pISSN:2349-5707 Volume:13,Issue 4, April -2026 eISSN:2349-5715

LEGAL REGULATION OF THE USE OF DATA FROM SOCIAL NETWORKS AS EVIDENCE

Saidkarimova Sadiyakhon Khurshidovna
Master's Student
Tashkent State University of Law
Tashkent, Republic of Uzbekistan
saidkarimovasadiya@gmail.com

Abstract

This article examines the legal aspects of using data from social networks as evidence in judicial proceedings. Based on an analysis of international law and the legislation of the Republic of Uzbekistan, the study explores issues of admissibility, reliability, and legality of digital evidence. Particular attention is paid to the provisions of new procedural norms of the Republic of Uzbekistan regulating the collection, submission, and evaluation of electronic data (correspondence, screenshots, audio and video recordings). The article provides examples from judicial practice, compares them with foreign approaches, and identifies problems related to authentication and personal data protection. Possible directions for further development of legal regulation in this area are formulated. Special emphasis is placed on the need to ensure procedural guarantees when handling digital materials.

Keywords

social networks, digital evidence, electronic data, personal data, judicial proceedings, proof.

Аннотация

В статье рассматриваются правовые аспекты использования данных из социальных сетей в качестве доказательств в судебных процессах. На основе анализа международного права и законодательства Республики Узбекистан исследуются вопросы допустимости, достоверности и законности цифровых доказательств. Подробно освещены положения новых процессуальных норм Республики Узбекистан, регламентирующих сбор, представление и оценку электронных данных (переписка, скриншоты, аудио- и видеозаписи). Приведены примеры судебной практики, сравнение с зарубежными подходами, выявлены проблемы аутентификации и защиты персональных данных. Формулируются возможные направления дальнейшего развития правового регулирования в указанной области. Особое внимание уделено необходимости соблюдения процессуальных гарантий при обращении с цифровыми материалами.

Ключевые слова

социальные сети, цифровые доказательства, электронные данные, персональные данные, судопроизводство, доказывание.

Аннотация

Мазкур мақолада ижтимоий тармоқлардан олинган маълумотларни суд жараёнларида далил сифатида қўллашнинг ҳуқуқий жиҳатлари кўриб чиқилади. Халқаро ҳуқуқ ҳамда Ўзбекистон Республикаси қонунчилиги таҳлили асосида рақамли далилларнинг мақбуллиги, ишончлилиги ва қонунийлиги масалалари ўрганилади. Ўзбекистон Республикасида қабул қилинган янги процессуал нормаларнинг электрон

pISSN:2349-5707 Volume:13,Issue 4, April -2026 eISSN:2349-5715

маълумотларни (ёзишмалар, скриншотлар, аудио ва видео ёзувлар) йиғиш, тақдим этиш ва баҳолаш тартибини тартибга солувчи қоидалари батафсил ёритилган. Суд амалиётидан мисоллар келтирилган, хорижий ёндашувлар билан таққослаш амалга оширилган ҳамда аутентификация ва шахсий маълумотларни ҳимоя қилиш билан боғлиқ муаммолар аниқланган. Ушбу соҳада ҳуқуқий тартибга солишни янада ривожлантиришнинг эҳтимолий йўналишлари таклиф этилган. Рақамли материаллар билан ишлашда процессуал кафолатларга риоя қилиш зарурлигига алоҳида эътибор қаратилган.

Калит сўзлар

ижтимоий тармоқлар, рақамли далиллар, электрон маълумотлар, шахсий маълумотлар, суд юритуви, исботлаш.

“По мере того как цифровые платформы все больше хранят личные данные, грань между законным сбором доказательств и правом на приватность может стираться”[1].

