.

[2] См.: Постановления Европейского Суда по делам «Владимир Харитонов против Российской Федерации» (Vladimir Kharitonov v. Russia) от 16 ноября 2020 г., жалоба № 10795/14 // Прецеденты Европейского Суда по правам человека. 2015. № 8; «ООО “Флавус” и другие против Российской Федерации» (OOO Flavus and Others v. Russia) от 16 ноября 2020 г., жалобы №№ 12468/15, 23489/15 и 19074/16 // Бюллетень Европейского Суда по правам человека. 2021. № 4; «Булгаков против Российской Федерации» (Bulgakov v. Russia) от 16 ноября 2020 г., жалоба № 20159/15 // Российская хроника Европейского Суда. 2021. № 1.

[3] См.: Постановление Европейского Суда по делу «Компания Magyar Jeti Zrt против Венгрии» (Magyar Jeti Zrt v. Hungary) от 4 декабря 2018 г., жалоба № 11257/16 // Бюллетень Европейского Суда по правам человека. 2020. № 12.

[4] См.: Решение Суда Европейского союза по делу «Компании “Гугл Спейн СЛ” и “Гугл Инк.” против Испанского агентства по защите данных (AEPD) и Марио Костехи Гонсалеса» (Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González) от 13 мая 2014 г., дело № C-131/12 // Бюллетень Европейского Суда по правам человека. 2015. № 2.

[5] См.: пункт 6 Регламента Европейского парламента и Совета Европейского союза от 27 апреля 2016 г. № 2016/679 «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных», а также об отмене Директивы 95/46/ЕС (Общий регламент о защите персональных данных / General Data Protection Regulation /GDPR).

[6] См.: подпункт «e» пункта 1 статьи 9 измененной Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных (Конвенция 108+) // https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=108.

Согласно законодательству ЕС[1], контролеры должны удалять персональные данные без неоправданной задержки при наличии одного из следующих условий: 1) персональные данные больше не нужны в отношении целей, для которых они были собраны или обработаны; 2) субъект данных отозвал согласие, на котором была основана обработка, и при этом нет другого правового основания для такой обработки; 3) субъект данных возражает против обработки, и отсутствуют правовые основания для ее проведения, или субъект данных возражает против обработки персональных данных для целей прямого маркетинга; 4) персональные данные были незаконно обработаны; 5) персональные данные должны быть удалены в целях исполнения обязанности, предусмотренной законодательством ЕС или государства-члена, которому подчиняется контролер; 6) персональные данные были собраны в связи с предложением услуг информационного общества непосредственно ребенку.

При этом бремя доказывания того, что обработка данных является законной, возложено на контролеров данных, поскольку именно они несут ответственность за законность обработки[2]. В соответствии с принципом подотчетности контролер должен в любое время иметь возможность продемонстрировать, что существует прочная правовая основа для обработки данных, в противном случае обработка должна быть приостановлена[3]. При этом право на забвение не абсолютно и предусматривает несколько исключений. Например, когда обработка персональных данных необходима для: 1) осуществления права на свободу выражения мнений; 2) соблюдения юридического обязательства, которое требует обработки данных в соответствии с законодательством ЕС или государства-члена, которому подчиняется контролер; 3) для выполнения задачи, выполняемой в общественных интересах; 4) при осуществлении официальных полномочий, возложенных на контролера; 5) если того требует общественный интерес в области здравоохранения; 6) для целей архивирования в общественных интересах, в целях научных или исторических исследований или в статистических целях.

При этом, если контролер сделал персональные данные общедоступными и должен удалить эту информацию, он обязан принять разумные меры для информирования других контролеров, которые обрабатывают те же данные, о запросе субъекта данных на удаление.

Рассмотренное правовое регулирование предполагает достаточно широкие возможности для законодателей правоприменителей стран – членов ЕС, что может повлечь за собой нарушение прав субъектов персональных данных. Для того чтобы рассмотреть, как реализуются анализируемые нормы, видится необходимым рассмотреть практику их применения.

3.1. Судебная практика

Европейский Суд по правам человека

В деле «Сегерстедт-Виберг и другие против Швеции»[4] заявители жаловались на то, что информация о них была внесена в базы данных полиции, и потребовали ее удаления. Власти государства-ответчика обосновывали необходимость сохранения таких данных интересами национальной безопасности. Хотя Европейский Суд отметил, что само по себе хранение персональных данных имело законное основание и преследовало законную цель, он решил, что дальнейшее хранение таких данных будет являться несоразмерным вмешательством в частную жизнь заявителей. В связи с этим он установил нарушение статьи 8 Конвенции в отношении четырех из пяти заявителей, поскольку, учитывая длительный промежуток времени, который прошел с момента совершения предполагаемых противоправных действий заявителями, дальнейшее хранение этих данных не имело отношения к делу.

