Дата поступления рукописи в редакцию: 18.02.2026 г.
Дата принятия рукописи в печать: 12.03.2026 г.
DOI: 10.24412/2782-3849-2026-2-214-223

АЗИЗОВ Фуад Эльдарович,
Аспирант кафедры уголовного права и правоохранительной деятельности,
Астраханский государственный университет им. В.Н. Татищева, г. Астрахань, Российская Федерация,
e-mail: Fuad.azizov.93@list.ru

Научный руководитель:
НОВИКОВ Алексей Валерьевич,
Профессор, Академик РАЕ,
доктор педагогических наук, кандидат юридических наук,
Астраханский государственный университет им. В.Н. Татищева,
e-mail: mail@law-books.ru

НОВЕЛЛЫ ГЛАВЫ 28 УК РФ О ПЕРЕДАЧЕ АБОНЕНТСКИХ НОМЕРОВ И ДАННЫХ АВТОРИЗАЦИИ: ПРОБЛЕМЫ КВАЛИФИКАЦИИ

Аннотация. *В статье анализируются новеллы законодательства Российской Федерации, принятые в целях противодействия преступлениям в сфере ИКТ: дополнение перечня отягчающих обстоятельств положением о совершении преступления с использованием программно-аппаратных средств доступа к информационным ресурсам и информационно-телекоммуникационным сетям, доступ к которым ограничен. Исследуются новые составы преступлений, предусмотренные ст. 274.4 и 274.5 УК РФ, направленные на пресечение организации деятельности по незаконной передаче абонентских номеров и информации, необходимой для регистрации и (или) авторизации пользователей в сети «Интернет». Параллельно рассматриваются административно-правовые составы ст. 13.29.1 и 13.29.2 КоАП РФ, закрепляющие ответственность за аналогичные действия при отсутствии признаков уголовно наказуемого деяния, а также исключения, призванные вывести из сферы наказуемого бытовые и правомерные ситуации передачи номера/данных [4; 5]. Обосновывается, что данные изменения являются реакцией на формирование теневого рынка «цифровых посредников» (SIM-карты, виртуальные номера, аккаунты и учетные данные), обеспечивающего анонимизацию и затрудняющего установление лица, фактически совершающего дистанционные преступления. Сформулированы предложения по снижению рисков расширительного толкования отягчающего обстоятельства и по уточнению критериев разграничения уголовной и административной ответственности с учётом доктринальных предостережений о «цифровой казуализации» уголовного закона [8; 9].*

Ключевые слова: *цифровизация преступности; преступления в сфере компьютерной информации; программно-аппаратные средства доступа; VPN; обстоятельства, отягчающие наказание; ст. 63 УК РФ; ст. 274.4, 274.5 УК РФ; ст. 13.29.1, 13.29.2 КоАП РФ; абонентский номер; регистрация и авторизация; цифровые посредники.*

AZIZOV Fuad Eldarovich,
Postgraduate Student,
Department of Criminal Law and Law Enforcement
Astrakhan State University named after V.N. Tatishchev.
Astrakhan, Russian Federation

Scientific supervisor:
NOVIKOV Alexey Valerevich,
Professor, Academician of RAE,
Doctor of Pedagogical Sciences, Candidate of Law,
Astrakhan State University named after V.N. Tatishchev

NOVEL AMENDMENTS TO CHAPTER 28 OF THE CRIMINAL CODE OF THE RUSSIAN FEDERATION ON THE TRANSFER OF SUBSCRIBER NUMBERS AND AUTHENTICATION DATA: ISSUES OF LEGAL QUALIFICATION

Annotation. *The paper examines recent amendments to Russian law aimed at countering ICT-enabled crime, including the aggravating circumstance for committing a crime using software-hardware tools enabling access to information resources and telecommunication networks with restricted access. It analyzes new Criminal Code provisions (Articles 274.4 and 274.5) targeting the organization of illegal transfer of mobile subscriber numbers and credentials required for online registration/authorization. The study also addresses administrative offences under Articles 13.29.1 and 13.29.2 of the Administrative Code, applicable in the absence of elements of a crime, and highlights statutory exclusions designed to cover lawful or everyday transfers [4; 5]. The article argues that these measures respond to the growth of "digital intermediaries" markets facilitating anonymity and complicating the identification of actual offenders. Recommendations are proposed to prevent overly broad interpretation and to improve the delineation between criminal and administrative liability in line with scholarly critiques of excessive "digital casuistry" in criminal law [8; 9].*

Key words: *digitalization of crime; computer-related offences; restricted-access tools; VPN; aggravating circumstances; Article 63 of the Criminal Code; Articles 274.4, 274.5; Articles 13.29.1, 13.29.2; subscriber number; registration and authorization; digital intermediaries.*

1. Введение

Цифровая трансформация общественных отношений в России и мире сопровождается изменением структуры преступности: значительная часть противоправных деяний опосредуется цифровой инфраструктурой (сети связи, учётные записи, идентификаторы, коды подтверждения), что усложняет установление фактического субъекта преступления и доказывание. В этой связи в 2025 г. законодатель предпринял комплексную корректировку уголовно-правовых и административно-правовых механизмов противодействия преступлениям в информационной сфере, закрепив новые элементы дифференциации ответственности и превентивного воздействия на инфраструктуру анонимизации.

К ключевым новеллам относится включение в перечень отягчающих обстоятельств положения о совершении преступления с использованием программно-аппаратных средств доступа к информационным ресурсам и информационно-телекоммуникационным сетям, доступ к которым ограничен (п. «ф» ч. 1 ст. 63 УК РФ). Данная формула является технологически широкой: она прямо не называет VPN, но на практике может охватывать и VPN-сервисы как частный случай средств доступа к ограниченным ресурсам/сетям, что требует особой аккуратности толкования.