I. ВВЕДЕНИЕ

С бурным развитием интернета и социальных сетей сведения, размещенные пользователями, становятся все более значимым источником информации. Одновременно их использование в судебной практике порождает ряд правовых вопросов: как сбалансировать интересы правосудия и неприкосновенности частной жизни, как обеспечить достоверность и допустимость цифровых материалов (скриншоты, переписки, записи) как доказательств. Международные документы подчеркивают необходимость такого баланса. Так, новые руководящие принципы ЮНЕСКО и Международной ассоциации прокуроров отмечают, что “цифровые платформы все больше хранят личные данные, и потому грань между законным сбором доказательств и правом на приватность может стираться”. Аналогично, Организация по безопасности и сотрудничеству в Европе (ОБСЕ) подчеркивает, что при использовании свидетельств из социальных сетей необходимо “защитить право на свободу выражения мнений и неприкосновенность частной жизни”, избегая необоснованного наблюдения и “охлаждения” публичной дискуссии[2].

Актуальность исследования обусловлена необходимостью выработки четких правовых критериев допустимости цифровых доказательств, особенно учитывая их массовое распространение, доступность фальсификации и неоднозначную судебную практику. В условиях цифровизации правосудия возрастает потребность в унифицированных подходах к оценке информации из социальных сетей, включая соблюдение прав на частную жизнь и процедурные гарантии.

Цель исследования состоит в комплексном анализе правового регулирования использования данных из социальных сетей в качестве доказательств, с учетом международных стандартов и национального законодательства Республики Узбекистан.

Задачи исследования включают:

- выявление ключевых международных подходов к допустимости цифровых доказательств;
- анализ норм процессуального и специального законодательства Республики Узбекистан;

pISSN:2349-5707 Volume:13,Issue 4, April -2026 eISSN:2349-5715

- определение правовых проблем, связанных с достоверностью и законностью получения данных из социальных сетей;
- проведение сравнительного анализа с зарубежной практикой;
- формулирование предложений по совершенствованию правового регулирования в Узбекистане.

В данной статье проводится анализ международных стандартов сбора цифровых доказательств и их правового статуса, а также детальное рассмотрение законодательства Республики Узбекистан в этой области. Рассмотрены положения уголовно-процессуального и гражданского процессуального кодексов Узбекистана, законов о цифровой подписи, электронном документе и защите персональных данных. Приводятся примеры судебной практики, в том числе разъяснения экспертов и прецеденты из других стран. Особое внимание уделено проблемам

допустимости, достоверности и легитимности использования материалов социальных сетей (скриншотов переписок, сообщений в мессенджерах и другие). В заключении даются выводы и рекомендации по совершенствованию законодательства.

II. Международные стандарты и практика

Право на неприкосновенность частной жизни и переписку закреплено в международных договорах. Статья 17 Международного пакта о гражданских и политических правах гласит: «Никто не может подвергаться произвольному или незаконному вмешательству в его личную и семейную жизнь, произвольным или незаконным посягательствам на неприкосновенность его жилища или переписки».

Хотя международные стандарты не предусматривают различий, законодательство Республики Узбекистан и других стран предусматривает их. В этих законах особое внимание уделяется общедоступным персональным данным (например, информации из открытых аккаунтов социальных сетей). Однако даже такая информация может потребовать специального разрешения суда для использования в качестве доказательства, чтобы избежать произвольного вмешательства в право на неприкосновенность частной жизни.

Европейский союз широко поддержал юридическое признание электронных доказательств. В нормативных актах ЕС прямо указано, что электронные подписи и другие электронные доказательства «не должны быть лишены юридической силы или допустимости в суде исключительно по причине их электронной формы». В Руководящих принципах Совета Европы по электронным доказательствам (2019 г.) содержатся определения и рекомендации, в частности: электронные доказательства могут состоять из текста, видео, фотографий, аудиозаписей и т. д., а также указывается

носитель, с которого они могут быть получены – мобильный телефон, веб-страница, компьютер или GPS-трекер. Самое главное, в этих руководящих принципах прямо указано, что электронные доказательства должны рассматриваться наравне с традиционными доказательствами и иметь такую же доказательную силу, как и традиционные доказательства[3].

