Мониторинг международных трендов правового регулирования для развития законодательства в сфере цифровой экономики в России

- **Ответственное использование ИИ**
- **Право на переносимость персональных данных**
- **Трансграничные потоки неперсональных данных**
- **Регулирование пикселей отслеживания**

Мониторинг №6 (18) (Июнь 2025)

Мониторинг подготовлен коллективом сотрудников лаборатории анализа лучших международных практик Института экономической политики имени Е. Т. Гайдара (Института Гайдара).

Авторский коллектив: науч. сотр. Гирич М.Г., науч. сотр. Ермохин И.С., ст. науч. сотр. Левашенко А.Д., науч. сотр. Магомедова О.С., науч. сотр. Черновол К.А., юрисконсульт Фонда Экономической политики Голованова Д.А.

«Что делать в городе в июне?
Не зажигают фонарей;
На яхте, на чухонской шхуне
Уехать хочется скорей!»
О. Мандельштам

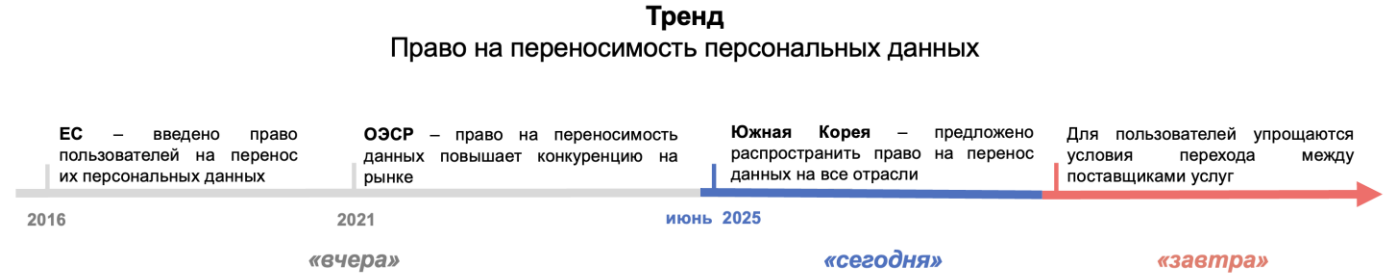
В июне 2025 г. можно выделить 4 события, которые определяют тренды развития регулирования цифровой экономики в мире.

Тренд № 1. Ответственное использование ИИ

В июне 2025 г. ОЭСР опубликовала рекомендации по ответственному использованию ИИ: раскрывать информацию о работе алгоритмов, обсуждать риски с сотрудниками, пользователями и регуляторами и т.д.

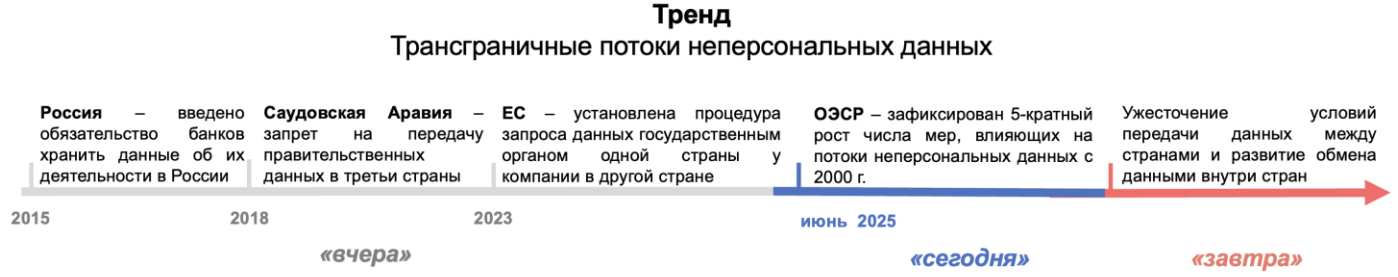
Тренд № 2. Право на переносимость персональных данных

С июня 2025 г. в Южной Корее расширяется право граждан на переносимость их персональных данных из одной организации в другую в любых отраслях.



