Дата поступления рукописи в редакцию: 26.05.2025 г.
Дата принятия рукописи в печать: 16.06.2025 г.
DOI: 10.24412/2782-3830-2025-5-296-301

ДОСАЕВА Алсу Османовна,
соискатель степени к.ю.н.,
Московский университет им. А.С. Грибоедова,
e-mail: a.dosaeva@mail.ru

Научный руководитель:
БЛИЗНЕЦ Иван Анатольевич,
д.ю.н., профессор Кафедры интеллектуальной собственности
Московского университета им. А.С. Грибоедова,
e-mail: mail@law-books.ru

ПРАВОМОЧИЯ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ В РАМКАХ КОНЦЕПЦИИ КОНТРОЛЯ ДОСТУПА К ПЕРСОНАЛЬНЫМ ДАННЫМ

Аннотация. *В статье рассматриваются правомочия субъектов персональных данных при использовании такой технологии, как система управления персональными данными, основанной на концепции контроля доступа к персональным данным, предлагаемой в ЕС и в США. Актуальность исследования вызвана обсуждением в научной доктрине такой проблемы, как коммерческий оборот персональных данных. По мнению автора, использование данной концепции способствует учету интересов, в том числе имущественных, субъектов персональных данных как потенциальных участников коммерческого оборота персональных данных.*

Ключевые слова: *персональные данные, субъект персональных данных, правомочия, контроль доступа.*

DOSAEVA Alsu Osmanovna,
Candidate of Ph.D. in Law,
A.S. Griboyedov Moscow University,

Scientific supervisor:
BLIZNETS Ivan Anatolievich,
Doctor of Law,
Professor of the Department of intellectual property
A.S. Griboyedov Moscow University

POWERS OF PERSONAL DATA SUBJECTS WITHIN THE FRAMEWORK OF THE CONCEPT OF ACCESS CONTROL TO PERSONAL DATA

Annotation. *The article examines the rights of personal data subjects when using such technology as a personal data management system based on the concept of access control to personal data offered in the EU and the USA. The relevance of the study is caused by the discussion in the scientific doctrine of such a problem as the commercial turnover of personal data. According to the author, the use of this concept helps to take into account the interests, including property, of personal data subjects as potential participants in the commercial turnover of personal data.*

Key words: *personal data, personal data subject, authority, access control.*

В связи с признанием экономической ценности персональных данных и увеличением на них спроса со стороны разнообразных участников современного информационного общества, возникает вопрос о соблюдении интересов самих субъектов персональных данных в сфере оборота данных. Это не только интерес по сохранению конфиденциальности личных данных, но и потенциальная имущественная выгода субъектов от использования собственных данных.

После вступления в действие Регламента Европейского Парламента и Совета Европейского Союза 2016/679 от 27 апреля 2016 г. о защите физических лиц при обработке персональных данных и о свободном обращении таких

данных, а также об отмене Директивы 95/46/ЕС (Общий Регламент о защите персональных данных) (General Data Protection Regulation), далее по тексту - GDPR), крупные технологические компании, такие, как Microsoft, Apple, Google, стали заверять своих клиентов, что их продукция создана таким образом, чтобы клиенты были обеспечены возможностью контролировать свои личные данные [5].

В 2018 году со стороны РФ был подписан Протокол о внесении изменений в Конвенцию Совета Европы о защите физических лиц при автоматизированной обработке персональных данных [6]. Согласно третьему разделу преамбулы указанной Конвенции, необходимо учитывать принцип автономии личности, который позволяет индивидам контролировать сбор и обработку их персональных данных. Таким образом, актуальной проблемой стало не только управление данными, но и обеспечение контроля за данными со стороны субъектов персональных данных.

В отличие от концепции владения персональными данными, которая получила свое обозначение и обсуждение в зарубежной правовой доктрине [1, с.542], концепция контроля доступа к персональным данным пока только намечается и, по нашему мнению, может получить свое развитие в разных направлениях в зависимости от используемых субъектом персональных данных технологий и его правомочий, закрепленных законодателем. Следует иметь в виду, что концепция контроля доступа к персональным данным в настоящем исследовании не связана с содержанием понятия «контролер» и понятием «система данных», используемых в GDPR.

В силу существования разных категорий, видов и уровней персональных данных, а также закрепления в законодательстве нескольких оснований для обработки персональных данных помимо добровольного согласия субъекта персональных данных, максимальный контроль в отношении персональных данных субъект может реализовывать только в отношении агрегированной совокупности некоторых видов личных данных, то есть данных, обособленных субъектом персональных данных с помощью определенной технологии.

