Цифровые технологии в правоохранительной деятельности: критерии правомерного сочетания публичных и частных интересов

Е.А. Мамай

***Аннотация*— В статье рассматривается использование цифровых технологий в правоохранительной деятельности сквозь призму соотношение публичных и частных интересов. Проанализирована система нормативного и правоприменительного регулирования, изучены нормативные правовые акты, регламентирующие отношения, складывающиеся в сфере использования информационно-телекоммуникационных технологий, изучено более 30 постановлений, определений и иных решений, принятых различными судебными инстанциями в России, а также более 20 решений Европейского суда по правам человека. Сравнительно-правовой материал получен автором в рамках проведения исследования законодательства некоторых зарубежных стран, в частности США, Соединенного Королевства Великобритании и Северной Ирландии, Франции, а также Европейского союза в целом. Полученные результаты позволили определить достигнутый уровень регулирования цифровых правоотношений с точки зрения сбалансированности интересов отдельных лиц, общества и государства в достижении частных и публичных интересов. Были выявлены пробелы и диспропорции в нормативном и правоприменительном регулировании рассматриваемой сферы, определены ключевые направления для их совершенствования.**

***Ключевые слова*— частная жизнь, электронные данные, база данных, баланс, правоохранительная деятельность, конкурирующие публичные и частные интересы, Европейский суд по правам человека, Конституционный суд Российской Федерации**

I. Теоретическое обоснование

В эпоху всеобщей цифровизации и развития информационно-комуникационных технологий (далее по тексту – ИКТ) граница между сферой приватности и публичности постепенно стирается. Интернет и современные технологии несут в себе значимый позитивный потенциал, определяющийся возможностями широкой коммуникации с людьми по всему миру, доступностью различной информации и сервисов, в том числе предоставляемых государством, открытием новых перспектив для экономических отношений в мире современной глобализации. Другой стороной того же процесса становится множество уязвимостей, каналов утечек информации, появление возможностей для вторжения в частную жизнь, нарушения личной и семейной тайны, неприкосновенности личной корреспонденции, тайны переписки и сообщений.

Основателями концепции неприкосновенности частной жизни (privacy concept) считаются американские юристы Луи Брандейс и Сэмюэл Уоррен, которые не только впервые обратили внимание на важность обеспечения неприкосновенности частной жизни каждого человека, но и предсказали угрозы нарушения такового в силу развития средств массовой информации, которые, к слову сказать, на момент их жизни ограничивались сугубо печатными изданиями [1].

В современном мире в силу развития ИКТ противоречия между всеобщей цифровизацией и приватностью стали предметом многих научных исследований. Библиометрический анализ, проведенный М.Свенссоном, К. Розенгреном, Ф.Острёмом (2016), показывает, что научные исследования в области пограничной между цифровизацией и конфиденциальностью довольно строго разделены, в основном, между тремя научными областями [2].

Во-первых, это сугубо технические исследования, нацеленные на разработку соответствующих систем и технологических решений охраны частной жизни. В этой связи изучаются технологии защиты конфиденциальности, именуемые «Trusted Computing» [3, 4], «Privacy Aware Design» [5] и «Privacy by Design» [6]. Во многих статьях информационные технологии оцениваются особенно критично, в силу чего авторы предлагают ограничения и минимизацию их использования в целях обеспечения неприкосновенности частной жизни [7, 8, 9].

Вторую группу наук составляют социальные науки, включая психологию, социологию, политологию, маркетинговые, управленческие исследования и многие другие. Исследования в данных областях ориентированы на изучение поведенческих особенностей участников цифровой коммуникации, в частности восприятие концепции приватности вообще [10], обучение цифровой безопасности [11], влияние цифровой грамотности на изменение поведенческих стереотипов [12, 13] и др.

Наконец, значительную группу составляют собственно юридические исследования, которые фокусируется на вопросах законодательной регламентации защиты частной жизни. Таковые в

Статья получена 20 октября 2022.
Мамай Евгений Алексеевич, кандидат юридических наук, доцент, Национальный исследовательский университет «Высшая школа экономики» (Нижний Новгород), доцент кафедры теории и истории права и государства, ORCID 0000-0002-9386-2747 (emamaj@hse.ru)
Статья подготовлена по итогам выступления на Международной объединённой конференции «Интернет и современное общество» (IMS-2022).

основном акцентируют внимание на двух взаимосвязанных сферах правового регулирования: регулирование производства информации различного рода и ее охрана от неправомерного использования, в том числе субъектами публичной власти. Объектами изучения в данном случае становятся цифровые права граждан [14, 15], цифровые средства идентификации личности [16, 17, 18], право на информацию, производимую пользователями средств цифровой коммуникации [19], хранение и использование персональных данных [20, 21, 22, 23]. Во втором десятилетии XXI века, особенно в годы, последовавшие за разоблачениями, опубликованными Эдвардом Сноуденом, на первые позиции в юридических публикациях вышли вопросы законности осуществления массовой слежки и защищенности населения от вмешательства властей в их частную жизнь [24, 25, 26, 27].

Отечественная юриспруденция в целом следует общим трендам развития правовой науки, но в значительной своей части акцентирует внимание на узко-специализированных, отраслевых аспектах защиты персональных данных и обеспечения неприкосновенности частной жизни [28, 29, 30, 31, 32, 33].

Важно отметить, что неприкосновенность частной жизни юридически гарантирована как на международном, так и национальном уровне. Недопустимость произвольного вмешательства в личную и семейную жизнь, посягательства на неприкосновенность жилища, тайны корреспонденции закреплена во Всеобщей декларации прав человека 1948 года (статья 12), Международном пакте о гражданских и политических правах 1966 года (статья 17), Европейской конвенции о защите прав человека и основных свобод 1950 года (статья 8, далее - Конвенции), многочисленных документах Европейского союза, Организации по безопасности и сотрудничеству в Европе и др. Без учета специфики цифровой сферы защита частной жизни гарантирована также статьей 23 Конституции Российской Федерации. Более того, в части 1 статьи 55 Конституции России сказано, что перечисление в указанном правовом акте основных прав и свобод не должно толковаться как отрицание или умаление других общепризнанных прав и свобод человека и гражданина. Таким образом, основной закон нашей страны открывает возможность для обеспечения правовых гарантий реализации прав граждан, в том числе в такой новой сфере общественных отношений как цифровая среда. Конституция России также четко определяет цели, в соответствии с которыми допустимо ограничение прав и свобод человека и гражданина (ч. 3 ст. 55). Таковое может осуществляться на основании федерального закона и только в той мере, в какой это необходимо *в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства (курсив наш – **Е.М.**).*

Важно отметить, что нередко нарушение неприкосновенности частной жизни становится необходимым для сохранения общественного порядка и обеспечения безопасности государства, борьбы с преступностью, предотвращения иных правонарушений, изобличения лиц, их совершивших, идентификации лиц, пропавших без вести и т.д. Декларируемая и гарантированная международными и национальными правовыми актами неприкосновенность частной жизни неизбежно становится полем столкновения частных и публичных интересов, между которыми принципиально важно найти должный баланс.

II. Гипотезы, цели, методика, объект и предмет исследования

Отечественное законодательство заимствовало многие стандарты в сфере охраны частной жизни из международного права, зарубежного законодательства и практики деятельности международных судебных инстанций. Так, долгое время система национального правового регулирования в нашей стране корректировалась с учетом практики Европейского суда по правам человека (далее по тексту - ЕСПЧ). На текущий момент ввиду состоявшегося выхода Российской Федерации из Совета Европы представляется важным оценить насколько правовые гарантии неприкосновенности частной жизни нашли свое отражение в отечественном законодательстве и судебной практике. Анонсируя свое намерение выйти из данной международной организации, МИД России заявлял: «Выход нашей страны из этой организации не повлияет на права и свободы российских граждан. В Конституции Российской Федерации установлены не меньшие их гарантии, чем в Европейской конвенции по правам человека. Положения основных договорно-правовых актов Совета Европы включены в российское законодательство» [34].

Исходной посылкой настоящего исследования стали два взаимосвязанных предположения. С одной стороны, длительное ориентирование отечественного законодателя на правовые стандарты обеспечения прав человека в ведущих странах мира не могло не отразиться на концептуальной сущности законодательства, затрагивающего различные аспекты цифровой сферы жизни общества. Определенные гарантии должны были найти свое отражение в законах, а на правоприменительном уровне закономерно должна была сформироваться практика реализации соответствующих норм. С другой стороны, можно предположить, что государство, имея широкий спектр правовых и организационных ресурсов, способно построить механизм взаимодействия с обществом, выгодный для себя, однако в ущерб интересам приватности и сохранения тайны частной жизни.

Объект настоящего исследования составляют подпадающие под правовое воздействие общественные отношения, складывающиеся в процессе использования индивидуальными и коллективными субъектами ИКТ. Предмет исследования составили сформулированные на нормативном правовом уровне социального регулирования и выработанные в референтной правоприменительной (в том числе судебной) практике основополагающие критерии правомерного сочетания

публичных и частных интересов при реализации ограничений правоохранительного характера в сфере ИКТ. Сознавая возможные разночтения в понимании терминов в рамках настоящего исследования мы будем использовать понятия «цифровые правоотношения», «правоотношения в сфере использования информационно-телекоммуникационных технологий» в качестве синонимов, означающих урегулированные нормами права общественные отношения, опосредованные компьютерами и иными ИКТ, в том числе сетью Интернет. Говоря о вышеобозначенной предметной области, мы будем использовать понятие «неприкосновенность частной жизни» для обозначения всей совокупности частных интересов, сопровождающих использование соответствующих технологий.

Цель настоящего исследования – формирование критериальной модели сопряжения и сбалансированности частных и публичных интересов в сфере цифровых правоотношений. Исходя из этого задачами могут быть определены: 1) выявление правовых гарантий неприкосновенности частной жизни в законодательстве, 2) определение состояния нормативно-правовой урегулированности таких гарантий на подзаконном нормативном уровне и их фактической реализации в правоприменительной сфере.

Методология исследования базируется на применении формально-юридического (догматического) метода научного познания, изучении доктринальных источников, системном, сравнительно-правовом, технически-юридическом и контент-анализе отечественного и зарубежного законодательства, а также материалов правоприменительной практики.

В рамках исследования автором изучено более 25 нормативных правовых актов, регламентирующих отношения, складывающиеся в сфере использования ИКТ, проанализировано более 30 постановлений, определений и иных решений, принятых различными судебными инстанциями в России, в том числе 20 решений, отражающих правовые позиции Конституционного суда Российской Федерации и Верховного суда Российской Федерации по вопросу ограничения конституционных прав человека и гражданина, а также более 20 решений Европейского суда по правам человека, принятым по делам связанным с ограничением неприкосновенности частной жизни в контексте использования ИКТ.

Сравнительно-правовой материал получен автором в рамках проведения исследования законодательства некоторых зарубежных стран, в частности США, Соединенного Королевства Великобритании и Северной Ирландии, Франции, а также Европейского союза в целом.

Помимо этого нами проведен экспертный опрос свыше 30 сотрудников правоохранительных органов на предмет правоприменительной практики использования ими ИКТ в свое профессиональной деятельности.

Изучение автором представленного массива информации позволило ему выявить и обобщить критерии правомерного ограничения неприкосновенности частной жизни, как закономерного средства установления должного баланса частных и публичных интересов.

III. Результаты исследования

В правоохранительной сфере ИКТ в основном используются как непосредственные источники юридически-значимой информации, средства и способы получения юридически-значимой информации, а также средства и способы хранения и обработки юридически-значимой информации.

В правовом регулировании всех из указанных направлений закономерно встает вопрос, сочетающий в себе комплекс этических и собственно правовой проблем: «Что важнее: публичные или частные интересы?». Со стороны общества, государства такие интересы представлены состоянием безопасности общества от внутренних и внешних угроз, обеспечением общественного порядка, предотвращением преступлений и иных правонарушений, сохранением нравственности в обществе, созданием надлежащих условий для его существования и развития, и т.д. Со стороны индивидов спектр частных интересов также не менее широк: идентификация личности, неприкосновенность личной и семейной тайны, сохранение конфиденциальности переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, свобода слова и самовыражения в цифровом пространстве и т.д.

Изучение массива источников доктринального, нормативного и правоприменительного характера позволило нам сформулировать условия (критерии) правомерного сочетания публичных и частных интересов, которые условно могут быть разделены на три группы:

— критерии правомерности *ante factum*, предшествующие наложению ограничений в сфере цифровых отношений. К таковым нами отнесена четкая законодательная регламентация любых мероприятий, направленных на ограничение конституционных прав граждан (в том числе оперативно-розыскных мероприятий или следственных действий), включая предварительное определение сферы применения ограничений, их продолжительности и круга лиц, в отношении которых таковые должны применяться;

— критерии правомерности *in ipso actu*, сопровождающие наложение ограничений – обязательное получение разрешения на проведение таких действий (предварительная судебная легализация), а также последующий судебный контроль проводимых мероприятий;

— критерии правомерности post factum – гарантии защиты неприкосновенности частной жизни, которые реализуются после наложения ограничений и запретов. К их числу следует отнести: ограничение продолжительности хранения собранных данных в государственных информационных системах и реестрах; установление регламентированного порядка удаления информации из них в автоматическом порядке и по официальному запросу, поступающему от гражданина;

обеспечение возможности информирования граждан о наличии в государственных реестрах информации о них.

