

Правовой разбор: получение сводным братом паспортных данных и СНИЛС без согласия и направление их субъекту на телефон

1. Краткая постановка вопроса

Заявитель указывает, что сводный брат получил (тем или иным путем «узнал») полный набор его идентификационных данных — паспортные данные и СНИЛС — без согласия заявителя, после чего направил эти данные на телефон заявителя. Согласия на сбор, хранение и передачу персональных данных заявитель не давал. Требуется установить: (а) образуют ли действия брата состав незаконного собирания сведений о частной жизни (ст. 137 УК РФ) и/или нарушения законодательства о персональных данных (ст. 13.11 КоАП РФ, Закон № 152-ФЗ), с учетом того, что брат не является оператором; (б) является ли направление данных самому субъекту «распространением» персональных данных и какие права возникают у заявителя; (в) возможна ли квалификация по ст. 272, 272.1 УК РФ, если данные получены из информационной системы либо через третьих лиц, и как это документируется.

Разбор построен по версиям: поскольку из описания не следует, каким именно способом брат получил данные (бытовой доступ к документам, доступ к устройству заявителя, получение от третьих лиц, доступ к информационной системе), каждая версия разобрана отдельно, поскольку правовые последствия в них принципиально различны.

Оговорка об исходных данных: разбор исходит из того, что заявитель — совершеннолетний дееспособный гражданин; речь идет о паспорте гражданина РФ и страховом номере индивидуального лицевого счета (СНИЛС); сообщение направлено лично заявителю (на его номер/устройство), а не третьим лицам и не в групповой чат.

2. Квалификация самих сведений: персональные данные и «личная/семейная тайна» — это не одно и то же

2.1. Паспортные данные и СНИЛС — безусловно персональные данные

Согласно п. 1 ст. 3 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», персональные данные — любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных). Фамилия, имя, отчество, дата и место рождения, серия и номер паспорта, кем и когда выдан, адрес регистрации, СНИЛС — типичный набор идентификаторов, позволяющий определить лицо. Споры о том, что это персональные данные, в практике нет.

Следовательно, любые операции с этим набором (сбор, запись, хранение, уточнение, извлечение, использование, передача, блокирование, удаление, уничтожение) образуют **обработку персональных данных** (п. 3 ст. 3 Закона № 152-ФЗ) и требуют законного основания (ст. 6, 9 Закона № 152-ФЗ).

2.2. Являются ли паспортные данные и СНИЛС «личной или семейной тайной» (предмет ст. 137 УК РФ, ст. 152.2 ГК РФ)

Здесь практика расходится, и это принципиально для уголовно-правовой квалификации.

Позиция 1 (узкая, преобладающая в правоприменении). Идентификационные реквизиты документов не относятся к сведениям о частной жизни, составляющим личную или семейную тайну. Статья 152.2 ГК РФ (п. 1) называет в качестве ориентира «сведения о происхождении, о месте пребывания или жительства, о личной и семейной жизни»; паспортные реквизиты и СНИЛС — это учетные атрибуты, а не сведения об интимной, семейной, медицинской, религиозной стороне жизни. Кроме того, абз. 2 п. 1 ст. 152.2 ГК РФ прямо исключает противоправность сбора и использования информации, которая «ранее стала общедоступной либо была раскрыта самим гражданином или по его воле», — а паспортные данные и СНИЛС гражданин многократно раскрывает сам (банки, работодатель, МФЦ, операторы связи, медицинские организации). По этой логике предмета ст. 137 УК РФ здесь нет.

Позиция 2 (широкая). Статья 152.2 ГК РФ говорит о «любой информации о его частной жизни», перечень в п. 1 — открытый («в частности»). Совокупность ФИО + даты рождения + паспортных реквизитов + СНИЛС

позволяет полностью идентифицировать лицо и создать на его имя юридически значимые последствия (кредиты, сим-карты, регистрации), то есть затрагивает охраняемую сферу автономии личности. В ряде случаев суды и органы предварительного расследования квалифицируют по ст. 137 УК РФ сбор именно таких «связок» данных, если они сопровождаются иными сведениями (адрес, состав семьи, место работы, состояние здоровья) и совершены из корыстной либо иной личной заинтересованности.