Внутри ЕС также действуют законодательные акты об обмене электронными уликами между государствами. Они направлены на унификацию процедур

pISSN:2349-5707 Volume:13,Issue 4, April -2026 eISSN:2349-5715

трансграничного получения электронных данных при расследовании преступлений, но оставляют на усмотрение национального права требования о допустимости, аутентификации и защите данных.

В США электронные доказательства рассматриваются через призму Четвертой поправки (запрет необоснованных обысков). К примеру, Верховный суд США в деле Riley v. California (2014) указал, что полицейским обычно необходим ордер для поиска содержимого мобильного телефона, даже если телефон изъят при аресте[4]. Суд особо отметил, что современные устройства хранят огромное количество личных данных, “нельзя считать, что возможность носить эту информацию с собой умаляет ее ценность для защиты прав, за которые боролись отцы-основатели”. То есть, в США аналогично подчеркивают высокий уровень приватности цифровой информации: ее поиск без разрешения считается недопустимым.

В целом, в сравнительных обзорах указывается, что во многих развитых юрисдикциях применяется принцип аутентификации электронных доказательств: необходимо подтверждать, что скриншот или копия точно передает оригинальное содержимое. Обычно для этого привлекаются эксперты и используются метаданные, криптографические

подписи, временные метки и др. Если это не сделано, такие материалы легко можно оспорить.

Организации, занимающиеся верховенством права, выпустили рекомендации по сохранению баланса между правосудием и правами человека при работе с цифровыми данными. Например, новый доклад ОБСЕ подчеркивает, что при доступе к сообщениям или активности в социальных сетях нужно “защитить право на свободу выражения” и не допускать “неоправданного наблюдения” за пользователями, которое может привести к “охлаждению” высказываний в интернете[5].

Международная ассоциация прокуроров и ЮНЕСКО в 2025 году выпустили Руководство “Сбор цифровых доказательств”, где подчеркивается необходимость привлечения к ответственности за соблюдение фундаментальных прав при расследовании в цифровой среде. Новые рекомендации делают акцент на строгом соблюдении законности, сохранении цепочки предоставления данных и минимальном вмешательстве в личную жизнь граждан[6].

Международная практика устанавливает, что электронные доказательства должны признаваться допустимыми не хуже традиционных, но при этом сбор таких данных должен строго соответствовать процессуальным гарантиям, исключать произвол и защищать права личности, особенно неприкосновенность частной жизни и свободу слова.

III. Позиция и законодательство Республики Узбекистан

[5] Beyond bits, bytes and borders : how we untangle digital evidence dilemmas in Central Asia. https://www.osce.org/blog/590168#:~:text=There%20are%20also%20legitimate%20human,This%20is%20why

%20a%20delicate

pISSN:2349-5707 Volume:13,Issue 4, April -2026 eISSN:2349-5715

Рассмотрим позицию Республики Узбекистан в данном вопросе. До 2024 года в Узбекистане не было четкого понятия цифровых доказательств. Сведения из социальных сетей формально попадали под общие нормы об электронных документах или просто рассматривались как распечатки переписок (бумажный носитель). Судебная практика и эксперты отмечали, что до сих пор суды принимают к рассмотрению в основном лишь платежные документы, а распечатки из социальных сетей обычно не удовлетворяют требованиям достоверности и допустимости[7]. По мнению одного эксперта, печатные копии сообщений могут усилить доказательную базу, но ни в коем случае не могут выступать единственным доказательством и оцениваются судом с большой осторожностью.

Однако, в ноябре 2024 года произошла фундаментальная перестройка законодательства: Президент подписал Закон “О внесении изменений и дополнений в некоторые законодательные акты Республики Узбекистан, направленных на совершенствование системы работы с цифровыми доказательствами”. Новая редакция УПК, ГПК и ряда других кодексов официально вводит понятие “цифровые доказательства” и регламентирует работу с ними. Закон определяет цифровые доказательства как электронные данные, содержащие сведения об обстоятельствах дела, в том числе файлы, записи разговоров, видеозаписи, переписки в мессенджерах и социальных сетях[8].

