

## РАЗДЕЛ 1

---

# ВЛИЯНИЕ ЦИФРОВИЗАЦИИ НА ПРОТИВОДЕЙСТВИЕ КОРРУПЦИИ

**Ц**ифровизация способствует росту взаимосвязей и взаимообусловленностей в большинстве сфер государственной и общественной жизни, а также повышению интенсивности обмена информацией, ускорению общественной жизни. Более того, она позволяет субъектам права отслеживать большой объем информации и оперативно реагировать на нее.

При анализе влияния цифровизации на развитие законодательства о противодействии коррупции обращается внимание на пересечение сфер правового регулирования вопросов противодействия коррупции с областями, в которых осуществляется цифровизация. Современные исследования показывают, что такие сферы могут не только пересекаться, но и совпадать<sup>1</sup>.

Во-первых, цифровые технологии используются для контроля за соблюдением и в целях предотвращения нарушений законодательства о противодействии коррупции. Цифровой контроль имущественного положения государственных служащих и иных категорий лиц может оказаться полезным инструментом для выявления отмыкания преступных доходов, участия в коррупционных схемах, уклонений от уплаты налогов. Внедрение цифровых технологий рассматривается многими исследователями и специалистами-практиками в качестве превентивной антикоррупционной меры.

---

<sup>1</sup> См.: Тихомиров Ю. А., Кичигин Н. В., Цомартова Ф. В., Бальхаева С. Б. Право и цифровая трансформация // Право. Журнал Высшей школы экономики. 2021. № 2. С. 4-23.

Во-вторых, цифровые технологии используются для расследования нарушений законодательства о противодействии коррупции, например для первичной проверки справок об имуществе, доходах, расходах, обязательствах имущественного характера.

В-третьих, новые цифровые технологии, включая использование искусственного интеллекта, могут применяться для решения глобальных проблем, связанных с противодействием коррупции и организованной преступности, включая отслеживание незаконных финансовых операций и оценку изменений имущественного положения отдельных категорий лиц.

Внедрение новых технологий может воздействовать на поведение людей<sup>2</sup>. Цифровизация оказывает влияние на существо правоотношений, возникающие, развивающиеся и заканчивающиеся в цифровой среде. Комментарий в социальной сети, репост или лайк могут быть квалифицированы как деяние, в котором усматривается состав коррупционного преступления<sup>3</sup>. В свою очередь, обещание, предложение и передача предмета незаконного вознаграждения могут осуществляться в цифровой среде, как и передача незаконного вознаграждения (например, криптовалюты). Информационные технологии могут также использоваться для обеспечения соблюдения запретов, ограничений и обязанностей, установленных в целях противодействия коррупции.

Цифровизация детерминирует трансформацию общественных отношений, которые, в свою очередь, выступают объектами правового регулирования. При этом расширяются возможности для противодействия коррупции, а право способствует легитимизации цифровых антикоррупционных практик. Так, Стратегией развития информационного общества в Российской Федерации на 2017–2030 годы, утвержденной Указом Президента Российской Федерации от 9 мая 2017 г. № 203

<sup>2</sup> См.: Bourgeois David T.; Smith, James L.; Wang, Shouhong; and Mortati, Joseph/ Information Systems for Business and Beyond, 2019. P. 23.

<sup>3</sup> См.: Талапина Э. В. Право и цифровизация: новые вызовы и перспективы // Журнал российского права. 2018. № 2. С. 11.

«О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы»<sup>4</sup>, информационные технологии отнесены к сфере безопасности государства, обеспечения правопорядка.

В современном государственном управлении практически не осталось задач, выполняемых без использования государственных информационных систем и баз данных. Государственные информационные системы консолидируют создаваемые государством и получаемые от граждан и организаций сведения. Основой функционирования таких систем является достоверная информация о гражданах и организациях, а также о совершении ими юридически значимых действий. Цифровые технологии дают возможность собирать информацию из нескольких источников для создания профилей людей.

В технологически развитых странах набирает силу тенденция, состоящая в интеграции в правовое пространство государственных информационных систем, агрегирующих не только сведения о действиях граждан, имеющих выражение в материальном мире (получение гражданства, заключение брака, уплата налогов, предоставление кредита, нарушение правил дорожного движения), но также и сведения о поступках, полностью совершаемых в информационной среде. К сведениям о действиях, совершаемых в информационной среде, например, относятся: трата времени на видеоигры, легкомысленные посты в социальных сетях, распространение ложных сведений. Ярким примером такой государственной информационной системы является система социального рейтинга (социального доверия) в Китае<sup>5</sup>.

Составной частью китайской системы социального доверия являются красные и черные списки. В черных списках содержатся

<sup>4</sup> СЗ РФ. 2017, № 20, ст. 2901.

<sup>5</sup> Подробнее об этом см.: Галиуллина С. Д., Бреслер М. Г., Сулейманов А. Р. и др. Система социального кредитования в Китае как элемент цифрового будущего // Вестник УГНТУ. Наука, образование, экономика. Серия: Экономика. 2018. № 4(26). С. 114–121.