Первое направление развития концепции контроля доступа к персональным данным формируется за счет применения таких технологий, как хранилища персональных данных (частные облака) и системы управления персональными данными.

Под частными облаками (Private clouds) понимаются пространства в интернете, инфраструктура которых находится в полном распоряжении определенных лиц. Такие пространства изолированы друг от друга на физическом уровне (или на уровне оборудования) и защищают хранилища данных от несанкционированного доступа. Примерами таких облаков являются платные и бесплатные сервисы для хранения и обмена файлами на серверах поставщиков услуг (Яндекс Диск, Облако Mail.ru, СберДиск, Google Drieve, Telegam, iCloud и др.).

Частные облака являются основой для систем управления персональными данными (Personal Information Management Systems, далее по тексту - PIMS). Согласно докладу Европейского надзорного органа по защите данных, концепция PIMS разработана в рамках ориентированного на человека подхода к персональным данным, для защиты от незаконного отслеживания и методов профилирования. Система может представлять из себя продукты и услуги, которые помогают частным лицам лучше контролировать свои персональные данные в частных облаках, устанавливать ограничения и запрет на обработку данных [2].

Как отмечается в докладе, архитектура системы может включать в себя следующие элементы (блоки):



Источник: Европейский надзорный орган по защите данных

Чтобы получить доступ к персональным данным, любое заинтересованное лицо должно будет пройти аутентификацию. Субъект персональных данных также может определять, какими категориями данных он хочет делиться и с кем. Другими обычно используемыми элементами PIMS являются безопасное хранение данных, безопасная передача данных (между системами и приложениями), а также совместимость на уровне данных и их переносимость.

Приведем несколько примеров таких систем.

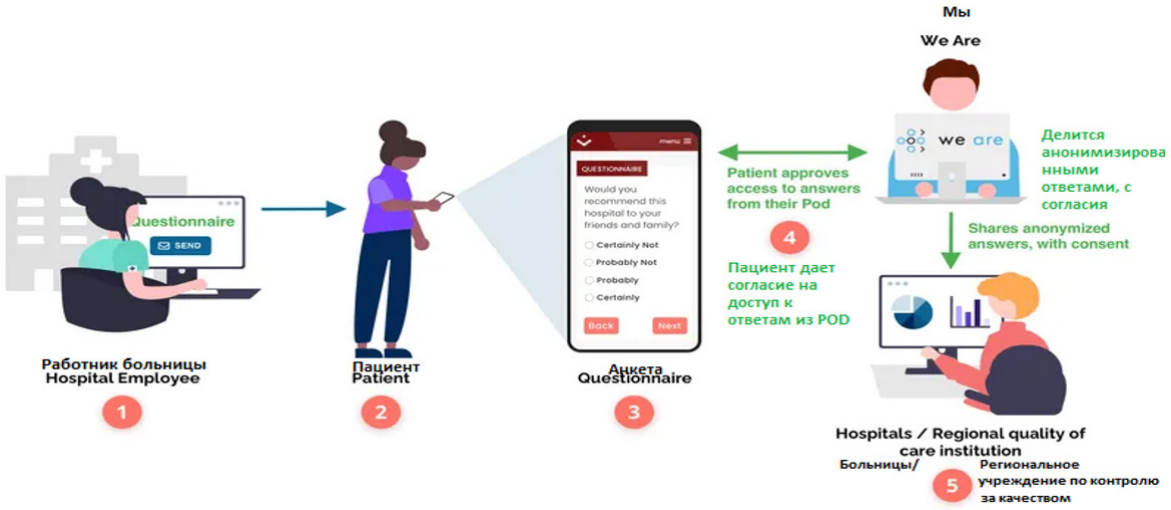
Пример 1. Solid

Американская компания Inrupt предлагает технологию Solid, заявленную создателем World Wide Web Тимом Бернерсом-Ли в 2017 году. Идея разработчика в том, что каждый пользователь интернета может иметь собственный сервер (модуль (POD)) для хранения и обмена персональными данными, к которому смогут подключаться другие сервисы. Если пользователь не захочет больше делиться своими данными с третьими лицами, он закроет доступ к своему серверу. Но эти модули предоставляются субъектам персональных данных не напрямую, а через организации и государственные органы.

Взаимодействие субъекта персональных данных и третьих лиц относительно использования персональных данных можно описать следующим образом.

