

Научная статья
УДК 347.965:004.62

Будущее адвокатской тайны в эпоху нейросетей и облачных сервисов

Дарья Андреевна Сарибекян

Адвокатская контора № 33 Владимирской областной коллегии адвокатов № 1,
Владимир, Россия
divanova28@yandex.ru

Аннотация. Статья посвящена исследованию института адвокатской тайны в условиях стремительного распространения облачных технологий и систем искусственного интеллекта. Рассматриваются ключевые технологические риски, возникающие при использовании внешних цифровых сервисов адвокатами, а также анализируются перспективные направления правового регулирования и технической защиты.

Ключевые слова: адвокатская тайна, искусственный интеллект, нейросети, облачные сервисы, цифровая безопасность, адвокатская этика, персональные данные

Original article

The future of advocate secrecy in the era of neural networks and cloud services

Daria A. Saribekyan

Law Firm No. 33, Vladimir Regional Bar Association No. 1, Vladimir, Russia
divanova28@yandex.ru

Abstract. This article examines the concept of attorney-client privilege amid the rapid expansion of cloud technologies and artificial intelligence systems. It examines the key technological risks arising from the use of external digital services by lawyers and analyzes promising areas for legal regulation and technical protection.

Keywords: attorney-client privilege, artificial intelligence, neural networks, cloud services, digital security, attorney ethics, personal data

Активное развитие информационных технологий радикально изменило способы хранения, обработки и анализа юридической информации. В XXI веке ежедневно каждый адвокат при оказании квалифицированной юридической помощи своему доверителю сталкивается с цифровыми средами: электронным документооборотом, промежуточными хранениями данных, коммуникацией через облачные платформы, применением аналитических систем на основе машинного обучения.

В ст. 33 Положения об адвокатуре РСФСР 1962 г. впервые была закреплена обязанность адвоката не разглашать сведения, сообщенные ему доверителем в

связи с оказанием юридической помощи по данному делу. Гарантией обеспечения данной обязанности был запрет допроса адвоката в качестве свидетеля об обстоятельствах дела, которые стали ему известны в связи с выполнением обязанностей защитника по данному делу [1].

Согласно ст. 6 Кодекса профессиональной этики адвоката: «Доверия к адвокату не может быть без уверенности в сохранении профессиональной тайны. Профессиональная тайна адвоката (адвокатская тайна) обеспечивает иммунитет доверителя, предоставленный последнему Конституцией Российской Федерации. Соблюдение профессиональной тайны является безусловным приоритетом деятельности адвоката. Срок хранения тайны не ограничен во времени» [2].

Адвокатская тайна, являющаяся неотъемлемой частью адвокатской деятельности и основой доверительных отношений между адвокатом и клиентом, сталкивается с новыми сложностями, обусловленными большим объемом данных, с которыми приходится работать адвокату. К примеру, это может быть многотомное уголовное дело, и адвокату при ознакомлении с материалами необходимо провести фотофиксацию всех процессуальных документов, а также перекопировать имеющиеся видеозаписи для ознакомления с ними перед судебным заседанием. В связи с тем, что адвокату приходится сталкиваться при изучении материалов дела с огромным количеством информации, для удобства работы с данными они могут передаваться через облачные сети, частично автоматизируются, а иногда становятся элементом для обработки искусственного интеллекта. В связи с чем возникает вопрос: может ли такое понятие, как адвокатская тайна, функционировать в цифровом мире?

Данная статья направлена на исследование будущего института адвокатской тайны в условиях цифрового развития, включая анализ технологических рисков и возможных моделей регулирования.

Адвокатская тайна как правовой институт в цифровую эпоху

Адвокатская тайна гарантирует защиту любой информации, полученной адвокатом от доверителя в связи с оказанием ему правовой помощи. В дореволюционной и советской адвокатуре данный институт рассматривался преимущественно в контексте материальных носителей и межличностных коммуникаций. Однако современная правовая среда существенно усложнилась в связи с появлением и стремительным развитием информационных технологий.

Как отмечают Р. Р. Мchedlishvili и В. Р. Чакрян, защита информации в правовой сфере является исключительно важной областью [6]. Поскольку в цифровую эпоху идёт развитие абсолютно всех отраслей права, не исключается и возможность развития деструктивных сообществ, способных всячески использовать информацию, сведения, данные для получения экономической выгоды. По некоторым данным, в мире более 40 миллионов хакеров, а общий вред, наносимый ими, оценивается в 500 млрд. долларов.

На сегодняшний день источником конфиденциальной информации может быть:

- электронная переписка в социальных сетях и различных мессенджерах;
- базы данных и облачные хранилища;

- юридические аналитические платформы;
- запросы, отправленные в системы искусственного интеллекта [8].