сведения о гражданах КНР, совершивших преступления (мошенничество, кражу, убийство и т. д.). Такие сведения доступны любому заинтересованному лицу, достаточно обратиться к соответствующему интернет-сайту<sup>6</sup>.

Отдельный черный список содержит данные о китайских гражданах, которым запрещено пользоваться поездами и самолетами. Как правило, в такие списки заносятся граждане, допустившие нарушение правил поведения, установленных перевозчиками, включая курение, употребление алкоголя, агрессивные действия в отношении других пассажиров и сотрудников компаний-перевозчиков. При этом в черном списке приводится описание конкретных действий, послуживших основанием для включения в него гражданина.

В отличие от черных списков красные списки содержат данные о добропорядочных гражданах, получивших признание в китайском обществе, в том числе имеющих государственные награды, меценатах и общественных деятелях. Одной из особенностей системы социального доверия является отнесение к объектам рейтингования не только физических лиц, но и организаций и даже административных единиц. Применительно к коммерческим организациям система социального рейтинга ориентирована на предоставление гражданам информации о надежности компании как потенциального контрагента (например, о том, что организация не принимала участие в мошеннических схемах, не имеет долгов по уплате налогов, что на нее не обращены судебные взыскания и т. д.).

В отношении государственных служащих в КНР на протяжении шести лет осуществлялись пилотные испытания информационной системы Zero Trust, получившей доступ к информации о государственных служащих, содержащейся приблизительно в 150 государственных базах данных. Указанная система анализирует служебную деятельность и образ жизни государственных служащих, выявляет сомнительные транзакции, соотносит доходы и расходы. При этом она просчитывает

---

<sup>6</sup> URL: <https://www.creditchina.gov.cn/>

вероятность того, что то или иное действие связано с коррупцией. Zero Trust анализирует государственные закупки, выявляя ситуации конфликта интересов, когда в закупках участвуют родственники государственного служащего или его друзья. Практика показала, что функционирование данной системы способно уберечь государственных служащих от злоупотреблений, поскольку у нанимателя появляется возможность воздействовать на них на раннем этапе возникновения конфликта интересов<sup>7</sup>.

Государственные информационные системы, подобные системам социального доверия КНР, а также Zero Trust способны оказывать значительное влияние на функционирование социума. Дело в том, что уже сама информация о ситуации в обществе влияет на его состояние<sup>8</sup>. Внедрение системы социального рейтингования не только наделяет субъектов права определенной характеристикой — публичной оценкой, но и ориентирует их на решение задач, связанных с повышением своего рейтинга. Более того, данные, содержащиеся в таких системах, могут обрабатываться с использованием технологий искусственного интеллекта и учитываться при принятии управленческих решений.

Опыт Китая показывает, что ключевыми компонентами развития цифровой среды и являются формирование и применение цифрового профиля в органах государственной власти<sup>9</sup>. В контексте функционирования государственных информационных систем цифровой профиль может рассматриваться в качестве базового информационного узла, выполняющего важные функции по актуализации и обмену

---

<sup>7</sup> World Bank. *Artificial Intelligence in the Public Sector: Maximizing Opportunities, Managing Risks*. Equitable Growth, Finance and Institutions Insight; World Bank, Washington, DC, 2020. 107 p.

<sup>8</sup> См.: Доронина Н. Г., Семилютина Н. Г., Цирина М. А. Правовое регулирование науки и научной деятельности в условиях цифровизации // *Юридическое образование и наука*. № 4. 2022. С. 30.

<sup>9</sup> См.: Трунцевский Ю. В., Севальнев В. В., Сухаренко А. Н. Противодействие коррупции в Китае: законодательство и правоприменение: монография. М.: Проспект, 2019; Цифровое право: учебник / под общ. ред. В. В. Блажеева, М. А. Егоровой. М.: Проспект, 2020. С. 27.

персонифицированной (относящейся к конкретному лицу) информацией, а также по идентификации данного лица.

Применительно к государственному управлению цифровые технологии способны многократно улучшить оперативность решений различных обеспечивающих задач посредством ускорения обмена информацией и повышения удобства коммуникации, сократить возможности для реализации негативных управленческих практик за счет большей автоматизации и контролируемости административных процедур, выполняемых органами государственной власти. Одним из таких механизмов является деперсонализация взаимодействия граждан и сотрудников органов власти, в рамках которой государственные услуги могут предоставляться в дистанционном формате, что позволяет снизить возможность неформального взаимодействия и риски коррупции. Другим таким механизмом является цифровое профилирование<sup>10</sup>.

Внедрение цифровых технологий рассматривается многими исследователями в качестве превентивной антикоррупционной меры, позволяющей со временем отказаться от субъективных решений отдельных должностных лиц. При этом государственные служащие будут не принимающими, а утверждающими (или отклоняющими) решения, предлагаемые алгоритмами цифровой платформы<sup>11</sup>.