Организация устанавливает Enterprise Solid Server в своих облачных или локальных средах для безопасного размещения хранилищ персональных данных (PODs) субъектов. PODs хранят данные о клиентах и являются центрами взаимодействия между одобренными клиентами приложениями или сервисами. Данные POD могут поступать из нескольких одобренных источников. Клиенты сами выбирают, какой объем доступа разрешить, тем самым они контролируют свои POD-данные.

Корпоративные версии платформы Solid уже используются европейскими частными организациями и государственными учреждениями. Например, фламандская исследовательская организация VITO разработала приложение We are [7] для хранения и контроля обработки медицинской информации пациентов больницы:



Источник: компания Inrupt

Сотрудник больницы создает ссылку на личную анкету для конкретного пациента, которая включает в себя список стандартных вопросов, используемых в различных больницах, и вопросов, специфичных для больницы, в которой он находился. Все ответы на эту анкету хранятся в личном кабинете пациента. Если пациент соглашается поделиться своими ответами для включения в сводный анонимный набор данных, то VITO анонимизирует ответы и предоставляет доступ к ним другой больнице или региональной организации, анализирующей качество медицинской помощи в бельгийских больницах. Пациент может дать согласие на то, чтобы его агрегированные в модуле POD персональные медицинские данные использовались для инноваций, и взамен получать более персонализированные продукты и услуги.

Пример 2. AURA

В 2017 году испанская телекоммуникационная компания Telefónica презентовала когнитивную платформу AURA, демонстрирующую возможности Telefónica по сбору, хранению, анализу и пониманию данных своих клиентов в режиме реального времени и предоставлению им персонализированного обслуживания [8]. В платформу

заложена функция Timeline, которая позволяет пользователям хронологически видеть данные, которые они генерируют, когда они используют продукты и услуги компании Telefónica. Aura также содержит функцию управления согласием пользователя, для определения того, могут ли его данные быть использованы и для каких конкретных целей.

Пример 3. Облако 152-ФЗ

Российские производители на данном этапе создают хранилища данных (частные облака) не для субъектов персональных данных, а для государственных и частных организаций. Например, компания Selectel, провайдер IT-инфраструктуры, предлагает организациям различных отраслей экономики в аренду защищенное облако Selectel-Облако 152-ФЗ, разработанную для работы с персональными данными клиентов этих организаций с учетом требований законодательства о защите персональных данных [9].

Хотелось бы отметить, что понимание «управление персональными данными» и «контроль за доступом к персональным данным» в виду отсутствия нормативного описания таких процессов может быть очень разным у разработчиков инноваций. Даже если декларируется в качестве цели создания частного облака возможность контроля над личными данными, заметно, что указанные примеры технологий созданы не столько в интересах субъектов, сколько в интересах производителей товаров и услуг, например, для помощи ответственным за обработку данных выполнять обязательства по конфиденциальности и защите данных, возложенных законодательством. Европейский надзорный орган по защите данных отмечает в своем докладе, что от проектирования системы зависит, на самом ли деле субъекты персональных данных будут наделены полномочиями по управлению личными данными и контролем доступа к ним [2].

Кроме того, об условности контроля над персональными данными говорит тот факт, что хранилища данных субъектов персональных данных находятся, как правило, в облаках или на платформах поставщиков услуг, которые диктуют условия пользования частным облаком (платно, бесплатно, сроки и др.).

Сказанное позволяет констатировать, что во всех перечисленных примерах речь на самом деле идет не о контроле субъекта за доступом к своим данным, а об управлении своим согласием.

Второе направление развития концепция контроля доступа к персональным данным может строиться на основе децентрализованной модели обработки данных, где обработка данных осуществляется в собственном устройстве субъекта, в том числе благодаря технологии Искусственного интеллекта. Разработчики таких моделей исходят из того, что субъект персональных данных, благодаря закрепленным в GDPR правам, в том числе правам запрашивать у компаний доступ к своим данным и переносить эти данные от одного поставщика к другому, может самостоятельно агрегировать копии своих персональных данных, собрав их с помощью встроенного в среду обработки данных робота, из разных источников (цифровые платформы, персональные носимые устройства, устройства Интернета вещей, данные с мобильных устройств, приложений и онлайн-сервисов).

Субъекту персональных данных предлагается самому определять объем и условия доступа к своему профилю через такой инструмент, как разрешения (лицензии):

1) Полная/ограниченная анонимность, например, при посещении сайтов потенциальных поставщиков услуг;
2) Разрешение на отслеживание (сбор поставщиком данных о поведении субъекта);
3) Разрешение на хранение данных;
4) Разрешение на объединение данных данного субъекта с данными других субъектов;
5) Разрешение на обмен данными (передача поставщиком услуг другим лицам):
6) Разрешение на продажу данных [10].