Тренд № 3. Трансграничные потоки неперсональных данных

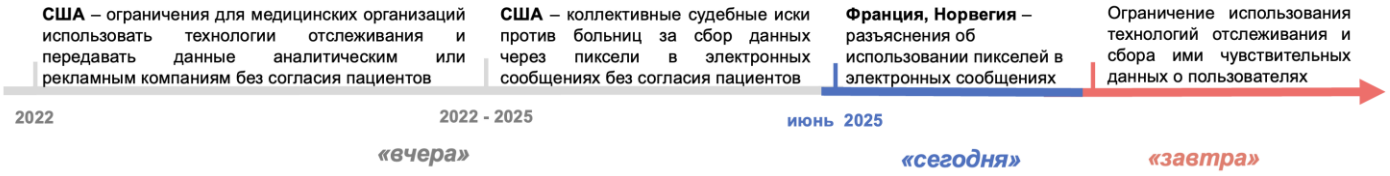
В июне 2025 г. ОЭСР представила доклад, отметив пятикратный рост числа мер, регулирующих трансграничные потоки неперсональных данных в 2000–2024 гг. Меры включают: требование локализации данных, процедуры обязательной передачи данных от компаний государственным органам, содействие трансграничному обмену данными и др.



Тренд № 4. Регулирование пикселей отслеживания

В июне 2025 г. Франция и Норвегия опубликовали разъяснения об использовании пикселей – трекинговой технологии сбора поведенческих данных пользователей, включая их использование в почтовых рассылках (время открытия письма, геолокация, IP-адрес и др.).

Тренд
Регулирование пикселей отслеживания



В июне 2025 г. в России введен ряд нововведений.

1. Будет разработан национальный мессенджер

В июне 2025 г. в России принят Закон[1] о создании многофункционального сервиса обмена информацией – фактически национального мессенджера как для личных сообщений другим пользователям, так и для общения с органами власти, учреждениями. Национальный мессенджер будет подключен к инфраструктуре Госуслуг, предоставляя несколько уникальных для граждан возможностей:

1) использовать усиленную электронную подпись для подписания документов;

2) взаимодействовать с участниками образовательных организаций (участие в школьных чатах) и использовать образовательные сервисы;

3) предоставлять через мессенджер различную информацию о гражданине. Например, можно будет предъявить документы для подтверждения возраста, прав на получение льгот, предъявлять документы для организаций общего и профессионального образования, гостиниц и других организаций.

Если гражданин предъявляет документы через мессенджер, то запрещается требовать от него документы в бумажном виде. Фактически мессенджер будет работать как цифровой ID, через который гражданин может предоставлять сведения о себе.

Разработчик такого сервиса будет определен решением Правительства. При этом важным критерием при отборе организации-разработчика будет наличие у нее социальной сети с посещаемостью более 500 тыс. пользователей в сутки. Создание такого мессенджера, с одной стороны, позволяет цифровизовать некоторые процессы (как безбумажное предъявление документов), но с другой стороны, создаются риски монополии на работу такого мессенджера в руках одного оператора. В таком случае потребуется, чтобы мессенджер был совместим с другими соцсетями, мессенджерами и пр.

2. Определен порядок наполнения ГИС ОПД

В июне 2025 г. Правительство РФ утвердило правила[2] формирования составов обезличенных персональных данных, которые должны передаваться компаниями в Государственную информационную систему обезличенных персональных данных (ГИС ОПД)[3].

Данные должны предоставляться не на регулярной основе, а по требованию Роскомнадзора. В соответствии с правилами при формировании составов данных Роскомнадзор проводит оценку рисков восстановления обезличенных данных до состояния оригинальных, что необходимо для обеспечения безопасности дальнейшего пользования этими данными в системе. Также Роскомнадзор проверяет качество данных для исключения повторяющихся или неточных данных. При этом доступ к данным осуществляется в порядке направления запроса компанией или физическим лицом уполномоченному органу.