Суд Европейского союза

В упомянутом деле «Компании “Гугл Спейн СЛ” и “Гугл Инк.” против Испанского агентства по защите данных (AEPD) и Марио Костехи Гонсалеса»» Суд ЕС рассмотрел вопрос о том, должна ли компания Google удалять уже устаревшую информацию о финансовом положении лица из результатов поиска[5]. Компания Google утверждала, что ее функции сводятся к простому предоставлению гиперссылки на веб-страницу издателя газеты, на которой размещена информация, сообщающая о несостоятельности заявителя. Компания отмечала, что запрос на удаление устаревшей информации с веб-страницы должен быть сделан в адрес самой веб-страницы, а она же просто предоставляет ссылку на исходную страницу. Однако Суд ЕС пришел к выводу, что компания Google, когда она ищет информацию в Интернете и индексирует контент для предостав-

[1] См.: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), article 17.

[2] См.: пункт 1 статьи 17 Общего регламента ЕС о защите персональных данных.

[3] См.: там же, пункт 2 статьи 5.

[4] См.: Постановление Европейского Суда по делу «Сегерстедт-Виберг и другие против Швеции» (Segerstedt-Wiberg and Others v. Sweden) от 6 июня 2006 г., жалоба № 62332/00, §§ 89–90 // http://hudoc.echr.coe.int/eng?i=001-75591.

[5] См.: упомянутое выше Решение Суда Европейского союза по делу «Компании “Гугл Спейн СЛ” и “Гугл Инк.” против Испанского агентства по защите данных (AEPD) и Марио Костехи Гонсалеса», §§ 55–58.

ления результатов поиска, становится контролером данных, на которого распространяются обязательства в соответствии с законодательством ЕС.

Суд ЕС пояснил, что поисковые системы в Интернете и результаты поиска, предоставляющие персональные данные, могут установить подробный профиль человека[1]. В частности, по мнению Суда ЕС, необходимо искать справедливый баланс между законным интересом пользователей Интернета в доступе к информации и основными правами субъекта данных в соответствии со статьями 7 и 8 Хартии ЕС об основных правах. Во все более оцифрованном обществе требование о том, чтобы личные данные были точными и не выходили за рамки необходимого (например, общедоступной информации), является фундаментальным для обеспечения высокого уровня защиты персональных данных отдельных лиц. Право на удаление личных данных, когда их обработка больше не нужна, также распространяется на контролеров данных, которые копируют персональную информацию[2].

Анализируя, требовалось ли от компании Google удалить ссылки, связанные с заявителем, Суд ЕС постановил, что при определенных условиях люди имеют право требовать удаления личных данных. На это право можно ссылаться, если информация, относящаяся к физическому лицу, является неточной, неадекватной, неуместной или чрезмерной для целей обработки данных. Суд ЕС признал, что это право не является абсолютным: оно должно быть сбалансировано с другими правами и интересами, в частности интересами широкой общественности в доступе к определенной информации. Каждый запрос на удаление должен оцениваться в индивидуальном порядке, чтобы обеспечить баланс между основными правами на защиту личных данных и частной жизни субъекта данных, с одной стороны, и законными интересами всех пользователей Интернета, включая издателей, с другой. Суд ЕС также определил факторы, которые следует учитывать в ходе этой балансировки. Наиболее важным из них является природа рассматриваемой информации. Если она относится к частной жизни человека и нет общественного интереса в доступности информации, защита данных и конфиденциальность будут иметь приоритет над правом общественности на доступ к информации. Напротив, если оказывается, что субъект данных является публичным лицом или что информация имеет такой характер, что оправдывает ее доступность для широкого круга лиц, тогда преобладающий интерес общественности в доступе к информации может оправдывать вмешательство в основные права субъекта данных на защиту данных и конфиденциальность.

Для реализации данного Решения Суда ЕС были приняты Руководящие принципы[3], которые включают в себя список общих критериев, которые надзорные органы должны использовать при рассмотрении жалоб, связанных с запросами отдельных лиц на удаление их персональных данных.