A. *Ante factum – законодательная регламентация*

Основополагающим требованием к правомерному введению ограничений и запретов в цифровой среде является их надлежащая *законодательная регламентация:* установление правовых и фактических оснований проведения мероприятий, определение объектов государственного воздействия, предметной области накладываемых ограничений, субъектов, наделенных соответствующими полномочиями, гарантий, исключающих злоупотребление полномочиями со стороны правоохранителей, а также и процедур, которые должны сопровождать вводимые ограничения.

Как правило, критерием установления правомерности ограничений в сфере цифровых правоотношений является относимость совершаемых людьми деяний к определенной категории правонарушений, за которые законодательством (как правило, уголовным) устанавливается конкретный вид и размер наказания. Так, согласно пункту 2 части первой статьи 7 Федерального закона «Об оперативно-розыскной деятельности» (далее по тексту – закон об ОРД) в случае отсутствия достаточных данных для решения вопроса о возбуждении уголовного дела, оперативно-розыскные мероприятия (в том числе связанные с ограничениями неприкосновенности частной жизни) могут быть проведены на основании полученных сведений о признаках подготавливаемого, совершаемого или совершенного противоправного деяния, а также о лицах, его подготавливающих, совершающих или совершивших [35]. При этом под противоправным деянием подразумевается лишь преступление, поэтому, как указал Конституционный Суд Российской Федерации в своем Определении от 14 июля 1998 года, если речь идет об ином виде правонарушений проведение соответствующего оперативно-розыскного мероприятия (далее по тексту – ОРМ) должно быть прекращено[36].

В судебной практике как российских, так и международных судов не раз возникали ситуации, когда ненадлежащая нормативная регламентация вопроса приводила к постановке вопроса о возможной неправомерности действий органов публичной власти (S. and Marper v. United Kingdom [37], Shimovolos v. Russia [38], Ben Faiza v. France [39]). Так, в деле Бен Фаиза против Франции, решение по которому ЕСПЧ вынес в 2018 году, суд рассматривал ситуацию установленного прослушивания телефонных переговоров и слежки за перемещением транспортного средства лица, подозреваемого в торговле наркотиками, однако счел, что французское законодательство на момент допущенного нарушения (в 2010 году) не предусматривало четких ограничений дискреционных полномочий властей по вторжению в сферу частной жизни. Позднее, в 2014 году, как установил сам суд, в соответствующем законодательстве был предусмотрен механизм осуществления геолокационной слежки полицией за подозреваемыми, гарантировав, тем самым защиту их частной жизни.

Важно отметить, что правовая регламентация ограничений любых конституционных прав должна быть осуществлена как собственно на законодательном уровне, так и на уровне подзаконного нормативного регулирования, что, в некоторых случаях, сопряжено с необходимостью решения вопроса о сохранении государственной тайны. В России механизм трансформации сведений, полученных в ходе оперативно-розыскной деятельности (об обнаружении признаков преступления, о результатах проведения оперативно-розыскных мероприятий), в информацию, имеющую доказательственное, уголовно-процессуальное значение прописан в УПК РФ, вышеупомянутом законе об ОРД, а также инструкциях ведомственного характера. Так, существует Инструкция о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд, которая утверждена совместным приказом правоохранительных ведомств от 27 сентября 2013 года [40]. Указанной инструкцией предписано, что результаты ОРД представляются в виде рапорта об обнаружении признаков преступления, который составляется должностным лицом органа, осуществляющего ОРД, в соответствии со статьей 143 УПК РФ и регистрируется в порядке, установленном нормативными правовыми актами органов, осуществляющих ОРД.

В законодательной регламентации наложения запретов и ограничений в сфере использования ИКТ предельно важное значение имеет конкретное *предварительное определение сферы применения ограничений, их продолжительности и круга лиц*, в отношении которых таковые могут осуществляться. В данном случае следует отметить, что цифровые технологии открывают практически безграничные возможности для контроля за жизнью граждан, поэтому принципиально важно, чтобы законодательные гарантии нашли свое непосредственное отражение и в правоприменительной практике. Как отметил ЕСПЧ в своем решении по делу С. и Марпер против Соединенного Королевства (S. and Marper v. the United Kingdom), любое государство, претендующее на роль первопроходца в разработке новых технологий, несет особую ответственность за соблюдение правильного баланса между публичными и частными интересами [37].

Исходным вопросом, определяющим сущность правового регулирования, в данном случае является понимание того, кто может становиться объектом контроля со стороны государства: все лица, осознанно или помимо собственной воли вовлеченные в цифровое пространство, осуществляющие те или иные формы цифровой коммуникации, или только отдельные категории лиц, чья деятельность угрожает охраняемым законом интересам государства, общества и частных лиц.

На текущий момент можно констатировать, что по отношению к обычным гражданам применяются общие правовые гарантии, а отдельное внимание в

законодательной регламентации уделяется защите правового положения тех лиц, чья роль в гражданском обществе особенно велика (правозащитники, журналисты, адвокаты и т.д.). В наделении их таким статусом как законодательство, так и практика разных стран имеют некоторые противоречия. С одной стороны, ЕСПЧ по делу азербайджанского правозащитника Расула Джафарова, принятом в марте 2016 г., выработал строгий стандарт относительно того, каким образом выявлять случаи политически мотивированного преследования правозащитников [41]. С другой стороны, известны случаи, когда страны, позиционирующие себя как либерально-демократические, активно используют имеющиеся технологии для защиты своих интересов от «неправильных» правозащитников. Так, в деле Кэтт против Соединенного Королевства (Catt v. the United Kingdom) [42] заявитель, являющийся активистом правозащитного движения обжаловал включение и хранение его персональных данных в полицейской базе «внутренних экстремистов». В другом деле «Дагрегорио и Москони против Франции» (Dagregorio and Mosconi v. France) [43] обжаловалось задержание и принуждение двоих активистов профсоюзного движения к прохождению обязательной биологической регистрации, результаты которой должны были быть включены в национальную геномную базу данных (FNAEG).

В России в силу неопределенности статуса правозащитников их положение не защищено какими-то особыми правовыми гарантиями. К примеру, дело Шимоволос против России (Shimovolos v. Russia) [38] выявило проблему существования баз данных в отношении лиц, вовлеченных, по мнению правоохранителей, в экстремистскую деятельность, что позволяет им отслеживать перемещение зарегистрированных лиц и осуществлять в отношении них профилактические мероприятия. Ведение таких баз данных регламентировано нормативными правовыми актами, имеющими подзаконный уровень и закрытый характер, что оставляет широкий простор для дискреционных полномочий властей.

По общей сложившейся практике строгими гарантиями от неправомерного вмешательства в их частную жизнь защищены *журналисты, адвокаты и судьи*, поскольку осуществление ими своих профессиональных полномочий невозможно без ограничения внешнего влияния на их деятельность.

В деле Нагла против Латвии (Nagla v. Latvia) [44] ЕСПЧ рассмотрел заявление *журналиста*, опубликовавшего материалы о налоговых правонарушениях публичных должностных лиц. Поскольку такие сведения были получены от хакера, осуществившего взлом государственной налоговой базы данных, полиция посчитала правомерным изъятие у заявительницы цифровых носителей информации, открывавших первичные источники журналистского расследования. Суд же усмотрел в деле нарушение статьи 10 Конвенции (свобода слова). Он подчеркнул, что право журналиста не раскрывать свои источники нельзя рассматривать как привилегию, зависящую от законности или незаконности таких источников, а скорее как неотъемлемую часть права на информацию, к которой следует относиться с максимальной осторожностью.

В России, как отмечают эксперты, должного процессуального обеспечения сохранности журналисткой тайны также не существует [45]. Закон о средствах массовой информации предусматривает *обязанность* редакции средства массовой информации *сохранять в тайне источник информации*, предоставивший сведения с условием неразглашения его имени, за исключением случая, когда соответствующее требование поступило от суда в связи с находящимся в его производстве делом [46]. При этом *журналисты не указаны* в числе лиц, которые в соответствии с частью 3 статьи 56 УПК РФ *не подлежат* допросу в качестве свидетелей, поэтому правоохранители, когда им это необходимо, обходят предусмотренный законом о СМИ запрет, привлекая журналистов в процессуальном статусе свидетелей.

В отличие от вышеуказанной категории адвокаты, защитники, судьи и даже священнослужители пользуются значительно большими правовыми гарантиями. Так, Стандарты независимости юридической профессии Международной ассоциации адвокатов (приняты 7 сентября 1990 года) указывают на необходимость обеспечения независимости адвокатов при оказании ими юридической помощи подзащитным и сохранения конфиденциальности соответствующих отношений, *включая защиту обычной и электронной систем адвокатского делопроизводства, документов* адвоката от изъятия и проверок, а также защиту от вмешательств *в используемые электронные средства связи и информационные системы* [47].

В российском законодательстве статус адвоката обеспечен особыми мерами правовой защиты. Так, ч. 3 ст. 8 ФЗ «Об адвокатской деятельности и адвокатуре в Российской Федерации» [48] предусмотрено, что «проведение оперативно-розыскных мероприятий и следственных действий в отношении адвоката (в том числе в жилых и служебных помещениях, используемых им для осуществления адвокатской деятельности) допускается *только на основании судебного решения*». Также в соответствии с уголовно-процессуальным законодательством России (ст. 447 УПК РФ) адвокаты, наряду с депутатами, судьями, прокурорами, следователями и другими, отнесены к категории лиц, в отношении которых применяется особый порядок производства по уголовным делам. В частности, уголовное дело в отношении данной категории граждан возбуждается руководителем следственного органа Следственного комитета Российской Федерации по субъекту Российской Федерации.

В судебной практике имеются случаи, когда адвокаты привлекались к уголовной ответственности за совершаемые ими преступления, при этом выносимые приговоры основывались на результатах ОРМ, ограничивающих конституционное право на неприкосновенность частной жизни. Как отметил

Конституционный Суд Российской Федерации, институт адвокатской тайны призван защищать информацию, полученную адвокатом относительно клиента или других лиц в связи с предоставлением юридических услуг [49], а судебная легализация при проведении в отношении адвоката ОРМ и следственных действий касается лишь сферы осуществления им собственно адвокатской деятельности, а не совершаемого им самим преступного деяния, как несовместимого со статусом адвоката [50].

В тоже время имеющаяся судебная практика свидетельствует, что суды первой инстанции нередко нарушают требования уголовно-процессуального законодательства, разрешая проведение обысков у адвоката в отсутствие в отношении него уголовного дела или привлечения его в качестве обвиняемого, если дело возбуждено в отношении других лиц [51]. Так, в деле «Колесниченко против России» [52] ЕСПЧ усмотрел нарушения Конвенции в том, что судом было разрешено следственному органу провести обыски в жилище и конторе адвоката, который не подозревался в совершении какого-либо преступления, а являлся защитником обвиняемого по уголовному делу.

Судьи, также как и адвокаты, защищены законом от неправомерного вмешательства в их жизнь. Использование результатов ОРМ, ограничивающих неприкосновенность частной жизни, в качестве доказательств по делам в отношении судей не допускается без наличия судебного решения или его копии в материалах уголовного дела [53]. В тоже время в силу возможного влияния корпоративной среды и сокрытия судейским сообществом преступлений, совершаемых коллегами, правоприменительная практика сформировала следующий механизм соблюдения установленных гарантий. Так, 9 июля 2009 года судебная коллегия в составе трех судей Краснодарского краевого суда дала разрешение Управлению ФСБ России по Ростовской области на ограничение прав судьи районного суда города Ростова-на-Дону И.В. Аносова на тайну телефонных и иных переговоров, на неприкосновенность занимаемых им служебных и жилых помещений, служебного и личного автотранспорта и проведение в отношении него соответствующих оперативно-розыскных мероприятий [54]. Целью таких мероприятий стала проверка информации о действиях И.В. Аносова, содержащих признаки особо тяжкого преступления (статья 290 «Получение взятки» УК РФ). Позднее в закон об ОРД были внесены изменения и предусмотрено, что при наличии обоснованных опасений относительно возможности рассекречивания ОРМ, планируемых в отношении судьи, указанного в абзаце третьем пункта 7 статьи 16 Закона Российской Федерации от 26 июня 1992 года № 3132-1 «О статусе судей в Российской Федерации», материалы о проведении ОРМ на основании решения Председателя Верховного Суда Российской Федерации или его заместителя, могут быть переданы для рассмотрения в иной равнозначный суд [35].

Отдельный вопрос, требующий внимания в силу принципиально новых возможностей, обусловленных развитием ИКТ, представляют собой базы данных, обеспечивающие учет сведений о человеке и гражданине, законность ведения которых (в широком смысле этого слова) следует рассматривать в качестве одного из основополагающих критериев правомерного ограничения частной жизни.