Одновременно УК РФ дополнен статьями 274.4 и 274.5, устанавливающими ответственность за организацию деятельности по незаконной передаче абонентских номеров и информации, необходимой для регистрации и (или) авторизации пользователя в сети «Интернет», а также за участие в такой деятельности [2; 3]. Комплементарные нормы появились в КоАП РФ — ст. 13.29.1 и 13.29.2, предусматривающие административную ответственность за передачу абонентских номеров и данных для регистрации/авторизации при отсутствии признаков уголовно наказуемого деяния и с учетом специальных исключений, защищающих бытовые и правомерные ситуации [4; 5].

Цель настоящей статьи — комплексно проанализировать указанные изменения, оценить их место в системе противодействия преступлениям в сфере ИКТ и выявить риски расширительного толкования, прежде всего в части «цифровых» отягчающих и квалифицирующих признаков.

Для достижения цели поставлены задачи: (1) раскрыть уголовно-правовой смысл п. «ф» ч. 1 ст. 63 УК РФ и обозначить критерии его ограничительного толкования; (2) проанализировать объект и объективную сторону ст. 274.4–274.5 УК РФ как составов, ориентированных на «инфраструктурные» формы содействия цифровой преступности; (3) показать разграничение УК и КоАП (ст. 274.4–274.5 УК РФ и ст. 13.29.1–13.29.2 КоАП РФ) и указать проблемные зоны правоприменения.

2. Методология и источниковая база

Методологическую основу исследования составляют диалектический метод, формально-юридический и системно-структурный методы, а также элементы сравнительного анализа уголовно-правовых конструкций (отягчающее обстоятельство — квалифицирующий признак — самостоятельный состав). Формально-юридический метод применяется при анализе нормативного текста ФЗ от 31.07.2025 № 282-ФЗ и взаимосвязанных норм УК РФ и КоАП РФ, включая приме-

чания к административным составам как инструмент законодательного «выведения» социально допустимых ситуаций из сферы наказуемого.

Источниковую базу составляют: (1) Федеральный закон от 31.07.2025 № 282-ФЗ, которым внесены изменения в УК РФ и КоАП РФ (включая п. «ф» ч. 1 ст. 63 УК РФ и ст. 274.4–274.5 УК РФ); (2) тексты ст. 13.29.1 и 13.29.2 КоАП РФ [4; 5]; (3) доктринальные публикации, посвящённые пределам «цифровой» модернизации уголовного закона и рискам цифровой казуализации [8; 9; 10; 11; 12]. Отдельно учитываются разъяснительные материалы прокуратуры как официальный ориентир для единообразного понимания новелл об ответственности за передачу данных для регистрации/авторизации и близких составов (в той мере, в какой они фиксируют общую направленность законодательного регулирования).

3. Теоретические рамки: «цифровая казуализация» и принцип технологической нейтральности

В научной литературе обоснована позиция, согласно которой появление нового (информационного) способа совершения преступления само по себе не означает априорного роста общественной опасности по сравнению с традиционными способами; часто оно отражает отставание механизмов социального контроля от развития технологий. Из этого следует методологически важный вывод: уголовно-правовая модернизация не должна автоматически сводиться к конструированию «цифровых двойников» традиционных запретов и к закреплению максимально широких «цифровых» признаков без доказуемой добавочной опасности.

Русскевич Е.А. последовательно указывает, что цифровой способ совершения преступления далеко не всегда свидетельствует об увеличении общественной опасности деяния, а неоправданная цифровая казуализация приводит к нарушению сложившихся моделей законодательного определения отдельных преступлений и противоречит доктринальным представлениям о пределах объективной стороны.

В прикладном измерении это означает необходимость отличать случаи, когда технология является лишь нейтральной средой (например, стандартные средства защиты трафика), от ситуаций, когда технология выступает функционально значимым способом достижения преступного результата либо способом обхода установленных ограничений доступа.

Применительно к анализируемым новеллам эта теоретическая рамка позволяет поставить вопрос о допустимых пределах расширения «цифрового» инструментария уголовного права: с одной стороны, криминализация организации деятельности по передаче идентификаторов может рассматриваться как ответ на устойчивую инфраструктурную практику, обеспечивающую анонимизацию; с другой стороны, универсализация «средств доступа» в качестве отягчающего обстоятельства требует особенно точного толкования, чтобы не подорвать технологическую нейтральность уголовного закона [8; 9].

4. Постановка проблемы исследования

Правоприменительная интрига п. «ф» ч. 1 ст. 63 УК РФ заключается в том, что норма использует открытую технологическую формулу («программно-аппаратные средства доступа…»), не называя конкретных решений (например, VPN) и тем самым потенциально расширяя пределы усмотрения при назначении наказания.

Чтобы избежать расширительного толкования, целесообразно исходить из функционального критерия: отягчение должно применяться тогда, когда использование средства доступа было направлено на получение доступа к ограниченному ресурсу/сети и находилось в причинной связи со способом совершения преступления (а не являлось сопутствующей настройкой безопасности или стандартным элементом корпоративной инфраструктуры).

В отношении ст. 274.4–274.5 УК РФ основная проблема смещается в плоскость разграничения уголовной и административной ответственности: уголовный закон ориентирует на «организацию деятельности» и наличие корысти либо цели совершения иного преступления, тогда как КоАП закрепляет ответственность за передачу номера/данных при отсутствии признаков преступления и одновременно содержит примечания-исключения для социально допустимых ситуаций [2; 3; 4; 5].