Следует отметить, что антикоррупционная составляющая цифровой среды заключается в максимальной автоматизации, алгоритмизации и усилении подконтрольности всех управленческих процессов, что серьезно затрудняет как непосредственное вступление в коррупционные отношения, так и возможности по их сокрытию. Вместе с тем

<sup>10</sup> См.: Цирин А. М., Севальнев В. В. Институциональные механизмы противодействия коррупции на государственной службе // Журнал российского права. 2021. № 9. С. 142.

<sup>11</sup> Федеральный портал госуслуг [www.gosuslugi.ru](http://www.gosuslugi.ru) также можно рассматривать как будущую цифровую платформу, на которой, с одной стороны, находятся органы власти всех уровней, а впоследствии будут размещаться и бюджетные организации, а с другой стороны — физические и юридические лица. Подробнее об этом см.: Государство как платформа: люди и технологии: доклад / под ред. М. С. Шклярук. — М: РАНХиГС, 2019.

система ограничений, запретов и обязанностей, установленных в целях противодействия коррупции, практически не охватывает лиц, администрирующих государственные информационные системы и электронные площадки, что в условиях неограниченного доступа граждан и организаций к чувствительной информации порождает существенные риски. Преодоление этих рисков требует дальнейшего развития антикоррупционного правового регулирования. Как справедливо отмечает академик РАН Т. Я. Хабриева, в российской науке заметен интерес к этой теме, «исследования нацелены на освоение отдельных, относительно узких, хотя бесспорно важных и требующих решения проблем, связанных с использованием цифровых технологий в правовой сфере»<sup>12</sup>.

В юридической литературе уже констатируется потребность выработки метода и релевантных инструментов правового воздействия на динамичные социально-экономические отношения в цифровом обществе с учетом баланса частных и публичных интересов, необходимости защиты прав человека, а также создания благоприятного инвестиционного климата и возможности реализации экономических свобод<sup>13</sup>.

Накопление научных знаний по отдельным исследовательским направлениям внедрения цифровых технологий в сфере противодействия коррупции способствует постановке вопроса о разработке концепции развития правового регулирования в данной сфере.

В сети «Интернет» физическое лицо может выбрать любое имя, работать под творческим псевдонимом или ником (от англ. *nickname* — кличка, прозвище). В связи с этим для целей правового регулирования необходима точная идентификация субъектов права в Интернете. Для обозначения анонимных участников

---

<sup>12</sup> Хабриева Т. Я. Право перед вызовами цифровой реальности // Журнал российского права. 2018. Вып. № 9. С. 6.

<sup>13</sup> См.: Цифровая экономика: актуальные направления правового регулирования: науч.-практ. пособие / под ред. И. И. Кучерова, С. А. Сеницына. М.: Норма; ИЗИСП, 2022. С. 15.



интернет-отношений используется категория виртуальной личности, которая, на наш взгляд, нуждается в конкретизации. Представляется, что виртуальная личность не является новой личностью, а больше похожа на результат анонимизации физического лица, которое по тем или иным причинам не хочет выступать в сети «Интернет» от своего имени. При этом она может представляться в любом амплуа — положительном, отрицательном, нейтральном, в привязке к какому-нибудь гендеру или без нее. Поэтому одним из последствий влияния цифровизации на законодательство является потребность в надлежащей идентификации участников общественных отношений. Актуальная задача права — определение правового содержания категории цифрового профилирования и подходов к его правовому регулированию.

С технической точки зрения деанонимизировать физическое лицо без встречных действий с его стороны крайне затруднительно. Отслеживание IP-адреса электронного устройства, с которого осуществляется доступ в сеть «Интернет», также не позволяет окончательно идентифицировать личность, поскольку устройством может пользоваться значительный круг лиц.

Наряду с несомненными положительными эффектами в контексте противодействия коррупции цифровые технологии имеют оборотную сторону, облегчая совершение коррупционных правонарушений, в том числе порождая новые латентные способы передачи незаконного вознаграждения и осуществления властных полномочий с противоправными целями, образуя своего рода теневой сектор коррупционных услуг (подробнее см. раздел 4 настоящего пособия).

Цифровой профиль и его атрибуты уже довольно прочно вошли не только в бизнес-процессы, но и в повседневную жизнь человека. Например, данные, образующие цифровой профиль, активно анализируются банками и иными кредитными учреждениями в качестве показателей финансового положения и интересов человека. Социальные

медиа также используют цифровой профиль и цифровой след<sup>14</sup> для того, чтобы определить личные интересы пользователей сети «Интернет», их привычки и предпочтения. В юридической литературе отмечается, что профиль в социальной сети содержит:

- персональные данные пользователя (имя, дата рождения, локация, образование, работа и т. п.);
- личные фотографии;
- список контактов;
- «стену», на которой создается контент<sup>15</sup>.