Практический вывод по разделу 2. Для обоснования состава ст. 137 УК РФ необходимо, чтобы предметом были именно сведения о частной жизни, составляющие личную/семейную тайну, плюс вред правам и законным интересам, плюс корыстная или иная личная заинтересованность (ч. 1 ст. 137 УК РФ). Одни паспортные данные и СНИЛС этот порог, как правило, не преодолевают. Для гражданско-правовой и административной линии (Закон № 152-ФЗ, ст. 152.2 ГК РФ) широкая трактовка не требуется: достаточно того, что это персональные данные.

3. Версия 1: данные получены бытовым путем, обрабатываются «для личных и семейных нужд»

3.1. Обстоятельства, при которых применяется версия

Брат взял данные из семейных документов, копий, переписки, увидел паспорт, знал СНИЛС из общих семейных бумаг; хранит их у себя и переслал заявителю, не преследуя цели извлечь выгоду, оформить что-либо, передать третьим лицам.

3.2. Правовое обоснование

Ключевая норма — **п. 1 ч. 2 ст. 1 Закона № 152-ФЗ**: действие закона не распространяется на отношения, возникающие при «обработке персональных данных физическими лицами исключительно для личных и семейных нужд, **если при этом не нарушаются права субъектов персональных данных**».

Это означает: - физическое лицо **может** быть оператором (п. 2 ст. 3 Закона № 152-ФЗ прямо называет физическое лицо в числе операторов), но при строго личном/семейном использовании режим закона не применяется; - исключение действует **только при отсутствии нарушения прав субъекта**. Как только обработка начинает нарушать права (сбор без согласия в целях, не связанных с семьей и бытом; дальнейшая передача; использование во вред), исключение

перестает работать, и лицо подпадает под режим оператора со всеми обязанностями (ст. 5, 6, 7, 9, 18.1, 19, 21 Закона № 152-ФЗ).

3.3. Практический вывод по версии 1

- **Уголовная ответственность по ст. 137 УК РФ** — маловероятна: нет ни предмета (личная/семейная тайна), ни, как правило, вреда правам и законным интересам, ни корыстной/личной заинтересованности в юридически значимом смысле.
- **Административная ответственность по ст. 13.11 КоАП РФ** — маловероятна, поскольку состав адресован операторам, а в этой версии лицо под режим оператора не подпадает; на практике Роскомнадзор не привлекает граждан за бытовую обработку данных родственников.
- **Гражданско-правовая линия по ст. 152.2 ГК РФ остается рабочей**, поскольку эта норма не содержит изъятия «для личных и семейных нужд»: п. 1 ст. 152.2 ГК РФ запрещает **без согласия гражданина сбор, хранение, распространение и использование любой информации о его частной жизни**, кроме случаев публичного интереса и случаев, когда информация ранее стала общедоступной либо раскрыта самим гражданином. То есть даже «по-родственному» хранение копии паспорта и СНИЛС без согласия формально противоправно, если эти сведения будут признаны относящимися к частной жизни (см. раздел 2.2).
- **Реальный инструмент в этой версии** — не наказание, а **требование прекратить обработку и уничтожить копии** (ст. 21 Закона № 152-ФЗ — при применимости закона; ст. 12, п. 1 ст. 152.2 ГК РФ — всегда) плюс фиксация факта на случай эскалации.

4. Версия 2: данные получены вне «личных и семейных нужд» либо с нарушением прав субъекта

4.1. Обстоятельства, при которых применяется версия

Брат получил данные через знакомых с доступом к базам (МВД, МФЦ, банк, оператор связи, страховая, работодатель), через приобретенные дампы, взлом аккаунта заявителя на «Госуслугах», доступ к его телефону/компьютеру, либо собирает данные для последующего использования (оформление кредита, сим-карт, шантаж, «помощь» третьим лицам).