В современном обществе ведется широкая дискуссия о том, что ИКТ и собираемые большие данные позволяют осуществлять косвенную идентификацию личности, хотя при этом формально могут не нарушаться правила автоматической обработки информации. Для этого, например, достаточно проведение анализа совокупности фактов совершения множества однотипных действий, поисковых запросов, покупок, имеющих общую временную и геолокационную привязку [55]. Более того, как утверждается, даже шифрование данных, не способно преодолеть всего комплекса угроз, ибо действует техническое правило: «все, что зашифровано, может быть дешифровано»» [56, с. 7].

Базы данных, находящиеся в руках информационно-коммуникационных сервисов, операторов связи и провайдеров информационных услуг в настоящее время не имеют исчерпывающей правовой регламентации, оставаясь «серой» зоной соприкосновения публичных и частных интересов. Должной законодательной регламентацией обладает лишь геномная и дактилоскопическая регистрация, которые благодаря развитию ИКТ постепенно сливаются в общий стандарт криминалистической регистрации, становятся важными инструментами в руках правоохранительных органов и нередко становятся предметом судебных споров в силу масштабирования пределов их применения (см. дела, рассмотренные ЕСПЧ: S. and Marper v. the United Kingdom, M.K. v. France, Gaughran v. the United Kingdom). С точки зрения реализации публичных интересов оба вида регистрации обладают очевидными преимуществами, открывая возможности для достоверной идентификации личности в различных правоприменительных ситуациях, однако этот же фактор становится определяющим, когда в адрес правоохранителей сыпятся обвинения в создании «полицейского государства».

Государственная дактилоскопическая регистрация в Российской Федерации имеет достаточно длительную историю, и в настоящее время осуществляется на основании Федерального закона «О государственной дактилоскопической регистрации в Российской Федерации» [57]. Данный закон содержит перечень из тридцати пяти категорий лиц, к которым применяется обязательное дактилоскопирование. В частности, таковому подлежат граждане Российской Федерации, иностранные граждане и лица без гражданства: *подозреваемые* в совершении преступления, *обвиняемые* в совершении преступления, *осужденные* за совершение преступления, *подвергнутые* административному аресту, а также совершившие административное правонарушение, если установить их личность иным способом невозможно.

Основные задачи по ведению баз дактилоскопической информации выполняет аппарат МВД России, взаимодействующий со множеством субъектов, чья деятельность строго регламентирована актами Правительства РФ [58], десятками ведомственных нормативно-правовых актов, а также совместными приказами межведомственном уровне, определяющими порядок информационного обмена [59].

Представляется важным оценить, каков же сравнительный объем информационных баз данных дактилоскопических учетов в России и зарубежных странах. В открытых источниках такие сведения по России нам найти не удалось, однако в научной литературе со ссылкой на Главный информационно-аналитический центр (ГИАЦ) МВД России упоминается цифра около 34 млн. дактокарт [60, с. 293], что составляет с учетом необходимой актуализации сведений на текущий момент порядка 25 % от общей численности населения страны. Для сравнения в Великобритании функционирует Национальная автоматическая система идентификации по отпечаткам пальцев (National Automated Fingerprint Identification System, NAFIS) (в настоящее время носит название IDENT1), которая по состоянию на 31 марта 2020 года включала в себя 26 298 205 отпечатков, относящихся к 8 397 761 лиц (при населении в 67,1 млн. человек это составляет около 12,5% населения) [61]. В данную базу попадают учетные данные всех лиц, подлежащих аресту.

Несмотря на существенный текущий охват дактилоскопических учетов, следует предположить, что с течением времени они постепенно утратят первостепенное значение в криминалистической регистрации, уступив первенство геномным учетам. Зарубежный опыт показывает, что базы данных ДНК начинают эффективно функционировать при условии содержания в них геномной информации не менее 1% от общего количества населения страны. По состоянию на 1 января 2020 г. в общероссийской базе данных геномной информации содержалась геномная информация 0,6% от общего количества населения Российской Федерации (965 315 объектов учета) [62]. Для сравнения Национальная база данных ДНК (National DNA Database, NDNAD) в Соединенном Королевстве Великобритании и Северной Ирландии, учрежденная в 1995 году, по состоянию на 31 марта 2020 года включала в себя 6 568 035 профилей лиц, что составляет около 9,8% населения при общей численности в 67,1 млн. человек [63]. Важно отметить, что в Соединенном Королевстве легализован сбор генетических идентификаторов личности арестованных, а также задержанных, подпадающих под так называемый «серьезный» статус, к которому относят убийство, изнасилование, преступления, связанные с терроризмом, ограбление, разбой, кражи (в том числе со взломом и при отягчающих обстоятельствах), преступления на транспорте, уничтожение чужого имущества, незаконный оборот наркотиков, оружия, взрывчатых веществ, поджоги, мошенничество, нарушение общественного порядка, похищение людей.

В Соединенных Штатах Америки геномная регистрация сильно фрагментирована, однако на федеральном уровне создан Национальный индекс ДНК (National DNA Index (NDIS), содержащий более 14 836 490 профилей преступников, 4 513 955 профилей арестованных и 1 144 255, образцов, изъятых с мест преступлений (по состоянию на октябрь 2021 года) [64]. Необходимо отметить, что несмотря на общефедеральный масштаб данной базы, ее наполнение ограничено особенностями законодательства отдельных штатов, поэтому общий объем базы относительно невелик – примерно 4,4 % от общей численности населения США в 335 млн. человек. Закон об идентификации ДНК от 1994 г. (34 U.S. Code § 12592), санкционировавший создание Национального индекса ДНК, определил категории лиц, чьи сведения могут храниться в NDIS: осужденные правонарушители, арестованные, задержанные, неопознанные человеческие останки, лица, пропавшие без вести и родственники пропавших без вести.

Геномная регистрация в России регламентирована Федеральным законом 2008 года «О государственной геномной регистрации в Российской Федерации» [65]. В соответствии со статьей 7 указанного закона обязательной геномной регистрации подлежат: 1) лица, осужденные и отбывающие наказание в виде лишения свободы за совершение тяжких или особо тяжких преступлений, а также всех категорий преступлений против половой неприкосновенности и половой свободы личности; 2) неустановленные лица, биологический материал которых изъят в ходе производства следственных действий, а также неопознанные трупы. Постановлением Правительства России утверждены компетентные учреждения, занимающиеся обязательной государственной геномной регистрации вышеуказанных лиц: это ЭКЦ МВД России, экспертно-криминалистические подразделения территориальных органов МВД России, учреждения УИС [66].

Многие ученые и специалисты из сферы правоприменительной практики поддерживают идею расширения количества лиц, подлежащих геномной регистрации лиц, осужденных за преступления средней тяжести, небольшой тяжести [67; 68; 69]. В Государственной Думе России сейчас находится на обсуждении законопроект [70], в соответствии с которым планируется расширить перечень регистрируемых лиц, за счет включения всех лиц, осужденных и отбывающих наказание в виде лишения свободы за совершение преступлений (независимо от тяжести преступления); лиц, подозреваемых в совершении преступлений, обвиняемые в совершении преступлений, а также лиц, подвергнутых административному аресту. По мнению разработчиков законопроекта, с учетом эффективности исследований ДНК расширение базы данных геномного учета будет способствовать существенному росту выявления и раскрытия преступлений, в особенности тяжких и особо тяжких.

B. In ipso actu – судебный контроль

По данным исследователей, более 50% поступающих в Конституционный суд РФ жалоб граждан, касающихся проведения оперативно-розыскных

мероприятий с использованием технических средств, поднимают вопрос законности их проведения без судебного решения [71, с. 17]. Законом об ОРД предписано, что в случае проведения ОРМ, ограничивающих такие конституционные права человека и гражданина как тайна переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, передаваемых по сетям электрической и почтовой связи, а также право на неприкосновенность жилища, органам, осуществляющим ОРД необходимо получать судебные решения. Как указано в Постановлении Пленума Верховного Суда Российской Федерации «О некоторых вопросах применения судами Конституции Российской Федерации при осуществлении правосудия» [72], результаты таких ОРМ могут быть использованы в качестве доказательств по делам, лишь когда они получены по разрешению суда на проведение таких мероприятий и проверены следственными органами в соответствии с уголовно-процессуальным законодательством.

Специфика осуществления ОРД и необходимость сохранения в тайне сведений о методах, средствах осуществления этой деятельности, лицах, оказывающих конфиденциальное содействие правоохранительным органам, в большинстве случаев не позволяет осуществлять нормативное регулирование этой деятельности исключительном правовыми актами открытого характера. В силу этого объективно необходимое сохранение неполной прозрачности законодательной регламентации должно компенсироваться механизмами судебного контроля, составляющими важнейшее условие правомерного вмешательства в частную жизнь граждан. Судебный контроль может осуществляться в виде *предварительной судебной легализации, а также в форме последующего судебного контроля,* направленного на оценку правомерности действий, сопровождающих ограничения и запреты в цифровой среде.

Важным условием судебной легализации правомерного ограничения конституционных прав граждан является ее заблаговременное получение. Ярким примером нарушения этого требования стало рассмотренное ЕСПЧ в 2017 году дело Трабахо Руэда против Испании (Trabajo Rueda v. Spain) [73]. Предметом рассмотрения в данном деле стали следующие обстоятельства. Заявитель оставил свой компьютер в мастерской для проведения технических работ. Мастер сервиса после проведенного ремонта осуществил проверку работоспособности компьютера и в папке «Мои документы», обнаружил файлы, содержащие детскую порнографию, после чего сообщил об этом в полицейский участок и передал компьютер сотрудникам полиции. Они изучили содержимое компьютера, начав проведение ОРМ и следственных действий, после чего арестовали заявителя и заключили его под стражу. Рассмотрев дело, ЕСПЧ пришел к выводу, что в данном случае имело место нарушение статьи 8 (право на уважение частной жизни) Конвенции, поскольку изъятие полицией компьютера и проверка содержащихся в нем файлов без предварительного судебного разрешения не были соразмерны преследуемым законным целям и не были «необходимы в демократическом обществе».

В законодательстве и правоприменительной практике в качестве оправданного исключения из общего правила о предварительной судебной легализации усматривается наличие безотлагательной ситуации [31]. В статье 8 закона об ОРД таковыми рассматриваются случаи, которые могут привести к совершению тяжкого или особо тяжкого преступления, а также при наличии данных о событиях и действиях (бездействии), создающих угрозу государственной, военной, экономической, информационной или экологической безопасности Российской Федерации. Если таковые усматриваются, на основании мотивированного постановления одного из руководителей органа, осуществляющего ОРД, допускается проведение ОРМ, ограничивающих конституционные права человека и гражданина, с обязательным уведомлением суда в течение 24 часов и получением судебного решения в течение 48 часов. Если акт судебной легализации в указанный срок не получен, ОРМ должно быть прекращено, а полученные результаты не могут быть в дальнейшем использованы в доказывании по делу. В соответствии со статьей 9 закона об ОРД судебная легализация ограничения частной жизни осуществляется путем вынесения судьей постановления, исчисляемого в сутках со дня его вынесения и не может превышать шести месяцев, если иное не указано в самом постановлении. Данное требование оправданно, что, однако, означает практическую невозможность предварительной легализации всех мероприятий по находящимся в производстве у правоохранительных органов делам.

В ходе проведенного экспертного опроса нами выявлены некоторые нюансы реализации указанного правового механизма. Во-первых, в ряде случаев судьи трактуют факт неотложности проводимого мероприятия крайне ограниченно: если его проведение необходимо в рабочее время, они считают, что неотложность отсутствует, и органы, осуществляющие ОРД, могут получить судебное решение без затруднений. Данное утверждение, с нашей точки зрения, ошибочно, поскольку, к примеру, задержание подозреваемого может произойти случайно, а заминка в изъятии у него цифрового носителя информации или доступа к нему может повлечь за собой уничтожение следов совершенного преступления. Во-вторых, автоматическая трансляция стандартов ЕСПЧ на российскую правоприменительную практику, по мнению опрошенных нами экспертов, невозможна по вполне банальной причине, определяющейся масштабами страны. Так, для многих регионов страны предварительная судебная легализация просто физически невозможна ввиду нахождения соответствующих органов, осуществляющих ОРД, на значительном расстоянии от судебных учреждений (цитата одного из опрошенных экспертов: «ближайший райцентр от меня в 150 км, и я не могу туда ездить

каждый день»). Практическое разрешение подобных трудностей возможно путем внедрения устойчивых и защищенных каналов видеоконференцсвязи, однако на данный момент даже уровень развития информационных технологий и Интернет-доступности в регионах нашей страны очень неравномерен, что, очевидно, будет влечь за собой сохранение описанной проблемы.