Как правило, пользователи оставляют на порталах рекрутинговых агентств следующие сведения: фамилия, имя и отчество, резюме, фотографию, сведения о предыдущих местах работы, контактные данные, разрешение на обработку персональных данных. Вместе с тем на практике сотрудники кадровых служб зачастую не ограничиваются этой информацией и анализируют личные профили будущих сотрудников и работников в социальных сетях с целью определения их лояльности и отношения к исполняемым должностным обязанностям<sup>16</sup>.

Полицейские службы в отдельных странах, например в США, анализируют данные цифрового профиля сотрудников для выявления склонности к нарушению дисциплины, а также к совершению правонарушений, в том числе коррупционных<sup>17</sup>.

Несмотря на развитие общественных отношений, связанных с использованием цифрового профиля, законодательное определение

---

<sup>14</sup> Цифровой след — совокупность информации (данных) о посещении информационно-коммуникационной сети пользователем и его действиях в цифровом пространстве.

<sup>15</sup> Подробнее об этом см.: Тясто Ю. А. Правовая защита цифровых активов: страница социальной сети // Журнал Суда по интеллектуальным правам. 2021. № 3 (33), сентябрь. С. 84-101.

<sup>16</sup> См.: Офман Е. М. Мониторинг поведения работников в социальных сетях: возможности и пределы работодателя // *Ex jure*. 2020. № 1. С. 85-94.

<sup>17</sup> Подробнее об этом см.: Carton, Samuel. Et al. «Identifying Police Officers at Risk of Adverse Events». Proceedings of the 22 ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, KDD 16. NY. USA: ACM, 2016, 67-76.

данной категории все еще не выработано, что образует пробел в праве. Необходимость установления данного понятия подчеркивается в юридической литературе. При этом предлагается выявить основные направления развития цифрового профилирования, сопутствующие ему вызовы и риски, а также роль и место в рамках осуществления публичной власти<sup>18</sup>.

Для определения понятия цифрового профиля не менее важна и функциональная составляющая, опосредующая обмен информацией и идентификацию лица, а также позволяющая осуществлять хранение, обработку и передачу соответствующих данных и документов, обращаться за получением различных государственных, муниципальных и иных услуг. Указанные характеристики делают цифровой профиль не только персональным архивом для хранения данных о важных документах, доступ к которому может быть открыт в любом месте в режиме онлайн, но и своего рода визитной карточкой лица, необходимой для получения широкого спектра различных услуг. Важно учитывать еще одну особенность цифрового профиля, проявляющуюся в том, что он также является единым порталом для получения (извлечения) данных не только гражданином или организацией, но и органами власти и иными пользователями соответствующих государственных информационных систем. Универсальность цифрового профиля проявляется также и в том, что он может использоваться для получения как государственных, так и негосударственных публичных услуг<sup>19</sup>.

В настоящее время предпринимаются активные попытки установления легальной дефиниции цифрового профиля. В одном из законопроектов цифровой профиль определяется в качестве совокупности сведений о гражданах и юридических лицах, содержащихся

---

<sup>18</sup> Подробнее об этом см.: Виноградова Е. В., Полякова Т. А., Минбалеев А. В. Цифровой профиль: понятие, механизмы регулирования и проблемы реализации // Правоприменение. 2021. Вып. 4. Т. 5. С. 5-19.

<sup>19</sup> Подробнее о соотношении государственных и негосударственных публичных услуг см.: Терещенко Л. К. Услуги: государственные, публичные, социальные // Журнал российского права. 2004. № 10.

в информационных системах государственных органов, органов местного самоуправления и организаций, осуществляющих в соответствии с федеральными законами отдельные публичные полномочия, а также в единой системе идентификации и аутентификации. Такая дефиниция была предложена в проекте федерального закона № 747513-7 «О внесении изменений в отдельные законодательные акты (в части уточнения процедур идентификации и аутентификации)» (далее — проект федерального закона № 747513-7)<sup>20</sup>. Следует отметить, что законопроект при определении понятия цифрового профиля отсылает не к какой-то конкретной информационной системе, а к совокупности систем.

Отсутствие привязки цифрового профиля к конкретным элементам информационной инфраструктуры не позволяет однозначно установить, что под ним понимается. Так, непонятно, чем цифровой профиль гражданина будет отличаться, например, от цифрового профиля государственного служащего или от цифрового профиля студента. Кроме того, в рассматриваемом определении речь идет о совокупности сведений о лицах, содержащихся в информационных системах различных органов власти и организаций, что также негативно влияет на точность предложенной дефиниции.

В юридической литературе приводится установление цифрового профиля как многоуровневой сложной системы, формирование которой обеспечивается анализом данных, содержащихся во всех информационных системах, а также в информационно-телекоммуникационных сетях<sup>21</sup>.