4.2. Правовое обоснование

1. **Исключение п. 1 ч. 2 ст. 1 Закона № 152-ФЗ не применяется** — права субъекта нарушены. Брат становится оператором: обязан иметь законное основание обработки (ст. 6, 9 Закона № 152-ФЗ), соблюдать конфиденциальность (ст. 7), принципы обработки (ч. 1, 2, 7 ст. 5 — законность, ограничение заранее определенными целями, хранение не дольше, чем требует цель), обеспечивать безопасность (ст. 19), уничтожать данные при отпадении цели (ст. 21).
2. **Ст. 13.11 КоАП РФ:** ч. 1 — обработка персональных данных в случаях, не предусмотренных законодательством, либо несовместимая с целями сбора (штраф на граждан от 1 000 до 3 000 руб.); ч. 2 — обработка без письменного согласия, когда оно обязательно, либо с нарушением требований к составу согласия (штраф на граждан от 3 000 до 5 000 руб.). Обе части содержат оговорку «если эти действия не содержат уголовно наказуемого деяния». Дополнительно ст. 13.11 КоАП РФ дополнена составами об утечках персональных данных (ч. 12–14 и последующие, введены Федеральным законом от 30.11.2024 № 420-ФЗ); для физического лица — «не-оператора» они, как правило, неприменимы, но показывают направление ужесточения режима.
3. **Ст. 13.14 КоАП РФ** (разглашение информации с ограниченным доступом) применима не к брату, а к тому должностному лицу/работнику, который передал ему данные, — если разглашение совершено лицом, получившим доступ в связи с исполнением служебных или профессиональных обязанностей.
4. **Ответственность источника утечки** — самостоятельное направление: оператор, допустивший передачу данных третьему лицу без согласия, нарушает ст. 7 и ст. 19 Закона № 152-ФЗ, а также может нести ответственность по ст. 13.11 КоАП РФ и обязан возместить моральный вред (ч. 2 ст. 24 Закона № 152-ФЗ).

4.3. Практический вывод по версии 2

- Жалоба в Роскомнадзор и заявление в полицию приобретают реальные перспективы, но центр тяжести смещается: привлекать проще и эффективнее **оператора-источник утечки**, чем физическое лицо-родственника.
- Требуется установить источник: кто имел легальный доступ к вашему набору данных и мог его передать. Это делается через запросы (в рамках проверки по заявлению в полицию) и через жалобу в Роскомнадзор.
- Административная ответственность брата по ст. 13.11 КоАП РФ возможна теоретически, но правоприменительная практика в отношении граждан

крайне скудна; срок давности по этой статье — один год со дня совершения правонарушения (ч. 1 ст. 4.5 КоАП РФ), что делает своевременность обращения критичной.

5. Версия 3 (ответ на вопрос о ст. 137 УК РФ): состав незаконного собирания сведений о частной жизни

5.1. Объективная сторона и ее дефициты в данной фабуле

Ч. 1 ст. 137 УК РФ требует одновременно: 1) **предмет** — сведения о частной жизни, составляющие личную или семейную тайну; 2) **деяние** — незаконное собирание или распространение этих сведений без согласия (либо распространение в публичном выступлении, произведении, СМИ); 3) **мотив** — корыстная или иная личная заинтересованность; 4) **последствие** — вред правам и законным интересам граждан.

Формулировка статьи дополнена оговоркой «за исключением случаев, предусмотренных статьей 272.1 настоящего Кодекса» (в ред. Федерального закона от 30.11.2024 № 421-ФЗ) — то есть законодатель развел составы: «компьютерный» сбор персональных данных ушел в ст. 272.1 УК РФ, «бумажно-бытовой» — остался в ст. 137 УК РФ.

В данной фабуле защита может опираться на версию о том, что незаконное собирание состоялось (данные не были раскрыты брату по воле заявителя), а вред выразился в нравственных страданиях и в необходимости принимать защитные меры (проверка кредитной истории, блокировки). Однако:

- **отсутствие «тайны»** — наиболее уязвимое место (см. раздел 2.2);
- **направление данных самому субъекту** существенно ослабляет аргумент о вреде: заявитель не утратил контроль над своей «личной тайной», поскольку он сам ее носитель (подробнее — раздел 6);
- **корыстная/личная заинтересованность** должна быть доказана: просто «узнал и переслал» — слабый мотив.

5.2. Практический вывод по версии 3

Квалификация по ст. 137 УК РФ в чистом виде («получил паспорт и СНИЛС, переслал владельцу») **маловероятна**. Она становится реалистичной, если: (а) собран расширенный набор сведений (адрес, состав семьи, здоровье, интимная жизнь); (б) установлен мотив (давление, подготовка к вымогательству, использование в интересах третьих лиц); (в) доказан вред

(например, оформленные на заявителя обязательства, отказ в кредите из-за «чужой» записи, нравственные страдания, подтвержденные лечением).

Заявление в полицию все равно имеет смысл подавать: оно (1) запускает проверку и дает официальный документ — талон-уведомление (Приказ МВД России от 29.08.2014 № 736), (2) позволяет через орган получить сведения об источнике данных, (3) фиксирует дату, с которой заявитель узнал о нарушении, и (4) при последующем мошенничестве станет доказательством того, что заявитель не давал согласия. Даже отказ в возбуждении дела (ст. 148 УПК РФ) не лишает гражданско-правовых требований.