Особую роль судебный контроль обретает в реализации механизмов массового и целевого сбора данных в цифровом пространстве. Этот вопрос рассматривался ЕСПЧ в целом ряде дел, имевших разную степень общественного резонанса (Big Brother Watch and Others v. the United Kingdom, Privacy International and Others v. the United Kingdom, Szabó and Vissy v. Hungary, и др.). Так, в деле Сабо и Висси против Венгрии [74] заявители обжаловали возможность использования властями Венгрии законодательства о тайном антитеррористическом наблюдении, принятого в 2011 году, которое позволяло осуществлять массовый мониторинг коммуникаций, прибегая к передовым технологиям. Рассматривая данное дело, суд посчитал, что даже в целях обеспечения национальной безопасности и борьбы с терроризмом, *органы исполнительной власти не могут получать* всю полноту дискреционных полномочий без надлежащего судебного контроля за объемом и обоснованностью принимаемых мер.

В широко нашумевшем деле «Big Brother Watch and Others v. the United Kingdom» [75] рассматривались разоблаченные Эдвардом Сноуденом программы наблюдения и обмена разведданными между США и Соединенным Королевством. Жалоба касалась британского Закона о регулировании следственных полномочий 2000 г. («Regulation of Investigatory Powers Act») и рассматривала три разных режима наблюдения: 1) массовый перехват сообщений; 2) получение материалов перехвата от иностранных правительств и спецслужб; 3) получение данных связи от поставщиков услуг связи. При рассмотрении данного дела мнения судей разделились, однако в целом Большая Палата ЕСПЧ сформулировала некоторые общие суждения. Прежде всего, суд пришел к выводу, что из-за множества угроз, с которыми государства сталкиваются в современном мире, применение режима массового прослушивания само по себе не нарушает Конвенцию. Будучи используемым, данный режим должен был быть предметом «сквозных гарантий», что подчеркивает важность осуществления оценки вводимых мер с точки зрения необходимости и соразмерности таких действий на каждом этапе процесса. Наконец, массовый перехват должен подлежать независимому контролю, как с самого начала, когда определяются цель и объем операции, так и независимой проверке постфактум. Должное санкционирование, может происходить только органом, независимым от исполнительной власти. Именно суд должен конкретизировать поисковые запросы и сообщения, которые подлежат проверке, конкретные условия поиска информации, например, персональные идентификаторы, адреса электронной почты и т.п.

С точки зрения российской правоприменительной практики, выраженной в позициях Конституционного Суда Российской Федерации [76, 77, 78], само по себе вынесение решения органами государственной власти при наличии гарантии последующего судебного контроля не противоречит требованиям Конституции Российской Федерации, поскольку позволяет исправить допущенные нарушения, обжаловав их в установленном порядке в компетентном суде.

C. Post factum – хранение, уничтожении полученной информации и информирование о ее наличии

Практикой ЕСПЧ и национальных судебных инстанций выработано достаточно четкое понимание обоснованной продолжительности как применения самих мер ограничения в цифровой среде (об этом мы писали выше), так и хранения собираемых данных в государственных информационных системах.

По логике ЕСПЧ, *продолжительность хранения данных должна определяться тяжестью преступления, характером общественной опасности лица, его совершившего, и быть пропорциональной цели сбора информации – предотвращения совершения новых преступлений*. По этой причине срок хранения информации, идентифицирующей человека, должен быть тем больше, чем более тяжким является совершенное им деяние. Бессрочное хранение информации, по мнению ЕСПЧ, должно быть исключительным. К примеру, в делах «B.B. v. France», «Gardel v. France» и «M.B. v. France» [79] ЕСПЧ установил, что продолжительность хранения сведений – максимум 30 лет – соответствовала цели размещения данных в базе лиц, совершивших сексуальные преступления (Sex Offender Database), поскольку заявители были осуждены за изнасилование 15-летних несовершеннолетних, будучи облеченным властью. В другом деле «Гогран против Соединенного Королевства» (Gaughran v. the United Kingdom) [80] была рассмотрена обратная ситуация: персональные данные заявителя (ДНК-профиль, отпечатки пальцев и фотографии) были получены в связи с совершением им управления транспортным средством в состоянии алкогольного опьянения, однако срок хранения данных не был ограничен каким-то определенным сроком. Суд посчитал, что Соединенное Королевство превысило допустимую свободу усмотрения, поскольку бессрочный период хранения данных представляет собой несоразмерное вмешательство в право заявителя на уважение частной жизни, которое не может считаться необходимым в демократическом обществе.

Руководствуясь вышеуказанными критериями, следует отметить, что отечественное законодательство и правоприменительная практика демонстрируют подход, принципиально отличающийся от стандартов, выработанных ЕСПЧ. Так, абз. 1 ст. 13 Федерального закона «О государственной дактилоскопической регистрации в Российской Федерации» предусматривает срок хранения такой информации до достижения регистрируемыми лицами возраста 100 лет или установления факта их смерти [57]. Аналогичным

образом в статье 7 Федерального закона «О государственной геномной регистрации в Российской Федерации срок хранения этих данных определен до установления факта смерти лиц, подлежащих геномной регистрации, а при отсутствии сведений об их смерти - до даты, когда им исполнилось бы 100 лет [65]. Таким образом, фактически отечественным законодательством предусмотрено бессрочное хранение дактилоскопической и геномной информации.

Еще менее прозрачны сроки хранения данных в базах, формируемых органами, осуществляющими ОРД, поскольку, как мы отмечали выше, их правовая регламентация происходит, в том числе в форме ведомственных нормативных правовых актов закрытого характера. Статьей 5 закона об ОРД предусмотрено, что полученные в результате проведения ОРМ материалы в отношении лиц, виновность которых в совершении преступления не доказана в установленном законом порядке, хранятся *один год*, а затем уничтожаются, *если служебные интересы или правосудие не требуют иного.* Фонограммы и другие материалы, полученные в результате прослушивания телефонных и иных переговоров лиц, в отношении которых не было возбуждено уголовное дело, уничтожаются *в течение шести месяцев* с момента прекращения прослушивания, о чем составляется соответствующий протокол. Данный подход может быть подвергнут объективной критике, однако разделяется большинством опрошенных нами экспертов правоохранительной сферы.

В связи с обозначенными выше критериями правомерности хранения информации в формируемых информационных системах, закономерно *установление регламентированного порядка удаления информации из государственных реестров и баз данных.* В целом таковое может осуществляться либо на основании заявления человека, если его регистрация происходила добровольно (как правило, такой порядок не предусматривает каких-либо формальных сложностей), либо в автоматическом порядке по истечению предельных сроков хранения соответствующей информации (применительно к нашей стране – практически бессрочно), либо в связи с прекращением обстоятельств, послуживших основанием для внесения соответствующих сведений в систему. Именно последний из вышеуказанных механизмов требует отдельного обсуждения.

Несоразмерность вмешательства в частную жизнь может усматриваться *в хранении данных о лицах, чей правовой статус определяет их как утративших или не несущих высокой степени общественной опасности.* ЕСПЧ выработал в этом отношению позицию: если лицо оправдано, имел место отказ в возбуждении уголовного дела или дело в отношении лица прекращено, собранные и хранящиеся в отношении него сведения должны быть удалены. Так, в деле М.К. против Франции (M.K. v. France) [81] рассматривалась следующая ситуация: в отношении заявителя велись два расследования о краже книг, закончившиеся в одном случае его оправданием, а в другом – решением об отказе в возбуждении уголовного дела. Предметом обжалования стал факт сохранения в базе данных, ведущейся французскими властями, отпечатков пальцев заявителя. Поскольку поданные заявителем прошения об удалении из базы данных его отпечатков пальцев были отклонены компетентными органами, ЕСПЧ постановил, что имело место нарушение статьи 8 (право на уважение частной жизни) Конвенции.

В другом деле Брюне против Франции (Brunet v. France) [82] предметом обжалования стало вмешательство в частную жизнь заявителя в результате добавления его сведений в базу данных полиции STIC (le système de traitement des infractions constatées, система обработки зарегистрированных правонарушений, используется с 1990-х годов, официально введена законом № 78-17 от 6 января 1978 года). Данная система учета содержит информацию из отчетов о расследованиях, список причастных лиц и потерпевших. Рассмотрев обстоятельства заявления, ЕСПЧ установил, что поскольку уголовное дело в отношении заявителя было прекращено, французское государство превысило пределы усмотрения по таким вопросам. По мнению суда, заявитель не имел реальной возможности добиться удаления из базы данных информации о нем, а продолжительность ее хранения (20 лет) хотя и не была бессрочной, являлась достаточно продолжительной.

Законодательство Российской Федерации в этом отношении максимально упрощено и не имеет сложной дифференциации в основаниях постановки на учет и хранения информации. Так, в случае геномной регистрации учету подлежат лица, осужденные и отбывающие наказание в виде лишения свободы, что подразумевает вступившее в силу решение суда, и означает, как правило, последующую неизменность правового статуса лица, а значит, и сроки хранения к ним применяются общие – до смерти лица или достижения им возраста 100 лет. В случае с дактилоскопической регистрацией правовая регламентация более сложная. В данном случае учету подлежат лица с разным правовым статусом, это и *подозреваемые*, и *обвиняемые* в совершении преступления, и *осужденные* за совершение преступления, и *подвергнутые* административному аресту, и *совершившие административное правонарушение*, если установить их личность иным способом невозможно. Парадоксальность правового регулирования состоит в том, что последние две из указанных категорий лиц находятся в условиях менее благоприятных, чем первые три. Абзац 3 статьи 15 Федерального закона «О государственной дактилоскопической регистрации в Российской Федерации» предусматривает уничтожение дактилоскопической информации *о лицах, подозреваемых в совершении преступления, обвиняемых в совершении преступления либо осужденных за совершение преступления,* по истечении одного года после прекращения уголовного дела по основаниям, влекущим возникновение права на реабилитацию либо вынесения оправдательного приговора. В остальных случаях срок хранения информации не различается: до

достижения возраста 100 лет или установления факта смерти лица.

Из изученного нами зарубежного законодательства, наиболее сложными и дифференцированными являются регистрационные требования во Франции. Так, срок хранения геномной информации в базе данных FNAEG разграничен в зависимости от возраста лица, подлежащего учету (совершеннолетний / несовершеннолетний), процессуального статуса и категории преступления. К примеру, максимальный срок хранения геномной информации о совершеннолетнем человеке, признанном виновным на основании вступившего в силу решения суда, составляет от 25 до 40 лет в зависимости от тяжести преступления, для несовершеннолетнего при тех же условиях срок хранения составит от 15 до 25 лет. Удаление информации из реестра ДНК осуществляется по заявлению лица, направленному в прокуратуру по месту жительства или месту осуществления соответствующих процессуальных действий при условии наличия у заявителя оправдательного решения суда или документального подтверждения освобождения его от ответственности [83].

Обеспечение рассмотренных выше правовых гарантий предопределяет важность *установления регламентированного порядка информирования граждан о наличии в государственных реестрах, базах данных информации о них.* В практике ЕСПЧ данный вопрос был поднят в деле «Молодежная инициатива за права человека» против Сербии (Youth Initiative For Human Rights v. Serbia) [84]. В 2005 году заявительница по делу, неправительственная правозащитная организация, обратилась к сербскому разведывательному агентству (Serbian Intelligence Agency) с просьбой сообщить ей, сколько лиц подвергалось электронному надзору со стороны этого агентства в 2005 году. Агентство отказало в удовлетворении заявления сначала со ссылкой на Закон о свободе информации 2004 года, а позднее, после внутригосударственных процедур урегулирования, сославшись на отсутствие запрашиваемой информации. Европейский суд посчитал, что в данном деле со стороны агентства имело место нарушение права на свободу слова, поскольку реализация такового подразумевает возможность правомерного сбора информации, представляющей всеобщий интерес.

Отечественным законодательством на данный момент предусмотрено как минимум два механизма обращения в органы государственной власти для получения информации об имеющихся о них сведениях: в общем порядке рассмотрения обращений граждан и в специальном, предусмотренном законом об ОРД. Каждый из них, в свою очередь, гарантирован судебным порядком оспаривания решений, действий (бездействия) органов государственной власти и их должностных лиц, предусмотренным ст. 125 УПК РФ, главой 22 КАС РФ, главой 24 АПК РФ.

Общий порядок рассмотрения обращений граждан в Российской Федерации был установлен Федеральным законом «О порядке рассмотрения обращений граждан Российской Федерации» [85]. В развитие положений Конституции России ч. 1 статьи 2 данного закона определяет право граждан обращаться лично, а также направлять индивидуальные и коллективные обращения в государственные органы власти, иные органы, учреждения и организации, осуществляющие публично значимые функции. Со дня регистрации письменного обращения срок его рассмотрения составляет 30 дней (ч. 1 статья 12).

Специальный порядок запроса информации установлен частью 4 статьи 5 Закона об ОРД: лицо, виновность которого в совершении преступления не доказана в установленном законом порядке, вправе истребовать от органа, осуществляющего оперативно-розыскную деятельность, сведения о полученной о нем информации в пределах, допускаемых требованиями конспирации и исключающих возможность разглашения государственной тайны.