Более точным и отвечающим потребностям законодательного регулирования представляется следующее определение цифрового профиля, данное в научной статье Е. В. Виноградовой, Т. А. Поляковой, А. В. Минбалева, посвященной понятию, механизмам регулирования и проблемам реализации цифрового профиля: цифровой

<sup>20</sup> URL: <https://sozd.duma.gov.ru/bill/747513-7>.

<sup>21</sup> См.: Жарова А. К. Вопросы обеспечения безопасности цифрового профиля человека // Юрист. 2020. № 3. С. 58.

профиль — это совокупность актуальных достоверных данных и иных сведений о физических или юридических лицах, формируемых в единой системе идентификации и аутентификации или других информационных системах органов государственной власти и местного самоуправления, а также подведомственных им организаций, контактирующих с ней благодаря единой системе межведомственного электронного взаимодействия в целях их предоставления с согласия соответствующих граждан или юридических лиц субъектам, запросившим доступ к этим сведениям посредством инфраструктуры цифрового профиля<sup>22</sup>.

В данном определении содержится указание на несколько государственных информационных систем: единую систему межведомственного электронного взаимодействия как ресурс, обеспечивающий связь с единой системой идентификации и аутентификации или другими информационными системами органов государственной власти и местного самоуправления, а также подведомственных им организаций. Кроме того, рассматриваемое определение ограничивает цифровой профиль данными, содержащимися в информационных системах органов власти и подведомственных организаций, исключая при этом данные информационно-телекоммуникационных сетей, которые будут носить официальный характер в отличие от данных, полученных из информационно-телекоммуникационных сетей.

Цифровой профиль государственного служащего целесообразно рассматривать в качестве элемента конкретных государственных информационных систем, содержащих не простую, а систематизированную по отдельным реквизитам совокупность данных об этом лице. В качестве одной из таких информационных систем целесообразно рассматривать прежде всего ЕСИА, охватывающую все сервисы цифрового профиля, к которым относятся: цифровые документы (выполняют

---

<sup>22</sup> См.: Виноградова Е. В., Полякова Т. А., Минбалеев А. В. Цифровой профиль: понятие, механизмы регулирования и проблемы реализации // Правоприменение. 2021. Вып. 4. Т. 5. С. 5–19.

функцию хранения информации), цифровые согласия<sup>23</sup> (содержат реестр цифровых согласий); цифровые ID и реестр рассылок (позволяют собирать необходимые данные); система идентификации. В ЕСИА находятся первичные данные цифрового профиля любого гражданина вне зависимости от его отношения к государственной службе. Другими информационными системами, агрегированными с цифровым профилем государственного служащего, должны стать ЕИСУКС, государственная информационная система в области противодействия коррупции «Посейдон» (далее — ГИС «Посейдон») и другие.

Правовая регламентация обработки персональных данных гражданина на портале государственных услуг включает в себя сведения о довольно внушительном наборе документов<sup>24</sup>. При этом увеличение объема информации, охватываемой цифровым профилем гражданина, позволяет получить доступ к более широкому спектру не только государственных, но и коммерческих услуг (предоставление кредита, страховые услуги и т. д.). По данным Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации, с 20 мая 2020 г. по 20 мая 2021 г. 3,5 млн граждан дали согласие на предоставление тех или иных сведений банкам и страховым организациям<sup>25</sup>.

Задачи разработки и апробации инфраструктуры цифрового профиля были определены в подп. «а» и «б» п. 3 Положения о проведении эксперимента по повышению качества данных. Инфраструктура цифрового профиля согласно подп. «а» п. 3 Положения должна предусматривать в том числе следующие функциональные возможности:

- сохранение необходимой информации о лице в единой системе идентификации и аутентификации с возможностью предо-

<sup>23</sup> Цифровое согласие является юридически значимой реестровой записью о предоставлении (отзыве) прав на сбор, передачу и использование данных в соответствии с указанной целью обработки.

<sup>24</sup> Паспорт; история ранее выданных паспортов; удостоверение личности на территории Российской Федерации иностранных граждан; удостоверение водителя; загранпаспорт; свидетельство о рождении; свидетельства о браках и разводах; свидетельства о смене фамилии, имени; свидетельство об отцовстве; свидетельство о смерти; сведения о личном транспортном средстве; СНИЛС и др.

<sup>25</sup> URL: <https://digital.gov.ru/ru/events/40998/>

ставления необходимых документов по запросу данного лица, а также корректировки соответствующих сведений в случае их недостоверности и (или) неточности;

- разрешение банкам и страховым организациям доступа к необходимой информации о клиентах по их инициативе или с их согласия;
- использование цифрового профиля для заполнения заявлений о предоставлении государственных и муниципальных услуг, кредитных и страховых услуг, а также при реализации активного избирательного права.

Кроме того, предусматривалась возможность автоматического получения данных о гражданах при условии их согласия, а также определения порядка использования цифрового профиля и иных идентификаторов (включая биометрическую идентификацию, облачную квалифицированную электронную подпись и др.), в том числе при совершении гражданско-правовых сделок.