[1] Федеральный закон от 24.06.2025 № 156-ФЗ "О создании многофункционального сервиса обмена информацией и о внесении изменений в отдельные законодательные акты Российской Федерации".
[2] Постановление Правительства РФ от 26.06.2025 № 961 "О формировании составов персональных данных, полученных в результате обезличивания персональных данных, сгруппированных по определенному признаку, при условии, что последующая обработка таких данных не позволит определить принадлежность таких данных конкретному субъекту персональных данных, и предоставлении доступа к составам таких данных".
[3] Постановление Правительства РФ от 28.05.2025 № 740 "О государственной информационной системе федерального органа исполнительной власти, осуществляющего функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере информационных технологий, указанной в статье 13.1 Федерального закона "О персональных данных".

Данный инструмент направлен исключительно на развитие качества государственного управления и не решает задачу развития рынка данных в России, так как составы открываемых данных будет определять государство, а не рынок, данные становятся доступны по запросу частных организаций (если они соответствуют требованиям закона) только через год после их передачи государству.

3. Введены меры регулирования беспилотников

В июне 2025 г. Минпромторгом был принят приказ[4], который разъясняет, как должны строиться так называемые С2-каналы – маршруты, по которым отправляются команды операторов и телеметрия дронов. Суть нововведения проста. Владелец дрона сам решает, будет ли посылать сигналы для управления дроном напрямую по радио или через внешнего провайдера, который даст инфраструктуру для сигналов и будет следить, чтобы не было обрывов связи с дроном. Владелец устанавливает нужную аппаратуру, получает разрешение на использование определенной радиочастоты[5] для управления, записывает каждый вылет и обязан фиксировать случаи потери канала связи с дроном во время полетов. Провайдер, в свою очередь, обязан держать линию связи без сбоев, обслуживать оборудование и сразу же оповещать владельца при неполадках. А государственный оператор (пока официально не определён)[6] распределяет радиочастоты, задаёт зоны, где дроны смогут ловить сигнал, и хранит их телеметрию[7] как «чёрные ящики».

В соответствии с приказом ответственность за эксплуатацию беспилотных авиационных систем несут: владелец отвечает за сам аппарат; провайдер — за качество сигнала: назначенная государством организация — за частоты и безопасность.

Этот приказ – продолжение истории с внедрением в России регулирования беспилотников. Еще в 2023 г. Воздушный кодекс дополнили требованиями о специальных авиационных правилах в отношении беспилотников (обязательная сертификация беспилотных авиасистем, правила для инфраструктуры управления беспилотниками и т.п.). В 2024 г. в России запустили нацпроект «Беспилотные авиационные системы».

[4] Приказ Минпромторга России от 14.05.2025 № 2266 "Об утверждении Федеральных авиационных правил "Порядок организации и обеспечения функционирования линий управления беспилотными авиационными системами и контроля беспилотных авиационных систем для беспилотных авиационных систем авиационных предприятий и организаций экспериментальной авиации".
[5] частота электромагнитных колебаний, устанавливаемая для обозначения единичной составляющей радиочастотного спектра.
[6] Государственный поставщик услуг по обслуживанию линий управления беспилотными авиационными системами и контроля беспилотных авиационных систем.
[7] Данные о состоянии линии связи и управления, объеме и скорости передаваемой информации, требуемой для безопасного управления беспилотником.

Ключевые аспекты

1. Ответственное использование ИИ

Опыт ОЭСР

ОЭСР в июне 2025 г. описала[8], как распространить должную осмотрительность в сфере ответственного ведения бизнеса (далее – ОВБ)[9] на регулирование ИИ. Принципы ОВБ ОЭСР касаются вопросов защиты прав человека, трудовых отношений, окружающей среды, борьбы с коррупцией, интересы потребителей и налоги. Они применимы к любой сфере бизнеса.