Субъект персональных данных будет определять комбинацию разрешений, а также продолжительность доступа к своему профилю, устанавливать размер вознаграждения за каждое разрешение или выбирать иную форму выгоды. В рамках системы обработки данных, ориентированной на человека, личные данные остаются у субъекта, он не теряет контроль над своими данными. Данные по умолчанию являются конфиденциальными: если стороннему приложению требуется доступ к данным пользователя, приложению необходимо предварительно получить разрешение пользователя на доступ к таким данным и обосновать необходимость доступа. Вместо того, чтобы полагаться на право “переносить” какие-то части данных субъекта от одного поставщика услуг к другому поставщику услуг (модель согласия и отказа), физические субъекты хранят свои данные при себе.

При этом предполагается, что обработка персональных данных, осуществляемая не на основании согласия, а по иным основаниям, предусмотренных законом, будет иметь приоритет над волей субъектов персональных данных, выраженной в выдаваемых им разрешениях (лицензиях) на обработку его данных [3,с.12].

Таким образом, децентрализованная модель основывается не просто на согласии субъекта персональных данных на их обработку, но и на дополнительном инструменте в виде разрешений (лицензий), выдаваемых субъектом третьим

лицам. Личные данные человека благодаря технологическому инструменту становятся экономическим активом [4].

Примером такой децентрализованной модели является технология под названием AITwins, предлагаемая американской компанией Prifina. Она разработала платформу для обработки данных, которая позволяет частным лицам разместить свои персональные данные в облаках, а для активации и управления ими создаются персональные цифровые помощники, которые будут действовать от имени субъектов персональных данных [11]. Уже сейчас такого рода продукт становится востребованным в сфере поиска работы. Ряд инновационных компаний (например, испанская Ooptimo [12], американская Crystalia Glass LLC [13]), получающих резюме от соискателей вакансий, предлагают проходить первичное интервью с Искусственным интеллектом - ботом. Во время интервью оценивается не только опыт соискателя, но и его эмоции при ответе на вопросы. По словам соискателей, это вызывает отторжение и дискомфорт, так как соискатель предпочел бы диалог с живым человеком. Поэтому, если интервью проводит бот, то почему бы и соискателю не направить на интервью своего цифрового двойника?

Это направление кажется наиболее отвечающим интересам субъектов персональных данных инструментом, но и в данном случае потенциальное хранилище данных субъекта персональных данных фактически находится у третьего лица, хотя и не предлагающего субъектам персональных данных никаких услуг и продуктов, кроме собственно размещения в пространстве интернета. Можно такое хранение сравнить с арендой банковской ячейки в банке. Клиент банка арендует ячейку в банке, размещает в ней ценные вещи, ему выдают ключ. Но в банке есть люди, которые потенциально могут воспользоваться содержимым ячейки, и за пределами банка есть люди, которые также могут получить доступ к ячейке.

В России такого рода технологии пока не предлагаются. Кроме того, для активного участия субъекта персональных данных в обороте персональных данных через использование названных технологий потребуется внести дополнения, изменения в гражданское законодательство и в законодательство в сфере защиты персональных данных, например, касающиеся правового обозначения агрегированной совокупности персональных данных, правового статуса субъекта персональных данных, нормативного описания процессов управления и контроля доступа, лицензионных соглашений.

Технологии как инструменты регулирования отношений между участниками информационного обмена имеют и негативный аспект. Субъект персональных прав, не являясь владельцем технологии или не имея достаточных технических навыков, навыков ведения предпринимательской деятельности, становится уязвимым и может быть зависим от условий использования технологии.

Список литературы:

[1] Эгамбердиев Э.Х. Технологии интернет вещей и персональные данные: вопросы собственности// Oriental Renaissance: Innovative, educational, natural and social sciences E) ISSN:2181-1784 www.oriens.uz 3(1/2), Jan., 2023. С.541-558.

[2] European Data Protection Supervisor (EDPS), 2020, Brief report “Personal Information Management Systems”, Issue 3, 2020.

[3] Jurcys P., Donewald C., Globocnik J., Lampinen M. My data, my terms: a proposal for personal data use licenses, Harvard Journal of Law & Technology, Volume 33, Digest Spring 2020.

