Observatoire ARGA

ARGA Atlas

ЦИФРОВАЯ ИДЕНТИЧНОСТЬ КАК ИСТОЧНИК РИСКА

Автор:

Сергей Храбрых — президент ARGA, PhD

Организация: Observatoire ARGA, ARGA Atlas

Адрес для корреспонденции: 21 route de l’Aviation, 12 C, 64600 Anglet, FRANCE

Контакты: info@argaobservatory.org, +33 7 58 49 62 27

Сайт: www.argaobservatory.org, https://www.arga-atlas.com/

Англет, 18 апреля 2026

Цель документа:

Настоящий доклад подготовлен с целью анализа цифровой идентичности не как нейтрального технологического удобства, а как самостоятельного источника правового, процессуального и трансграничного риска. Практическая задача документа состоит в том, чтобы показать, каким образом цифровой профиль лица, его цифровые документы, учетные данные, следы поведения, взаимосвязанные записи, а также инфраструктуры цифровой идентификации и верификации начинают функционировать как каналы допуска, исключения, подозрения, селекции, комплаенс-проверки, миграционного контроля, правоохранительного внимания и более широкого трансграничного давления. Для ARGA данная тема имеет прикладное значение в делах, где защита лица все чаще зависит не только от содержания правовых документов, но и от того, каким образом его цифровой след уже интегрирован в системы принятия решений до начала формального юридического спора. Управление Верховного комиссара ООН по правам человека рассматривает неприкосновенность частной жизни в цифровую эпоху как самостоятельную правозащитную тему, тогда как Европейская комиссия подтверждает, что к концу 2026 года государства - члены ЕС должны сделать Европейские цифровые кошельки идентичности доступными для граждан, резидентов и бизнеса, что придает теме непосредственную институциональную актуальность.

Оглавление

Исполнительное резюме

Цифровая идентичность больше не сводится к вопросу о том, как лицо подтверждает свою личность в сети. В современной институциональной среде она превращается в сложную систему данных, признаков, проверяемых атрибутов, поведенческих сигналов и связей, через которые государственные органы, финансовые организации, платформы, работодатели, миграционные службы и правоохранительные структуры получают возможность не только распознавать человека, но и формировать предварительное представление о нем. В этой логике цифровая идентичность начинает работать не как техническая оболочка, а как ранний фильтр допуска, доверия и подозрения.

Практический риск состоит в том, что цифровая идентичность начинает функционировать как инструмент предвосхищающего суждения. Лицо все чаще оценивается через совокупность цифровых следов, документов, социальных связей, историй перемещений, записей о взаимодействии с системами и иных массивов данных, привязанных к его идентичности. Когда такие данные агрегируются и анализируются государственными или частными системами, цифровая идентичность превращается из технической функции в инфраструктуру юридического риска.

Значение темы усиливается тем, что цифровая идентичность в Европе и за ее пределами институционализируется как нормальная часть доступа к услугам и юридически значимым действиям. Европейские цифровые кошельки идентичности, надзорные документы о рисках для частной жизни и растущий интерес международных правозащитных органов к цифровой среде подтверждают, что речь идет не о редкой технологии, а о нормативно поддерживаемом направлении развития, в котором удобство, верификация и правовой риск растут одновременно.

Почему эта тема имеет правовое и международное значение

Тема цифровой идентичности имеет международное значение потому, что сегодня значительная часть правового и социального доступа опосредуется цифровыми инфраструктурами. Лицо все чаще подтверждает себя не только паспортом или личным присутствием, но и цифровыми документами, кошельками идентичности, электронными идентификаторами, учетной верификацией и совместимыми удостоверяющими средствами, которые легко подключаются к государственным и частным системам. Это означает, что допуск к услугам, процедурам и пространствам все чаще зависит от того, как именно система считывает цифровое представление о человеке.

С правозащитной точки зрения проблема состоит в том, что цифровая идентичность создает новый слой предварительной нормативной реальности. Человек сначала проходит через систему цифрового распознавания, сопоставления и оценки, и только затем получает возможность вступить в формальное взаимодействие с институтом. Следовательно, тема цифровой идентичности должна анализироваться не как узкий вопрос удобства, а как правовая среда, в которой заранее распределяются доверие и подозрение, доступ и исключение, благонадежность и риск.

В трансграничных делах данный риск особенно заметен. Цифровой профиль лица способен воздействовать на визовые решения, миграционный контроль, банковский комплаенс, проверку работодателями, платформенную верификацию, полицейское сопоставление данных, оценку рисков при поездках и иные процессы. Поэтому цифровая идентичность становится не второстепенной темой, а частью архитектуры современного трансграничного давления.

