Дата поступления рукописи в редакцию: 15.10.2026 г.
Дата принятия рукописи в печать: 02.11.2026 г.
DOI: 10.24412/3033-6724-2026-4-24-27

АЛЕКСАНДРОВА Анна Сергеевна,
аспирант,
Самарский национальный исследовательский
Университет имени академика С.П. Королева,
г. Самара, Россия,
anna.alex2000@yandex.ru

ДИФФЕРЕНЦИАЦИЯ ТРЕБОВАНИЙ К ПОЛИТИКЕ В ОТНОШЕНИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ НА ОСНОВЕ ФУНКЦИОНАЛЬНОЙ КЛАССИФИКАЦИИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Аннотация. *Статья посвящена проблеме дифференциации требований к содержанию политики в отношении обработки персональных данных. Отмечается, что универсальная модель, закрепленная Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», утратила эффективность: политика превращается в формальный барьер, легитимирующий сбор данных. Автор обосновывает необходимость функционального подхода, основанного на классификации персональных данных по их роли в цифровой репрезентации личности (идентифицирующие, профилирующие и статусные данные). Для каждого типа данных выявлены специфические риски и сформулированы дифференцированные требования к полноте и доступности раскрываемых сведений об осуществляемой обработке персональных данных. Предлагаются критерии содержательного контроля со стороны Роскомнадзора: дифференциация требований к понятности, оценка полноты раскрытия алгоритмической логики, мониторинг «темных паттернов», оценка доступности информации о правах. Автор приходит к выводу о необходимости закрепить дифференцированные требования к политике в отношении обработки персональных данных на уровне законодательства о персональных данных, а также добиться, чтобы раскрываемая в ней информация была полной. Работа продолжает линию, начатую в более ранних публикациях автора, посвящённых функционально-сущностной классификации персональных данных и принципам их обработки.*

Ключевые слова: *обработка персональных данных, политика в отношении обработки персональных данных, законодательство, Роскомнадзор, функциональная классификация, идентифицирующие данные, профилирующие данные, статусные данные, дифференциация требований, риск-ориентированный подход, алгоритмическая прозрачность, человеческий пересмотр решений.*

ALEKSANDROVA Anna Sergeevna,
postgraduate,
Samara National Research University,
Samara, Russia

DIFFERENTIATION OF REQUIREMENTS FOR POLICY REGARDING PERSONAL DATA PROCESSING BASED ON THE FUNCTIONAL CLASSIFICATION OF PERSONAL DATA

Annotation. *The article addresses the issue of differentiating requirements for the content of a policy on personal data processing. It is noted that the universal model established by Federal Law No. 152-FZ of 27 July 2006 «On Personal Data» has lost its effectiveness: the policy is turning into a formal barrier legitimizing data collection. The author substantiates the need for a functional approach based on the classification of personal data according to their role in the digital representation of the individual (identifying, profiling, and status data). For each type of data, specific risks are identified and differentiated requirements are formulated regarding the completeness and accessibility of disclosed information about the personal data processing carried out. Criteria for substantive control by Roskomnadzor are proposed: differentiation of requirements for comprehensibility, assessment of the completeness of disclosure of algorithmic logic, monitoring of «dark patterns,» and assessment of the accessibility of information about rights. The author concludes that it is necessary to consolidate differentiated requirements for the Policy at the level of personal data legislation, as*

well as to ensure that the information disclosed therein is complete. This work continues the line initiated in the author's earlier publications on the functional-substantive classification of personal data and the principles of their processing.

Key words: *personal data processing, policy on personal data processing, legislation, Roskomnadzor, functional classification, identifying data, profiling data, status data, differentiation of requirements, risk-based approach, algorithmic transparency, human review of decisions.*

Введение. Политика в отношении обработки персональных данных, или, как её обычно называют, «политика конфиденциальности» (далее – Политика), являясь императивным требованием статьи 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Закон № 152-ФЗ) [1], призвана обеспечивать баланс технологических возможностей обработки персональных данных и гарантий частной жизни, выполняя функции прозрачности и формирования доверия в отношениях между субъектом и оператором персональных данных. Правовая природа Политики реализуется в трех аспектах: как локальный акт оператора персональных данных, фиксирующий процедуры и меры защиты; как публичное обязательство по информированию субъектов, необходимое для получения согласия; как средство раскрытия информации для Роскомнадзора как органа, контролирующего соблюдение законодательства о персональных данных.

Требование разместить на интернет-сайте Политику сегодня соблюдают почти все операторы. Однако наличие документа ещё не означает, что субъект понимает, какие сведения о нём собираются. Пользователь обычно не читает политику до конца – мешают объём, язык, структура. Причина не сводится к одной лишь привычке: даже внимательное прочтение документа не всегда позволяет установить, какие сведения собираются, кому они передаются и какие решения принимаются на их основе.