Необходимо отметить, что несмотря на предусмотренные законами формальные юридические гарантии фактическая реализация описанных механизмов защиты прав граждан сталкивается с объективными ограничениями. Материалы изученной нами судебной практики, и проведенный экспертный опрос свидетельствует, что в значительном числе случаев граждане получают от государственных органов «отписки», подобные тем, что были рассмотрены в вышеуказанном деле «Молодежная инициатива за права человека» против Сербии. В общих категориях сложно дать рекомендации о процедурах преодоления подобных проблем, поскольку в данном случае на чашах весов оказываются абсолютно равновесные ценности: конспирация и государственная тайна, с одной стороны, и права человека и гражданина, с другой. По мнению Конституционного суда России, негласные по своему характеру ОРМ стали бы просто невозможны, а сама оперативно-розыскная деятельность утратила бы смысл, если бы материалы негласных ОРМ рассматривались в открытом судебном процессе [36]. По этой причине проверяемое лицо не может быть участником процедуры, в которой испрашиваются судебное разрешение на проведение негласных ОРМ. Открытости, гласности и состязательности сторон в таком процессе, подчеркнул Конституционный Суд Российской Федерации, быть не может. Оценка законности и обоснованности действий правоприменительных органов, отказывающихся разглашать сведения, ставшие известными в процессе проведения ОРМ, является прерогативой соответствующих органов прокуратуры и судов общей юрисдикции [86].

IV. Заключение

На основании проведенного исследования автор пришел к выводу, что в российском законодательстве нашел свое воплощение весь массив передовых правовых гарантий, выработанных на международном уровне и в национальном законодательстве зарубежных стран. В значительной степени включение таких гарантий в систему правового регулирования в России

произошло в результате осмысленной имплементации передовых решений и практик, принятых в странах с высоким уровнем развития ИКТ и цифровых правоотношений. Несомненно, высокую роль сыграло постепенное изменение отечественного законодательства и правоприменительной практики под влиянием правовых позиций Конституционного суда Российской Федерации и решений, принятых Европейским судом по правам человека, которые при рассмотрении конкретных правоприменительных ситуаций нередко формулируют обобщенные стандарты и критерии правомерного сочетания публичных и частных интересов в сфере цифровых правоотношений.

Европейский суд по правам человека, рассматривая различные дела, связанные с использованием цифровых технологий, неоднократно отмечал, что использование современных научных методов в системе уголовного правосудия не может быть разрешено ни при каких обстоятельствах без тщательной оценки уравновешенности потенциальных выгод от широкого использования таких методов в ущерб интересам частной жизни отдельных лиц. На любом государстве, претендующем на роль первопроходца в разработке новых технологий, лежит особая ответственность за нахождение правильного баланса.

Важно отметить, что сама специфика цифровой среды влечет за собой презюмирование надлежащего исполнения установленных правовых гарантий в деятельности органов государственной власти, должностных лиц и граждан. Цифровая информация достаточно легко копируется, размножается по множеству носителей, поэтому ее уничтожение всегда в большей или меньшей степени имеет характер вероятности. В тоже время непрекращающееся развитие цифровых технологий влечет за собой постоянное балансирование между сопряженными интересами государства, общества и отдельного человека.

В России законодательная регламентация ограничений и запретов в цифровой среде строится на общих началах обеспечения неприкосновенности частной жизни и соблюдения конституционных прав человека и гражданина. В сравнении с изученным автором британским и американским опытом законодательного регулирования ограничения неприкосновенности частной жизни, российское законодательство построено более четко, поскольку основные гарантии введены в федеральное законодательство, а не спущены на уровень исполнительной ветви власти, что особенно свойственно для законодательства отдельных штатов США. В тоже время, во Франции воплощение существующей практики ЕСПЧ нашло свое выражение в более развернутой и дифференцированной, нежели в России, регламентации множества узких вопросов вторжения государства в частную жизнь граждан.

Российское законодательство имеет несомненный крен в сторону обеспечения публичных интересов в ущерб интересам частным, однако это не является исключением для мировой практики, идет в общем тренде развития международного сообщества и обосновывается необходимостью эффективной борьбы с преступлениями и иными правонарушениями. Фактически правовое регулирования в России строится, исходя из тезиса о том, что для правопослушных граждан цифровой надзор со стороны государства не угрожает их приватности. В тоже время судебная практика отдельных европейских стран демонстрирует ярко выраженную тенденцию к злоупотреблению правовыми гарантиями со стороны правонарушителей, что влечет за собой обратную ситуацию: крен в сторону приоритета частной жизни в ущерб интересам общества и государства. Одновременно следует отметить, что излишняя формализация, процедурная загруженность органов государственной власти существенным образом влияют на эффективность их деятельности, удорожают их функционирование и снижают оперативность реагирования на общие угрозы безопасности, возникающие в силу постоянного развития конкурентных преимуществ теневого сектора общественных отношений в цифровой среде.

Изучение автором судебной и иной правоприменительной практики позволяет ему утверждать, что российские правоохранительные органы, сталкиваясь с комплексностью правового регулирования, нередко пренебрегают гарантиями, установленными законодательством, что выражается во множестве судебных споров, обусловленных нарушением прав граждан на неприкосновенность частной жизни. Исходя из практики решений вышестоящих судебных инстанций, а также правовых позиций Конституционного суда России, вносятся соответствующие изменения в законодательство, а отечественная правоприменительная практика постепенно меняется, медленно двигаясь по пути достижения баланса частных и публичных интересов.

Библиография

[1] Brandeis L., Warren S. The right to privacy // Harvard Law Review. 1890. Vol. IV. No. 5.

[2] Svensson M., Rosengren C., Åström F. Digitalization and Privacy: A systematic literature review. Lund University (Media-Tryck). URL: https://portal.research.lu.se/en/publications/ digitalization-and-privacy-a-systematic-literature-review (дата обращения: 24.10.2022).

[3] Zhang Z., Lian S., Pei Q., Pu J. Fuzzy Risk Assessments on Security Policies for Digital Rights Management. 2010. URL: https://www.researchgate.net/profile/Zhiyong-Zhang-14/publication/228671422_Fuzzy_Risk_Assessments_ on_Security_Policies_for_Digital_Rights_Management/links/55fc01a908ae07629e07d10a/Fuzzy-Risk-Assessments-on-Security-Policies-for-Digital-Rights-Management.pdf (дата обращения: 24.10.2022).

[4] Winkler T., Rinner B. Securing Embedded Smart Cameras with Trusted Computing // Eurasip Journal on Wireless Communications and Networking. 2011. DOI: 10.1155/2011/530354.

[5] Wicker S., Schrader D. Privacy-Aware Design Principles for Information Networks // Proceedings of the IEEE. 2011. 99. P. 330–350. DOI: 10.1109/JPROC.2010.2073670.

[6] Cavoukian A. Privacy by Design The 7 Foundational Principles. 2011. URL: https://www.ipc.on.ca/wp-content/uploads/resources/ 7foundationalprinciples.pdf (дата обращения: 24.10.2022).

[7] McKee H.A. Policy Matters Now and in the Future: Net Neutrality, Corporate Data Mining, and Government Surveillance // Computers and Composition. 2011. No. 28(4). P. 276–291. DOI: 10.1016/j.compcom.2011.09.001.

[8] Michelfelder D. The moral value of informational privacy in cyberspace // Ethics and Information Technology. 2001. No. 3. P. 129–135. DOI: 10.1023/A:1011802227136.

[9] Vitaliev D. Big brother is watching you [Internet security] // Communications Engineer. 2007. No. 5(5). P. 20–25. DOI: 10.1049/ce:20070502.

[10] Amos C., Zhang L., Pentina I. Investigating Privacy Perception and Behavior on Weibo // Journal of Organizational and End User Computing. 2014. No. 26(4). P. 43–56. DOI: 10.4018/joeuc.2014100103.

[11] Barnard-Wills D. E-safety education: Young people, surveillance and responsibility // Criminology & Criminal Justice. 2012. No. 12(3). P. 239–255. DOI: 10.1177/1748895811432957.

[12] Park Y.J., Jang S.M., Mo Jang S. Understanding privacy knowledge and skill in mobile communication // Computers in Human Behavior. 2014. No. 38. P. 296–303. DOI: 10.1016/j.chb.2014.05.041.

[13] Preibusch S. Privacy behaviors after Snowden // Communications of the ACM. 2015. No. 58(5). P. 48–55. DOI: 10.1145/2663341.

[14] Champion A. Trusted Computing and Digital Rights Management Clearinghouse. 2007. URL: https://www.researchgate.net/publication/34658680_Trusted_Computing_and_Digital_Rights_Management_Clearinghouse (дата обращения: 24.10.2022).

[15] Garlinger P.P. Privacy, Free Speech, and The Patriot Act: First and Fourth Amendment Limits on National Security Letters // New York University Law Review. 2009. No. 84(4). P. 1105–1147.

[16] Beck E.N. The Invisible Digital Identity: Assemblages in Digital Networks // Computers and Composition. 2015. No. 35. P. 125–140. DOI: 10.1016/j.compcom.2015.01.005.

[17] Cover A.Y. Corporate Avatars and the Erosion of the Populist Fourth Amendment // Iowa Law Review. 2015. No. 100(4). P. 1441–1502.

[18] Hu M. Biometric ID Cybersurveillance // Indiana Law Journal. 2013. No. 88(4). P. 1475–1558.

[19] Grodzinsky F.S., Tavani H.T. P2P Networks and the Verizon v. RIAA Case: Implications for Personal Privacy and Intellectual Property // Ethics and Information Technology. 2005. No. 7(4). P. 243–250. DOI: 10.1007/s10676-006-0012-4.

[20] Konstadinides T. Destroying democracy on the ground of defending It? The Data Retention Directive, the surveillance state and our constitutional ecosystem // European Law Review. 2011. No. 36(5). 722–736. URL: https://openresearch.surrey.ac.uk/esploro/outputs/journalArticle/Destroying-democracy-on-the-ground-of-defending-it-The-Data-Retention-Directive-the-surveillance-state-and-our-constitutional-ecosystem/99516662902346 (дата обращения: 24.10.2022).

[21] Mantelero A. The future of consumer data protection in the EU Re-thinking the «notice and consent» paradigm in the new era of predictive analytics // Computer Law & Security Review. 2014. No. 30(6). P. 643–660. DOI: 10.1016/j. clsr.2014.09.004.

[22] Peppet S.R. Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security and Consent // Texas Law Review. 2014. No. 93(1). P. 85–178.

[23] Roberts A. Privacy, Data Retention and Domination: Digital Rights Ireland Ltd v Minister for Communications // Modern Law Review. 2015. No. 78(3). P. 535–548. DOI: 10.1111/1468-2230.12127.

[24] Riedy M.K., Wen J.H. Electronic surveillance of Internet access in the American workplace: implications for management // Information & Communications Technology Law. 2010. No. 19(1). P. 87–99. DOI: 10.1080/13600831003726374.

[25] Desai D.R. Constitutional Limits on Surveillance: Associational Freedom in The Age of Data Hoarding // Notre Dame Law Review. 2014. No. 90(2). P. 579–632.

[26] Fairfield J.A.T., Luna, E. Digital Innocence // Cornell Law Review. 2014. No. 99(5). P. 981–1076.

[27] Ojanen T. Privacy Is More Than Just a Seven-Letter Word: The Court of Justice of the European Union Sets Constitutional Limits on Mass Surveillance Court of Justice of the European Union, Decision of 8 April 2014 in Joined Cases C-293/12 and C-594/12, Digital Right // European Constitutional Law Review. 2014. No. 10(3). P. 528–541. DOI: 10.1017/S1574019614001345.

[28] Железняк Н.С. К вопросу об уточнении терминологии в решениях Конституционного Суда Российской Федерации // Вестник Сибирского юридического института МВД России. 2017. № 4(29). С. 7–13.

[29] Карл А.М. Соотношение негласных следственных действий и оперативно-розыскных мероприятий // Вестник Санкт-Петербургского университета МВД России. 2019. № 3(83). С. 144–151.

[30] Одношевин И.А. Судебный контроль - гарантия конституционных прав граждан, вовлеченных в сферу оперативно-розыскной деятельности // Юристъ - Правоведъ. 2018. № 4(87). С. 187-192.

[31] Омелин В.Н. О проведении оперативно-розыскных мероприятий в случаях, не терпящих отлагательства // Закон и право. 2019. № 3. С. 112–114. DOI:10.24411/2073-3313-2019-10123.

[32] Ховавко С.М. Правовые гарантии соблюдения конституционных прав человека и гражданина при проведении оперативно-розыскных мероприятий // Общество и право. 2016. № 4(58). С. 131–136.

[33] Чечетин А.Е. О совершенствовании прокурорского надзора за оперативно-розыскной деятельностью // Вестник Санкт-Петербургского университета МВД России. 2018. № 3(79). С. 134-139.

[34] Заявление МИД России о запуске процедуры выхода из Совета Европы 15 марта 2022 года. URL: https://www.mid.ru/ru/press_service/spokesman/official_statement/1804379/ (дата обращения: 16.03.2022).

[35] Федеральный закон от 12 августа 1995 года № 144-ФЗ (ред. от 30.12.2021) «Об оперативно-розыскной деятельности» // Российская газета. 1995. 18 августа.