Нормативная и институциональная рамка

Первый слой нормативной рамки образуют международные стандарты прав человека в цифровой среде. Управление Верховного комиссара ООН по правам человека ведет самостоятельную работу по темам неприкосновенности частной жизни в цифровую эпоху и цифрового пространства как сферы действия прав человека. Это подтверждает, что цифровые технологии и цифровые профили личности рассматриваются как непосредственная часть правозащитной повестки, связанная с автономией, надзором, ошибкой, вторичным использованием данных и доступом к защите.

Второй слой составляет европейская рамка защиты данных и информационного самоопределения. Совет Европы в рамках цифрового развития и управления прямо подчеркивает значение права на защиту данных и права человека сохранять содержательный контроль над тем, как сведения о нем структурируются, связываются, циркулируют и используются повторно. Для цифровой идентичности это принципиально, поскольку речь идет не только о хранении данных, но и о праве лица влиять на архитектуру их использования.

Третий слой образует развивающаяся правовая архитектура Европейского союза в сфере цифровой идентичности. Европейская комиссия указывает, что Регламент о Европейской цифровой идентичности создает правовую основу для кошельков идентичности и что к концу 2026 года такие кошельки должны стать доступными во всех государствах - членах. Это означает институциональную нормализацию цифровой идентичности как опоры для значимых юридических и квазиюридических действий.

Четвертый слой составляет надзорное и регуляторное внимание к рискам для частной жизни. Европейский надзорный орган по защите данных специально рассматривает цифровые кошельки идентичности как среду с особыми рисками для частной жизни, а материалы Европейского совета по защите данных показывают, что вопросы цифровой идентичности и смежной обработки данных находятся в активной зоне регуляторного внимания. Тем самым сами надзорные органы подтверждают, что цифровая идентичность является нормативно чувствительной инфраструктурой, а не нейтральной технологией.

Ключевые механизмы практики, злоупотребления и конфликта

Первый механизм риска - агрегирование данных. Цифровая идентичность становится опасной не тогда, когда существует один идентификатор, а тогда, когда разные потоки данных начинают соединяться между собой. Официальные удостоверяющие сведения,

платформенная активность, записи о поездках, сигналы социальных связей, следы занятости и сведения, близкие к правоохранительным, начинают образовывать составной портрет лица. Именно в этой связи технологическая видимость превращается в управляемое юридическое воздействие.

Второй механизм - переносимость и повторное использование. Как только сведения, связанные с идентичностью, переводятся в стандартизированные цифровые форматы, их становится проще повторно использовать в разных институциональных средах. Один и тот же цифровой образ лица может начать влиять сразу на несколько решений в публичном и частном секторе, причем пользователь формально соглашается лишь на один акт подтверждения личности, а фактически запускает цепочку более широких последствий.

Третий механизм - расширение выводов. Система, созданная для подтверждения личности, постепенно начинает использоваться для вывода о благонадежности, риске, статусе, доверии или подозрении. Правовая опасность состоит в том, что человек может согласиться на один уровень использования данных, не осознавая масштаба последующего наслоения выводов, основанных на корреляции и анализе наборов данных.

Четвертый механизм - трансграничная воспроизводимость. Чем более совместимы и взаимно признаваемы цифровые системы идентичности, тем быстрее сигналы, прикрепленные к профилю лица, начинают действовать в разных юрисдикциях и секторах. В чувствительных делах это означает, что цифровой риск редко остается локальным, если инфраструктуры идентичности построены на принципе совместимости.

Типовые сценарии и модели применения

Первый типовой сценарий - необъяснимое трение при проверке. Лицо сталкивается с задержками верификации, расширенной проверкой, отказом в услуге, затруднениями при перемещении или иным режимом повышенного внимания, при том что никакого явного неблагоприятного юридического акта не видно. В таких ситуациях цифровая идентичность может действовать как скрытый носитель агрегированных сигналов, используемых для фильтрации и подозрения.

Второй сценарий - использование цифрового профиля как канала воздействия на правозащитников, журналистов или политически чувствительных лиц. В подобных делах цифровая идентичность перестает быть нейтральным способом верификации и становится каналом наблюдения, картирования контактов, выявления уязвимостей и давления.

Третий сценарий - постепенное расширение роли цифрового кошелька за пределы аутентификации. Изначально кошелек может восприниматься как удобное хранилище и инструмент подтверждения личности. Но по мере того как вокруг него формируется инфраструктура хранения документов, доступа к услугам, использования электронных подписей и взаимодействия с государственными и частными контрагентами, его сбои или предвзятости начинают затрагивать сразу несколько юридически значимых взаимодействий.

Четвертый сценарий - наложение систем искусственного интеллекта на насыщенные данными профили идентичности. Когда аналитика, использующая социальные связи, записи о поездках, сведения о взаимодействии с системами и другие наборы данных, наслаивается на цифровую идентичность, лицо становится объектом не только распознавания, но и вероятностной оценки, которая может иметь существенные последствия и слабо поддаваться оспариванию.