Закон требует, чтобы Политика была доступна субъекту персональных данных. Доступность при этом трактуется буквально – как возможность открыть документ. Насколько понятно и полно его содержание, во внимание не принимается. Формально субъект информирован, фактически же он дал согласие на то, о чём ему не сообщили.

Разрыв между формальным соблюдением и реальным информированием обусловлен рядом факторов:

– избыточная детализация зачастую приводит лишь к формальному исполнению требований законодательства;

– алгоритмизация скрывает логику автоматизированных решений;

– коммерческие соображения побуждают операторов к неполному раскрытию информации: развернутое и понятное описание обработки данных требует дополнительных издержек, снижает возможности монетизации персональных данных, а также увеличивает риск оспаривания правомерности обработки этих данных оператором.

Ключевой методологический пробел – отсутствие дифференцированного подхода к раскрытию информации. Персональные данные функционально неоднородны и порождают различные риски – от подмены идентичности до дискриминации. Следовательно, требования к раскрытию информации должны быть соразмерны этим рискам, что достигается применением функционального подхода [4] к содержанию Политики. Такой подход согласуется с логикой риск-ориентированности, которая уже реализована в подзаконном техническом регулировании. Постановление Правительства РФ от 01.11.2012 № 1119 и Приказ ФСТЭК России от 18.02.2013 № 21 устанавливают четыре уровня защищенности информационных систем, а также дифференцированный состав мер для каждого из них [2; 3]. Представляется логичным распространить ту же логику соразмерности и на содержание Политики [5].

Основная часть. Требования к Политике, установленные статье 18.1 Закона № 152-ФЗ [1], сформулированы одинаково для всех видов обрабатываемых сведений и не учитывают их функциональных различий и связанных с ними рисков. Исключение составляют лишь отдельные категории: специальные и биометрические данные, для которых закон устанавливает более строгий режим. Однако цифровая среда показывает обратное: разные сведения выполняют в ней разные функции. Одни служат для того, чтобы отличить одного человека от другого, – это идентифицирующие данные (ФИО, паспортные данные, СНИЛС, биометрические верификаторы). Другие складываются в описание привычек и предпочтений – профилирующие данные (история запросов, геолокация, метаданные коммуникаций). Третьи представляют собой готовую оценку, присвоенную алгоритмом, – статусные данные (кредитные рейтинги, скоринговые баллы, уровни доступа к сервисам) [4].

Предлагаемое разграничение не следует понимать как жёсткое. Границы между типами подвижны: поведенческий профиль, собранный для персонализации интерфейса, при смене цели превращается в основание для скоринга, а значит, переходит в разряд статусных данных. Именно эта способность данных менять функцию и создаёт основную сложность для регулирования, построенного на статических перечнях.

Функциональные различия между типами данных проявляются и в характере угроз, которые они создают. Идентифицирующие данные уязвимы к подмене личности. Профилирующие – к скрытому воздействию на поведение. Что касается статусных, основной риск здесь – алгоритмическая дискриминация личности [4; 5]. Именно

разнородность этих рисков и обусловливает необходимость дифференциации требований к содержанию Политики.

Рассмотрим эти требования применительно к каждому типу данных.

Например, если данные используются для идентификации и аутентификации субъекта, ключевое значение имеет информирование о конкретном перечне собираемых идентификаторов. Отдельного раскрытия требуют цели их сбора. При этом важно указать, ограничиваются ли они только идентификацией или включают иные задачи. Политика должна также указывать сроки хранения, порядок уточнения, блокирования и уничтожения сведений, а равно меры защиты от несанкционированного доступа и подмены.

Следовательно, в данном случае Политика должна четко разграничивать обязательные и добровольные идентификаторы, а при использовании биометрических данных – раскрывать, применяются ли они для верификации или идентификации, поскольку это определяет уровень риска.

Данные, формирующие профилирующий (поведенческий) профиль пользователя. Процесс их сбора часто носит скрытый характер, а ценность представляет не каждый отдельный факт, а их совокупность.

Именно поэтому требования к раскрытию информации о профилирующих данных должны быть особенно конкретными.

Политика должна содержать:

1) явное указание на факт сбора профилирующих данных, а не общие фразы о «технической информации»;

2) раскрытие конкретных целей сбора: персонализация, маркетинговые исследования, таргетирование рекламы;

3) информацию о передаче данных третьим лицам (рекламным сетям, аналитическим платформам, информационным брокерам);

4) понятную инструкцию о возможности отказа от сбора данных с указанием способов реализации такого отказа.

Особого внимания требует информирование об использовании интерфейсных решений, манипулирующих выбором пользователя в пользу более интенсивного сбора данных («темные паттерны»). Регуляторная практика должна ориентировать операторов на добросовестное раскрытие всех способов сбора такого типа информации.