Следовательно, для обеспечения справедливости и единообразия практики требуется конкретизация критериев «организации деятельности» (устойчивость, повторяемость, распределение ролей, извлечение дохода, использование каналов сбыта), иначе возрастает риск как избыточной криминализации пограничных случаев, так и ухода организованных схем в административную плоскость путем дробления на формально разрозненные эпизоды.

5. Совершение преступления с использованием программно-аппаратных средств доступа к ресурсам/сетям с ограниченным доступом как отягчающее обстоятельство (п. «ф» ч. 1 ст. 63 УК РФ)

5.1. Нормативное содержание и место в системе ст. 63 УК РФ

Федеральным законом от 31.07.2025 № 282-ФЗ ч. 1 ст. 63 УК РФ дополнена пунктом «ф»,

предусматривающим отягчающее обстоятельство — совершение преступления с использованием программно-аппаратных средств доступа к информационным ресурсам и информационно-телекоммуникационным сетям, доступ к которым ограничен. Включение указанного пункта в ст. 63 УК РФ означает придание универсального значения определённому способу совершения преступления при назначении наказания: применимость не привязана к конкретным составам Особенной части и потенциально охватывает широкий круг деяний.

Содержательно формула «программно-аппаратные средства доступа…» не равна термину «VPN»: VPN-сервисы могут выступать частным случаем таких средств, но сама норма оперирует функциональным описанием, а не перечнем технологий. Отсюда вытекает, что правоприменитель должен установить не «факт наличия VPN», а причинно-функциональную роль средства в обеспечении доступа именно к ограниченному ресурсу/сети.

Отдельно важно учитывать момент вступления новеллы в силу: п. «ф» ч. 1 ст. 63 УК РФ введён 282-ФЗ и действует с 01.09.2025. Следовательно, применение данного отягчающего возможно лишь по преступлениям, совершённым после указанной даты (в пределах общих правил действия уголовного закона во времени).

5.2. Что именно должен доказать суд (минимальный «порог» применения)

Норма говорит именно об использовании средств доступа к ресурсам/сетям, «доступ к которым ограничен». Значит, логически необходимы три элемента установления (как минимум на уровне фактов дела):

1. Наличие ограничения доступа к соответствующему ресурсу/сети (то есть речь не о любом интернет-ресурсе, а о таком, где доступ ограничен).
2. Применение программно-аппаратного средства как инструмента доступа (а не просто его установка, наличие подписки, включённость «по умолчанию» и т.п.).
3. Связь между использованием средства и совершением преступления (использование должно быть частью способа совершения, а не посторонним фоном).

Эта конструкция по смыслу отличается от ситуаций, когда лицо просто совершает преступление «с использованием сети Интернет»: здесь законодатель выделяет более узкий и «усиленный» способ — обход или преодоление ограничения доступа посредством специализированного инструментария.

Поэтому корректная линия ограничительного толкования — не подменять предмет доказывания формулой «использовал Интернет/анонимайзер», а устанавливать функциональную роль средства именно в доступе к ограниченному сегменту цифровой среды.

5.3. Соотношение с квалифицирующими признаками «с использованием сети «Интернет»»

Пункт «ф» ч. 1 ст. 63 УК РФ введён как общее отягчающее обстоятельство и применяется на стадии назначения наказания независимо от того, предусмотрен ли в конкретной статье Особенной части признак «с использованием информационно-телекоммуникационных сетей (в том числе сети „Интернет»)».

Тем самым возникает риск фактического «накопления» цифровых признаков: деяние может быть квалифицировано по составу с «интернет-признаком», а дополнительно — отягчено по п. «ф» ст. 63 УК РФ. Чтобы сохранить соразмерность, целесообразно п. «ф» применять лишь при наличии дополнительного по сравнению с обычным использованием сети обстоятельства — доступа к ограниченному ресурсу/сети посредством специального средства. Иначе отягчающее начнёт «дублировать» типовые квалифицирующие признаки, не добавляя самостоятельного криминально-правового смысла.

5.4. Риски расширительного толкования

Законодатель использовал широкую технологическую формулу («программно-аппаратные средства доступа…») без легального определения, при этом связал её с категорией «доступ к которым ограничен». В правоприменении это создаёт минимум три зоны неопределённости:

- Что считать «средством доступа»: только инструменты обхода блокировок, или также корпоративные шлюзы, прокси, защищённые каналы удалённого доступа, средства шифрования трафика.
- Что считать «ограниченным доступом»: государственные блокировки; ограничения по географическому признаку; авторизационные барьеры; платный доступ; ограничения по внутренним правилам площадки.
- Где граница между «использованием средства» и «его наличием» (например, включён системный VPN на устройстве, но преступление совершено в офлайн-контексте).

С учётом изложенного предлагаемый критерий (для доктрины и практики): п. «ф» ч. 1 ст. 63 УК РФ подлежит применению, когда установлено, что (а) имело место объективное ограничение доступа к ресурсу/сети, (б) лицо осознанно использовало специальное программно-аппаратное средство именно для преодоления такого ограничения, (в) это использование было функционально значимым элементом способа совершения преступления.

Такое толкование сохраняет идею законодателя (усилить ответственность за «обход ограничений» как криминогенно значимый способ) и одновременно удерживает норму от превращения в «универсальное цифровое отягчение» за любую ИБ-настройку.

