



**Руслан Тимурович
БАЙГАРИН,**

аспирант кафедры
информационного права
и цифровых технологий
Университета имени
О.Е. Кутафина (МГЮА)
ruslanbaygarin@gmail.com
125993, Россия, г. Москва,
ул. Садовая-Кудринская, д. 9

Правовые проблемы обеспечения кибербезопасности генетических данных в Российской Федерации

Аннотация. В статье рассматриваются проблемные вопросы нормативно-правового регулирования обеспечения кибербезопасности генетических данных. Автором указывается на пробелы в правовой базе, регламентирующей требования по сбору, хранению, обработке и передаче генетических данных как особого вида персональных данных. Исследуются аспекты недостаточной защищенности генетической информации и основные причины и источники угроз для частных и публичных интересов. Предлагаются пути по совершенствованию законодательства в целях противодействия киберрискам в условиях значительного роста объема генетических данных в интернет-пространстве, в частности необходимо утверждение обязательных требований безопасности при работе с генетической информацией, увеличение ответственности за нарушение законодательства в области персональных данных, ограничение круга лиц, имеющих доступ к генетическим базам данных и другие механизмы правового регулирования.

Ключевые слова: генетическая информация, безопасность, киберугрозы, геномные исследования, персональные данные, информационно-аналитическая система, база генетической информации.

DOI: 10.17803/2311-5998.2023.102.2.168-176

RUSLAN T. BAYGARIN,

Postgraduate student of the Department of information law
and digital technologies

of the Kutafin Moscow State Law University (MSAL)

ruslanbaygarin@gmail.com

9, ul. Sadovaya-Kudrinskaya, Moscow, Russia, 125993

Legal challenges in ensuring the cybersecurity of genetic data in the Russian Federation

Abstract. The article explores problematic issues of legal regulation of genetic data cybersecurity. The author points out gaps in the legal framework regulating the requirements for collection, storage, processing and transfer of genetic data as a special type of personal data. The author investigates the aspects of insufficient protection of genetic information and the main reasons and sources of threats for private and public interests. The author proposed ways to improve the legislation in order to counteract cyber risks

in conditions of a significant growth of genetic data in the Internet space, in particular, to approve mandatory security requirements when dealing with genetic information, to increase responsibility for violation of legislation in the field of personal data, to limit the range of persons having access to genetic databases and other mechanisms of legal regulation.

Keywords: *genetic information, security, cyber threats, genomic research, personal data, information analysis system, genetic information database.*

Исследования в области обработки генетических данных являются одной из наиболее перспективных и стремительно развивающихся областей человеческого знания. Научные и технологические достижения в области генетики обеспечили существенное повышение качества человеческой жизни, но они также несут в себе и дополнительные риски использования научных знаний во вред человеку, что обязывает совершенствовать государственное регулирование этой сферы общественных отношений.

С появлением так называемой геномики больших данных (Big Data Genomics) использование генетических данных становится все более распространенным явлением, появляются новые участники отношений по использованию генетических данных¹. По мере того, как объем данных продолжает быстро увеличиваться, возникает все больше вопросов, связанных с разработкой и контролем соблюдения требований по консолидации данных, получаемых в результате гено-инженерной деятельности.

Рост объема генетических данных коррелирует с динамичным развитием интернет-технологий, методов оцифровки данных и способов их хранения, которые применяются в том числе при работе с генетической информацией, что ведет к необходимости разработки комплексных механизмов регулирования этой сферы киберправового поля. Одним из факторов, способствовавших ускорению цифровых процессов и, как следствие, возрастанию роли киберправа, генетических исследований и потребности в регулировании стремительно развивающихся информационных правоотношений, стала пандемия коронавируса (COVID-19).

Разработка конкретных мер, обеспечивающих хранение, обработку и анализ генетических данных в Российской Федерации при соблюдении должного уровня их безопасности, является комплексной задачей, в рамках которой потребуются разрешить как существующие, так и потенциальные правовые проблемы.

