

Научная статья

УДК 343.9

EDN: SNZYAN



## **Права на доступ в ходе расследования к цифровым аккаунтам и данным умершего**

**Дарья Вячеславовна Терещенко**

*Северо-Западный филиал, Российский государственный университет  
правосудия имени В. М. Лебедева, Санкт-Петербург, Российская Федерация*

✉ *tereschenko27281@gmail.com*

*Научный руководитель: К. А. Краснова, к.ю.н., доцент, доцент кафедры  
уголовного права Северо-Западного филиала Российского государственного  
университета правосудия имени В. М. Лебедева*

**Аннотация.** В статье исследуется правовой конфликт между необходимостью получения следственными органами цифровых доказательств из аккаунтов умерших пользователей и законодательными ограничениями, защищающими конфиденциальность данных. Эта ситуация подрывает эффективность расследования преступлений и создает правовую неопределенность в цифровой среде, требуя детального комплексного рассмотрения.

Выявлен и проанализирован правовой дуализм цифрового следа умершего, который одновременно рассматривается как имущественный актив в наследственном праве и как источник доказательств в уголовном процессе. Классифицировано содержимое цифрового аккаунта по доказательственной ценности (личные коммуникации, пользовательский контент, цифровые активы). Установлено, что процедуры наследования цифровых прав неприменимы для оперативных нужд следствия, а механизмы УПК РФ, относящие цифровые данные к вещественным доказательствам, блокируются положениями пользовательских соглашений интернет-платформ о конфиденциальности.

В отличие от исследований, сосредоточенных исключительно на цивилистической или процессуальной стороне вопроса, данная статья предлагает комплексный подход к разрешению коллизии. Подчеркивается необходимость разработки специальной юридической процедуры, которая обеспечила бы следователям легитимный доступ к важным цифровым данным умершего, преодолевая барьер пользовательских соглашений, при одновременной судебной проверке таких запросов для гарантии защиты прав на неприкосновенность частной жизни.

**Ключевые слова:** цифровые доказательства, правовой конфликт, данные умершего пользователя, доступ правоохранительных органов, конфиденциальность данных, цифровой аккаунт, цифровые активы, вещественные доказательства

**Для цитирования:** Терещенко Д. В. Права на доступ в ходе расследования к цифровым аккаунтам и данным умершего // Фемида.Science. 2026. № 1 (18). С. 175–181.

Original article

## Rights to Access the Digital Accounts and Data of the Deceased During the Investigation

**Daria V. Tereshchenko**

*North-Western Branch, Russian State University of Justice  
named after V. M. Lebedev,*

*St. Petersburg, Russian Federation*

✉ *tereschenko27281@gmail.com*

*Scientific supervisor: K. A. Krasnova*, Candidate of Science (Law), Associate Professor, Associate Professor at the Criminal Law Department of the North-Western Branch of the Russian State University of Justice named after V. M. Lebedev

**Abstract.** This article comprehensively examines the legal conflict between the need for investigative authorities to obtain digital evidence from the accounts of deceased users and legislative restrictions protecting data privacy. This contradiction undermines the effectiveness of crime investigation and creates legal uncertainty in the digital environment, requiring a detailed comprehensive review.

The legal dualism of the digital footprint of the deceased has been identified and analyzed, which is simultaneously considered as a property asset in inheritance law and as a source of evidence in criminal proceedings. The content of the digital account is classified according to its evidentiary value (personal communications, user content, digital assets). It has been established that the procedures for inheriting digital rights are inapplicable to the operational needs of the investigation, and the mechanisms of the Criminal Procedure Code of the Russian Federation, which classify digital data as physical evidence, are blocked by the provisions of user agreements on Internet platforms on confidentiality.

Unlike studies focused solely on the civil or procedural side of the issue, this article offers a comprehensive approach to conflict resolution. It emphasizes the need to create a special legal procedure that would provide investigators with legitimate access to important digital data of the deceased, overcoming the barrier of user agreements, while simultaneously conducting judicial review of such requests to ensure the protection of privacy rights.

**Keywords:** digital evidence, legal conflict, data of a deceased user, access of law enforcement agencies, confidentiality of data, digital account, digital assets, physical evidence

**For citation:** Tereshchenko D. V. Rights to access the digital accounts and data of the deceased during the investigation. *Femida.Science = Themis.Science*. 2026;(1):175-181. (In Russ.)