6. Новые составы преступлений: ст. 274.4 и 274.5 УК РФ (уголовно-правовая реакция на рынок «цифровых идентификаторов»)

6.1. Законодательная логика и предмет криминализации

Федеральным законом от 31.07.2025 № 282-ФЗ глава 28 УК РФ дополнена статьями 274.4 и 274.5 (вместе со ст. 274.3), вступившими в силу с 01.09.2025 [1; 2; 3]. Смысл новелл заключается в криминализации не «конечного» дистанционного преступления (например, мошенничества), а инфраструктуры, которая обеспечивает преступникам анонимность и оперативную заменяемость цифровых следов — прежде всего через оборот SIM-карт/номеров и учетных данных/аккаунтов [2; 3].

Разъяснительные материалы прокуратуры прямо увязывают введение ст. 274.4 УК РФ с многочисленными фактами использования номеров, зарегистрированных на третьих лиц, в дистанционном мошенничестве. Это важно для постановки вопроса о превентивной природе составов: законодатель стремится «перерезать» канал ресурсного обеспечения дистанционных схем до наступления имущественного ущерба.

6.2. Статья 274.4 УК РФ: объект, предмет, объективная сторона, санкции

Статья 274.4 УК РФ устанавливает ответственность за организацию деятельности по передаче абонентских номеров, выделенных по договорам подвижной радиотелефонной связи (или предоставленных в пользование в рамках таких договоров), иным лицам в нарушение требований законодательства Российской Федерации, если деяния совершены из корыстной заинтересованности либо в целях совершения иного преступления.

Санкция ч. 1 ст. 274.4 УК РФ предусматривает альтернативно: штраф до 700 тыс. руб. (или в размере дохода до 2 лет) с возможным лишением права занимать должности/заниматься деятельностью до 2 лет, либо принудительные работы до 3 лет, либо лишение свободы до 3 лет.

Часть 2 ст. 274.4 УК РФ вводит самостоятельную ответственность за участие в деятельности, указанной в ч. 1, и предусматривает штраф до 300 тыс. руб. (или доход до 1 года), либо принудительные работы до 2 лет, либо лишение свободы до 2 лет.

Прокуратура в разъяснениях подчёркивает, что обязательным условием состава является наличие корыстной заинтересованности либо совершение деяния в целях совершения иного преступления, а максимальное наказание — до 3 лет лишения свободы.

Непосредственный объект состава целесообразно раскрывать как общественные отношения, обеспечивающие установленный порядок идентификации абонентов и пользователей услуг связи, а также устойчивость правового режима оборота абонентских номеров. Предмет — абонентский номер (и фактически связанная с ним SIM-карта/право пользования услугами связи), выделенный по договору связи; это соответствует буквальному тексту диспозиции.

Ключевой дискуссионный элемент — признак «организация деятельности». Из текста следует, что уголовно наказуемой является не любая передача номера, а именно организационный, «инфраструктурный» уровень: создание/координация схемы передачи, подбор участников, каналы сбыта, распределение функций, систематичность. Именно на этом уровне новелла адресует феномен «цифровых посредников»: организаторы извлекают доход из предоставления ресурса анонимизации (номеров), при этом сами могут не совершать «основное» дистанционное преступление.

6.3. Статья 274.5 УК РФ: «учетные данные» как криминогенный ресурс

Статья 274.5 УК РФ построена по сходной логике, но предметом выступает информация, необходимая для регистрации и (или) авторизации пользователя сети «Интернет» для получения доступа к функциональным возможностям информационного ресурса. Состав ч. 1 описывает организацию деятельности по передаче такой информации иным лицам при наличии корыстной заинтересованности либо цели совершения иного преступления, а ч. 2 — участие в соответствующей деятельности.

В прикладном плане речь идет об обороте логинов/паролей, кодов подтверждения, комплектов данных для создания аккаунтов и иных сведений, позволяющих третьим лицам получать управляемые учетные записи, которые затем используются в мошеннических и иных схемах. Важная особенность конструкции — ориентация на пресечение именно «сервиса»/схемы передачи учетных данных, а не единичной передачи пароля «по доверенности» (последняя может подпадать под исключения административного регулирования при соблюдении условий законности).

6.4. «Организация деятельности» и «участие»: как разграничивать роли

Обе статьи (274.4 и 274.5) задают двузвенную модель: организаторы (ч. 1) и участники (ч. 2) [2; 3]. Это требует в правоприменении отделять:

– Организацию деятельности (управление схемой: подбор номеров/данных, каналы передачи, контроль качества, расчеты, распределение ролей).
– Участие (исполнение отдельных функций внутри схемы: регистрация SIM на подставных лиц, получение кодов подтверждения, массовая регистрация аккаунтов, курьерская доставка, прием платежей и т.п.).

Прокурорские разъяснения по ст. 274.4 показывают практический вектор: уголовное преследование должно быть направлено на пресечение организованных схем, обусловленных корыстным интересом или преступными целями. С точки зрения принципа справедливости важно, чтобы ответственность «низового звена» (курьеры/регистраторы) дифференцировалась с учетом реального объема осведомлённости о целях схемы и фактической роли в её устойчивом функционировании.

6.5. Соотношение с КоАП РФ: где «граница» между преступлением и проступком

Законодатель построил связку УК и КоАП как систему «ступеней» общественной опасности: при отсутствии признаков уголовно наказуемого деяния действует КоАП (ст. 13.29.1 и 13.29.2), а при наличии признаков организованной деятельности + корысти/цели иного преступления — УК [2; 3; 4; 5].