Согласно новому регулированию, цифровые доказательства рассматриваются как отдельная категория наряду с вещественными и письменными. При этом закон ясно указывает: бумажная распечатка цифрового доказательства не приравнивается к письменному доказательству. Это означает, что простые скриншоты без сопутствующих

мер не рассматриваются как полноценный документ - требуется сохранение оригинальной цифровой формы или надлежащая ее заверка. Пользователи и стороны процесса теперь имеют право представлять копии цифровых доказательств, распечатанных в бумажной форме, но сами печатные формы не считаются самостоятельным письменным доказательством.

Изменениями предусмотрены специальные правила изъятия и исследования цифровых носителей. Так, изъятие электронных данных должно проводиться под опись в присутствии понятых, причем без участия специального эксперта подобные изъятия попадают под риск признания недопустимыми. В частности, УПК РУз устанавливает, что электронные данные, полученные при выемке или осмотре без участия специалиста, признаются недопустимыми доказательствами. Аналогичные требования касаются протокола представления цифровых доказательств: при их поступлении в органы следствия или суд в протоколе обязательно фиксируются, кто и на каком основании их представил.

Также закон подчеркивает важность сохранения цепочки хранения: электронные носители (жесткие диски, флешки и т.д.) должны храниться наравне с вещдоками, а их пересылка в суд или между инстанциями осуществляется по процедуре почтовой или курьерской доставки с обязательной описью содержимого. Суд может в случае необходимости требовать осмотр цифровых доказательств по месту их хранения[9].

С учетом прежнего опыта, новый закон устанавливает особые меры по заверению копий. Теперь при подаче в суд электронных данных копиями (скриншотами, распечатками) заинтересованная сторона обязана их нотариально заверить. Это нововведение призвано повысить достоверность представляемых материалов. Однако при этом по закону не

pISSN:2349-5707 Volume:13,Issue 4, April -2026 eISSN:2349-5715

требуется нотариальное заверение оригиналов электронных файлов - они могут быть поданы на любом носителе (CD, флешке, онлайн-каналом) без бумажной формы[10]. Иными словами, внимание смещается на проверку аутентичности именно цифрового контента.

Законом предусмотрены и гарантии против фальсификации: введен механизм экспертного исследования цифровых доказательств. Например, цифровые данные могут быть признаны орудием преступления (свидетельством совершения деяния) или объектом судебной экспертизы. Сотрудники правоохранительных органов вправе использовать специальные технические средства для детального анализа носителей, если это не приведет к порче данных. В законодательстве Республики Узбекистан также появились положения о протоколе представления электронных данных, где фиксируются метаданные: дата, время создания/ изменения файла, IP - адрес сервера или аккаунта и др. Все это направлено на подтверждение связки данных с определенным лицом или событием.

Использование сообщений и материалов из социальных сетей неминуемо затрагивает нормы о защите персональных данных. ЗРУ “О персональных данных” (2019) устанавливает принципы конфиденциальности: персональные данные гражданина не должны раскрываться без его согласия или иного законного основания. В то же время в закон введена категория общедоступных данных: информация, доступ к которой свободен “с согласия субъекта или на которую не распространяются требования конфиденциальности”[11]. К таким относят, например, биографические справочники, открытые электронные ресурсы, публичные аккаунты и т.д.

С практической точки зрения это означает, что посты и переписки, размещенные в публичном доступе (открытые группы, паблики и т.д.),

могут рассматриваться как общедоступные данные и использоваться без специального согласия автора. В то же время переписка в закрытых сообществах или личных аккаунтах остается личной информацией и ее сбор без разрешения нарушает конфиденциальность. Закон содержит и обязанность граждан предоставлять свои данные в интересах конституционного строя, общественной морали и безопасности, однако применение этого пункта для доступа к данным социальных сетей пока не отработано. В Узбекистане сохраняется важное ограничение: доказательства, полученные путем незаконного получения персональных данных (взлом аккаунта, перехват без санкции суда), должны признаваться недопустимыми.