В другом деле[4] Суд ЕС должен был проверить, имело ли физическое лицо право на удаление своих персональных данных, опубликованных в публичном реестре компаний после того, как его компания была ликвидирована. Пытаясь найти баланс между правом физического лица на защиту своих личных данных и интересом широкой общественности в доступе к информации, Суд ЕС сначала изучил цель публичного реестра. Он указал на тот факт, что раскрытие информации было предусмотрено законом, в частности директивой ЕС, направленной на облегчение доступа к информации компании третьим лицам. Целью раскрытия информации была гарантия правовой определенности в связи с активизацией торговли между государствами-членами, и требовалось удостовериться, что третьи стороны имеют доступ ко всей соответствующей информации о компаниях в ЕС.

Суд ЕС также отметил, что даже после ликвидации компании права и юридические обязательства, связанные с нею, часто продолжают существовать. Судебные разбирательства, касающиеся ликвидации, могут быть длительными, и вопросы, касающиеся компании, ее менеджеров, могут возникать в течение многих лет после прекращения существования компании. Из-за законной цели раскрытия и трудностей с установлением периода, по истечении которого личные данные могут быть удалены из реестра без ущерба для интересов третьих лиц, Суд ЕС постановил, что в подобной ситуации право на удаление личных данных лица не может быть гарантировано.

4. Правовое регулирование в Российской Федерации

Статья 21 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» устанавливает случаи, когда допускается блокирование или уничтожение персональных данных. К ним

[1] Упомянутое выше Решение Суда Европейского союза по делу «Компании “Гугл Спейн СЛ” и “Гугл Инк.” против Испанского агентства по защите данных (AEPD) и Марио Костехи Гонсалеса», §§ 36, 38, 80–81 и 97.

[2] Там же, § 88.

[3] Статья 29 руководящих принципов Рабочей группы по выполнению упомянутого выше Решения Суда Европейского союза по делу «Компании “Гугл Спейн СЛ” и “Гугл Инк.” против Испанского агентства по защите данных (AEPD) и Марио Костехи Гонсалеса».

[4] См.: Решение Суда Европейского союза по делу «Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni» от 9 марта 2017 г., дело № C-398/15 // https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62015CJ0398.

относятся: 1) выявление неправомерной обработки персональных данных; 2) выявление неточных персональных данных; 3) достижение цели обработки персональных; 4) отзыв субъектом персональных данных согласия на обработку его персональных данных; 5) если сохранение персональных данных более не требуется для целей обработки персональных данных; 6) отсутствие возможности уничтожения персональных данных в течение срока, предусмотренного данным Законом. В соответствии со статьей 8 этого Закона сведения о субъекте персональных данных должны быть в любое время исключены из общедоступных источников персональных данных по требованию такого субъекта персональных либо по решению суда или иных уполномоченных государственных органов.

С 1 марта 2021 г. вступили в силу поправки к данному Федеральному закону. В частности, в него была включена новая статья 10.1, которая закрепляет особенности обработки персональных данных, разрешенных субъектом персональных данных для распространения. Предполагается, что эти изменения будут способствовать более эффективной защите прав субъектов персональных данных.

Вывод

Подводя итог, стоит отметить, что, хотя за последние 50 лет технологии совершили огромный прорыв и информация стала наиболее ценным ресурсом, права человека в основном остались такими же, как они и были закреплены в первых международно-правовых актах о правах человека. Благодаря эволютивному толкованию, которое дает Европейский Суд, содержание прав и свобод претерпевает определенные изменения, чтобы соответствовать реалиям современного времени.

Именно государства в первую очередь обязаны защищать и обеспечивать реализацию прав человека, прежде всего, посредством принятия соответствующего законодательства. Однако при этом государства постоянно сталкиваются с необходимостью установления баланса между конкурирующими публичными и частными интересами. И хотя государства имеют некую свободу усмотрения, в практике Европейского Суда и Суда ЕС были выработаны критерии, которые должны учитываться законодателем и правоприменителем, в том числе при защите прав человека в информационном обществе.

Библиографический список

1. *Carey Peter*. Data protection: A practical guide to UK and EU law. Oxford: Oxford University Press, 2009. 529 p.

2. *Hornung Gerrit*. Christoph Schnabel, Data protection in Germany I: The population census decision and the right to informational self-determination // Computer Law and Security Review. 2009. Vol. 25. Issue 1. P. 84–88.

3. *Kodde Claudia*. Germany's «Right to be forgotten» – between the freedom of expression and the right to informational self-determination // International Review of Law, Computers and Technology. 2016. Vol. 30. P. 17–31.