Статья 13.29.1 КоАП РФ устанавливает ответственность за незаконную передачу абонентского номера иному лицу при отсутствии признаков преступления, при этом прямо закрепляет исключение: не образует правонарушения безвозмездная кратковременная передача номера в личных целях. Этот элемент важен для практики: он позволяет отграничить бытовое «дать позвонить» или передать телефон члену семьи на короткое время от социально опасных схем оборота номеров.

Статья 13.29.2 КоАП РФ аналогично устанавливает ответственность за передачу информации для регистрации/авторизации при отсутствии признаков преступления и закрепляет исключение: не является правонарушением передача таких данных другому лицу для правомерного использования функциональных возможностей ресурса по поручению пользователя или с его согласия.

Таким образом, законодатель прямо «закрыл» наиболее типичную легальную ситуацию — когда пользователь разрешает иному лицу действовать от его имени (например, администратору/помощнику) при правомерном использовании ресурса.

В сумме эти примечания КоАП образуют важный ориентир и для уголовно-правового толкования: если ситуация очевидно подпадает под законодательно признанные модели социально допустимого поведения, ее криминализация через расширительное понимание «организации деятельности» или «корыстной заинтересованности» будет противоречить логике дифференциации ответственности, заложенной в пакете 2025 года [2; 3; 4; 5].

6.6. Предложения по правоприменительным критериям

Для повышения определенности разграничения уголовной и административной ответственности целесообразно использовать совокупность индикаторов «организации деятельности» (каждый по отдельности не является решающим, но в системе повышает доказанность):

1. Повторяемость и устойчивость (многоэпизодность, стабильный канал передачи).
2. Распределение ролей (координатор, регистратор, курьер, «диспетчер», получатель платежей).
3. Коммерциализация (вознаграждение, прайс, поток платежей).
4. Инструментальная направленность на создание ресурса анонимизации (подбор номеров/аккаунтов под конкретные «задачи», массовость).
5. Осведомленность о противоправных целях (переписка, инструкции, предупреждения, «термины рынка»).

Такая модель согласуется с тем, что сама ст. 274.4 требует корысти либо цели совершения иного преступления как обязательного условия состава, на что обращают внимание и официальные разъяснения прокуратуры [2; 7].

7. Административная ответственность за передачу номера и данных для авторизации: ст. 13.29.1 и 13.29.2 КоАП РФ

7.1. Место норм и дата введения

Статьи 13.29.1 и 13.29.2 КоАП РФ введены в действие с 1 сентября 2025 г. [4; 5]. Их конструкция — «если эти действия не содержат признаков уголовно наказуемого деяния» — закрепляет роль КоАП как фильтра для менее опасных случаев передачи идентификаторов, которые не достигают порога уголовной ответственности [4; 5].

7.2. Статья 13.29.1 КоАП РФ: передача абонентского номера / предоставление возможности пользования связью

Диспозиция ч. 1 ст. 13.29.1 КоАП РФ охватывает незаконную передачу абонентом-физическим лицом (либо пользователем услугами связи абонента-организации/ИП) абонентского номера, выделенного по договору подвижной радиотелефонной связи (или предоставленного в пользование по такому договору), иному лицу — при отсутствии признаков преступления.

Санкция ч. 1: административный штраф для граждан 30 000–50 000 руб.

Часть 2 ст. 13.29.1 КоАП РФ адресована корпоративному сектору и охватывает два типовых варианта поведения: (а) предоставление юрлицом/ИП возможности пользоваться корпоративной связью лицам, не работающим по трудовому договору или возмездному ГПД, (б) неисполнение обязанности предоставить оператору связи сведения о пользователях услугами связи по правилам оказания услуг связи — также при отсутствии признаков преступления.

Санкция ч. 2: штраф для ИП 50 000–100 000 руб., для юридических лиц 100 000–200 000 руб.

Примечание к ст. 13.29.1 КоАП РФ имеет принципиальное значение для разграничения «социально допустимого» поведения и административного проступка: не является правонарушением безвозмездная кратковременная передача абонентского номера (или предоставленного в пользование) иному лицу для получения услуг связи в личных целях.

7.3. Статья 13.29.2 КоАП РФ: передача данных для регистрации/авторизации в «Интернете»

Статья 13.29.2 КоАП РФ предусматривает ответственность за передачу информации, необходимой для регистрации и (или) авторизации пользователя сети «Интернет» для доступа к функциональным возможностям информационного ресурса, иному лицу — если действия не содержат признаков уголовно наказуемого деяния.

Санкция: штраф для граждан 30 000–50 000 руб., для ИП 50 000–100 000 руб., для юридических лиц 100 000–200 000 руб.

Примечание к ст. 13.29.2 КоАП РФ формирует ключевое исключение: не является правонарушением передача таких данных иному лицу для правомерного использования функционала ресурса по поручению пользователя сети «Интернет» или с его согласия. Эта оговорка важна для практики, поскольку легализует распространённые модели делегирования доступа (администрирование аккаунта, помощник, представитель), если использование действительно правомерно.

7.4. Разграничение КоАП и УК: практическая «логика порога»

Обе административные статьи построены по единой формуле «при отсутствии признаков уголовно наказуемого деяния», что методологически предполагает первичную проверку: не образуют ли фактические обстоятельства признаки ст. 274.4 или 274.5 УК РФ (в частности, «организация деятельности», а также корыстная заинтересованность или цель совершения иного преступления) [2; 3; 4; 5].

Тем самым КоАП-составы предназначены, как правило, для эпизодических случаев и/или для ситуаций, где нет доказанности «инфраструктурного» характера схемы и её криминальной направленности [4; 5].