Поскольку взаимодействие субъектов и объектов общественных отношений по поводу генетической информации в значительной степени происходит в онлайн-формате, одним из ключевых аспектов при разработке правовых механизмов является обеспечение высокой степени их гибкости и адаптивности применяемых методов.

В первую очередь следует обратить внимание на общие тенденции в рассматриваемой области информационного пространства: рост потребностей в обеспечении конфиденциальности, особенно в отношении защиты финансовых,

¹ Чубукова С. Г. Правовые проблемы защиты генетической информации: субъектный подход // Вестник Университета имени О.Е. Кутафина (МГЮА). 2020. № 5. С. 96—103.



генетических, медицинских данных и сведений о местонахождении; осложнение работы с генетической информацией трансграничной передачей данных; непрерывную потребность организаций в совершенствовании управления собственными киберрисками.

Другой опасной тенденцией, требующей своевременного и эффективного контроля, является усиление интереса киберпреступников к цифровым активам, в частности к персональным, генетическим данным людей².

На сегодняшний день нормативно-правовая база не отражает все особенности генетической информации как объекта информационных правоотношений, а также как особого вида персональных данных, что требует развития и совершенствования российского законодательства.

Генетические данные нуждаются в особой правовой и технической защите. В российском законодательстве имеется пробел в части защиты информации о человеке, полученной из его биоматериала, который содержит генетическую информацию, позволяющую получить о нем дополнительные сведения (о состоянии здоровья, питания, образа жизни, поведенческих особенностях, чувствительности к фармакологическим препаратам или аллергенам и другие индивидуальные характеристики).

В отечественном законодательстве содержится легальное определение геномной информации. В соответствии с Федеральным законом от 03.12.2008 № 242-ФЗ «О государственной геномной регистрации в Российской Федерации»³ геномная информация представляет собой персональные данные, включающие кодированную информацию об определенных фрагментах дезоксирибонуклеиновой кислоты (ДНК) физического лица или неопознанного трупа, не характеризующих их физиологические особенности.

Такой подход законодателя к генетической информации подвергается критике в юридическом сообществе, так как ДНК является носителем генетической информации не только о конкретном лице, но и о его родственниках и потомках. Другими словами, с молекулой ДНК, помимо ее индивидуальности, связано и другое основополагающее свойство — наследственность и способ передачи наследственной информации, касающейся неопределенного круга лиц⁴.

Само по себе обеспечение кибербезопасности является многогранным процессом. Представляется, что для поддержания должного уровня безопасности данных все устройства, используемые в компаниях и государственных органах, деятельность которых связана с генетической информацией, должны иметь установленное программное обеспечение для защиты от вредоносного ПО, а при удаленной работе критически важно применять виртуальные частные сети. При нарушении сетевого соединения пользователям должен автоматически блокироваться доступ к документам, электронной почте и другим важным программам,

² Jeffrey D. Neuburger and Jonathan P. Mollod. Trends in Privacy and Data Security: 2021 // Practical Law. 2021. URL: <https://content.next.westlaw.com/w-034-2241?isplc=true&transitiontype=default&contextdata=%28sc.default%29> (дата обращения: 17.01.2023).

³ СЗ РФ. 2008. № 49. Ст. 5740.

⁴ Кубитович С. Н. ДНК как носитель информации неограниченного круга лиц // Вестник экономической безопасности. 2017. № 4. С. 186.

содержащим конфиденциальную информацию. Многофакторная аутентификация также является необходимым атрибутом (особенно при работе с базами генетических данных), позволяющим усложнить процесс взлома систем.

Указанные требования безопасности принимаются на уровне локальных нормативных актов, однако для объективного повышения уровня кибербезопасности следует законодательно закрепить их обязательность при работе с генетической информацией, соответствующие меры ответственности.

Отсутствие серьезных мер ответственности за нарушения порядка проведения работ с генетическими данными фактически приводит к безнаказанному пренебрежению мерами кибербезопасности, а нарушения законодательства о персональных данных происходят повсеместно.