Основные риски, правовые уязвимости и проблемные зоны

Первый риск - видимость без возможности оспаривания. Цифровая идентичность делает лицо более видимым для систем, но не обязательно предоставляет ему соразмерную возможность понять, проверить или оспорить сделанные о нем выводы. Возникает структурное напряжение между растущим институциональным знанием и уменьшающимся индивидуальным контролем.

Второй риск - расползание функции. Система, внедренная для аутентификации, начинает обслуживать слежение, профилирование, присвоение баллов риска, исключение или вторичное использование данных. Опасность здесь заключается не только в утечке, но и в архитектурном расширении назначения системы.

Третий риск - межсекторное распространение. Один и тот же сигнал, связанный с идентичностью, может начать работать одновременно в банковском, миграционном, трудовом, платформенном и правоохранительном контекстах. Тогда ошибка или подозрение, однажды встроенные в профиль, начинают жить собственной жизнью в разных институциональных средах.

Четвертый риск - асимметрия в трансграничных контекстах. Государства и крупные институты способны быстро сопоставлять данные и сигналы, тогда как затронутое лицо часто не может восстановить цепочку использования или вывода. В условиях государственного интереса, безопасности или политической чувствительности такая асимметрия особенно усиливает правовую уязвимость.

Институциональные ограничения, пробелы и дефицит гарантий

Первая системная слабость - нормализация права быстрее, чем ясность средств защиты. Европейский союз активно строит правовую основу и среду внедрения цифровых кошельков идентичности, однако практические пути, с помощью которых лицо может понять, оспорить и ограничить последующий вред, заметны значительно слабее, чем сама архитектура внедрения. Когда инфраструктура растет быстрее понятных механизмов оспаривания, право сначала создает удобство, а уже потом - защиту.

Вторая слабость - слишком узкая рамка неприкосновенности частной жизни. Защита данных крайне важна, но цифровая идентичность как источник риска затрагивает также свободу передвижения, равенство, надлежащую правовую процедуру, профилирование, исключение и трансграничное наведение. Если вопрос рассматривать только как проблему

соблюдения правил о частной жизни, более широкие нарушения прав могут остаться недоосмысленными.

Третья слабость - фрагментация надзора. Разные части проблемы распределены между регуляторами по защите данных, судами, миграционными органами, полицией, платформами, банками и правозащитными механизмами. В результате один и тот же риск виден всем понемногу и никому полностью. Именно поэтому тему цифровой идентичности необходимо рассматривать как вопрос управления правами, а не как узкий технический сектор.

Практические рекомендации и модель правового действия

Первый шаг - рассматривать цифровую идентичность как доказательственную среду. В каждом чувствительном деле необходимо задаваться вопросом, какие цифровые представления о лице уже могут влиять на поведение институтов: использование официальной электронной идентичности, данные кошелька, поисковые следы, предыдущие результаты проверок, связанные социальные или транспортные данные. Без этого защита рискует спорить лишь с видимым актом, не замечая цифровой среды, которая его подготовила.

Второй шаг - картировать риск, связанный с идентичностью, по секторам. Один и тот же цифровой профиль по-разному работает для пограничного органа, банка, платформы, работодателя или суда. Поэтому практическая защита требует матрицы: где данные циркулируют, кто на них полагается, для какой цели и с каким потенциальным вредом.

Третий шаг - настаивать на минимизации, выборочном раскрытии и возможности оспаривания. Там, где используются цифровые системы идентичности, защитная стратегия должна поддерживать такие архитектуры и практики, которые сокращают ненужное раскрытие данных, ограничивают вторичное использование и сохраняют возможность оспаривать неблагоприятные выводы.

Четвертый шаг - интегрировать цифровую идентичность в анализ прав человека и трансграничного давления. В политически чувствительных, экстрадиционных и иных рискованных делах цифровой профиль должен рассматриваться как часть основного защитного досье, а не как техническое приложение в конце документа.

Рекомендации по правовому и институциональному подходу

Во-первых, управление цифровой идентичностью должно строиться вокруг архитектуры, сохраняющей права, а не только вокруг показателей внедрения. Массовое распространение без сильной оспоримости, минимизации и четких пределов последующего использования рискует превратить инфраструктуру удобства в инфраструктуру риска для прав.

Во-вторых, политикам следует прямо учитывать пересечение цифровой идентичности, наблюдения, искусственного интеллекта и трансграничного риска.

Рассматривать эти области как отдельные административные отсеки - значит бюрократически упростить жизнь самому риску.

В-третьих, юридическая практика должна выработать доктрину цифровой идентичности как источника риска для чувствительных трансграничных дел. Такая доктрина должна исходить из того, что лицо может быть оценено, отфильтровано или ограничено через цифровые представления о нем задолго до появления явного неблагоприятного юридического акта.