6. Версия 4 (ключевой вопрос): является ли направление данных самому субъекту «распространением»

6.1. Разграничение режимов

Закон № 152-ФЗ различает (ст. 3): - **распространение** (п. 5) — действия, направленные на раскрытие персональных данных **неопределенному кругу лиц**; - **предоставление** (п. 6) — действия, направленные на раскрытие персональных данных **определенному лицу или определенному кругу лиц**; - **передача** как обобщающая категория, включающая распространение, предоставление и доступ (п. 3).

Субъект персональных данных уже обладает своими данными. Направление их самому субъекту **не является ни распространением (круг лиц не неопределенный), ни предоставлением (нет раскрытия третьему лицу)**. Это не «раскрытие» охраняемой информации — это ее возврат носителю. Соответственно, ст. 7 Закона № 152-ФЗ (обязанность не раскрывать третьим лицам и не распространять) в этой части **не нарушена**.

6.2. Что тогда нарушено

Нарушением является **незаконный сбор и хранение** (ст. 3, ст. 5, 6, 9 Закона № 152-ФЗ) — то есть предшествующие действия брата, а не сам факт отправки сообщения. Это важно: спор сдвигается с «он разгласил» на «он незаконно собрал и хранит», а доказывать нужно именно сбор и хранение (наличие данных у брата), а не факт их раскрытия.

Кроме того, сообщение может иметь самостоятельное значение, если: - данные направлены **в общий/групповой чат, при свидетелях, на публичную страницу** — тогда это распространение (п. 5 ст. 3 Закона № 152-

ФЗ) со всеми последствиями; - данные направлены **третьему лицу**, а не заявителю (ошибка в номере, пересылка «в семью») — тогда предоставление (п. 6 ст. 3 Закона № 152-ФЗ); - сообщение сопровождается **угрозами** — включается ст. 119 УК РФ (угроза убийством или причинением тяжкого вреда здоровью, если имелись основания опасаться осуществления), а при требованиях имущественного характера под угрозой распространения сведений, способных причинить существенный вред правам, — ст. 163 УК РФ (вымогательство; диспозиция ч. 1 охватывает угрозу распространением «иных сведений», не обязательно порочащих).

6.3. Права заявителя в этой конфигурации

1. **Требование о прекращении обработки и уничтожении копий** — ст. 17, 20, 21 Закона № 152-ФЗ (право требовать уточнения, блокирования, уничтожения незаконно полученных данных и корреспондирующая обязанность оператора прекратить неправомерную обработку и уничтожить данные) и ст. 12, п. 1 ст. 152.2 ГК РФ (пресечение действий, нарушающих право). Направляется брату письменно, с уведомлением о вручении, с указанием срока (разумно — 10 дней) и предупреждением о последствиях.
2. **Жалоба в Роскомнадзор** — ч. 2 ст. 17 и ст. 23 Закона № 152-ФЗ (уполномоченный орган рассматривает жалобы субъектов персональных данных); порядок рассмотрения — Федеральный закон от 02.05.2006 № 59-ФЗ, ст. 12 (30 дней). Жалоба подается через официальный сайт Роскомнадзора либо письменно. Практическая ценность: орган может проверить, не является ли брат оператором, а также установить источник утечки.
3. **Обращение в полицию** — по признакам ст. 137, 272, 272.1 УК РФ (см. раздел 7). Регистрация — Приказ МВД России от 29.08.2014 № 736; проверка — ст. 144–145 УПК РФ; обжалование отказа — ст. 124, 125 УПК РФ.
4. **Иск о компенсации морального вреда** — ст. 150, 151, 1099–1101 ГК РФ; ч. 2 ст. 24 Закона № 152-ФЗ: моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав и правил обработки, подлежит возмещению в соответствии с законодательством РФ, независимо от возмещения имущественного вреда и убытков. По требованиям о компенсации морального вреда, вытекающим из нарушения личных неимущественных прав, исковая давность не применяется (ст. 208 ГК РФ).
5. **Иск об удалении информации** — если данные где-либо размещены: ст. 12, п. 1 ст. 152.2 ГК РФ; при размещении в сети «Интернет» дополнительно работает механизм ст. 10.3 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите

информации» (требование об удалении ссылок на информацию, распространяемую с нарушением закона).