К примеру, в начале 2022 г. стало известно об утечке персональных данных 30 миллионов человек в крупнейшей федеральной медицинской компании «Гемотест», выполняющей лабораторную диагностику⁵. По итогам проверки был обнаружен факт предоставления незаконного доступа к базам данных, что спровоцировало распространение персональных данных пациентов в Интернете.

Согласно официальному ответу представителей лаборатории, произошла хакерская атака: на просторы сети, помимо сведений об оказанных пациентам услугах со стороны лаборатории, также были выгружены гигабайты персональных данных клиентов. Несмотря на отрицание лабораторией вины, суд признал компанию виновной в утечке данных, а также определил сумму штрафа в 60 000 рублей⁶. Очевидно, что данный размер ответственности несопоставим с ущербом, нанесенным широкому кругу лиц, пользовавшихся услугами медицинской компании.

Другой правовой проблемой, стоящей перед законодателем, является сложность соблюдения конфиденциальности и обезличенности генетических данных. Председатель Конституционного Суда РФ В. Д. Зорькин определяет цифровые права в том числе как право на неприкосновенность частной информационной сферы, включая право на конфиденциальность, анонимность (обезличенность) его уже оцифрованной персональной информации⁷.

В некоторых случаях цели геномных исследований не позволяют соблюдать требование по обезличиванию получаемых в результате работы данных. Тем не менее для соблюдения конфиденциальности и защиты частных интересов данные, которые будут передаваться в базы генетической информации, должны быть псевдонимизированы. В европейском Генеральном регламенте о защите

⁵ Гемотест начал расследование об утечке данных 30 млн клиентов // URL: https://www.rbc.ru/society/04/05/2022/6272665b9a794713ec6698dd?f rom=article_body (дата обращения: 27.01.2023).

⁶ Постановление мирового судьи судебного участка № 281 района Вешняки города Москвы от 08.07.2022 по делу 05-0564/287/2022 // URL: <https://mos-sud.ru/287/cases/admin/details/8d9658fc-9304-417c-bf8f-9389ef8772ac?caseNumber=05-0564/287/2022> (дата обращения: 27.01.2023).

⁷ Зорькин В. Д. Право в цифровом мире. Размышление на полях Петербургского международного юридического форума // Российская газета. 2018. Столичный выпуск. № 7578 (115).



персональных данных от 27.04.2016⁸ под этой процедурой понимается определенная обработка данных для невозможности ее отнесения к конкретному субъекту данных без использования дополнительной информации. Специальным условием является то, что указанная дополнительная информация должна храниться отдельно с применением технических и организационных мер, предотвращающих ее несанкционированное разглашение⁹.

Представляется, что европейский опыт правового регулирования данных может быть полезен при разработке соответствующих правовых механизмов в национальном законодательстве.

Совсем недавно был принят Федеральный закон от 29.12.2022 № 643-ФЗ «О внесении изменений в Федеральный закон “О государственном регулировании в области генно-инженерной деятельности”»¹⁰, закрепляющий ряд важных положений в области правового регулирования общественных отношений, возникающих, изменяющихся и прекращающихся в процессе обеспечения оборота генетической информации в Российской Федерации.

Основной объем внесенных изменений касается создания информационно-аналитической системы «Национальная база генетической информации», основными целями которой заявлены обеспечение национальной безопасности, охраны жизни и здоровья граждан, суверенитета в сфере хранения и использования генетических данных. Информационно-аналитическая система также призвана обеспечить обмен генетической информацией между обладателями генетических данных и государственными органами.

Перед законодателем стоит задача разработки положения о Национальной базе генетической информации, детально регулирующего различные аспекты ее работы, в частности формат обработки и состав предоставляемых сведений, а также иные аспекты ее функционирования. С учетом того, что информация, содержащаяся в информационно-аналитической системе, будет общедоступной и предоставляться на безвозмездной основе, возникает вопрос об ограничении круга субъектов, имеющих право на получение содержащейся в ней информации.