Рабочая конструкция разграничения:

– «КоАП»: передача номера/данных без признаков устойчивой схемы и без установленных целей/мотивов, при этом примечания прямо защищают кратковременную личную передачу номера и делегирование данных для правомерного использования [4; 5].
– «УК»: организованный оборот идентификаторов как деятельность (системность, распределение ролей, извлечение выгоды/корыстный интерес) либо передача в целях обеспечения совершения другого преступления [2; 3].

7.5. Типовые ошибки квалификации

Ошибка 1: игнорирование примечаний КоАП (например, квалификация кратковременной безвозмездной передачи номера «в личных целях» как правонарушения).

Ошибка 2: подмена предмета доказывания по ст. 13.29.2 КоАП РФ: важно устанавливать, что передавалась именно информация, необходимая для регистрации/авторизации для доступа к функциональным возможностям ресурса, и что отсутствуют уголовные признаки.

Ошибка 3: «автоматический переход» к уголовной оценке без установления организационного характера деятельности (для ст. 274.4–274.5), что повышает риск криминализации пограничных случаев [2; 3].

8. Проблемы разграничения уголовной и административной ответственности и предложения по снижению рисков расширительного толкования

8.1. Почему «порог» разграничения здесь особенно чувствителен

Связка ст. 274.4–274.5 УК РФ и ст. 13.29.1–13.29.2 КоАП РФ построена по модели «двухуровневого реагирования»: административный состав применяется при отсутствии признаков преступления, уголовный — при наличии признаков более высокой общественной опасности (организация деятельности + корысть/цель иного преступления) [2; 3; 4; 5].

Проблема в том, что «организация деятельности» — оценочная категория, и при недостаточной конкретизации она способна «втягивать» в уголовную плоскость случаи, которые по смыслу законодателя должны оставаться на уровне КоАП [2; 3].

Дополнительный фактор риска — наличие в КоАП специальных примечаний-исключений, которые прямо легитимируют ряд жизненных ситуаций (кратковременная безвозмездная передача номера в личных целях; передача данных

для авторизации по поручению/с согласия пользователя для правомерного использования) [4; 5]. Если эти исключения игнорируются, возникает правовая неопределенность и подрывается заложенная законодателем дифференциация ответственности [4; 5].

8.2. «Организация деятельности»: минимальные признаки, которые разумно требовать в доказывании

Текст ст. 274.4 УК РФ криминализует именно организацию деятельности по передаче абонентских номеров (и отдельно — участие), при обязательном условии корыстной заинтересованности либо цели совершения иного преступления. Следовательно, для уголовной квалификации недостаточно «самого факта передачи» — требуется доказать управленческий/координационный характер поведения (создание схемы, распределение функций, контроль/координация, устойчивость).

Официальные разъяснения прокуратуры также акцентируют, что уголовная ответственность по ст. 274.4 УК РФ связана с организацией передачи номеров в нарушение требований закона при наличии корысти или цели иного преступления, и что наказуемо также участие.

Практико-ориентированное предложение: при оценке наличия «организации деятельности» целесообразно учитывать совокупность индикаторов — устойчивость (многоэпизодность/поток), распределение ролей, каналы передачи (площадки/мессенджеры/боты/сервисы), коммерциализация (вознаграждение, тарифы), управление рисками (инструкции, конспирация), складирование ресурса (пул номеров/аккаунтов) [2; 3].

При отсутствии таких признаков предпочтительным является административно-правовой режим (при выполнении условий КоАП и с учетом примечаний-исключений) [4; 5].

8.3. «Участие» (ч. 2 УК) vs «передача» (КоАП): где грань

Часть 2 ст. 274.4 УК РФ (и аналогично ч. 2 ст. 274.5 УК РФ) вводит ответственность за участие в деятельности, указанной в ч. 1 соответствующей статьи [2; 3].

Риск перекоса здесь заключается в том, что низовые исполнители (регистраторы, «дропы», курьеры) могут формально попадать под «участие», даже если их вклад эпизодичен и отсутствует доказанность осведомленности о цели «иного преступления» либо о корыстной инфраструктурной природе схемы [2; 3].

Чтобы удержать разграничение в русле принципов справедливости, разумно требовать установления хотя бы двух элементов:

1. Включенность лица в деятельность как процесс (а не случайное действие).
2. Знание/понимание криминальной направленности схемы (корысть организаторов или цель обеспечить иное преступление) [2; 3].

Иначе уголовное «участие» начнет конкурировать с административным составом передачи, для которого законодатель специально предусмотрел исключения и «бытовые» оговорки [4; 5].

8.4. Доказательственные ориентиры: чему учит практика применения «цифровых» составов в целом

Хотя Постановление Пленума ВС РФ № 37 от 15.12.2022 не посвящено напрямую ст. 274.4–274.5 УК РФ, оно дает полезные общие ориентиры для дел, связанных с использованием электронных/информационно-телекоммуникационных сетей. Пленум указывает, что при квалификации действий как совершенных с использованием сетей необходимо установить, какие именно компьютерные устройства и программы использовались и какие действия совершены с их помощью.

Этот подход уместно транслировать и на новеллы 2025 года: для 274.4–274.5 важно документировать цифровые следы схемы (переписка, инструкции, платежи, списки номеров/аккаунтов, распределение ролей), а для п. «ф» ст. 63 УК РФ — цифровые следы функционального использования средства доступа к ограниченному ресурсу/сети (включая установление самого факта ограничения доступа) [1; 6].

Тем самым предмет доказывания должен быть ориентирован не на «ярлык технологии» (VPN/прокси/бот), а на фактический механизм совершения деяния и роль цифровой инфраструктуры в нем.