6.4. Практический вывод по версии 4

Сам факт отправки данных владельцу **не образует распространения** и сам по себе не создает права на крупную компенсацию: суд, скорее всего, укажет, что заявитель не лишился контроля над своими данными и не претерпел распространения. Однако: - факт сбора и хранения доказан самим сообщением — это хорошая доказательственная база для требования об уничтожении и для жалобы в Роскомнадзор; - если в сообщении есть угрозы или требования — квалификация меняется на ст. 119/163 УК РФ, и это уже совсем другой уровень реагирования; - если данные ушли третьим лицам (в чат, родне, «проверяющим») — включается полноценный режим распространения, и перспективы иска по ст. 152.2 ГК РФ и ч. 2 ст. 24 Закона № 152-ФЗ резко возрастают.

7. Версия 5 (вопрос о ст. 272 УК РФ): получение данных из информационной системы или через третьих лиц

7.1. Ст. 272 УК РФ («Неправомерный доступ к компьютерной информации»)

Состав требует: неправомерный доступ к охраняемой законом компьютерной информации, повлекший уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ/системы/сети. Санкция ч. 1 — до 2 лет лишения свободы; ч. 2 (крупный ущерб, корыстная заинтересованность) — до 4 лет; ч. 3 (группа лиц, служебное положение) — строже. Статья содержит оговорку «за исключением случаев, предусмотренных статьей 272.1 настоящего Кодекса» (в ред. Федерального закона от 30.11.2024 № 421-ФЗ).

Применимость: - **да** — если брат получил доступ к вашему телефону/компьютеру/аккаунту с преодолением защиты (пароль, биометрия, двухфакторная аутентификация), скопировал данные; либо если он через свое служебное положение вошел в ведомственную базу и скопировал сведения (тогда же возможны ст. 285, 286 УК РФ); - **нет** — если он физически взял бумажный паспорт, сфотографировал его или переписал данные из бумажной копии: компьютерная информация как предмет отсутствует. В этом случае работает «бумажная» линия (ст. 152.2 ГК РФ, при наличии признаков — ст. 137 УК РФ).

7.2. Ст. 272.1 УК РФ (введена Федеральным законом от 30.11.2024 № 421-ФЗ)

Диспозиция ч. 1: незаконное использование и (или) передача (распространение, предоставление, доступ), сбор и (или) хранение компьютерной информации, содержащей персональные данные, **полученной путем неправомерного доступа к средствам ее обработки, хранения или иного вмешательства в их функционирование либо иным незаконным путем**, за исключением деяний, предусмотренных ч. 2 (данные несовершеннолетних, специальные категории, биометрия). Санкция ч. 1 — штраф до 300 тыс. руб. либо принудительные работы/лишение свободы до 4 лет; ч. 2 — до 700 тыс. руб. и до 5 лет; ч. 3 — при корыстной заинтересованности или крупном ущербе.

Применимость к факту: - паспортные данные и СНИЛС **не относятся** к специальным категориям (ст. 10 Закона № 152-ФЗ) и не являются биометрическими (ст. 11), поэтому ч. 2 неприменима — только ч. 1 или ч. 3; - ключевой вопрос — **«незаконный путь» получения**. Если брат получил данные через неправомерный доступ к информационной системе (например, база МФЦ, банковская АБС, база оператора связи, «Госуслуги») либо через третье лицо, которое получило их неправомерно, формально признаки ч. 1 ст. 272.1 УК РФ усматриваются; - **но**: практика по ст. 272.1 УК РФ на момент подготовки разбора не сформирована (статья действует с декабря 2024 года), а доктрина и правоприменение спорят о том, охватывает ли «хранение» бытовое сохранение данных на личном устройстве и требуется ли специальная цель. Для бытового семейного случая высок риск прекращения по ч. 2 ст. 14 УК РФ (малозначительность) либо отказа в возбуждении; - отдельная сложность — **доказывание способа получения**. Сам по себе факт, что брат «знает» данные, не доказывает неправомерный доступ.

7.3. Административная ответственность при получении данных через третьих лиц

- Если данные передал работник оператора (банка, МФЦ, оператора связи), ответственность несут: работник — по ст. 13.14 КоАП РФ (разглашение информации с ограниченным доступом лицом, получившим доступ в связи с исполнением служебных обязанностей) и потенциально по ст. 272.1 УК РФ; оператор — по ст. 13.11 КоАП РФ (в том числе по составам об утечках, ч. 12–14, в ред. Федерального закона от 30.11.2024 № 420-ФЗ) и по ст. 7, 19 Закона № 152-ФЗ.
- Если данные получены из открытых источников (например, вы сами их где-то публиковали) — противоправность сбора снимается: сведения стали

общедоступными (абз. 2 п. 1 ст. 152.2 ГК РФ; п. 10 ч. 2 ст. 6 Закона № 152-ФЗ — обработка данных, доступ к которым предоставлен самим субъектом).