ОЭСР рекомендует, чтобы компании, создающие и внедряющие ИИ-системы, применяли процедуру «шести шагов»:

– включали управление рисками в корпоративные политики. Например, в 2025 г. Microsoft в отчетности показала, что каждый ИИ-проект компании до запуска проходит более 30 обязательных внутренних проверок;

– выявляли и ранжировали потенциальные и фактические негативные воздействия алгоритмов на права человека, безопасность и окружающую среду. В июне 2025 г. Google рассказала[10], как её «красная команда» заранее атакует модель Gemini 2.5 вредоносными запросами, чтобы научить систему правильно реагировать на них;

– принимать меры по предотвращению и минимизации рисков на всех этапах жизненного цикла модели. Например, YouTube с мая 2025 г. обязывает авторов маркировать видео, созданное с помощью ИИ[11];

– обеспечивать независимый аудит и публичную отчётность о ходе реализации плана. Например, в декабре 2024 г. OpenAI пригласила Институты безопасности ИИ протестировать новую модель ChatGPT до выпуска и опубликовала их выводы[12];

– вести содержательный диалог с заинтересованными сторонами и предоставлять механизм рассмотрения жалоб с эффективным возмещением ущерба. Например, в марте 2025 г. OpenAI пообещала платить до 100 000 долл. каждому, кто найдёт серьёзную уязвимость в её системах ИИ, поощряя тем самым пользователей сообщать о проблемах[13];

– отслеживать эффективность мер и раскрывать результаты в открытых отчётах. Например, в апреле 2025 г. Google раскрыла, что её ИИ заблокировал 5,1 млрд вредоносных объявлений и отключил 39,2 млн мошеннических аккаунтов[14].

Должная осмотрительность основана на оценке рисков: глубина проверки должна соответствовать вероятности и серьёзности возможного вреда. Для «высокорисковых» систем, указанных, например, в Законе ЕС об ИИ 2024 г., проверка должна быть постоянной и включать внутренний и внешний контроль. Для разработчиков и поставщиков ИИ должная осмотрительность — это система выявления и снижения угроз правам человека, безопасности потребителей и экологии. Её внедрение уменьшит юридические и репутационные риски компании в случае сбоев и упростит соблюдение законов об ИИ.

Особенно ОВБ актуально при использовании генеративного ИИ. В новом докладе ОЭСР отмечает[15], что исследования в сфере генеративного ИИ вышли за рамки ИТ-сектора: в 2000–2023 гг. в мире опубликовано свыше 71 000 патентов по генеративному ИИ в 21 секторе, из них свыше 32 000 – в области ПО. Помимо ПО ключевыми по числу патентов являются биологические и медицинские науки, бизнес-решения, работа с документами, промышленное производство[16]. В 2024 г.

[8] https://www.oecd.org/en/publications/responsible-business-conduct-and-anticipatory-governance-of-emerging-technology_1308a723-en.html

[9] Ответственное ведение бизнеса – это меры, которые позволяют компании понять, какие её решения и операции могут навредить людям, окружающей среде или честной конкуренции, и вовремя принимать меры, чтобы такой вред предотвратить или компенсировать. Это включает: честное обращение с работниками и поставщиками, уважение прав человека, заботу об экологии, прозрачную уплату налогов, противодействие коррупции и пр.

[10] https://security.googleblog.com/2025/06/mitigating-prompt-injection-attacks.html?

[11] https://ppc.land/youtube-introduces-mandatory-disclosure-for-ai-content

[12] https://www.aisi.gov.uk/work/pre-deployment-evaluation-of-openais-o1-model

[13] https://www.forbes.com/sites/daveywinder/2025/03/29/hack-openai-win-100000-what-you-need-to-know

[14] https://services.google.com/fh/files/misc/ads_safety_report_2024.pdf

[15] https://www.oecd.org/en/publications/is-generative-ai-a-general-purpose-technology_704e2d12-en.html

[16] В частности, в ЕС, штатах США, Великобритании, Канаде, Австралии и др.

внедрение генеративного ИИ в компаниях остается низким: в ЕС лишь 5,4% используют чат-боты, в Канаде – 9,3%. В США 22% работников применяют ИИ еженедельно. При этом свыше 50% мирового использования приходится на страны со средним доходом. По данным ОЭСР, это свидетельствует о более глубокой интеграции ИИ в экономики с растущей цифровой зрелостью[17].