Поскольку новую норму ввели лишь недавно, авторитетных прецедентов нет. Тем не менее, на основе экспертных комментариев и ранее действующих норм можно сделать выводы. Уже до 2024 года существовали уголовные дела, где в качестве доказательств использовались сообщения из мессенджеров. Обычно это происходило через запрос к оператору связи или социальные сети (с судебным разрешением) или предъявление сторонами распечаток. Ключевыми проблемами оставались аутентификация и легальность получения: если ответчик отрицал авторство сообщений, то в отсутствие других улик суды к таким материалам относились критически[12].

Например, в гражданском деле о долге суд отклонил чат в “Одноклассниках”, где ответчик якобы признавал долг, поскольку распечатка переписки не отвечала принципам достоверности и относимости. Эксперт отметила, что без подтверждения подлинности через администратора социальные сети или телефоны сама переписка считается слабым доказательством. Перевод чата в нотариально

заверенный документ вообще не гарантировал принятие: “даже нотариальное заверение не спасет, суд просто отклонит доказательство, ссылаясь на то, что оно

pISSN:2349-5707 Volume:13,Issue 4, April -2026 eISSN:2349-5715

достоверно (нотариально удостоверено), но не относимо и не допустимо". В итоге распечатка сообщения расценивалась лишь как вспомогательное доказательство.

Новые нормы призваны изменить такую практику. По заявлениям властей и СМИ, скриншоты, аудио- и видеозаписи, переписки в мессенджерах официально признаны допустимыми цифровыми доказательствами. Главное - соблюдать процедуру: правильно изъять данные с участием эксперта, обеспечить опись, представить оригиналы или надлежащие заверенные копии.

IV. Сравнительный анализ и проблемы допустимости

Основная трудность цифровых доказательств - легко ли их подделать? Скриншоты и копии сообщений легко фальсифицируются, редактируются в графическом редакторе. Поэтому международная практика требует подтверждения подлинности: например, извлечение метаданных из файла, связка с IP-адресами, результатом компьютерной экспертизы. В Узбекистане это частично обеспечивается нормами: если речь идет о данных с телефона или компьютера, проводится компьютерно-техническая экспертиза, в которой сравнивается содержимое носителя с предъявленным файлом. Важно и участие понятых при изъятии

- чтобы исключить "руки следователя"[13].

В США аналогичные вопросы решаются через правила доказывания. Так, снимки экрана социальных сетей обычно требуют подтверждения автора под присягой или свидетеля. Без этого они считаются не подтвержденной копией чужого сообщения (в США они скорее

квалифицируются как "представление содержания" и запрещены правилом о свидетельских показаниях третьих лиц). Лишь публичные записи, например, твиты известных лиц, иногда принимаются без доказательств авторства.

В странах ЕС действует директива о взаимодействии служб при получении электронных данных, но процедуры допустимости зависят от национального права. Тем не менее подчеркивается, что любое доказательство, полученное с нарушением закона о персональных данных или с превышением полномочий, должно считаться недопустимым. Например, вмешательство в переписку без ордера квалифицируется как нарушение права на неприкосновенность.

Особую проблему представляет легальность сбора данных в социальных сетях. Если гражданин сам снял скриншот и принес его в суд, вопрос более простой - он передал свое сообщение (или из открытого источника). Но когда данные извлекаются сотрудниками без согласия, требуется соблюдение процессуальных норм. Новое законодательство Республики Узбекистан требует обоснованного ходатайства о получении цифровых доказательств: лицо, запрашивающее их, должно указать, почему они важны и где их искать. Суд может выдать официальный запрос, в порядке, подобном допросу лица, располагающего данными. При необходимости дознания или следствия сотрудники могут обратиться в компанию - оператора связи или саму социальную сеть, но опять же только по решению суда. Несанкционированный доступ, как взлом аккаунта, рассматривается недопустимым.