7.4. Практический вывод по версии 5

- Ст. 272 УК РФ «включается» только при доступе к устройству/системе с преодолением защиты и копированием. Ст. 272.1 УК РФ — при получении данных из информационной системы или через цепочку третьих лиц; это наиболее перспективная линия, если удастся доказать источник.
- Ст. 13.11 КоАП РФ в отношении брата-физлица малоперспективна, но **в отношении оператора-источника** — вполне реальна, и именно там лежит экономический смысл жалобы в Роскомнадзор.
- Порядок документирования: заявление в полицию (регистрация по Приказу МВД № 736) → проверка в порядке ст. 144–145 УПК РФ → при необходимости обжалование по ст. 124, 125 УПК РФ; параллельно — жалоба в Роскомнадзор (ст. 23 Закона № 152-ФЗ) с приложением скриншотов и хронологии.

8. Порядок действий и фиксация доказательств (общий для всех версий)

8.1. Немедленная фиксация (первые дни)

1. **Сохранить сообщение в исходном виде:** не удалять чат, сделать скриншоты с видимыми датой, временем, номером отправителя; экспортировать переписку (в WhatsApp/Telegram — функция экспорта чата), сохранить на отдельный носитель и в облако.
2. **Нотариальное обеспечение доказательств** — осмотр письменных доказательств и (или) информации в сети «Интернет»: ст. 102–103 Основ законодательства РФ о нотариате. Это самый устойчивый в суде способ фиксации переписки, если есть риск ее удаления.
3. **Судебное обеспечение доказательств** — ст. 64–66 ГПК РФ (если спор уже назревает).
4. **Детализация соединений** — у оператора связи можно получить только по судебному запросу, поскольку сведения о переписке относятся к тайне связи (ст. 63 Федерального закона от 07.07.2003 № 126-ФЗ «О связи»). Поэтому в иске/жалобе имеет смысл сразу заявлять ходатайство об истребовании.
5. **Письменное требование брату** (ст. 17, 20, 21 Закона № 152-ФЗ; ст. 12, п. 1 ст. 152.2 ГК РФ): прекратить обработку, уничтожить все копии и производные (фото, сканы, записи в блокнотах, файлы), подтвердить

уничтожение. Отправлять заказным письмом с описью вложения и уведомлением; копию — себе. Отсутствие ответа само по себе станет доказательством.

8.2. Обращения

Куда	Основание	Что дает
Полиция (заявление о преступлении)	ст. 137, 272, 272.1 УК РФ; ст. 141–145 УПК РФ; Приказ МВД № 736	Проверка источника данных, официальная фиксация, потенциальное уголовное дело
Роскомнадзор	ч. 2 ст. 17, ст. 23 Закона № 152-ФЗ; ст. 12 Закона № 59- ФЗ	Проверка оператора- источника, возможное привлечение по ст. 13.11 КоАП РФ
Прокуратура	ст. 10 Федерального закона от 17.01.1992 № 2202-1	Надзор за проверкой по заявлению
Суд	ст. 150, 151, 1099–1101 ГК РФ; ч. 2 ст. 24 Закона № 152-ФЗ; ст. 152.2 ГК РФ	Компенсация морального вреда, запрет обработки, удаление информации

При подаче иска о компенсации морального вреда нужно учитывать правило ст. 333.36 НК РФ: освобождение от госпошлины предусмотрено для требований о возмещении вреда, причиненного преступлением; в остальных случаях пошлина уплачивается в общем порядке.

8.3. Состав доказывания по иску

1) факт обработки данных братом (сообщение, содержание данных в тексте); 2) отсутствие согласия (презумпция — согласие должен доказывать тот, кто на него ссылается, ст. 9 Закона № 152-ФЗ: согласие должно быть конкретным, предметным, информированным и сознательным); 3) противоправность (отсутствие законного основания по ст. 6 Закона № 152-ФЗ или нарушение ст. 152.2 ГК РФ); 4) нравственные страдания (сами по себе презюмируются при доказанности нарушения, но размер зависит от их глубины: практика по небольшим «бытовым» делам — обычно от 1 000 до 15 000 руб.; значимые суммы взыскиваются при доказанном распространении и материальных последствиях).