Опыт России

В России есть инициативы, которые способствуют внедрению принципов ОВБ в разработку и использование ИИ. Например, добровольный Кодекс этики в сфере ИИ[18]. В июне 2025 г. Банк России также опубликовал Кодекс этики в сфере ИИ для финансовых институтов.

Реальные регуляторные меры по обеспечению ответственного поведения при использовании ИИ, в том числе генеративного, за пределами стратегий и поручений в России на данный момент отсутствуют.

2. Право на переносимость персональных данных

Опыт Южной Кореи

В июне 2025 г. Правительство Южной Кореи предложило расширить «право на переносимость» с отдельных сфер (медицина, телеком) на все отрасли экономики. То есть гражданин может требовать от оператора персональных данных (организации) передать ему или по его указанию любой третьей стороне его персональные данные. Организация будет обязана реализовать требование пользователя о переносе его персональных данных, если:

– имеет выручку свыше 110 млн долл. и более 1 млн пользователей;

– имеет более 5 тыс. пользователей и накапливает чувствительные[19] или уникальные данные таких пользователей;

– университеты с более 20 тыс. студентов или операторы систем публичного управления (например, поликлиники).

Однако из-под действия регулирования выведены данные, которые оператор обогатил иными данными или аналитикой, например, база данных о лайках пользователей, агрегированная по полу и возрасту и совмещенная с данными о музыкальных предпочтениях пользователей. Тем самым закон защищает право компаний на создание баз данных и иных продуктов, основанных на данных пользователей.

Интересно, что пользователь может потребовать передавать персональные данные как непосредственно себе (например, скачать файл с данными на свой компьютер), так и третьим лицам – специализированным посредническим организациям. Такие организации выступают в качестве доверенных лиц субъектов данных, поэтому вправе от имени гражданина получать и осуществлять хранение данных, предоставлять доступ гражданину к данным, и по его требованию передавать третьим организациям, но не могут анализировать полученные данные. Организации должны соблюдать требования информационной безопасности, технические и организационные меры для предотвращения утечки данных и др.

Опыт ЕС

В зарубежной законодательной практике право на переносимость персональных данных впервые появляется в европейском Регламенте о защите персональных данных в 2016 г. Право было введено для наделения пользователей возможностью свободного перехода между компаниями, в первую очередь цифровыми платформами, конкурирующими между собой.[20]

Корейская инициатива по созданию института специализированных организаций по управлению данными пользователей аналогична институту посредника по передаче данных в ЕС. Однако в ЕС такой посредник может оказывать услуги не только в отношении персональных данных, но и неперсональных.

Опыт России

[17] https://www.oecd.org/en/publications/is-generative-ai-a-general-purpose-technology_704e2d12-en.html
[18] https://ethics.a-ai.ru/
[19] Чувствительные данные - данные об идеологии, политических взглядах, судимости, данные биометрии и др. Уникальные данные – номер паспорта, водительского удостоверения и пр.
[20] https://iapp.org/news/a/data-portability-in-the-eu-an-obscure-data-subject-right

В России в настоящее время право на переносимость персональных данных не закреплено – нет ни права на получение копии обрабатываемых данных, ни права запрашивать передачу обрабатываемых данных другому оператору данных. Также не существует специального регулирования для лиц, оказывающих услуги посредничества по передаче данных.

3. Трансграничные потоки неперсональных данных

Опыт ОЭСР

В июне 2025 г. ОЭСР выпустила доклад о классификации мер, оказывающих воздействие на трансграничные потоки неперсональных данных (т.е. данных, не идентифицирующих конкретных физических лиц – далее НПД)[21]. С 2000 г. по 2024 г. число мер регулирования НПД выросло в 5 раз, причем как стимулирующих, так и ограничивающих потоки данных. ОЭСР рассматривает в качестве мер, воздействующих на потоки данных, не только меры в отношении трансграничной передачи данных, но также меры, затрагивающие доступность данных между странами (например, возможность просматривать и использовать данные, хранящиеся в одной стране, пользователями из другой страны). По оценкам экспертов ОЭСР, трансграничный обмен данными может увеличить ВВП до 2,5%.