Ключевой проблемой, рассматриваемой в исследовании, является правовой конфликт между потребностью следственных органов в получении цифровых доказательств, необходимых для расследования преступлений, и установленными законодательными ограничениями, призванными защищать конфиденциальность данных умершего пользователя. Актуальность данной темы обусловлена стремительным ростом числа пользователей интернет-сервисов. В связи с этим целью статьи является проведение анализа правовых механизмов, связанных с обеспечением доступа правоохранительных органов к цифровым аккаунтам и данным умершего лица.

На практике данный конфликт приводит к существенным процессуальным затруднениям. Следственные органы, сталкиваясь с необходимостью получения доступа к электронной переписке, данным геолокации или истории посещений сайтов умершего, часто оказываются в правовом вакууме. С одной стороны, они обязаны использовать все законные средства для установления истины по делу, с другой – операторы связи и интернет-сервисов, руководствуясь положениями о защите персональных данных и пользовательскими соглашениями, отказывают в предоставлении информации даже по официальным запросам. Это может привести к утрате критически важных доказательств, срок актуальности которых часто ограничен.

В научной литературе рассматриваются вопросы правового регулирования доступа к цифровым аккаунтам и данным умершего лица. Например, О. В. Костина высказывает мнение о спорности автоматического распространения общих норм наследственного права на распоряжение личными данными, предлагая взамен формирование специального института частного права, который включал бы, помимо наследственных норм, положения, регулирующие отдельные виды посмертных распоряжений [1, с. 6].

Другой аспект освещен в работе А. И. Чучак, где анализируется французский закон Digital Republic, предоставляющий наследникам право требовать актуализации персональных данных умершего. При этом отмечается, что указанный правовой акт сфокусирован преимущественно на вопросах обработки персональных данных, а не на комплексном регулировании цифрового наследия в широком смысле [2, с. 23].

Отдельного внимания заслуживает сравнительно-правовое исследование Н. А. Данилова и В. В. Силкина [3]. Проведя анализ законодательства США, Франции, Германии и Канады, авторы выделяют в рамках данной проблемы два ключевых аспекта. Первый – личностный, делающий акцент на неприкосновенности данных и принципе автономии воли пользователя в определении их посмертной судьбы. Второй – имущественный, рассматривающий отдельные категории цифровой информации через призму гражданско-правовых отношений.

В противовес американскому подходу, основанному на собственности, в ряде европейских стран, например в Германии и Франции, доминирует личностно-ориентированная модель. Доступ к данным умершего рассматривается как право на защиту персональных данных, делегированное близким родственникам, которое жестко ограничивается рамками конфиденциальности переписки. Это создает для правоохранительных органов еще более высокий барьер, чем имущественная модель, делая судебный запрос практически единственным возможным выходом [3, с. 87].

При расследовании преступлений цифровой аккаунт умершего лица рассматривается прежде всего как источник доказательственной информации, а не как имущественный актив [4, с. 134]. В этой связи необходимо классифицировать содержимое аккаунта, исходя из его значимости для установления обстоятельств дела.

Наиболее ценной является категория цифровых доказательств, под которыми следует понимать любую информацию, хранящуюся в аккаунте,

чья ценность определяется не коммерческой стоимостью, а способностью подтвердить или опровергнуть ключевые версии расследования [5]. К таким данным относятся личные сведения и коммуникации, такие как переписка в мессенджерах, электронные письма, история контактов и звонков, позволяющие восстановить круг общения и взаимоотношений умершего. Не менее важными представляются контент, созданный пользователем, – фотографии, видео, заметки, а также история его онлайн-активности, которая может раскрывать его намерения и образ жизни. Особую доказательственную роль играют метаданные и техническая информация, такие как история сеансов входа, IP-адреса и геолокация, поскольку они фиксируют действия и перемещения пользователя в цифровой среде [6, с. 336].

Ключевой задачей следствия при работе с этими категориями данных является не только их получение, но и обеспечение допустимости доказательств. Это требует соблюдения процедур осмотра, изъятия и протоколирования, которые должны гарантировать сохранность цифрового следа, исключая любое несанкционированное изменение информации с момента ее обнаружения.