8.5. Встроенные «предохранители» КоАП и их значение для толкования УК

Примечание к ст. 13.29.1 КоАП РФ прямо исключает административную ответственность за безвозмездную кратковременную передачу номера в личных целях. Примечание к ст. 13.29.2 КоАП РФ исключает ответственность за передачу данных для регистрации/авторизации по поручению пользователя или с его согласия для правомерного использования функционала ресурса.

Эти исключения важны не только «внутри КоАП», но и как контекст для толкования смежных уголовных новелл: если законодатель прямо признаёт допустимость соответствующих жизненных моделей, расширительное понимание «организации деятельности» или «участия» не должно криминализировать такие ситуации через УК [2; 3; 4; 5].

Иными словами, примечания КоАП можно рассматривать как нормативные маркеры границы социальной допустимости, которые следует учитывать при оценке общественной опасности и при выборе между УК и КоАП [4; 5].

8.6. Предложения

1. Для единообразия правоприменения целесообразно разработать разъяснения (практико-ориентированные обзоры) по разграничению 274.4–274.5 УК РФ и 13.29.1–13.29.2 КоАП РФ с примерами достаточных/недостаточных признаков «организации деятельности» [2; 3; 4; 5].
2. По п. «ф» ч. 1 ст. 63 УК РФ важно закрепить (хотя бы на уровне методических рекомендаций) функциональный стандарт: отягчение применяется при доказанности использования средства именно для доступа к ограниченному ресурсу/сети и значимости этого использования для способа совершения преступления.
3. При квалификации «участия» по ч. 2 ст. 274.4/274.5 следует акцентировать доказательность осведомленности и включенности в деятельность как процесс, чтобы не допускать подмены уголовного «участия» административной «передачей» в эпизодических ситуациях [2; 3; 4; 5].

9. Заключение

Пакет изменений 2025 года (ФЗ от 31.07.2025 № 282-ФЗ) формирует связку уголовно-правовых и административно-правовых мер, ориентированных на пресечение инфраструктуры анонимизации в цифровой среде: (а) общий «цифровой» механизм назначения наказания через п. «ф» ч. 1 ст. 63 УК РФ; (б) специальные составы ст. 274.4–274.5 УК РФ; (в) «фильтрующие» нормы КоАП РФ ст. 13.29.1–13.29.2 при отсутствии признаков преступления [1; 2; 3; 4; 5].

Введение п. «ф» ч. 1 ст. 63 УК РФ позволяет учитывать при назначении наказания совершение преступления с использованием программно-аппаратных средств доступа к ресурсам/сетям с ограниченным доступом, однако широта формулы повышает риск расширительного толкования и требует функционального подхода: отягчение должно применяться при доказанности того, что средство использовалось именно для доступа к ограниченному ресурсу/сети и было значимым элементом способа совершения преступления.

Новеллы ст. 274.4–274.5 УК РФ представляют собой криминализацию «инфраструктурных» практик — организации деятельности по передаче абонентских номеров и данных регистрации/авторизации при наличии корыстной заинтересованности либо цели совершения иного преступления, а также участия в такой деятельности, что согласуется с превентивной логикой пресечения рынка «цифровых посредников» [2; 3; 7].

Введение ст. 13.29.1–13.29.2 КоАП РФ закрепляет административную ответственность за передачу номера/учётных данных при отсутствии признаков уголовно наказуемого деяния и одновременно содержит нормативные «предохранители» (исключения), защищающие бытовые и правомерные модели поведения, что делает КоАП-уровень ключевым инструментом разграничения по степени общественной опасности [4; 5].

Для обеспечения единообразия и справедливости правоприменения целесообразно ориентироваться на общий подход Верховного Суда РФ к делам о преступлениях, совершаемых с использованием сетей: необходимо устанавливать, какие именно устройства/программы применялись и какие действия совершены с их помощью, а в контексте 274.4–274.5 — дополнительно документировать цифровые следы устойчивости схемы и распределения ролей.

С учётом доктринальных предостережений о рисках «цифровой казуализации» уголовного закона, дальнейшее развитие регулирования должно строиться на принципе технологической нейтральности: уголовно-правовое значение следует придавать не «названию» технологии (например, VPN), а доказуемому увеличению общественной опасности способа и его функциональной роли в совершении преступления [8; 9].

Список литературы:

[1] О внесении изменений в отдельные законодательные акты Российской Федерации : федеральный закон от 31.07.2025 № 282-ФЗ. URL: http://kremlin.ru/acts/bank/52312 (дата обращения: 15.02.2026).

[2] Уголовный кодекс Российской Федерации. Статья 274.4. Организация деятельности по передаче абонентских номеров. URL: https://base.garant.ru/10108000/05155e1b0e8c56601ff6d554c8dcaf36/ (дата обращения: 15.02.2026).

[3] Уголовный кодекс Российской Федерации. Статья 274.5. Организация деятельности по передаче информации, необходимой для регистрации и (или) авторизации. URL: https://base.garant.ru/10108000/7423041a2cd5d50f28714391156c84df/ (дата обращения: 15.02.2026).

[4] Кодекс Российской Федерации об административных правонарушениях. Статья 13.29.1. Передача абонентского номера либо предоставление возможности пользования услугами подвижной радиотелефонной связи. URL: https://base.garant.ru/12125267/30451228ff07b33ce70d15ad13e52dfc/ (дата обращения: 15.02.2026).