На основе анализа 124 мер эксперты ОЭСР выделяют 3 категории мер:

1) меры, стимулирующие трансграничный доступ к НПД и обмену данными (17% мер). Например, к данной категории относятся и инициативы по открытым государственным данным, которые доступны в том числе для иностранных пользователей. Например, Закон США об открытых правительственных данных 2019 г. устанавливает условия публикации открытых данных федеральными агентствами, в числе которых доступность данных неограниченному кругу лиц, в том числе пользователям из третьих стран;

2) меры, обязывающие компании обеспечивать трансграничный доступ к их НПД для правительства и других компаний. Например, в США Закон о правомерном использовании данных за рубежом 2018 г. (CLOUD Act) обязывает американских провайдеров услуг электронных коммуникаций предоставлять американским государственным органам доступ к информации, в том числе хранящейся за пределами США. В данной категории 84% мер обязывают раскрывать данные государственным органам, и только 16% – третьим лицам;

3) меры, запрещающие трансграничный доступ к НПД и обмен ими, например, ограничения трансграничной передачи данных (получение разрешения органа на каждую передачу данных, проведение органом оценки рисков безопасности передачи данных за рубеж и др.), а также требование локализации данных, которое ограничивает возможность компаний передавать данные с целью хранения на серверах в третьих странах. Всего в мире на требования локализации приходится 35% выявленных всех мер регулирования НПД.

Наибольшее количество мер принято в отношении таких данных, как производственные данные (например, данные с устройств Интернета вещей на заводе), данные о деятельности бизнеса (например, о перевозках товаров), правительственные данные (данные об управлении бюджетом). Примечательно, что в отношении правительственных данных 50% мер имеют эффект ограничения потоков таких данных для публичного доступа, и только 40% приходится на инициативы по открытым данным, в том числе для зарубежных пользователей.

Опыт России

В России большинство мер направлено на регулирование персональных данных.

В отношении неперсональных данных мало инициатив. Например, с 2012 г. Россия развивает концепцию открытых правительственных данных, однако публикуемые данные мало вовлечены в цифровую экономику страны. В России нет принципа «открытости государственных данных по умолчанию» (т.е. принципа

[21] https://www.oecd.org/en/publications/a-preliminary-mapping-of-measures-affecting-the-cross-border-flow-of-non-personal-data_0825c57c-en.html

«публиковать все, что не запрещено к публикации»). Как следствие, раскрываются только те данные, которые требуется публиковать по закону.

Данные по сферам деятельности собираются и публикуются в разной мере: государство публикует подробные финансовые данные (например, данные по налогам), но не ведет сбор данных по качеству жизни. Данные открываются без учета спроса пользователей на конкретные составы данных.

4. Регулирование пикселей отслеживания

Опыт Франции и Норвегии

В июне 2025 г. во Франции начались общественные обсуждения по проекту рекомендации об использовании пикселей отслеживания в электронных сообщениях[22]. Аналогичное руководство опубликовано в Норвегии[23].

Пиксель отслеживания – это специальная трекинговая технология, представляющая изображение (размером 1x1 пиксель), которое встраивается в электронные сообщения (а также рекламу, браузеры и пр.) и позволяет собирать данные об активности пользователя (например, прочитано ли письмо, время открытия письма, IP-адрес, устройство и браузер, с которого открыто письмо, геолокация и т.д.). Пиксели размещаются не в самом письме, а на удаленных серверах (вне сайта, где находится пользователь), что позволяет осуществлять сбор данных пользователей на удаленном сервере с дальнейшей обработкой таких данных.