9. Риск мошенничества с паспортом и СНИЛС: превентивные меры

Даже если брат действовал без злого умысла, сам факт «утечки» создает риск использования данных для оформления займов, сим-карт, регистраций. Рекомендуемый набор действий:

1. **Проверить кредитную историю** во всех бюро кредитных историй — по два бесплатных отчета в год в каждом БКИ (ст. 8 Федерального закона от 30.12.2004 № 218-ФЗ «О кредитных историях»), удобнее всего через «Госуслуги». При обнаружении чужих записей — заявление в БКИ об оспаривании (ст. 8 Закона № 218-ФЗ) и в полицию.
2. **Установить самозапрет на заключение договоров потребительского кредита (займа)** — механизм, действующий с 1 марта 2025 года (поправки в Закон № 218-ФЗ и Закон о потребительском кредите), подается через «Госуслуги», снимается тоже через «Госуслуги» (с задержкой).
3. **Проверить зарегистрированные на вас сим-карты и абонентские номера** (через «Госуслуги»/операторов).
4. **Усилить защиту учетной записи «Госуслуги»:** двухфакторная аутентификация, контроль активных сессий, смена пароля; при подозрении на доступ — заявление в Минцифры/техподдержку и в полицию.
5. **Уведомить банки**, где у вас счета, о компрометации данных (особенно если брат знает и кодовое слово).
6. **Проверить ЕГРН** на предмет регистрации прав/обременений, ФССП — на предмет исполнительных производств.
7. **Не пытаться «заменить паспорт»** по факту утечки: замена производится по основаниям Положения о паспорте гражданина РФ (утв. Постановлением Правительства РФ от 08.07.1997 № 828) — утрата, хищение, изменение данных, непригодность; сам факт осведомленности третьего лица основанием не является. СНИЛС также не меняется.

10. Сводные практические выводы по каждой версии

Версия	Ключевое основание	Перспектива
1. Бытовое получение, личные/семейные нужды	п. 1 ч. 2 ст. 1 Закона № 152-ФЗ (исключение); ст. 152.2 ГК РФ	Уголовная и административная ответственность маловероятны; рабочий инструмент — письменное требование об уничтожении копий +

Версия	Ключевое основание	Перспектива
		иск по ст. 152.2 ГК РФ (небольшая компенсация)
2. Получение вне личных/семейных нужд или с нарушением прав	ст. 3, 5, 6, 7, 9, 21 Закона № 152-ФЗ; ч. 1–2 ст. 13.11 КоАП РФ	Реальна жалоба в Роскомнадзор; эффективнее привлечь оператора-источник утечки; срок давности по КоАП — 1 год
3. Незаконное собирание сведений о частной жизни	ч. 1 ст. 137 УК РФ	Маловероятно без расширенного набора сведений, мотива и доказуемого вреда; заявление в полицию все равно целесообразно
4. Направление данных самому субъекту	п. 3, 5, 6 ст. 3, ст. 7 Закона № 152-ФЗ	Распространения нет; нарушение — в сборе/хранении; права: требование уничтожения, жалоба в РКН, моральный вред (умеренный)
5. Получение из ИС / через третьих лиц	ст. 272, 272.1 УК РФ; ст. 13.14, 13.11 КоАП РФ	Наиболее перспективная уголовная линия при доказанном источнике; практика по ст. 272.1 УК РФ еще не сложилась; ключ — установление источника через полицию и РКН

Итоговая рекомендация по последовательности: (1) фиксация сообщения и нотариальный осмотр при риске удаления; (2) письменное требование брату об уничтожении копий; (3) одновременная подача заявления в полицию и жалобы в Роскомнадзор; (4) превентивные меры по кредитной истории и самозапрету; (5) по результатам проверки — решение об иске о компенсации морального вреда (ст. 151, 1099–1101 ГК РФ; ч. 2 ст. 24 Закона № 152-ФЗ) и/или об удалении информации (ст. 152.2 ГК РФ). Если в сообщении прозвучат угрозы или требования — немедленно переквалифицировать реагирование на ст. 119/163 УК РФ.