[5] Кодекс Российской Федерации об административных правонарушениях. Статья 13.29.2. Передача информации, необходимой для регистрации и (или) авторизации. URL: https://base.garant.ru/12125267/d967ec8c01993723d1d7661e7d5d9e37/ (дата обращения: 15.02.2026).

[6] О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» : постановление Пленума Верховного Суда Российской Федерации от 15.12.2022 № 37. URL: https://www.vsrf.ru/documents/own/31913/ (дата обращения: 15.02.2026).

[7] Прокуратура Свердловской области. Прокурор разъясняет: уголовная ответственность за организацию деятельности по передаче абонентских номеров. URL: https://epp.genproc.gov.ru/ru/proc_66/activity/legal-education/explain/e8317194/ (дата обращения: 15.02.2026).

[8] Русскевич Е. А. Цифровизация уголовного законодательства: непростые последствия простых решений // Вестник Университета имени О.Е. Кутафина (МГЮА). 2025. № 5. URL: https://vestnik.msal.ru/jour/article/view/2736 (дата обращения: 15.02.2026).

[9] Русскевич Е. А., Дмитренко А. П., Кадников Н. Г. Кризис и палингенезис (перерождение) уголовного права в условиях цифровизации // Вестник Санкт-Петербургского университета. Право. 2022. Т. 13. Вып. 3. С. 585–598. DOI: 10.21638/spbu14.2022.301.

[10] Кузнецова А. С., Николаев Д. О., Латыпов Д. А. Преступления в информационной сфере: анализ, проблемы квалификации // Международный журнал гуманитарных и естественных наук. 2023. № 1–3 (76). URL: https://sciup.org/prestuplenija-v-informacionnoj-sfereanaliz-problemy-kvalifikacii-170197698 (дата обращения: 15.02.2026).

[11] Меретуков Г. М., Грицаев С. И., Помазанов В. В. Актуальные вопросы цифровизации уголовного судопроизводства: взгляд в будущее // Правоприменение. 2022. Т. 6, № 3. С. 172–185. DOI: 10.52468/2542-1514.2022.6(3).172-185.

[12] Григорьев П. А. Уголовно-правовая охрана обращения сведений публичных реестров в условиях цифровизации // Право и государство: теория и практика. 2024. № 3. С. 249–252. DOI: 10.33184/pravgos-2024.3.15/

References:

[1] On amending certain legislative acts of the Russian Federation: federal law of 31.07.2025 No. 282-FZ. URL: http://kremlin.ru/acts/bank/52312 (access date: 15.02.2026).

[2] Criminal Code of the Russian Federation. Article 274.4. Organization of activities for the transfer of subscriber numbers. URL: https://base.garant.ru/10108000/05155e1b0e8c56601ff6d554c8dcaf36/ (access date: 15.02.2026).

[3] Criminal Code of the Russian Federation. Article 274.5. Organization of activities for the transfer of information necessary for registration and (or) authorization. URL: https://base.garant.ru/10108000/7423041a2cd5d50f-28714391156c84df/ (access date: 15.02.2026).

[4] Code of Administrative Offences of the Russian Federation. Article 13.29.1. Transfer of a subscriber number or provision of the possibility of using mobile radiotelephone services. URL: https://base.garant.ru/12125267/30451228ff07b33ce70d15ad-13e52dfc/ (access date: 15.02.2026).

[5] Code of Administrative Offences of the Russian Federation. Article 13.29.2. Transfer of information necessary for registration and (or) authorization. URL: https://base.garant.ru/12125267/d967ec-8c01993723d1d7661e7d5d9e37/ (access date: 15.02.2026).

[6] On certain issues of judicial practice in criminal cases of crimes in the field of computer information, as well as other crimes committed using electronic or information and telecommunication networks, including the Internet: decision of the Plenum of the Supreme Court of the Russian Federation of 15.12.2022 No. 37. URL: https://www.vsrf.ru/documents/own/31913/ (access date: 15.02.2026).

[7] The prosecutor's office of the Sverdlovsk region. The prosecutor explains: criminal liability for organizing activities for the transfer of subscriber numbers. URL: https://epp.genproc.gov.ru/ru/proc_66/activity/legal-education/explain/e8317194/ (дата обращения: 15.02.2026).

[8] Russkevich E. A. Digitalization of criminal legislation: the difficult consequences of simple decisions//Bulletin of the University named after O.E. Kutafin (MSLA). 2025. № 5. URL: https://vestnik.msal.ru/jour/article/view/2736 (access date: 15.02.2026).

[9] Russkevich E.A., Dmitrenko A.P., Kadnikov N.G. Crisis and palingenesis (rebirth) of criminal law in the context of digitalization//Bulletin of St. Petersburg University. Right. 2022. T. 13. No. 3. S. 585-598. DOI: 10.21638/spbu14.2022.301.

[10] Kuznetsova A. S., Nikolaev D. O., Latypov D. A. Crimes in the information sphere: analysis, qualification problems//International Journal of Humanities and Natural Sciences. 2023. № 1–3 (76). URL: https://sciup.org/prestuplenija-v-informacionnoj-sfereanaliz-problemy-kvalifikacii-170197698 (дата обращения: 15.02.2026).

[11] Meretukov G.M., Gritsaev S.I., Pomazanov V.V. Topical issues of digitalization of criminal proceedings: a look into the future//Law enforcement. 2022. T. 6, NO. 3. S. 172-185. DOI: 10.52468/2542-1514.2022.6(3).172-185.

[12] Grigoriev P. A. Criminal law protection of the circulation of public registries in the context of digitalization//Law and state: theory and practice. 2024. № 3. S. 249-252. DOI: 10.33184/pravgos-2024.3.15