Представляется, что при установлении перечня получателей данной информации следует предусмотреть разрешительный порядок доступа к информационно-аналитической системе для лиц, не являющихся российскими гражданами и юридическими лицами. В частности, в условиях сложной геополитической ситуации целесообразно ограничить доступ для лиц, связанных с недружественными государствами.

Впервые о необходимости создания базы генетической информации было заявлено Президентом РФ в 2020 г. в период пандемии коронавируса (COVID-19)¹¹,

⁸ Генеральный регламент о защите персональных данных от 27.04.2016 // URL: <https://gdpr.eu/tag/gdpr/> (дата обращения: 25.01.2023).

⁹ Столбов А. П. О стандартизации методов псевдонимизации персональных данных в здравоохранении // Проблемы стандартизации в здравоохранении. 2017. № 9–10. С. 25–36.

¹⁰ СЗ РФ. 2023. № 1 (ч. I). Ст. 90.

¹¹ Поручение Президента РФ от 04.06.2020 № Пр-920 «Перечень поручений по итогам совещания по вопросам развития генетических технологий» // URL: <https://base.garant.ru/74229773/> (дата обращения: 19.01.2023).

что частично объясняет цели данного поручения — обеспечение как научного развития, так и оперативного реагирования на потенциальные биологические угрозы. Риск несанкционированного доступа к информации, содержащейся в консолидированных базах данных, несет в себе опасности как для частных, так и для публичных интересов, вплоть до угроз национальной безопасности.

В результате цифровизации персональные данные в цифровом пространстве должны быть защищены от несанкционированного доступа, модификации, раскрытия путем передачи, а также от уничтожения или повреждения. Для обеспечения безопасности персональных данных необходимо разработать порядок обращения с персональными данными в условиях развития киберугроз; внедрить систему контроля за соблюдением конфиденциальности и защитой данных; определить масштабы рисков, которые могут возникнуть в случае несанкционированной обработки персональных данных и ответственность в случае причинения ущерба, связанного с личными данными, в рамках интернет-пространства.

По всем процессам, связанным с обработкой больших персональных данных, необходимо проводить в соответствии с требованиями законодательства объективную оценку вреда субъектам персональных данных, который потенциально может быть причинен¹². Это даст возможность своевременной корректировки мер по обеспечению безопасности данных со стороны операторов персональных данных во взаимоотношениях с внешними подрядчиками (например, с облачными провайдерами).

В целом можно утверждать, что новые риски и киберугрозы появляются по мере того, как сбор и использование генетических данных становятся широко распространенным явлением. Возникновение таких рисков частично связано со стремительным падением стоимости секвенирования ДНК, а также достижениями в области синтетической биологии. За последние несколько лет стоимость секвенирования целого генома снизилась с 1 000 долларов США до 100 долларов США за один геном¹³, а всего 15 лет назад стоимость данной процедуры была на уровне около 1 миллиона долларов США¹⁴.

Вследствие этого генетические данные становятся все более доступными из ряда различных информационных источников. Представители частного сектора экономики осуществляют сбор генетических данных, начиная с поставщиков услуг в области ДНК-диагностики и составления родословных, которые также записываются и в цифровом виде, и заканчивая фармацевтическими компаниями, ведущими анализ данных о состоянии здоровья потребителей. Также данные генерируются в ходе исследований, финансируемых государством, и попадают в электронные базы.

¹² Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных». Подпункт 5 ч. 1 ст. 18.1 // СЗ РФ. 2006. № 31 (ч. I). Ст. 3451.

¹³ Regalado A. China's BGI says it can sequence a genome for just \$100 // MIT Technology review. 26.02.2020. URL: <https://www.technologyreview.com/2020/02/26/905658/china-bgi-100-dollar-genome/> (дата обращения: 23.01.2023).

¹⁴ Wetterstrand K. A. DNA Sequencing Costs: Data // National Human Genome Research Institute. URL: <https://www.genome.gov/about-genomics/fact-sheets/dna-sequencing-costs-data> (дата обращения: 23.01.2023).