Соотношение с законом о персональных данных тоже важно. Например, копируя чужой чат, человек незримо обрабатывает чужую личную информацию. По закону он должен иметь на это основание: согласие лица или разрешение суда. В противном случае само представление переписки в суде может нарушать конфиденциальность

pISSN:2349-5707 Volume:13,Issue 4, April -2026 eISSN:2349-5715

третьих лиц. Поэтому эксперты советуют лицам, использующим социальные данные, соблюдать принципы минимизации: представлять только ту часть переписки, которая необходима делу, и закрывать лишние личные данные.

Современные технологии позволяют повысить надежность. Уже существуют сервисы документирования веб-страниц и мессенджеров, фиксирующие момент снимка и место хранения. Blockchain и иные системы могут обеспечить неизменяемую фиксацию цифровых следов. К примеру, кодифицировано, что “в случае затруднений доставка данных возможна через проведение осмотра цифровых доказательств по месту их хранения”, что позволяет проводить анализ на серверах провайдеров.

V. Проблемы и рекомендации

Несмотря на новшества, остаются проблемные моменты. Во-первых, достоверность данных все еще сильно зависит от внешних факторов. Любой цифровой файл можно подделать перед печатью или сохранением[14]. Нужна поэтапная процедура скрепления оригинального файла и его копий. Например, не хватает закона механизмов простой “цифровой печати” или хеширования при изъятии, о которых говорят эксперты.

Во-вторых, необходимо усилить правовые гарантии прав личности. Закон «О персональных данных» существует в общих чертах, но на практике он не четко определяет, как обязанности граждан предоставлять данные соотносятся с их правом на неприкосновенность частной жизни. Необходимо ввести в Уголовно-процессуальный и Гражданско-процессуальный кодексы положение, требующее соблюдения

Закона «О персональных данных» при изъятии цифровых доказательств, а также установить наказания за его нарушение.

В-третьих, необходимо обучать судей и адвокатов особенностям работы с цифровыми доказательствами. Как показывает международная практика, без знания того, как данные возникают и хранятся, невозможно корректно оценить их достоверность. Например, можно выпускать методические рекомендации или проводить региональные семинары на несколько более информированной основе.

Наконец, нужно упростить международное сотрудничество. Чаще всего социальные сети хранят данные на серверах за рубежом. Даже если в Узбекистане закон обязывает предоставить эти сведения, без договоров экстрадиции или международных соглашений это затруднительно. Узбекистан уже участвует в проекте E-VIDENCE ОБСЕ; следует продолжать работу над двусторонними договорами с крупными IT-компаниями (мессенджерами, социальными сетями) или участвовать в многосторонних механизмах трансграничного доступа к данным.

VI. ЗАКЛЮЧЕНИЕ

Вопрос правового регулирования доказательств из социальных сетей демонстрирует необходимость баланса между эффективностью правосудия и защитой частной жизни. Расширение цифровых коммуникаций и повсеместное использование онлайн-платформ делают их значимым источником сведений, способных повлиять на исход правовых споров и уголовных дел. Узбекистан предпринял значительный шаг, признав цифровые материалы допустимыми доказательствами и введя процедуры их представления, хранения и оценки. Тем не менее вызовы, связанные с надежностью

pISSN:2349-5707 Volume:13,Issue 4, April -2026 eISSN:2349-5715

источников, а также охраной персональных данных, остаются актуальными и требуют комплексного подхода.

Практика применения новых норм сталкивается с трудностями, связанными с отсутствием устоявшихся процедур аутентификации цифровых материалов, неурегулированностью механизмов трансграничного получения данных, а также недостаточной технической оснащенностью правоприменителей. Для полноценной реализации принятых положений необходима разработка разъяснений, повышение цифровой грамотности судей и следователей, внедрение безопасных каналов фиксации и хранения цифровых доказательств. Немаловажным остается и развитие международного сотрудничества, особенно в части доступа к информации, размещенной на иностранных платформах.