Заключение

Цифровая идентичность перестала быть всего лишь удобной надстройкой над юридической жизнью. Она становится одной из инфраструктур, через которые эта юридическая жизнь организуется, фильтруется и направляется. Международные и европейские правозащитные, регуляторные и надзорные материалы с разных сторон подтверждают одну и ту же реальность: системы цифровой идентичности могут повышать удобство и доверие, но одновременно порождают концентрацию информации, прослеживаемость, риски для частной жизни, возможность неблагоприятных выводов и межсекторные последствия.

Для ARGA основной вывод состоит в том, что в современных чувствительных делах цифровой профиль необходимо защищать не менее серьезно, чем бумажное досье, показания или международно-правовой статус. Когда институты все чаще видят человека прежде всего через цифровую идентичность, защита, игнорирующая эту идентичность, начинает спорить уже после того, как значительная часть решения была незаметно сформирована системой.

Приложение A. Терминология

Цифровая идентичность. Совокупность цифровых средств, данных и идентификаторов, через которые лицо аутентифицируется, описывается, верифицируется и распознается в цифровых и институциональных системах. В современном правовом контексте включает как официальные компоненты электронной идентификации, так и более широкий набор цифровых представлений о лице.

Цифровой кошелек идентичности. Цифровой инструмент, позволяющий подтверждать личность, получать доступ к услугам, хранить и передавать цифровые документы, а также использовать юридически значимые учетные данные и подписи.

Информационное самоопределение. Право и фактическая возможность лица сохранять содержательный контроль над сбором и использованием данных о себе, включая способы их связывания, распространения и повторного применения.

Расползание функции. Постепенное расширение использования систем, связанных с идентичностью, за пределы их первоначально заявленной цели, например от аутентификации к профилированию, наблюдению или исключению.

Вывод, связанный с идентичностью. Суждение о лице, формируемое на основе агрегированных или коррелированных цифровых данных, а не на основе прямого и явного доказательства.

Приложение B. Матрица рисков, полномочий и правовых последствий

Матрица ниже отражает повторяющуюся логику рисков, вытекающую из международных и европейских материалов о цифровой идентичности, частной жизни и цифровом управлении.

Задача	Правовой риск	Юридический предел	Возможное последствие	Практический комментарий
Рассматривать цифровую идентичность как чисто технический фон	Недооценка правового значения агрегирования данных	Цифровая идентичность влияет на права, доступ и институциональное отношение	Источник фильтрации или исключения остается незамеченным	Начинать чувствительное дело с картирования среды цифровой идентичности
Полагаться на кошелек идентичности или электронный идентификатор как на нейтральное удобство	Расползание функции и вторичное использование данных	Системы идентичности должны оставаться ограниченными правами и целями использования	Профилирование, прослеживаемость, институциональное расширение полномочий	Требовать минимизации данных и ограничения целей использования
Игнорировать межсекторное использование данных, связанных с идентичностью	Фрагментированная защита	Публичные и частные сервисы могут опираться на одну и ту же инфраструктуру	Банковские, миграционные, трудовые и репутационные последствия	Картировать все сектора, затронутые цифровым профилем
Считать неприкосновенность частной жизни единственным вопросом	Слишком узкая правовая рамка	Могут затрагиваться также равенство, надлежащая процедура и свобода передвижения	Потеря значительной части аргументации	Рассматривать тему как многоправовую проблему
Не учитывать наложение искусственного интеллекта и наблюдения	Скрытая эскалация выводов	Насыщенные данными профили могут питать автоматизированные решения	Присвоение баллов риска или наведение при слабой оспоримости	Искать выводы и корреляции, а не только сырые записи
Ждать явного формального вреда	Позднее распознавание	Многие формы вреда возникают до	Упущено окно превентивной	Защищать цифровой

	цифрового риска	формального неблагоприятного акта	защиты	профиль до окончательного неблагоприятного действия

Официальные источники

- Управление Верховного комиссара ООН по правам человека. Неприкосновенность частной жизни в цифровую эпоху.
- Управление Верховного комиссара ООН по правам человека. Цифровое пространство и права человека.
- Управление Верховного комиссара ООН по правам человека. Призыв 2026 года к представлению материалов о защите правозащитников в цифровую эпоху.
- Совет Европы. Направление по цифровому развитию и управлению на 2024-2025 годы.
- Европейская комиссия. Страницы и материалы по Европейской цифровой идентичности и кошелькам идентичности.
- Европейская комиссия. Часто задаваемые вопросы о Европейской цифровой идентичности.
- Европейский надзорный орган по защите данных. TechDispatch № 3 за 2025 год о цифровых кошельках идентичности.
- Управление Верховного комиссара ООН по правам человека. Документ 2025 года об искусственном интеллекте и борьбе с терроризмом.