Эти исследовательские программы несут в себе огромный потенциал для развития науки и медицины, который даст возможность предсказывать предрасположенность к болезням и проводить лечение с учетом индивидуальных особенностей генетики. Для такого прогресса необходимы большие базы генетических данных, включающие разнообразные личные данные, начиная от данных о состоянии здоровья и заканчивая выбранным образом жизни. Именно поэтому они становятся объектом для возможных кибератак. Как правило, такие базы данных обезличиваются или деидентифицируются путем присвоения участникам цифровых идентификаторов вместо личных имен, однако в некоторых случаях данные могут быть повторно идентифицированы.

Угрозы, связанные с этими незащищенными базами данных, усугубляются с развитием искусственного интеллекта, особенно машинного обучения — области искусственного интеллекта, связанной с обработкой данных. Применение машинного обучения к генетическим данным способствует ускоренному развитию возможностей медицинской науки и врачебной практики по разработке методов геномной диагностики и терапии.

В то же время эти достижения предоставляют злоумышленникам опасные средства для использования генетических данных с целью причинения ущерба и масштабирования угроз. Например, с помощью методов машинного обучения можно определить рост с точностью до нескольких сантиметров¹⁵ или реконструировать черты лица¹⁶. При наличии базы данных лиц с именами, к примеру базы данных фотографий водительских прав, генетические данные могут быть повторно идентифицированы с помощью машинного обучения¹⁷.

Применение искусственного интеллекта к генетической информации уже привело к значительным открытиям и революционным методам лечения, но некоторые из этих достижений также могут быть использованы для разработки биооружия. Научные открытия в области генеалогии позволяют достичь беспрецедентного понимания истории, но также могут привести к потере анонимности как в онлайн-, так и в офлайн-пространстве.

Особенный характер генетических данных делает их особенно интимными, значимыми и ценными для их обладателей. Это объясняется тем, что генетические данные являются постоянными и принадлежат человеку на протяжении всей его жизни, что неотъемлемо привязывает их к личности. Нарушения безопасности генетических данных из-за их неизменной природы могут иметь долгосрочные последствия, и их правовой режим должен регулироваться отдельно от иных

¹⁵ Lello L., Avery S. G., Tellier L., Vazquez A. I., Los Campos G. de, Hsu S. D. H. Accurate Genomic Prediction of Human Height // *Genetics*. 2018. No. 210 (2). P. 477—497. URL: <https://doi.org/10.1534/genetics.119.302946> (дата обращения: 23.01.2023).

¹⁶ Robust genome-wide ancestry inference for heterogeneous datasets: illustrated using the 1,000 genome project with 3D facial images / J. Li, T. G. Zarzar, J. D. White [et al.] // *Scientific Reports*. No. 10. 11850. 2020. URL: <https://doi.org/10.1038/s41598-020-68259-w> (дата обращения: 19.01.2023).

¹⁷ Facial recognition from DNA using face-to-DNA classifiers / D. Sero, A. Zaidi, J. Li [et al.] // *Nature Communications*. No. 10, 2557. 2019. URL: <https://doi.org/10.1038/s41467-019-10617-y> (дата обращения: 19.01.2023).

видов данных, так как в случае нарушения конфиденциальности или непосредственного вмешательства в наследственность одного человека последствия могут затронуть его родственников.

Если генетические данные дальнего родственника раскрыты, то множество родственных людей оказываются под угрозой установления личности посредством сопоставления семейных особенностей генетики. Целый ряд генетических баз данных открытого и частично открытого типа уже доступны публично, а другие базы данных признаны уязвимыми перед несанкционированным доступом¹⁸. Используя эти данные, уже сейчас можно идентифицировать многих людей только по ДНК их родственников.

Характер и значимость генетических данных, обеспечение безопасности которых предоставит защиту для будущих поколений, имеет под собой конституционное обоснование, с учетом того, что в преамбуле Конституции РФ определена ответственность народа Российской Федерации перед своими потомками¹⁹.