11. Список использованных нормативных источников

Нормативные правовые акты 1. Конституция РФ — ст. 23, 24 (право на неприкосновенность частной жизни, тайну переписки). 2. Гражданский кодекс РФ, часть первая — ст. 12 (способы защиты), 150 (нематериальные блага), 151 (компенсация морального вреда), 152.1, 152.2 (охрана частной жизни), 208 (требования, на которые исковая давность не распространяется), 1064 (общие

основания ответственности за вред). 3. Гражданский кодекс РФ, часть вторая — ст. 1099, 1100, 1101 (компенсация морального вреда, ее размер). 4. Уголовный кодекс РФ — ст. 14 (понятие преступления, ч. 2 — малозначительность), 119 (угроза), 137 (нарушение неприкосновенности частной жизни), 138, 159 (мошенничество), 163 (вымогательство), 272 (неправомерный доступ к компьютерной информации), 272.1 (незаконные использование, передача, сбор, хранение компьютерной информации, содержащей персональные данные), 285, 286. 5. Кодекс РФ об административных правонарушениях — ст. 4.5 (сроки давности), 13.11 (нарушение законодательства о персональных данных, в том числе ч. 1, 2; ч. 12-14 в ред. Федерального закона от 30.11.2024 № 420-ФЗ), 13.14 (разглашение информации с ограниченным доступом), 28.1 (поводы к возбуждению дела). 6. Уголовно-процессуальный кодекс РФ — ст. 124, 125, 141-145, 148. 7. Гражданский процессуальный кодекс РФ — ст. 64-66 (обеспечение доказательств), 131-132. 8. Налоговый кодекс РФ — ст. 333.36 (льготы по госпошлине). 9. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» — ст. 1 (ч. 2 п. 1 — изъятие для личных и семейных нужд), 3 (понятия: персональные данные, оператор, обработка, распространение, предоставление, блокирование, уничтожение, обезличивание), 5 (принципы обработки), 6 (условия обработки), 7 (конфиденциальность), 9 (согласие), 10 (специальные категории), 11 (биометрические данные), 10.1 (согласие на распространение), 14, 17 (права субъекта), 18.1, 19 (меры защиты), 20, 21 (обязанности оператора, уничтожение), 22 (уведомление), 23 (уполномоченный орган), 24 (ответственность, ч. 2 — моральный вред). 10. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» — ст. 10.3. 11. Федеральный закон от 07.07.2003 № 126-ФЗ «О связи» — ст. 63 (тайна связи). 12. Федеральный закон от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации» — ст. 12. 13. Федеральный закон от 30.12.2004 № 218-ФЗ «О кредитных историях» — ст. 8 (право на кредитный отчет, оспаривание записи); поправки о самозапрете на кредиты, действующие с 01.03.2025. 14. Федеральный закон от 30.11.2024 № 421-ФЗ (введение ст. 272.1 УК РФ, корректировка ст. 137, 272 УК РФ). 15. Федеральный закон от 30.11.2024 № 420-ФЗ (ужесточение ст. 13.11 КоАП РФ, составы об утечках). 16. Федеральный закон от 02.07.2013 № 142-ФЗ (введение ст. 152.2 ГК РФ). 17. Постановление Правительства РФ от 08.07.1997 № 828 «Об утверждении Положения о паспорте гражданина Российской Федерации...». 18. Приказ МВД России от 29.08.2014 № 736 «Об утверждении Инструкции о порядке приема, регистрации и разрешения в территориальных органах МВД России заявлений и сообщений о преступлениях...». 19. Основы законодательства РФ о нотариате — ст. 102, 103 (обеспечение доказательств).

Судебная практика и разъяснения 20. Постановление Пленума Верховного Суда РФ от 15.11.2022 № 38 (применение законодательства о персональных данных: понятие оператора, основания обработки, компенсация морального вреда). 21. Постановление Пленума Верховного Суда РФ от 23.06.2015 № 25 (применение положений ГК РФ о возмещении вреда, в том числе морального). 22. Постановление Пленума Верховного Суда РФ от 20.12.1994 № 10 (компенсация морального вреда; исковая давность по требованиям из личных неимущественных прав). 23. Постановление Пленума Верховного Суда РФ от 24.02.2005 № 3 (защита чести, достоинства и деловой репутации — в части разграничения распространения сведений и их предоставления).

Документ подготовлен для внутренней редакционной публикации и не заменяет индивидуальную правовую консультацию по конкретному делу; при наличии признаков мошенничества, угроз или вымогательства требуется незамедлительное обращение в правоохранительные органы.