При этом в рамках аккаунта могут находиться и цифровые активы – объекты, обладающие самостоятельной экономической ценностью и выступающие в роли полноценного предмета гражданско-правовых отношений, такие как криптовалюты, средства на электронных кошельках или виртуальные предметы. Для целей уголовного расследования их значимость часто оказывается производной и может проявляться не в их стоимости, а, например, в возможности проследить финансовые операции умершего или установить имущественные мотивы совершенного преступления.

Правовая природа цифрового следа умершего характеризуется дуализмом: для наследственного права это потенциальное имущество, а для уголовного процесса – прежде всего источник доказательственной информации. Этот дуализм и порождает коллизию, поскольку процедуры, разработанные для наследования имущества (цифровых активов), часто неприменимы или недостаточны для оперативного получения следствием критически важных данных.

В мировой практике наблюдается разнообразие подходов к решению вопроса о посмертном доступе к цифровым данным. В Соединенных Штатах Америки в ряде штатов получила распространение модель «цифрового наследника», реализуемая через закон FADA (Fiduciary Access to Digital Assets Act). Данный законодательный акт предоставляет владельцам цифровых аккаунтов правовой инструмент для сохранения контроля над своей цифровой собственностью, позволяя заранее определить порядок распоряжения ею после смерти<sup>1</sup>.

В отечественном законодательстве этот дуализм проявляется в наличии двух независимых правовых режимов. С одной стороны, правовые основы обращения цифровых прав закреплены в ст. 141.1 ГК РФ. Следует отме-

<sup>1</sup> CA Revised Uniform Fiduciary Access to Digital Assets Act // Law Office of Rodney Gould. URL: <https://www.rodneygouldlaw.com/blog/ca-revised-uniform-fiduciary-access-to-digital-assets-act/> (дата обращения: 14.01.2026).

титель, что данная норма устанавливает специальный режим, распространяющийся исключительно на те права, которые прямо обозначены законом в качестве цифровых. Ключевой особенностью является то, что содержание и порядок их реализации целиком определяются правилами соответствующей информационной системы. Анализ рассматриваемой нормы позволяет выделить несколько особенностей.

Во-первых, оборот цифровых прав ограничен рамками информационной системы и не требует привлечения третьих лиц.

Во-вторых, обладателем права признается лицо, которое в соответствии с правилами системы имеет фактическую возможность таким правом распоряжаться.

По состоянию на декабрь 2025 г. подавляющее большинство социальных сетей и игровых платформ в своих пользовательских соглашениях прямо запрещают передачу аккаунтов по наследству. В то же время некоторые площадки допускают наследование отдельных видов цифровых активов, таких как криптовалюты и NFT-токены, доступ к которым обеспечивается через передачу приватных ключей.

С другой стороны, доступ следственных органов к цифровым данным регламентирован положениями УПК РФ, которые рассматривают данные в контексте вещественных доказательств. Электронные носители информации, содержащие следы преступления или иную значимую для дела информацию, приравниваются к вещественным доказательствам. Основными процессуальными действиями, направленными на их обнаружение и изъятие, являются осмотр, обыск, выемка и личный обыск, проводимые в соответствии со ст. 176, 177, 180, 182, 183 и 184 УПК РФ. Однако описанные процедуры УПК РФ сталкиваются с практическим препятствием – пользовательскими соглашениями интернет-платформ. Если данные умершего находятся не на личном устройстве, а в облачном хранилище, оператор услуги, ссылаясь на конфиденциальность, может отказать в предоставлении доступа даже правоохранительным органам без надлежащего судебного решения.

Федеральным законом от 28 июля 2012 г. № 143-ФЗ<sup>2</sup> в УПК РФ были внесены дополнения, устанавливающие более детальный порядок доступа к данным и закрепляющие процедуры изъятия, хранения, возврата электронных носителей. Во-первых, проведение обыска и выемки обязательно требует участия специалиста. Во-вторых, для копирования информации необходимо подать письменное ходатайство на имя следователя, дознавателя или судьи. В-третьих, законодательством предусмотрены ограничения для копирования, если этот процесс может воспрепятствовать расследованию или, по заключению специалиста, привести к утрате или изменению данных. Кроме того, изъятые электронные носители подлежат хранению в опечатанном виде в условиях, полностью исключающих возможность ознакомления с их содержимым посторонних лиц.

---

<sup>2</sup> Федеральный закон от 28 июля 2012 г. № 143-ФЗ «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации» (п. 5, 6) // Собрание законодательства Российской Федерации. 2012. № 31. Ст. 4332.