[36] Определение Конституционного Суда РФ от 14 июля 1998 года № 86-О «По делу о проверке конституционности отдельных положений Федерального закона «Об оперативно - розыскной деятельности» по жалобе гражданки И.Г. Черновой» // Российская газета. 1998. 11 августа.

[37] Case of S. and Marper v. United Kingdom (Applications № 30562/04 and 30566/04). URL: https://hudoc.echr.coe.int/eng-press?i=003-2571936-2784147 (дата обращения: 19.09.2022).

[38] Case of Shimovolos v. Russia (Application № 30194/09). URL: https://hudoc.echr.coe.int/eng-press?i=003-3581541-4053078 (дата обращения: 19.09.2022).

[39] Affaire Ben Faiza c. France (Requête № 31446/12). URL: https://hudoc.echr.coe.int/eng?i=001-180657 (дата обращения: 19.09.2022).

[40] Приказ МВД России № 776, Минобороны России № 703, ФСБ России № 509, ФСО России № 507, ФТС России № 1820, СВР России № 42, ФСИН России № 535, ФСКН России № 398, СК России № 68 от 27.09.2013 «Об утверждении Инструкции о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд» // Российская газета. 2013. 13 декабря.

[41] Дело Расула Джафарова против Азербайджана (Заявление № 69981/14). URL: https://hudoc.echr.coe.int/rus?i=001-165559 (дата обращения: 24.10.2022).

[42] Case of Catt v. the United Kingdom (Application № 43514/15). URL: https://hudoc.echr.coe.int/rus?i=001-189424 (дата обращения: 24.10.2022).

[43] Affaire Félix Dagregorio et Alain Mosconi c. France (Requête № 65714/11). URL: https://hudoc.echr.coe.int/rus?i=001-175036 (дата обращения: 24.10.2022).

[44] Case of Nagla v. Latvia (Application № 73469/10). URL: https://hudoc.echr.coe.int/eng?i=001-122374 (дата обращения: 24.10.2022).

[45] Обыск у журналиста как способ раскрыть его источники. URL: https://www.bfm.ru/news/376395 (дата обращения: 24.10.2022).

[46] Закон РФ от 27 декабря 1991 года № 2124-1 (ред. от 01.07.2021) «О средствах массовой информации» // Российская газета. 1992. 8 февраля.

[47] The principle of independence of lawyers: UN and IBA reference instruments. Basic Principles on the Role of Lawyers and the IBA Standards for the Independence of the Legal Profession / INTERNATIONAL BAR ASSOCIATION. URL: https://www.ibanet.org/MediaHandler?id=3b458c65-53f4-41b1-a1b2-0f765a7c39b3 (дата обращения: 06.04.2022).

[48] Федеральный закон от 31 мая 2002 года № 63-ФЗ (ред. от 31.07.2020) «Об адвокатской деятельности и адвокатуре в Российской Федерации» // Российская газета. 2002. 5 июня.

[49] Определение Конституционного Суда РФ от 8 ноября 2005 года № 439-О «По жалобе граждан С.В. Бородина, В.Н. Буробина, А.В. Быковского и других на нарушение их конституционных прав статьями 7, 29, 182 и 183 Уголовно-процессуального кодекса Российской Федерации» // Российская газета. 2006. 31 января.

[50] Определение Конституционного Суда РФ от 22 марта 2012 № 629-О-О «Об отказе в принятии к рассмотрению жалобы гражданина Абдулхамидова Ахмедшапи Гамзатовича на нарушение его конституционных прав положениями статей 8 и 9 Федерального закона «Об оперативно-розыскной деятельности», а также статей 7, 29 и 450 Уголовно-процессуального кодекса Российской Федерации». URL: http://www.consultant.ru (дата обращения: 06.04.2022).

[51] Апелляционное постановление Верховного Суда Чеченской Республики № 22-К-221/2020 от 7 июля 2020 года по уголовному делу № 3/6-124/20. URL: https://sudact.ru (дата обращения: 06.04.2022).
[52] Case of Kolesnichenko v. Russia (Application o. 19856/04). URL: https://hudoc.echr.coe.int/eng?i=001-92147 (дата обращения: 06.04.2022).
[53] Определение Конституционного Суда РФ от 15 июля 2008 года № 460-О-О «Об отказе в принятии к рассмотрению жалобы гражданина Букреева Владимира Викторовича на нарушение его конституционных прав отдельными положениями статей 5, 11 и 12 Федерального закона «Об оперативно-розыскной деятельности» и пунктом 13 Инструкции о порядке представления результатов оперативно-розыскной деятельности дознавателю, органу дознания, следователю, прокурору или в суд». URL: http://www.consultant.ru (дата обращения: 06.04.2022).
[54] Постановление Конституционного Суда РФ от 9 июня 2011 года № 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. 2011. 22 июня.
[55] Вычисляемые данные могут рассказать о нас больше, чем персональные. URL: https://radiovesti.ru/brand/63899/episode/1366965/ (дата обращения: 15.03.2021).
[56] Талапина, Э.В. Право и цифровизация: новые вызовы и перспективы // Журнал российского права. 2018. № 2 (254). С.5–17.
[57] Федеральный закон от 25 июля 1998 года № 128-ФЗ (ред. от 01.07.2021) «О государственной дактилоскопической регистрации в Российской Федерации» // Собрание законодательства РФ. 1998 . № 31. Ст. 3806.
[58] Постановление Правительства РФ от 31 октября 2018 года № 1296 «Об утверждении Правил направления дактилоскопической информации в органы внутренних дел» // Собрание законодательства РФ. 2018. № 46. Ст. 7046.
[59] Приказ МВД России, МЧС России, Минобороны России, Минфина России, Минюста России, Минтранспорта России, СВР России, ФСБ России, ФСО России, Росгвардии, ГУСП, Генпрокуратуры России, СК России от 23 сентября 2020 года № 659/717/473/208н/209/385/63/429/185/376/145/502/94 «Об утверждении Порядка формирования направляемой в органы внутренних дел дактилоскопической информации» URL: http://publication.pravo.gov.ru/Document/View/0001202009250035 (дата обращения: 19.09.2022).
[60] Михайлов М.А. Совершенствование системы дактилоскопической регистрации: конференция в государственной думе // Ученые записки Крымского федерального университета имени В.И. Вернадского. Юридические науки. 2015. № 1. С. 292–305.
[61] Forensic Information Databases Service (FINDS): The Forensic Information Databases Strategy Board policy for access and use of DNA samples, DNA profiles, fingerprint images, and associated data URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1052529/FIND_Strategy_Board_Policy_Access_and_Use.pdf (дата обращения: 19.09.2022).
[62] Пояснительная записка к проекту Федерального закона «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам государственной геномной регистрации». Законопроект № 1048800-7. URL: https://sozd.duma.gov.ru/bill/1048800-7 (дата обращения: 19.09.2022).
[63] National DNA Database Strategy Board Biennial Report 2018 - 2020 URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/913011/NDNAD_Strategy_Board_AR_2018-2020_Web_Accessible.pdf (дата обращения: 19.09.2022).
[64] CODIS - NDIS Statistics. URL: https://www.fbi.gov/services/laboratory/biometric-analysis/codis/ndis-statistics (дата обращения: 19.09.2022).
[65] Федеральный закон от 3 декабря 2008 года № 242-ФЗ «О государственной геномной регистрации в Российской Федерации» // Собрание законодательства Российской Федерации. 2008. № 49. Ст. 5740; 2009. № 51. Ст. 6150.
[66] Постановление Правительства РФ от 11 октября 2011 года № 828 «Об утверждении Положения о порядке проведения обязательной государственной геномной регистрации лиц, осужденных и отбывающих наказание в виде лишения свободы» // Собрание законодательства РФ. 2011. № 42. Ст. 5926.
[67] Шхагапсоев З.Л., Карданов Р.Р. Геномная регистрация как элемент противодействия преступлениям террористического характера на современном этапе // Известия Тульского государственного университета. Экономические и юридические науки. 2016. № 1-2. С. 84–90.
[68] Грибунов О.П. Всеобщая дактилоскопическая регистрация граждан как элемент реализации криминалистического предупреждения преступлений // Вестник Томского государственного университета. 2016. № 402. С. 188–191.
[69] Попова Т.В., Сергеев А.Б. Федеральная база данных геномной информации в системе обеспечения баланса частных и публичных интересов в уголовном судопроизводстве // Юридическая наука и правоохранительная практика. 2017. № 1 (39). С. 132–139.
[70] Законопроект № 1048800-7 «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам государственной геномной регистрации (в части расширения перечня лиц. подлежащих обязательной государственной геномной регистрации)». URL: https://sozd.duma.gov.ru/bill/1048800-7 (дата обращения: 19.09.2022).
[71] Черных А.А. Подходы Конституционного Суда Российской Федерации к вопросу о необходимости получения судебных решений при проведении оперативно-розыскных мероприятий с использованием технических средств // Вестник Сибирского юридического института МВД России. 2019. №. 2 (35). С. 16–24.
[72] Постановление Пленума Верховного Суда РФ от 31 октября 1995 года № 8 (ред. от 03.03.2015) «О некоторых вопросах применения судами Конституции Российской Федерации при осуществлении правосудия» // Российская газета. 1995. 28 декабря.
[73] Affaire Trabajo Rueda c. Espagne (Requête № 32600/12). URL: https://hudoc.echr.coe.int/eng?i=001-173787 (дата обращения: 19.09.2022).
[74] Case of Szabó and Vissy v. Hungary (Application № 37138/14). URL: https://hudoc.echr.coe.int/eng?i=001-160020 (дата обращения: 19.09.2022).
[75] Case of Big Brother Watch and others v. The United Kingdom (Applications №№ 58170/13, 62322/14 and 24960/15). URL: https://hudoc.echr.coe.int/eng?i=001-210077 (дата обращения: 19.09.2022).
[76] Постановление Конституционного Суда РФ от 20 мая 1997 года № 8-П «По делу о проверке конституционности пунктов 4 и 6 статьи 242 и статьи 280 Таможенного кодекса Российской Федерации в связи с запросом Новгородского областного суда» // Российская газета. 1997. 29 мая.
[77] Постановление Конституционного Суда РФ от 11 марта 1998 года № 8-П «По делу о проверке конституционности статьи 266 Таможенного кодекса Российской Федерации, части второй статьи 85 и статьи 222 Кодекса РСФСР об административных правонарушениях в связи с жалобами граждан М.М. Гаглоевой и А.Б. Пестрякова» // Российская газета. 1998. 26 марта.
[78] Постановление Конституционного Суда РФ от 16 июля 2008 года № 9-П «По делу о проверке конституционности положений статьи 82 Уголовно-процессуального кодекса Российской Федерации в связи с жалобой гражданина В.В. Костылева» // Российская газета. 2008. 1 августа.
[79] Chamber Judgments B.B.. Gardel. M.B. v. France. URL: https://hudoc.echr.coe.int/fre-press?i=003-4480954-5400075 (дата обращения: 07.03.2022).
[80] Case of Gaughran v. The United Kingdom (Application № 45245/15) URL: https://hudoc.echr.coe.int/rus?i=001-200817 (дата обращения: 07.03.2022).
[81] Case of M.K. v. France (Application № 19522/09). URL: https://hudoc.echr.coe.int/eng?i=001-119075 (дата обращения: 07.03.2022).
[82] Affaire Brunet c. France (Requête № 21010/10). URL: https://hudoc.echr.coe.int/eng?i=001-146389 (дата обращения: 07.03.2022).
[83] Fichier national automatisé des empreintes génétiques (FNAEG). URL: https://www.service-public.fr/particuliers/vosdroits/F34834 (дата обращения: 07.03.2022).
[84] Case of Youth Initiative for Human Rights v. Serbia (Application № 48135/06). URL: https://hudoc.echr.coe.int/eng?i=001-120955 (дата обращения: 07.03.2022).

[85] Федеральный закон от 2 мая 2006 года №59-ФЗ (ред. от 27.12.2018) «О порядке рассмотрения обращений граждан Российской Федерации» // Российская газета. 2006. 5 мая.
[86] Определение Конституционного Суда РФ от 20 октября 2005 года № 375-О «Об отказе в принятии к рассмотрению жалобы гражданина Макаренко Анатолия Михайловича на нарушение его конституционных прав частью четвертой статьи 29 Уголовно-процессуального кодекса Российской Федерации и статьями 6 - 9 Федерального закона "Об оперативно-розыскной деятельности». URL: http://www.consultant.ru (дата обращения: 07.03.2022).

Мамай Евгений Алексеевич, кандидат юридических наук, доцент, Национальный исследовательский университет «Высшая школа экономики» (Нижний Новгород), доцент кафедры теории и истории права и государства, ORCID 0000-0002-9386-2747 (emamaj@hse.ru)

Digital technologies in law enforcement: criteria for a legitimate combination of public and private interests

E.A. Mamay

Abstract—The article discusses the use of digital technologies in law enforcement through the prism of the balance of public and private interests. The author analyses the system of legal regulation, studies the normative legal acts regulating digital relations and the use of information and communication technologies. Empirical ground of the study constitutes of more than 30 decisions adopted by various judicial instances in Russia, as well as more than 20 decisions of the European Court of Human Rights. Comparative legal material is represented by the study of foreign legislation, in particular the United States, the United Kingdom of Great Britain and Northern Ireland, France, and the European Union as a whole. The obtained results made it possible to determine the achieved level of regulation of digital relations, to assess the balance of competing public and private interests. In the sphere under consideration gaps and disproportions in legal regulation and law enforcement are identified, the key areas for their improvement are offered.