Когда пользователь открывает письмо, изображение пикселя автоматически загружается, отправляя запрос на сервер, где расположен этот пиксель. Запрос содержит технические данные, включая IP-адрес, информацию об устройстве и браузере, метку времени и пр. – в этот момент данные об активности пользователя поступают на сервер. То есть сам по себе пиксель не собирает никакой информации, но факт его загрузки позволяет отправителю письма получить информацию о том, что конкретное письмо было просмотрено определённым пользователем, время просмотра, геолокацию и др.

Регуляторы концентрируются на разработке правил именно для этой технологии в связи с ростом судебных исков. Например, в 2022 г. были поданы иски против трети из 100 крупнейших больниц США, которые отправляли конфиденциальные данные в Facebook[24] через пиксели на своих сайтах[25].

Технология позволяет осуществлять сбор данных о получателя письма, поэтому регуляторы во Франции и Норвегии рекомендуют следующее:

1. Учитывать, что отправитель электронного сообщения становится контролером данных, собранных через пиксели отслеживания, так как именно отправитель принимает решение об использовании технологии для сбора данных, а также определяет цели обработки данных.

Поставщик услуг электронной почты обеспечивает получение и отображение электронных сообщений пользователей, он не влияет на использование отправителями пикселей (хотя может блокировать автоматическую загрузку изображений), поэтому не является ни обработчиком, ни контролером данных;

2. При внедрении пикселей отслеживания в электронные сообщения потребуется предварительное согласие получателя:

– при анализе открытия писем. Например, если отправитель оценивает свои маркетинговые стратегии (как часто получатели читают письма, насколько привлекательны заголовки писем и др.) для повышения читаемости писем, корректировки частоты их отправки;

– при индивидуальном анализе интереса получателя к письмам для персонализации контента, например, настройка содержания писем в зависимости от выявленных предпочтений и интересов, получателя; персонализация канала отправки (email, SMS, push-уведомления и

[22] https://www.cnil.fr/fr/consultation-publique-projet-recommandation-pixels-de-suivi
[23] https://www.datatilsynet.no/personvern-pa-ulike-omrader/internett-og-apper/bruk-av-sporingsverktoy-pa-nettsteder-og-i-apper/
[24] Деятельность компании Meta признана экстремистской и запрещена на территории Российской Федерации.
[25] https://www.infosecurity-magazine.com/opinions/website-tracking-tech-risk-analysis?utm_source=twitterfeed&utm_medium=twitter

др.) в зависимости от того, каким каналом получатель пользуется чаще.

Согласие не требуется при:

– использовании пикселей для безопасности и аутентификации пользователя. Пиксель позволяет удостовериться, что письмо с ссылкой на сброс пароля открыто на устройстве, которое принадлежит конкретному пользователю;

– при измерении статистики открытия рассылаемых писем. В таком случае следует использовать пиксели для анонимной статистики, без индивидуального отслеживания отдельных пользователей;

3. Следует раскрывать цели использования пикселей. Например, можно отправить получателю предупреждение, что при открытии письма, информация о его действиях может использоваться для показа персонализированной рекламы или контента на других платформах;

4. Согласие на использование пикселей можно запросить в момент получения согласия на отправку электронных писем, предупреждая, что при открытии письма будет происходить трекинг с использованием пикселей;

5. Должна быть установлена простая процедура отзыва согласия на использование пикселей отслеживания. Например, рекомендуется вставлять ссылку для отзыва согласия в каждое письмо, содержащее пиксель. Такая ссылка должна вести на сайт, где можно отозвать согласие без дополнительных действий (например, ввода электронного адреса).

Опыт России

Сегодня в России Роскомнадзор не выпускает специальных руководств об использовании трекинговых технологий, в том числе таких технологий как cookie-файлы. Однако поведенческие данные, собранные такими трекинговыми технологиями, подпадают под определение персональных данных, предусмотренное в ФЗ №152 «О персональных данных». В частности, российские суды квалифицируют данные cookie-файлов как персональные данные[26]. Таким образом, данные, собранные с помощью пикселей отслеживания, подлежат такой же правовой защите, как и другие персональные данные.

[26] Постановление Девятого арбитражного апелляционного суда по делу № 09АП-17574/2016.