Также адвокат в своей деятельности в связи с большим объёмом информации и невозможностью хранить все данные на мобильном телефоне или компьютере помещает фотографии, цифровые копии документов, аудио- и видеоматериалы в облачные хранилища (Яндекс.Диск, Облако Mail и т.д.). Однако перед использованием того или иного облачного хранилища в своей деятельности необходимо ответственно подойти к выбору безопасного облачного сервиса, а именно – перед использованием хранилища нужно тщательно ознакомиться с его политикой безопасности. Рекомендуется выбирать сервисы с двухфакторной аутентификацией и высоким уровнем защиты данных, таких как end-to-end шифрование. А также необходимо обеспечить настройку безопасности доступов – например, использование двухфакторной аутентификации через ключ-пароль, код доступа, сообщение, звонок или кодовое слово. В таком случае у злоумышленников не получится завладеть данными в хранилище, используя лишь одно устройство.

Таким образом, при общении с клиентом в различных социальных сетях объект защиты уже выходит за пределы традиционных представлений и включает динамичные цифровые следы, существующие в распределённой инфраструктуре. В связи с чем при общении адвоката с доверителем возникает важный вопрос о сохранении полной конфиденциальности информации, передаваемой доверителем, поэтому с клиентом целесообразно общаться при личной встрече, а также через телефонные звонки.

Технологические вызовы адвокатской тайне

1. Проблематика облачных сервисов.

Использование облачного хранилища – одно из наиболее уязвимых мест в контексте соблюдения адвокатской тайны. Главные риски хранения данных на облачном хранилище включают в себя:

- 1) факт хранения данных у третьих лиц, что усложняет контроль за доступом;
- 2) атаки на инфраструктуру провайдера, приводящие к массовым утечкам;
- 3) неоднозначность контрактных условий, позволяющих провайдеру использовать лог-файлы или технические данные для собственных целей, включая улучшение сервисов [4].

Такие риски требуют более строгих стандартов аудита облачных провайдеров и внедрения моделей Zero Trust.

Рассмотрим ключевые механизмы работы Zero Trust:

- многоуровневая проверка доступа – от пароля и токена до биометрии и поведения пользователя (MFA, поведенческая аналитика);
- анализ контекста – система учитывает местоположение, IP, устройство, время суток, историю активности;
- динамический уровень доверия – при изменении контекста (новое устройство, другой регион) политика безопасности автоматически ужесточается.

2. Нейросети, большие языковые модели и адвокатская тайна.

Использование языковых моделей (LLM) может повысить эффективность юридической работы, однако это порождает два принципиальных вопроса:

а) судьба вводимых данных.

По умолчанию многие публичные ИИ-сервисы используют запросы клиентов для логирования или дообучения моделей, так как программы с искусственным интеллектом появились недавно, и пользователи начинают ими активно пользоваться, но в то же время некоторые относятся к этому скептически. Для адвокатской сферы это недопустимо: данные могут быть восстановлены или косвенно утечь через ответы другим пользователям;

б) проблема аудита алгоритмов.

Современные LLM обладают «чёрным ящиком» принятия решений, то есть их внутренняя работа непрозрачна, и пользователи не могут понять, как система принимает решения. Доказать, что конфиденциальная информация не использовалась, затруднительно, что создаёт коллизию между технологическим прогрессом и принципом профессиональной тайны.

Развитие нормативного регулирования

Итак, ИИ может быть использован для автоматизации повседневных, рутинных задач, таких как анализ больших объёмов документации, проверка фактов, подготовка документов, что позволяет сэкономить время юристов и повысить общую эффективность [5].

Современный регуляторный ландшафт Российской Федерации в отношении технологий искусственного интеллекта заметно меньше, чем у ряда других крупных юрисдикций. В настоящий момент основополагающим стратегическим документом РФ в области ИИ является Национальная стратегия развития искусственного интеллекта на период до 2030 г., утверждённая Указом Президента РФ от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации». Статья 19 вышеуказанного документа выделяет следующие основные принципы развития и использования технологий искусственного интеллекта: защита прав и свобод человека, безопасность, прозрачность, технологический суверенитет, целостность инновационного цикла, разумная бережливость, поддержка конкуренции.

Также ожидается появление норм, прямо запрещающих:

- использование публичных ИИ-платформ для передачи клиентских данных;
- передачу информации адвокатской тайны в облака без соответствующей сертификации;
- отсутствие локализации и шифрования данных.

Перспективные технологические решения

Локальные и изолированные ИИ-системы.

С целью повышения конфиденциальности адвокатские образования в ближайшем будущем будут переходить к созданию:

- автономных моделей на собственных серверах;
- нейросетей, не обучающихся на пользовательских данных;

- систем fine-tuning с полной локальной изоляцией. Fine-tuning (тонкая настройка) – метод адаптации уже обученной языковой модели (LLM) к конкретным задачам или области.

Цель – дополнить модель информацией из нового или уникального набора данных, чтобы повысить её точность в рамках выбранного направления.