Таким образом, цифровой профиль может рассматриваться в качестве портала доступа к информации о гражданине, первичной ячейки или соты, содержащей систематизированные данные, которыми оперируют различные информационные системы. При этом образующие его (их) сведения могут как формироваться самими гражданами и органами власти, так и быть собраны и систематизированы в автоматическом режиме.

Государство создает централизованный информационный ресурс, содержащий базовые сведения о населении и предоставляющий органам власти и организациям возможность получения полных и достоверных сведений о физическом лице. Ведение федерального ресурса о населении осуществляется в порядке, установленном Федеральным законом от 8 июня 2020 г. № 168-ФЗ «О едином федеральном информационном регистре, содержащем сведения о населении Российской Федерации».

Федеральный регистр содержит две группы сведений: данные физического лица и идентификаторы. К первой группе относятся,

например, фамилия, имя и отчество (при наличии) лица; дата рождения; сведения о его семейном положении; гражданство Российской Федерации и (или) гражданство (подданство) иностранного государства или иностранных государств.

Ко второй группе сведений, т. е. к идентификаторам, относятся записи документов или отметок, удостоверяющих личность, подтверждающих право иностранного гражданина и лица без гражданства на пребывание (проживание) в Российской Федерации; сведения о регистрационном учете гражданина Российской Федерации и миграционном учете иностранного гражданина, а также сведения о регистрации физического лица в качестве индивидуального предпринимателя и др.

Для соблюдения ограничений, запретов и обязанностей, установленных в целях противодействия коррупции, важными представляются сведения о семейном положении, а также о наличии гражданства (подданства) иностранного государства или иностранных государств, а также о наличии у гражданина Российской Федерации документа на право постоянного проживания в иностранном государстве.

Соответствующие сведения позволяют судить о соблюдении ограничений, связанных с гражданской службой (п. 6 и 7 Закона № 79-ФЗ)<sup>26</sup>. В соответствии с п. 1 ч. 1 ст. 14 Федерального закона от 25 июля 2002 г. № 115-ФЗ «О правовом положении иностранных граждан в Российской Федерации»<sup>27</sup> иностранный гражданин не имеет права находиться на муниципальной службе. Наличие иностранного гражданства или иного документа на право постоянного проживания в иностранном государстве свидетельствует о присутствии политических, экономических и иных жизненных интересов в данном государстве, что может повлечь конфликт интересов при выполнении служебных обязанностей.

<sup>26</sup> СЗ РФ. 2004. № 31. Ст. 3215.

<sup>27</sup> СЗ РФ. 2002. № 30. Ст. 3032.



Представляется, что идентификаторы, включенные в федеральный регистр сведений о населении, также могут использоваться в целях получения информации о соблюдении государственными служащими ограничений, запретов и обязанностей, предусмотренных в целях противодействия коррупции. Например, п. 3.1 ч. 1 Закона № 79-ФЗ<sup>28</sup> установлен запрет заниматься предпринимательской деятельностью лично или через доверенных лиц. При обнаружении в федеральном регистре сведений о наличии у лица статуса индивидуального предпринимателя может быть поставлен вопрос о проведении соответствующих проверочных мероприятий.

Одной из функций цифрового профиля<sup>29</sup> является предоставление сведений о гражданине, содержащихся в ЕСИА, ЕФИР и иных государственных информационных системах.

Между увеличением объема данных, содержащихся в цифровом профиле гражданина, и повышением комфортности получения гражданином государственных, муниципальных и иных услуг существует определенная корреляция. Удобство получения соответствующих сведений выступает основным стимулом увеличения информационного массива о физических лицах. Уже сейчас, используя данные цифрового профиля гражданина, можно получить доступ к таким услугам, как выпуск и обслуживание банковской или кредитной карты, предоставление кредита или ипотеки, направление запроса в бюро кредитных историй, оформление страховки и др.

Развитие правового регулирования общественных отношений, связанных с использованием цифрового профиля гражданина или юридического лица, позволит повысить удобство и качество оказания услуг гражданам, юридическим лицам и индивидуальным предпринимателям, а также предоставит государственным органам

<sup>28</sup> СЗ РФ. 2004. № 31. Ст. 3215.

<sup>29</sup> Подробнее об этом см.: Сценарии использования инфраструктуры цифрового профиля. Верс. 1.2. Методические рекомендации Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации // digital.gov.ru // URL: <https://digital.gov.ru/uploaded/presentations/stsenariiispolzovaniyatspv12.pdf>

и организациям дополнительные возможности по реализации своих функций.