[4] Fenwick, Mark and Jurcys, Paul and Minssen, Timo, Data Portability Revisited: Toward the Human-Centric, AI-Driven Data Ecosystems of Tomorrow (June 10, 2023). Vanderbilt Journal of Entertainment & Technology Law, Forthcoming.

[5] Julie Brill, Microsoft’s Commitment to GDPR, Privacy and Putting Customers in Control of Their Own Data, MICROSOFT (May 21, 2018). URL: https://blogs.microsoft.com/on-the-issues/2018/05/21/microsofts-commitment-to-gdpr-privacy-and-putting-customers-in-control-of-their-own-data/ (дата обращения – 05.05.2025); Privacy, APPLE, URL: https://www.apple.com/privacy/ (дата обращения- 05.05.2025).

[6] Распоряжение Президента РФ от 10 октября 2018 г. № 294-рп [Электронный ресурс] // СПС Гарант.

[7] Сайт: https://www.inrupt.com/case-study/vito-securely-shares-personal-health-data-using-solid (дата обращения- 05.05.2025).

[8] Сайт: https://media.telefonicatech.com/telefonicatech/uploads/2021/1/42752_aurastory-tomo-1-digital.pdf (дата обращения- 05.05.2025).

[9] https://selectel.ru/services/cloud/servers/152fz// (дата обращения- 05.05.2025).

[10] Продажа данных допускается в некоторых штатах США, см. Раздел 2, параграф i, (3) Калифорнийского Закона о Защите Прав Потребителей 2018г. (The California Consumer Privacy Act of 2018), URL: https://theccpa.org/ (дата обращения- 05.05.2025).

[11] Сайт: https://www.prifina.com (дата обращения- 05.05.2025).

[12] Сайт: https://www.ooptimo.com (дата обращения- 05.05.2025).

[13] Сайт: https://crystaliaglass.com (дата обращения- 05.05.2025).

Spisok literatury:

[1] E`gamberdiev E.X. Texnologii internet veshhej i personal`ny`e danny`e: voprosy` sobstvennosti// Oriental Renaissance: Innovative, educational, natural and social sciences E) ISSN:2181-1784 www.oriens.uz 3(1/2), Jan., 2023. S.541-558.

[2] European Data Protection Supervisor (EDPS), 2020, Brief report "Personal Information Management Systems", Issue 3, 2020.

[3] Jurcys P., Donewald C., Globocnik J., Lampinen M. My data, my terms: a proposal for personal data use licenses, Harvard Journal of Law & Technology, Volume 33, Digest Spring 2020.

[4] Fenwick, Mark and Jurcys, Paul and Minssen, Timo, Data Portability Revisited: Toward the Human-Centric, AI-Driven Data Ecosystems of Tomorrow (June 10, 2023). Vanderbilt Journal of Entertainment & Technology Law, Forthcoming.

[5] Julie Brill, Microsoft's Commitment to GDPR, Privacy and Putting Customers in Control of Their Own Data, MICROSOFT (May 21, 2018). URL: https://blogs.microsoft.com/on-the-issues/2018/05/21/microsofts-commitment-to-gdpr-privacy-and-putting-customers-in-control-of-their-own-data/ (data obrashheniya – 05.05.2025); Privacy, APPLE, URL: https://www.apple.com/privacy/ (data obrashheniya- 05.05.2025).

[6] Rasporyazhenie Prezidenta RF ot 10 oktyabrya 2018 g. № 294-rp [E`lektronny`j resurs] // SPS Garant.

[7] Sajt: https://www.inrupt.com/case-study/vito-securely-shares-personal-health-data-using-solid (data obrashheniya- 05.05.2025).

[8] Sajt: https://media.telefonicatech.com/telefonicatech/uploads/2021/1/42752_aurastory-to-mo-1-digital.pdf (data obrashheniya- 05.05.2025).

[9] https://selectel.ru/services/cloud/servers/152fz// (data obrashheniya- 05.05.2025).

[10] Prodazha danny`x dopuskaetsya v nekoto-ry`x shtatax SShA, sm. Razdel 2, paragraf i, (3) Kalifornijskogo Zakona o Zashhite Prav Potrebitelej 2018g. (The California Consumer Privacy Act of 2018), URL: https://theccpa.org/ (data obrashheniya- 05.05.2025).

[11] Sajt: https://www.prifina.com (data obrashheniya- 05.05.2025).

[12] Sajt: https://www.ooptimo.com (data obrashheniya- 05.05.2025).

[13] Sajt: https://crystaliaglass.com (data obrashheniya- 05.05.2025).