Это позволит адвокату в своей работе использовать искусственный интеллект, не нарушая конфиденциальность, то есть не загружая в открытый доступ какую-либо информацию о доверителе.

Применение современных методов криптографии

Тенденции, которые могут использоваться в защитных технологиях, включают в себя:

- сквозное (end-to-end) шифрование (принцип: информация шифруется непосредственно на устройстве отправителя и остаётся в таком виде до тех пор, пока не будет расшифрована на устройстве получателя. В связи с чем никакие промежуточные звенья – ни серверы поставщиков услуг, ни интернет-провайдеры, ни любые другие третьи стороны – не имеют технической возможности получить доступ к исходному, незашифрованному содержимому данных);

- Secure Enclave и аппаратные модули защиты. Secure Enclave – это встроенная система на кристалле (SoC), присутствующая во всех современных устройствах Apple. Эта технология обеспечивает безопасное создание и хранение ключей для шифрования данных, находящихся на устройстве, а также защищает и обрабатывает биометрические данные для Face ID и Touch ID, обеспечивая надежную аутентификацию и защиту конфиденциальной информации [3].

Эти современные технологии смогут сделать утечки информации маловероятными даже при попытках взлома аккаунта, на котором хранится информация.

Этика будущего: новая профессиональная культура

В то время как правовые стандарты обновляются, особую роль играет этическая адаптация профессии. Адвокатам в своей деятельности необходимо:

- владеть компетенциями цифровой гигиены;
- информировать клиентов о применяемых технологиях;
- выбирать инструменты, отвечающие принципам конфиденциальности по умолчанию (privacy by design).

Таким образом адвокат сможет контролировать сохранность и конфиденциальность информации, предоставляемой клиентом.

Эпоха нейросетей и облачных сервисов трансформирует адвокатскую тайну не столько в направлении ослабления, сколько в сторону усложнения и расширения. Объект защиты становится распределённым и динамичным, а технологические риски требуют принципиально новых подходов к безопасности и регулированию [7].

Адвокатская тайна будущего будет опираться на три ключевых элемента.

1. Жёсткие правовые стандарты и надзор, включая регулирование облаков и ИИ.

2. Технологическую инфраструктура, обеспечивающая защищённую обработку данных.

3. Профессиональная культура, ориентированная на цифровую компетентность и этику.

Таким образом, адвокатская тайна в настоящее время остаётся фундаментальным институтом, без которого осуществление адвокатской деятельности невозможно, и в развивающуюся цифровую эпоху должна сочетать в себе строгие нормы и новую модель профессиональной ответственности.

Список источников

1. Об утверждении Положения об адвокатуре РСФСР : Закон РСФСР от 25.07.1962 г. URL: <http://www.consultant.ru> (дата обращения: 05.12.2025).

2. Кодекс профессиональной этики адвоката : принят I Всероссийским съездом адвокатов 31 января 2003 г. : с изменениями и дополнениями, утверждёнными II Всероссийским съездом адвокатов 8 апреля 2005 г.; III Всероссийским съездом адвокатов 5 апреля 2007 г.; VI Всероссийским съездом адвокатов 22 апреля 2013 г.; VII Всероссийским съездом адвокатов 22 апреля 2015 г.; VIII Всероссийским съездом адвокатов 20 апреля 2017 г.; X Всероссийским съездом адвокатов 15 апреля 2021 г.; XII Всероссийским съездом адвокатов 18 апреля 2025 г. URL: base.garant.ru/12130519/ (дата обращения: 04.12.2025).

3. Волхова А. А. Адвокатская тайна и нейросети: проект «безопасного контура» // Юридическая наука. – 2025. – № 10. – С. 60-63.

4. Магдеева Д. И. Адвокатская тайна в цифровую эпоху: вызовы и способы защиты // Вестник Пензенского государственного университета. – 2025. – № 2 (50). – С. 22-26.

5. Мальцев В. А., Сучкова Т. Е. Адвокатская тайна в эпоху искусственного интеллекта // Научный Альманах ассоциации France-Kazakhstan. – 2025. – № 3. – С. 73-79.

6. Мchedlishvili Р. Р., Чакрян В. Р. Кибербезопасность в юридической сфере: угрозы и защита данных // Инновационная наука. – 2023. – № 12-1. – С. 141-145.

7. Степанов О. А., Басангов Д. А. О перспективах влияния искусственного интеллекта на судопроизводство // Вестн. Том. гос. ун-та. – 2022. – № 475. – С. 229-237.

8. Шайкова Е. С. Цифровизация юриспруденции // Е-SCIO. – 2022. – № 11 (74). – С. 742-748.

Статья поступила в редакцию 26.01.2026; одобрена 16.02.2026; принята к публикации 20.02.2026.

The article was submitted 26.01.2026; approved after reviewing 16.02.2026; accepted for publication 20.02.2026.