Одной из проблем внедрения цифрового профиля государственного служащего является обеспечение безопасности и конфиденциальности данных. Цифровые профили государственных служащих находятся в зоне риска, обусловленного следующими обстоятельствами. Во-первых, такая категория лиц, как государственные служащие, имеет стабильный доход, что вызывает заинтересованность злоумышленников. Во-вторых, цифровой профиль государственного служащего аккумулирует сведения, обладание которыми позволят потенциальным правонарушителям лучше спланировать нападение. К тому же при централизованной обработке персональных данных (принципиальное положение проекта федерального закона № 747513-7), утечка данных будет грозить всем государственным служащим. В указанном контексте перспективным видится принятие не только технических мер защиты информации, но и мер организационно-правового характера. В частности, целесообразно рассмотреть вопрос о создании на базе Межведомственной рабочей группы по противодействию информационной преступности<sup>30</sup> и рабочей группы «Информационная безопасность» АНО «Цифровая экономика»<sup>31</sup> специальных подгрупп по информационной безопасности цифрового профиля, на которые следует возложить функции выработки подходов к противодействию угрозам<sup>32</sup> безопасности

---

<sup>30</sup> Генеральным прокурором Российской Федерации в 2020 г. создана межведомственная рабочая группа по противодействию информационной преступности, включающая в себя представителей Генеральной прокуратуры Российской Федерации, МИДа России и других заинтересованных министерств и ведомств. Подробнее об этом см.: Официальный портал «Координационный совет генеральных прокуроров государств — участников Содружества Независимых Государств // URL: <http://www.ksgp-cis.ru/news/news-item/7975>.

<sup>31</sup> Подробнее о рабочей группе «Информационная безопасность» см.: URL: <https://data-economy.ru/security>

<sup>32</sup> См.: Панин О. Н. Угрозы безопасности цифрового профиля гражданина Российской Федерации / О. Н. Панин, Р. Д. Сулейменова // Молодой ученый. 2022. № 16 (411). С. 34–35.

цифрового профиля. Кроме того, предлагается установить специфические статусные требования, запреты, ограничения и обязанности в отношении лиц, администрирующих государственные информационные системы, работающих с цифровым профилем государственного служащего.

Во исполнение Указа Президента РФ от 24 июня 2019 г. № 288 «Об основных направлениях развития государственной гражданской службы Российской Федерации на 2019–2021 годы»<sup>33</sup> распоряжением Правительства РФ от 24 июля 2019 г. № 1646-р был утвержден План мероприятий («дорожной карты») по реализации основных направлений развития государственной гражданской службы Российской Федерации на 2019–2021 годы (далее — План мероприятий). План мероприятий предусматривает формирование единой и закрытой цифровой информационно-коммуникационной среды для государственной гражданской службы, предполагающей оцифровку кадрового делопроизводства, включая ведение личных дел исключительно в цифровой форме, а также создание системы различных сервисов кадровой службы.

В указанной среде должен обрабатываться внушительный объем информации о государственных служащих, а также должны выполняться задачи, связанные с их профессиональным развитием, внутренними коммуникациями, интерактивным наставничеством и др.

Следует отметить, что еще до принятия Плана мероприятий производилось обработка сведений, оставляемых государственными служащими в информационно-телекоммуникационных сетях. В соответствии с Законом № 79-ФЗ (ст. 20.2) гражданский служащий должен сообщать все адреса сайтов и (или) страниц сайтов в сети «Интернет», на которых он размещал общедоступную информацию, а также иные данные, позволяющие провести его идентификацию. В рамках исполнения данной обязанности государственными служащими предоставляются, например, сведения

---

<sup>33</sup> СЗ РФ. 2019. № 26. Ст. 3410.

о созданных ими страницах в социальных сетях, на сайтах знакомств, досках объявлений, в видеохостингах, на других ресурсах, а также сведения обо всех созданных государственным служащим аккаунтах. Появляется необходимость в качественной аналитике цифрового профиля, которая позволяет обобщить имеющую информацию по отдельным параметрам и оформить соответствующие выходные данные.

Значение цифрового профилирования на государственной службе будет возрастать в связи с потребностью в укреплении информационной основы для работы информационных систем, а также с необходимостью выполнения ряда сопутствующих задач кадрового, антикоррупционного, образовательного и просветительского характера.

Поворотным моментом в декларировании как форме финансового контроля в сфере противодействия коррупции стало принятие Конвенции ООН против коррупции 2003 г. (далее — КПК ООН), в которой признается потенциал систем раскрытия информации об активах, и предусматривается, что все стороны, подписавшие это соглашение, должны создать механизмы, обязывающие публичных должностных лиц сообщать соответствующим органам о своих инвестициях и активах (п. 5 ст. 8). Конвенция определяет гибкий механизм декларирования, который подробно описан в Техническом руководстве по Конвенции ООН<sup>34</sup>.

Цифровые технологии позволяют аккумулировать значительные массивы информации об имущественном положении отдельных категорий лиц. Так, в Российской Федерации применяется Специальное программное обеспечение «Справки БК» для выполнения следующих основных функций: формирование печатных форм<sup>35</sup>; заполнение

---

<sup>34</sup> Техническое руководство по осуществлению Конвенции ООН против коррупции. Управление Организации Объединенных Наций по наркотикам и преступности. Нью-Йорк, 2010. 256 с.