***Keywords*—privacy, electronic data, database, balance, law enforcement, competing public and private interests, European Court of Human Rights, Constitutional Court of the Russian Federation**

REFERENCES

[1] L. Brandeis, S. Warren, “The right to privacy”, *Harvard Law Review*, vol. IV, no. 5, 1890.

[2] M. Svensson, C. Rosengren, F. Åström, „Digitalization and Privacy: A systematic literature review”, Lund University (Media-Tryck) [Online]. Available: https://portal.research.lu.se/en/publications/digitalization-and-privacy-a-systematic-literature-review (accessed: 24.10.2022).

[3] Z. Zhang, S. Lian, Q. Pei, J. Pu, Fuzzy Risk Assessments on Security Policies for Digital Rights Management, 2010 [Online]. Available: https://www.researchgate.net/profile/Zhiyong-Zhang-14/publication/228671422_Fuzzy_Risk_Assessments_on_Security_Policies_for_Digital_Rights_Management/links/55fc01a908ae07629e07d10a/Fuzzy-Risk-Assessments-on-Security-Policies-for-Digital-Rights-Management.pdf (accessed: 24.10.2022)

[4] T. Winkler, B. Rinner, “Securing Embedded Smart Cameras with Trusted Computing”, *Eurasip Journal on Wireless Communications and Networking*, 2011, doi: 10.1155/2011/530354.

[5] S. Wicker, D. Schrader, “Privacy-Aware Design Principles for Information Networks:, in *Proceedings of the IEEE*, 2011, no. 99, pp. 330–350, doi: 10.1109/JPROC.2010.2073670.

[6] A. Cavoukian, Privacy by Design The 7 Foundational Principles, 2011 [Online]. Available: https://www.ipc.on.ca/wp-content/uploads/resources/ 7foundationalprinciples.pdf (accessed: 24.10.2022).

[7] H.A. McKee, “Policy Matters Now and in the Future: Net Neutrality, Corporate Data Mining, and Government Surveillance”, *Computers and Composition*, no. 28(4), pp. 276–291, 2011, doi: 10.1016/j.compcom.2011.09.001.

[8] D. Michelfelder, “The moral value of informational privacy in cyberspace”, *Ethics and Information Technology*, no. 3, pp. 129–135, 2001, doi: 10.1023/A:1011802227136.

[9] D. Vitaliev, “Big brother is watching you [Internet security]”, *Communications Engineer*, no. 5(5), pp. 20–25, 2007, doi: 10.1049/ce:20070502.

[10] C. Amos, L. Zhang, I. Pentina, “Investigating Privacy Perception and Behavior on Weibo”, *Journal of Organizational and End User Computing*, no. 26(4), pp. 43–56, 2011, doi: 10.4018/joeuc.2014100103.

[11] D. Barnard-Wills, “E-safety education: Young people, surveillance and responsibility”, *Criminology & Criminal Justice*, vol. 12, no. 3, pp. 239–255, 2012, doi: 10.1177/1748895811432957.

[12] Y.J. Park, S.M. Jang, S. Mo Jang, “Understanding privacy knowledge and skill in mobile communication”, *Computers in Human Behavior*, no. 38, pp. 296–303, 2014, doi: 10.1016/j.chb.2014.05.041.

[13] S. Preibusch, “Privacy behaviors after Snowden”, *Communications of the ACM*, vol. 58, no. 5, pp. 48–55, 2015, doi: 10.1145/2663341.

[14] A. Champion, Trusted Computing and Digital Rights Management Clearinghouse. 2007 [Online]. Available: https://www.researchgate.net/publication/34658680_Trusted_Computing_and_Digital_Rights_Management_Clearinghouse (accessed: 24.10.2022).

[15] P.P. Garlinger, “Privacy, Free Speech, and The Patriot Act: First and Fourth Amendment Limits on National Security Letters”, *New York University Law Review*, vol. 84, no. 4, pp. 1105–1147, 2009.

[16] E.N. Beck, “The Invisible Digital Identity: Assemblages in Digital Networks”, *Computers and Composition*, no. 35, pp. 125–140, 2015, doi: 10.1016/j.compcom.2015.01.005.

[17] A.Y. Cover, “Corporate Avatars and the Erosion of the Populist Fourth Amendment”, *Iowa Law Review*, vol. 100, no. 4, pp. 1441–1502, 2015.

[18] M. Hu, “Biometric ID Cybersurveillance”, *Indiana Law Journal*, vol. 88, no. 4, pp. 1475–1558, 2013.

[19] F.S. Grodzinsky, H.T. Tavani, “P2P Networks and the Verizon v. RIAA Case: Implications for Personal Privacy and Intellectual Property”, *Ethics and Information Technology*, vol. 7, no. 4, pp. 243–250, 2005, doi: 10.1007/s10676-006-0012-4.

[20] T. Konstadinides, “Destroying democracy on the ground of defending It? The Data Retention Directive, the surveillance state and our constitutional ecosystem”, *European Law Review*, vol. 36, no. 5, pp. 722–736, 2011 [Online]. Available: https://openresearch.surrey.ac.uk/esploro/outputs/journalArticle/Destroying-democracy-on-the-ground-of-defending-it-The-Data-Retention-Directive-the-surveillance-state-and-our-constitutional-ecosystem/99516662902346 (accessed: 24.10.2022).

[21] A. Mantelero, “The future of consumer data protection in the EU Re-thinking the «notice and consent» paradigm in the new era of predictive analytics”, *Computer Law & Security Review*, vol. 30, no. 6, pp. 643–660, 2014, doi: 10.1016/j. clsr.2014.09.004.

[22] S.R. Peppet, “Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security and Consent”, *Texas Law Review*, vol. 93, no. 1, pp. 85–178, 2014.

[23] A. Roberts, “Privacy, Data Retention and Domination: Digital Rights Ireland Ltd v Minister for Communications”, *Modern Law Review*, vol. 78, no. 3, pp. 535–548, 2015, doi: 10.1111/1468-2230.12127.

[24] M.K. Riedy, J.H. Wen, “Electronic surveillance of Internet access in the American workplace: implications for management”, *Information & Communications Technology Law*, vol. 19, no. 1, pp. 87–99, 2010, doi: 10.1080/13600831003726374.

[25] D.R. Desai, “Constitutional Limits on Surveillance: Associational Freedom in The Age of Data Hoarding”, Notre *Dame Law Review*, vol. 90, no. 2, pp. 579–632, 2014.

[26] J.A.T. Fairfield, E. Luna, “Digital Innocence”, *Cornell Law Review*, vol. 99, no. 5, pp. 981–1076, 2014.

[27] T. Ojanen, “Privacy Is More Than Just a Seven-Letter Word: The Court of Justice of the European Union Sets Constitutional Limits on Mass Surveillance Court of Justice of the European Union, Decision of 8 April 2014 in Joined Cases C-293/12 and C-594/12”, Digital Right. European Constitutional Law Review, vol. 10, no. 3, pp. 528–541, 2014, doi: 10.1017/S1574019614001345.

[28] N.S. Zheleznyak, “K voprosu ob utochnenii terminologii v resheniyah Konstitucionnogo Suda Rossijskoj Federacii”, *Vestnik Sibirskogo yuridicheskogo instituta MVD Rossii*, no. 4(29), pp. 7–13, 2017. (In Russian)

[29] A.M. Karl, “Sootnoshenie neglasnyh sledstvennyh dejstvij i operativno-rozysknyh meropriyatij”, *Vestnik Sankt-Peterburgskogo universiteta MVD Rossii*, no. 3(83), pp. 144–151, 2019. (In Russian)

[30] I.A. Odnoshevin, “Sudebnyj kontrol' - garantiya konstitucionnyh prav grazhdan, vovlechennyh v sferu operativno-rozysknoj deyatel'nosti”, *Yurist – Pravoved*, no. 4(87), pp. 187-192, 2018. (In Russian)

[31] V.N. Omelin, “O provedenii operativno-rozysknyh meropriyatij v sluchayah, ne terpyashchih otlagatel'stva”, *Zakon i pravo*, no. 3, pp. 112–114, 2019, doi:10.24411/2073-3313-2019-10123. (In Russian)

[32] S.M. Hovavko, “Pravovye garantii soblyudeniya konstitucionnyh prav cheloveka i grazhdanina pri provedenii operativno-rozysknyh meropriyatij”, *Obshchestvo i pravo*, no. 4(58), pp. 131–136, 2016. (In Russian)

[33] A.E. Chechetin, “O sovershenstvovanii prokurorskogo nadzora za operativno-rozysknoj deyatel'nost'yu”, *Vestnik Sankt-Peterburgskogo universiteta MVD Rossii*, no. 3(79), pp. 134-139, 2018. (In Russian)

[34] Zayavlenie MID Rossii o zapuske procedury vyhoda iz Soveta Evropy 15 marta 2022 goda [Online]. Available: https://www.mid.ru/ru/press_service/spokesman/official_statement/1804379/ (accessed: 16.03.2022).

[35] Federal'nyj zakon ot 12 avgusta 1995 goda № 144-FZ (red. ot 30.12.2021) «Ob operativno-rozysknoj deyatel'nosti», *Rossijskaya gazeta*, 1995, August 18. (In Russian)

[36] Opredelenie Konstitucionnogo Suda RF ot 14 iyulya 1998 goda № 86-O «Po delu o proverke konstitucionnosti otdel'nyh polozhenij Federal'nogo zakona «Ob operativno - rozysknoj deyatel'nosti» po zhalobe grazhdanki I.G. Chernovoj», *Rossijskaya gazeta*, 1998, August 11. (In Russian)

[37] Case of S. and Marper v. United Kingdom (Applications № 30562/04 and 30566/04) [Online]. Available: https://hudoc.echr.coe.int/eng-press?i=003-2571936-2784147 (accessed: 19.09.2022).

[38] Case of Shimovolos v. Russia (Application № 30194/09) [Online]. Available: https://hudoc.echr.coe.int/eng-press?i=003-3581541-4053078 (accessed: 19.09.2022).

[39] Affaire Ben Faiza c. France (Requête № 31446/12) [Online]. Available: https://hudoc.echr.coe.int/eng?i=001-180657 (accessed: 19.09.2022).

[40] Prikaz MVD Rossii № 776, Minoborony Rossii № 703, FSB Rossii № 509, FSO Rossii № 507, FTS Rossii № 1820, SVR Rossii № 42, FSIN Rossii № 535, FSKN Rossii № 398, SK Rossii № 68 ot 27.09.2013 «Ob utverzhdenii Instrukcii o poryadke predstavleniya rezul'tatov operativno-rozysknoj deyatel'nosti organu doznaniya, sledovatelyu ili v sud», *Rossijskaya gazeta*, 2013, December 13. (In Russian)

[41] Delo Rasula Dzhafarova protiv Azerbajdzhana (Zayavlenie № 69981/14) [Online]. Available: https://hudoc.echr.coe.int/rus?i=001-165559 (accessed: 24.10.2022). (In Russian)

[42] Case of Catt v. the United Kingdom (Application № 43514/15) [Online]. Available: https://hudoc.echr.coe.int/rus?i=001-189424 (accessed: 24.10.2022).

[43] Affaire Félix Dagregorio et Alain Mosconi c. France (Requête № 65714/11 [Online]. Available: https://hudoc.echr.coe.int/rus?i=001-175036 (accessed: 24.10.2022).

[44] Case of Nagla v. Latvia (Application № 73469/10) [Online]. Available: https://hudoc.echr.coe.int/eng?i=001-122374 (accessed: 24.10.2022).

[45] Obysk u zhurnalista kak sposob raskryt' ego istochniki [Online]. Available: https://www.bfm.ru/news/376395 (accessed: 24.10.2022). (In Russian)

[46] Zakon RF ot 27 dekabrya 1991 goda № 2124-1 (red. ot 01.07.2021) «O sredstvah massovoj informacii», *Rossijskaya gazeta*, 1992, February 8. (In Russian)

[47] The principle of independence of lawyers: UN and IBA reference instruments. Basic Principles on the Role of Lawyers and the IBA Standards for the Independence of the Legal Profession, INTERNATIONAL BAR ASSOCIATION [Online]. Available: https://www.ibanet.org/MediaHandler?id=3b458c65-53f4-41b1-a1b2-0f765a7c39b3 (accessed: 06.04.2022).