В целях разрешения коллизии представляется необходимым комплексное совершенствование законодательства. Во-первых, должно быть разработано четкое легальное определение понятия «цифровые данные умершего пользователя» в контексте уголовного судопроизводства, отделяющее их от наследуемых цифровых прав. Во-вторых, целесообразно установить в УПК РФ специальную упрощенную процедуру получения судебного решения на доступ к таким данным по запросу следователя, с предъявлением обоснованных подозрений о причастности этих данных к преступлению. В-третьих, на уровне федерального закона необходимо закрепить обязанность операторов интернет-сервисов сотрудничать с правоохранительными органами на основании такого решения, внося соответствующие изменения в пользовательские соглашения и определив механизм передачи информации.

Проведенный анализ позволяет сделать вывод о том, что основной правовой конфликт заключается в столкновении интересов уголовного судопроизводства, требующего доступа к цифровым данным умершего, и законодательных норм, защищающих конфиденциальность такой информации. В Российской Федерации доступ регулируется в рамках института вещественных доказательств, однако он осложняется положениями пользовательских соглашений. Таким образом, требуется разработка сбалансированных правовых механизмов, обеспечивающих эффективность расследования при соблюдении гарантий неприкосновенности частной жизни.

#### Список источников

1. Костина О. В. Новый вид распоряжений на случай смерти в условиях цифровизации: Digital Legacy // Наследственное право. 2023. № 1. С. 6–8.
2. Чучак А. И. Наследование цифровых активов по праву европейских стран // Право и бизнес. 2024. № 4. С. 23–28.
3. Данилов Н. А., Силкин В. В. Правовое регулирование доступа к информации пользователя сети интернет после его смерти: сравнительно-правовое исследование // Журнал зарубежного законодательства и сравнительного правоведения. 2021. Т. 17, № 1. С. 86–101.
4. Канузель А. Е. Использование информации социальных сетей при выявлении, расследовании и предупреждении преступлений // Криминалистика: вчера, сегодня, завтра. 2024. № 2. С. 132–139.
5. Яровая К. Р. Проблемы правового регулирования цифровых доказательств и электронной информации в уголовном судопроизводстве // Электронный научный журнал «Дневник науки». 2025. № 10. URL: <https://dnevniknauki.ru/images/publications/2025/10/law/Yarova4.pdf>.
6. Егорова А. А. Цифровые следы преступника и потенциал их использования в расследовании преступления // Молодой ученый. 2024. № 15 (514). С. 335–338.

#### References

1. Kostina O. V. A new type of testamentary arrangements in the conditions of digitalization: Digital Legacy. *Inheritance Law*. 2023;(1):6-8. (In Russ.)
2. Chuchak A. I. Inheritance of digital assets under the law of European countries. *Law and Business*. 2024;(4):23-28. (In Russ.)

3. Danilov N. A., Silkin V. V. Legal regulation of access to information of the Internet user after his death: comparative legal research. *Journal of Foreign Legislation and Comparative Law*. 2021;17(1):86-101. (In Russ.)
4. Kanuzel A. E. Use of social network information in detection, investigation and prevention of crimes. *Kriminalistika: vchera, segodnya, zavtra = Forensics: Yesterday, Today, Tomorrow*. 2024;(2):132-139. (In Russ.)
5. Yarovaya K. R. Problems of legal regulation of digital evidence and electronic information in criminal proceedings. *Elektronnyj nauchnyj zhurnal "Dnevnik nauki" = Electronic Scientific Journal "Diary of Science"*. 2025;(10). (In Russ.) URL: <https://dnevniknauki.ru/images/publications/2025/10/law/Yarovaya4.pdf>.
6. Egorova A. A. Digital traces of a criminal and the potential of their use in the investigation of a crime. *Molodoj uchenyj = Young Scientist*. 2024;(15):335-338. (In Russ.)

#### **Информация об авторе**

Д. В. Терещенко – студент 2 курса.

#### **Information about the author**

D. V. Tereshchenko – 2nd year student.

#### **Конфликт интересов**

Автор заявляет об отсутствии конфликта интересов.

#### **Conflict of interests**

The author declares no relevant conflict of interests.

Статья поступила в редакцию 15.01.2026; одобрена после рецензирования 26.01.2026; принята к публикации 28.01.2026.

The article was submitted 15.01.2026; approved after reviewing 26.01.2026; accepted for publication 28.01.2026.