<sup>35</sup> В соответствии с Указом Президента Российской Федерации от 23 июня 2014 г. № 460 «Об утверждении формы справки о доходах, расходах, об имуществе и обязательствах имущественного характера и внесении изменений в некоторые акты Президента Российской Федерации» в редакции Указов Президента Российской Федерации

необходимых сведений о соответствующих лицах для последующей печати в установленном виде; ввод и отображение введенных данных; проверка корректности ввода данных. Цифровые технологии декларирования имущественного положения отдельных категорий лиц получают свое нормативное закрепление.

Например, Национальным планом противодействия коррупции на 2021–2024 годы, утвержденным Указом Президента РФ от 16 августа 2021 г. № 478<sup>36</sup> (раздел XVI), предусмотрено применение цифровых технологий в целях противодействия коррупции. В частности, дано следующее поручение Министерству цифрового развития, связи и массовых коммуникаций Российской Федерации: с участием Министерства труда и социальной защиты Российской Федерации необходимо рассмотреть вопрос о создании и внедрении цифровых технологий, позволяющих осуществлять в электронной форме прием сведений о доходах, расходах, об имуществе и обязательствах имущественного характера, автоматическую обработку, анализ таких сведений и их хранение, в том числе централизованное. В данном контексте интерес представляет российская разработка ГИС «Посейдон»<sup>37</sup>, которая консолидирует ресурс информационно-коммуникационных технологий для ввода и анализа сведений о доходах, расходах, об имуществе и обязательствах имущественного характера государственных служащих и иных категорий лиц. Кроме того, ГИС «Посейдон» позволяет проводить контрольные мероприятия в области противодействия коррупции. При этом она объединяет в единую сеть потенциал государственных информационных систем и участников антикоррупционной деятельности, что дает возможность автоматизировать большинство выполняемых ими функций.

Таким образом, цифровое профилирование на государственной службе не только преследует цели формирования базы данных,

---

Федерации от 19 сентября 2017 г. № 431, от 9 октября 2017 г. № 472, от 15 января 2020 г. №13, от 10 декабря 2020 г. №778.

<sup>36</sup> СЗ РФ. 2021. № 34. Ст. 6170.

<sup>37</sup> СЗ РФ. 2022. № 18. Ст. 30

содержащей сведения о государственных служащих, но также решает задачи по обеспечению соблюдения ими специфических ограничений, запретов и обязанностей, профессионального развития и специализации.

В этом контексте интересным представляется идея разработки научно-обоснованных критериев системы оценки (скоринга) государственных гражданских служащих. Данные критерии будут учитывать соблюдение служащими ограничений, запретов и обязанностей, требований к служебному поведению, а также правил служебного поведения, в том числе содержащихся в типовом кодексе этики государственных и муниципальных служащих. Это позволит ориентировать последних на решение задач, связанных с улучшением своих показателей и развитием профессиональных компетенций, а также с повышением объективности оценки их профессиональной служебной деятельности.

Цифровизация может способствовать противодействию коррупции не только в публичном, но и в корпоративном секторе посредством внедрения систем цифрового комплаенса и аудита, а также электронных систем антикоррупционного информирования и консультирования работников.

Перспективным представляется предложение о создании для субъектов малого и среднего предпринимательства (МСП) специального антикоррупционного мобильного приложения<sup>38</sup>, выполняющего консультационную и антикоррупционную функции<sup>39</sup>.

Цифровизация воздействует на все управленческие процессы, повышая их эффективность, обеспечивая деперсонализацию

---

<sup>38</sup> Противодействие коррупции в сфере бизнеса: научно-практическое пособие / отв. ред. Т.Я. Хабриева, О.С. Капинус; ИЗИСП. — М., 2020.

<sup>39</sup> В функционал отмеченного приложения могут входить: определение типового профиля и карты коррупционных рисков организации; предоставление доступа к сервису по проверке контрагентов; предоставление доступа к базе типовых локальных нормативных актов, рекомендуемых к принятию, а также информация о действующих нормативных правовых актах и об актуальных методических рекомендациях в сфере противодействия коррупции.

взаимодействия граждан и служащих органов власти, усиливая контроль за их доходами и расходами, а также обеспечивая прозрачность оказания государственных и муниципальных услуг, что способствует снижению коррупционных рисков. С помощью технологий Big data можно формировать и обрабатывать большие массивы информации, выявлять системные причины и условия, опосредующие возникновение и распространение коррупционных практик. Специальное программное обеспечение уже сейчас применяется для выполнения отдельных задач в области правового мониторинга и антикоррупционной экспертизы. Цифровые технологии противодействия коррупции, становясь неотъемлемой частью государственного управления, оказывают все большее влияние на модернизацию самих антикоррупционных мер и процедур. Данный процесс затронет различные нормативные массивы, включая законодательство о противодействии коррупции.