Наиболее высокие требования к прозрачности предъявляют статусные данные, выступающие результатом алгоритмической обработки и непосредственно определяющие правовое или экономическое положение субъекта: кредитные рейтинги, балльные оценки платежеспособности, репутационные категории, уровни доступа к сервисам. При обработке таких данных в Политику также целесообразно включить:

1) указание на факт принятия автоматизированных решений, затрагивающих права субъекта;

2) описание логики алгоритма – основных факторов, влияющих на принятие решений (даже если полная математическая логика остается коммерческой тайной);

3) информацию о мерах по обеспечению справедливости модели: проводилась ли валидация на предмет предвзятости, принимались ли меры для минимизации дискриминационных эффектов;

4) четкую процедуру реализации права на человеческий пересмотр автоматизированного решения;

5) порядок оспаривания дискриминационных решений (обращение к оператору, в надзорный орган, в суд) [5].

Накопленные противоречия ведут к тому, что Политика начинает работать не на защиту субъекта, а против него. Вместо информирования она обеспечивает лишь юридическое оформление уже состоявшегося сбора данных. На сегодняшний день Роскомнадзор оценивает лишь наличие документа, структуру и полноту сведений, а ответственность наступает только за сам факт отсутствия политики, но не за ее нечитаемость или сокрытие алгоритмической обработки. В результате юридически безупречный, но намеренно усложненный текст успешно проходит контроль, не достигая цели закона – информированности субъекта персональных данных.

Предлагаемый функциональный подход позволяет сформулировать несколько критериев содержательного контроля.

Во-первых, требования к понятности изложения должны дифференцироваться. Если речь идёт об обработке данных, влекущих наиболее серьёзные риски, прежде всего алгоритмических оценок. Следовательно, информация о них должна излагаться максимально доступно, с примерами и пояснениями.

Во-вторых, должна подлежать проверке полнота раскрытия алгоритмической логики. Роскомнадзор оценивает, достаточно ли субъекту предоставлено сведений, чтобы понять, как формируется затрагивающая его алгоритмическая оценка.

В-третьих, необходим мониторинг «тёмных паттернов». Речь идёт о выявлении интерфейсных приёмов, которые незаметно склоняют пользователя к согласию на сбор склоняют пользователя к согласию на избыточный сбор его персональных данных.

Наконец, в-четвёртых, необходимо оценивать реальную доступность инструкций по реализации прав. Политика должна содержать понятные пошаговые указания, охватывающие каждое право субъекта персональных данных, с указанием порядка обращения, сроков, способов связи с оператором и порядка обжалования его решений.

Заключение. Таким образом, Политика должна перестать быть универсальным документом и стать дифференцированным инструментом информирования субъектов персональных данных.

Объем и характер раскрываемой информации должны определяться функциональным типом обрабатываемых данных, а не универсальным шаблоном. Соответствующие изменения целесообразно закрепить в статье 18.1 Закона № 152-ФЗ, дополнив их критериями содержательного контроля со стороны Роскомнадзора. Такой подход позволит преодолеть формализацию согласия, а Политика вновь начнет работать именно в интересах самих субъектов персональных данных.

Список литературы:

[1] Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 05.09.2026).

[2] Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_137356/ (дата обращения: 05.09.2026).

[3] Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_146520/a6615f7b0ffcc68aa0e0796336836d16febbfb4b/ (дата обращения: 05.09.2026).

[4] Александрова А.С. Дифференциация правового регулирования обработки персональных данных: обоснование на основе функционально-сущностной классификации // Юридические исследования. 2026. № 1. С. 47-59.

[5] Александрова А.С. Принципы обработки персональных данных: функциональная классификация как основа дифференцированного правового регулирования // Юридические исследования. 2026. № 3. С. 1-16.

References:

[1] Federal Law No. 152-FZ of July 27, 2006, «On Personal Data» // ConsultantPlus Legal Reference System. URL: https://www.consultant.ru/document/cons_doc_LAW_61801/ (accessed: 05.09.2026).

[2] Decree of the Government of the Russian Federation No. 1119 of November 1, 2012, «On Approval of Requirements for the Protection of Personal Data During Their Processing in Personal Data Information Systems» // ConsultantPlus Legal Reference System. URL: https://www.consultant.ru/document/cons_doc_LAW_137356/ (accessed: 05.09.2026).

[3] Order of the FSTEC of Russia No. 21 of February 18, 2013, «On Approval of the Composition and Content of Organizational and Technical Measures to Ensure the Security of Personal Data During Their Processing in Personal Data Information Systems» // ConsultantPlus Legal Reference System. URL: https://www.consultant.ru/document/cons_doc_LAW_146520/a6615f7b0ffcc68aa0e0796336836d16febbfb4b/ (accessed: 05.09.2026).

[4] Aleksandrova A.S. Differentiation of Legal Regulation of Personal Data Processing: A Rationale Based on a Functional-Essential Classification // Legal Studies (Yuridicheskie issledovaniya). 2026. No. 1. pp. 47–59.

[5] Aleksandrova A.S. Principles of Personal Data Processing: Functional Classification as a Basis for Differentiated Legal Regulation // Legal Studies (Yuridicheskie issledovaniya). 2026. No. 3. Pp. 1–16.