[48] Federal'nyj zakon ot 31 maya 2002 goda № 63-FZ (red. ot 31.07.2020) «Ob advokatskoj deyatel'nosti i advokature v Rossijskoj Federacii», *Rossijskaya gazeta*, 2002, June 5. (In Russian)

[49] Opredelenie Konstitucionnogo Suda RF ot 8 noyabrya 2005 goda № 439-O «Po zhalobe grazhdan S.V. Borodina, V.N. Burobina, A.V. Bykovskogo i drugih na narushenie ih konstitucionnyh prav stat'yami 7, 29, 182 i 183 Ugolovno-processual'nogo kodeksa Rossijskoj Federacii», *Rossijskaya gazeta*, 2006, January 31. (In Russian)

[50] Opredelenie Konstitucionnogo Suda RF ot 22 marta 2012 № 629-O-O «Ob otkaze v prinyatii k rassmotreniyu zhaloby grazhdanina Abdulhamidova Ahmedshapi Gamzatovicha na narushenie ego konstitucionnyh prav polozheniyami statej 8 i 9 Federal'nogo zakona «Ob operativno-rozysknoj deyatel'nosti», a takzhe statej 7, 29 i 450 Ugolovno-processual'nogo kodeksa Rossijskoj Federacii» [Online]. Available: http://www.consultant.ru (accessed: 06.04.2022).

[51] Apellyacionnoe postanovlenie Verhovnogo Suda CHechenskoj Respubliki № 22-K-221/2020 ot 7 iyulya 2020 goda po ugolovnomu delu № 3/6-124/20 [Online]. Available: https://sudact.ru (accessed: 06.04.2022) (In Russian).

[52] Case of Kolesnichenko v. Russia (Application o. 19856/04) [Online]. Available: https://hudoc.echr.coe.int/eng?i=001-92147 (accessed: 06.04.2022).

[53] Opredelenie Konstitucionnogo Suda RF ot 15 iyulya 2008 goda № 460-O-O «Ob otkaze v prinyatii k rassmotreniyu zhaloby grazhdanina Bukreeva Vladimira Viktorovicha na narushenie ego konstitucionnyh prav otdel'nymi polozheniyami statej 5, 11 i 12 Federal'nogo zakona «Ob operativno-rozysknoj deyatel'nosti» i punktom 13 Instrukcii o poryadke predstavleniya rezul'tatov operativno-rozysknoj deyatel'nosti doznavatelyu, organu doznaniya, sledovatelyu, prokuroru ili v sud» [Online]. Available: http://www.consultant.ru (accessed: 06.04.2022). (In Russian)

[54] Postanovlenie Konstitucionnogo Suda RF ot 9 iyunya 2011 goda № 12-P «Po delu o proverke konstitucionnosti polozhenij punkta 7 stat'i 16 Zakona Rossijskoj Federacii «O statuse sudej v Rossijskoj Federacii» i chasti pervoj stat'i 9 Federal'nogo zakona «Ob operativno-rozysknoj deyatel'nosti» v svyazi s zhaloboj grazhdanina I.V. Anosova», *Rossijskaya gazeta*, 2011, 22 июня. (In Russian)

[55] Vychislyaemye dannye mogut rasskazat' o nas bol'she, chem personal'nye [Online]. Available: https://radiovesti.ru/brand/63899/episode/ 1366965/ (accessed: 15.03.2021). (In Russian)

[56] E.V. Talapina, “Pravo i cifrovizaciya: novye vyzovy i perspektivy”, *Zhurnal rossijskogo prava*, no. 2 (254), pp. 5–17, 2018. (In Russian)

[57] Federal'nyj zakon ot 25 iyulya 1998 goda № 128-FZ (red. ot 01.07.2021) «O gosudarstvennoj daktiloskopicheskoj registracii v Rossijskoj Federacii», *Sobranie zakonodatel'stva RF*, 1998, no. 31, St. 3806. (In Russian)

[58] Postanovlenie Pravitel'stva RF ot 31 oktyabrya 2018 goda № 1296 «Ob utverzhdenii Pravil napravleniya daktiloskopicheskoj informacii v organy vnutrennih del», *Sobranie zakonodatel'stva RF*, 2018, no. 46, st. 7046. (In Russian)

[59] Prikaz MVD Rossii, MCHS Rossii, Minoborony Rossii, Minfina Rossii, Minyusta Rossii, Mintransporta Rossii, SVR Rossii, FSB Rossii, FSO Rossii, Rosgvardii, GUSP, Genprokuratury Rossii, SK Rossii ot 23 sentyabrya 2020 goda № 659/717/473/208n/209/385/63/429/185/376/145/502/94 «Ob utverzhdenii Poryadka formirovaniya napravlyaemoj v organy vnutrennih del daktiloskopicheskoj informacii» [Online]. Available: http://publication.pravo.gov.ru/Document/View/0001202009250035 (accessed: 19.09.2022). (In Russian)

[60] M.A. Mihajlov, “Sovershenstvovanie sistemy daktiloskopicheskoj registracii: konferenciya v gosudarstvennoj dume”, *Uchenye zapiski Krymskogo federal'nogo universiteta imeni V.I. Vernadskogo. YUridicheskie nauki*, no. 1, pp. 292–305, 2015. (In Russian)

[61] Forensic Information Databases Service (FINDS): The Forensic Information Databases Strategy Board policy for access and use of DNA samples, DNA profiles, fingerprint images, and associated data [Online]. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1052529/FIND_Strategy_Board_Policy_Access_and_Use.pdf (accessed: 19.09.2022).

[62] Poyasnitel'naya zapiska k proektu Federal'nogo zakona «O vnesenii izmenenij v otdel'nye zakonodatel'nye akty Rossijskoj Federacii po

voprosam gosudarstvennoj genomnoj registracii». Zakonoproekt № 1048800-7 [Online]. Available: https://sozd.duma.gov.ru/bill/1048800-7 (accessed: 19.09.2022). (In Russian)

[63] National DNA Database Strategy Board Biennial Report 2018 – 2020 [Online]. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/913011/NDNAD_Strategy_Board_AR_2018-2020_Web_Accessible.pdf (accessed: 19.09.2022).

[64] CODIS - NDIS Statistics [Online]. Available: https://www.fbi.gov/services/ laboratory/biometric-analysis/codis/ndis-statistics (accessed: 19.09.2022).

[65] Federal'nyj zakon ot 3 dekabrya 2008 goda № 242-FZ «O gosudarstvennoj genomnoj registracii v Rossijskoj Federacii», *Sobranie zakonodatel'stva Rossijskoj Federacii*, 2008, no. 49, st. 5740; 2009, no. 51, st. 6150. (In Russian)

[66] Postanovlenie Pravitel'stva RF ot 11 oktyabrya 2011 goda № 828 «Ob utverzhdenii Polozheniya o poryadke provedeniya obyazatel'noj gosudarstvennoj genomnoj registracii lic, osuzhdennyh i otbyvayushchih nakazanie v vide lisheniya svobody», *Sobranie zakonodatel'stva RF*, 2011, no. 42, st. 5926. (In Russian)

[67] Z.L. Shkhagapsoev, R.R. Kardanov, "Genomnaya registraciya kak element protivodejstviya prestupleniyam terroristicheskogo haraktera na sovremennom etape", *Izvestiya Tul'skogo gosudarstvennogo universiteta. Ekonomicheskie i yuridicheskie nauki*, no. 1-2, pp. 84–90, 2016. (In Russian)

[68] O.P. Gribunov, "Vseobshchaya daktiloskopicheskaya registraciya grazhdan kak element realizacii kriminalisticheskogo preduprezhdeniya prestuplenij", *Vestnik Tomskogo gosudarstvennogo universiteta*, no. 402, pp. 188–191, 2016. (In Russian)

[69] T.V. Popova, A.B. Sergeev, "Federal'naya baza dannyh genomnoj informacii v sisteme obespecheniya balansa chastnyh i publichnyh interesov v ugolovnom sudoproizvodstve", YUridicheskaya nauka i pravoohranitel'naya praktika. No. 1 (39), pp. 132–139, 2017. (In Russian)

[70] Zakonoproekt № 1048800-7 «O vnesenii izmenenij v otdel'nye zakonodatel'nye akty Rossijskoj Federacii po voprosam gosudarstvennoj genomnoj registracii (v chasti rasshireniya perechnya lic. podlezhashchih obyazatel'noj gosudarstvennoj genomnoj registracii)» [Online]. Available: https://sozd.duma.gov.ru/bill/1048800-7 (accessed: 19.09.2022). (In Russian)

[71] A.A. Chernyh, "Podhody Konstitucionnogo Suda Rossijskoj Federacii k voprosu o neobhodimosti polucheniya sudebnyh reshenij pri provedenii operativno-rozysknyh meropriyatij s ispol'zovaniem tekhnicheskih sredstv", *Vestnik Sibirskogo yuridicheskogo instituta MVD Rossii*, no. 2 (35), pp. 16–24, 2019. (In Russian)

[72] Postanovlenie Plenuma Verhovnogo Suda RF ot 31 oktyabrya 1995 goda № 8 (red. ot 03.03.2015) «O nekotoryh voprosah primeneniya sudami Konstitucii Rossijskoj Federacii pri osushchestvlenii pravosudiya», *Rossijskaya gazeta*, 1995, December 28. (In Russian)

[73] Affaire Trabajo Rueda c. Espagne (Requête № 32600/12) [Online]. Available: https://hudoc.echr.coe.int/eng?i=001-173787 (accessed: 19.09.2022).

[74] Case of Szabó and Vissy v. Hungary (Application № 37138/14) [Online]. Available: https://hudoc.echr.coe.int/eng?i=001-160020 (accessed: 19.09.2022).

[75] Case of Big Brother Watch and others v. The United Kingdom (Applications №№ 58170/13, 62322/14 and 24960/15) [Online]. Available: https://hudoc.echr.coe.int/eng?i=001-210077 (accessed: 19.09.2022).

[76] Postanovlenie Konstitucionnogo Suda RF ot 20 maya 1997 goda № 8-P «Po delu o proverke konstitucionnosti punktov 4 i 6 stat'i 242 i stat'i 280 Tamozhennogo kodeksa Rossijskoj Federacii v svyazi s zaprosom Novgorodskogo oblastnogo suda», *Rossijskaya gazeta*, 1997, May 29. (In Russian)

[77] Postanovlenie Konstitucionnogo Suda RF ot 11 marta 1998 goda № 8-P «Po delu o proverke konstitucionnosti stat'i 266 Tamozhennogo kodeksa Rossijskoj Federacii, chasti vtoroj stat'i 85 i stat'i 222 Kodeksa RSFSR ob administrativnyh pravonarusheniyah v svyazi s zhalobami grazhdan M.M. Gagloevoj i A.B. Pestryakova», *Rossijskaya gazeta*, 1998, March 26. (In Russian)

[78] Postanovlenie Konstitucionnogo Suda RF ot 16 iyulya 2008 goda № 9-P «Po delu o proverke konstitucionnosti polozhenij stat'i 82 Ugolovno-processual'nogo kodeksa Rossijskoj Federacii v svyazi s zhaloboj grazhdanina V.V. Kostyleva», *Rossijskaya gazeta*, 2008, August 1. (In Russian)

[79] Chamber Judgments B.B.. Gardel. M.B. v. France [Online]. Available: https://hudoc.echr.coe.int/fre-press?i=003-4480954-5400075 (accessed: 07.03.2022).

[80] Case of Gaughran v. The United Kingdom (Application № 45245/15) [Online]. Available: https://hudoc.echr.coe.int/rus?i=001-200817 (accessed: 07.03.2022).

[81] Case of M.K. v. France (Application № 19522/09) [Online]. Available: https://hudoc.echr.coe.int/eng?i=001-119075 (accessed: 07.03.2022).

[82] Affaire Brunet c. France (Requête № 21010/10) [Online]. Available: https://hudoc.echr.coe.int/eng?i=001-146389 (accessed: 07.03.2022).

[83] Fichier national automatisé des empreintes génétiques (FNAEG) [Online]. Available: https://www.service-public.fr/particuliers/vosdroits/F34834 (accessed: 07.03.2022).

[84] Case of Youth Initiative for Human Rights v. Serbia (Application № 48135/06) [Online]. Available: https://hudoc.echr.coe.int/eng?i=001-120955 (accessed: 07.03.2022).

[85] Federal'nyj zakon ot 2 maya 2006 goda №59-FZ (red. ot 27.12.2018) «O poryadke rassmotreniya obrashchenij grazhdan Rossijskoj Federacii», *Rossijskaya gazeta*, 2006, May 5. (In Russian)

[86] Opredelenie Konstitucionnogo Suda RF ot 20 oktyabrya 2005 goda № 375-O «Ob otkaze v prinyatii k rassmotreniyu zhaloby grazhdanina Makarenko Anatoliya Mihajlovicha na narushenie ego konstitucionnyh prav chast'yu chetvertoj stat'i 29 Ugolovno-processual'nogo kodeksa Rossijskoj Federacii i stat'yami 6 - 9 Federal'nogo zakona "Ob operativno-rozysknoj deyatel'nosti» [Online]. Available: http://www.consultant.ru (accessed: 07.03.2022). (In Russian)

Mamay Evgeny Alekseevich, Candidate of Science (Law), Associate Professor, HSE University (Nizhny Novgorod), ORCID 0000-0002-9386-2747 (emamaj@hse.ru).