Возможности машинного обучения по обработке сведений о культуре, эпигенетических и этнических особенностях могут привести к созданию моделей, позволяющих получать точные прогнозы даже в отношении заболеваний, не обладающих высокой степенью наследуемости²⁰. Умение предсказывать предрасположенность к заболеваниям и применение методов превентивной медицины станут ключевыми элементами медицины будущего. Однако возможность прогнозирования даже незначительных по тяжести заболеваний в больших масштабах позволит использовать уязвимости в рамках целых социальных групп или популяций.

Таким образом, для ряда киберугроз, связанных с получением и обработкой генетических данных, крайне высок риск причинения ущерба как конкретному человеку, так и отдельным группам населения, в связи с чем особенно возрастает роль процесса усовершенствования правовой базы в рамках цифрового поля.

По мере развития биотехнологий могут возникнуть и другие потенциальные угрозы, которые в настоящее время не учитываются или не прогнозируются. Здесь применима известная цитата бывшего министра обороны США Дональда Рамсфелда: «Есть известные известные — вещи, о которых мы знаем, что знаем их. Есть также известные неизвестные — вещи, о которых мы знаем, что не знаем. Но еще есть неизвестные неизвестные — это вещи, о которых мы не знаем, что не знаем их».

Хотя для предотвращения или смягчения будущих угроз можно применить ряд мер, включая ограничение развертывания моделей искусственного интеллекта,

¹⁸ Greshake B., Bayer P. E., Rausch H., Reda J. openSNP — A Crowdsourced Web Resource for Personal Genomics // PLoS ONE. 9(3). URL: <https://doi.org/10.1371/journal.pone.0089204> (дата обращения: 21.01.2023).

¹⁹ Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // URL: <http://www.pravo.gov.ru> (дата обращения: 20.01.2023).

²⁰ Finding the missing heritability of complex diseases / T. Manolio, F. Collins, N. Cox [et al.] // Nature. 2009. 461. P. 747—753. URL: <https://doi.org/10.1038/nature08494> (дата обращения: 20.01.2023).



жесткое нормативно-правовое регулирование и контроль за биотехнологиями, неизбежные достижения в данной области следует учитывать при определении баланса между необходимостью обеспечения доступа к генетическим данным и защитой их безопасности. Обмен генетическими данными и развитие технологий не могут и не должны быть остановлены.

Создание парадигмы безопасности генетических данных требует объединения усилий широкого круга заинтересованных сторон, привлечения соответствующих ресурсов и всеобщего признания генетической информации как критически важной составляющей инфраструктуры, нуждающейся в защите, аналогичной другим фундаментальным активам.

БИБЛИОГРАФИЯ

1. Болтанова Е. С., Имекова М. П. Генетическая информация в системе объектов гражданских прав // Lex russica. — 2019. — № 6. — С. 110—121.
2. Кубитович С. Н. ДНК как носитель информации неограниченного круга лиц // Вестник экономической безопасности. — 2017. — № 4.
3. Минбалева А. В. Право и современные информационные технологии: основные проблемы // Информационное пространство: обеспечение информационной безопасности и право : сборник научных трудов / под ред. Т. А. Поляковой, В. Б. Наумова, А. В. Минбалева. — М. : ИГП РАН, 2018. — С. 86—91.
4. Рассолов И. М., Чубукова С. Г. Правовое регулирование использования банков генетической информации // Генетические технологии и право в период становления биоэкономики. — 2020. — С. 329—340.
5. Рассолов И. М., Чубукова С. Г., Микурова И. В. Правовое регулирование использования генетической информации в Евросоюзе // Аграрное и земельное право. — 2019. — № 7 (175). — С. 120—123.
6. Чубукова С. Г. Правовые проблемы защиты генетической информации: субъектный подход // Вестник Университета имени О.Е. Кутафина (МГЮА). — 2020. — № 5. — С. 96—103.