Новое законодательство Республики Узбекистан заложило правовой фундамент для обращения с цифровыми доказательствами, но дальнейшее совершенствование должно строиться с учетом международных стандартов и правовых позиций развитых государств, что даст возможность обеспечить надежность, легитимность и справедливость судебных решений в условиях цифровизации общества.

ИСПОЛЬЗУЕМАЯ ЛИТЕРАТУРА

I. Международные документы и акты

1. Международный пакт о гражданских и политических правах 1966 г. https://www.un.org/ru/documents/decl_conv/conventions/pactpol.shtml
2. Европейская конвенция о защите прав человека и основных свобод 2010 г. https://www.coe.int/ru/web/compass/the-european-convention-on-human- rights-and-its-protocols
3. Конвенция о компьютерных преступлениях 2001 г. https://rm.coe.int/1680081580
4. Конвенция о защите частных лиц в отношении автоматизированной обработки данных личного характера 1981 г. https://rm.coe.int/1680078c46
5. Регламент ЕС о защите физических лиц относительно обработки персональных данных и о свободном перемещении таких данных, а также об отмене Директивы 95/46/EC https://rppa.pro/_media/world/gdpr.pdf

II. Законодательство Республики Узбекистан

1. Закон Республики Узбекистан “О персональных данных” от 01.10.2019 г. https://lex.uz/uz/docs/4396428
2. Закон Республики Узбекистан “О внесении изменений и дополнений в некоторые законодательные акты Республики Узбекистан, направленных на совершенствование системы работы с цифровыми доказательствами” от 24.10.2024 г. https://lex.uz/ru/docs/7228823
3. Закон Республики Узбекистан “Об информатизации” от 11.12.2003 г. https://lex.uz/docs/82956?ONDATE2=30.03.2021&action=compare
4. Закон Республики Узбекистан “Об электронном документообороте” от 29.04.2004 г. https://lex.uz/docs/165074
5.

pISSN:2349-5707 Volume:13,Issue 4, April -2026 eISSN:2349-5715

6. Гражданский процессуальный кодекс Республики Узбекистан https://lex.uz/docs/3517334

7. Уголовно-процессуальный кодекс Республики Узбекистан https://lex.uz/docs/111463

III. Учебники, научные статьи и доклады

1. А.А. Абдылкалыков. Социальные сети. Как использовать их в качестве доказательства в суде. // Научная статья // https://cyberleninka.ru/article/n/sotsialnye-seti-kak-ispolzovat-ih-v-kache stve-dokazatelstva-v-sude

2. Электронные доказательства в гражданском и административном судопроизводстве. Руководящие принципы комитета министров Совета Европы. https://rm.coe.int/prems-147419-rus-2019-cm-2018-169-lignes-directrice s-digital-evidence-/16809ef160

3. П.С. Пастухов. Электронное вещественное доказательство в уголовном судопроизводстве. // Научная статья // https://www.researchgate.net/publication/287118707_ELECTRONIC_EV IDENCE_IN_CRIMINAL_PROCEEDINGS

4. В.Н. Чернышов и Е.С. Лоскутова. Проблемы собирания и использования цифровых доказательств. // Научная статья // https://cyberleninka.ru/article/n/problemy-sobiraniya-i-ispolzovaniya-tsifr ovyh-dokazatelstv

5. М.Э. Гурциев. Правовое регулирование социальных сетей: опыт усиления контроля за онлайн - пространством в разных странах. // Научная статья // http://mediascope.ru/2878

6. И.В. Малышева. Социальные сети как правовой феномен. // Научная статья // https://slh-journal.isu.ru/ru/article/file?id=483

7. Ю.А. Тясто. Правовая защита цифровых активов: страница социальной сети. // Научная статья // https://ipcmagazine.ru/articles/1729250/

8. Д. Нагорная. Цифровые доказательства - 2025: тенденции и выводы судов. // Научная статья // https://www.eg-online.ru/article/494534/

Электронные ресурсы

1. Balancing Privacy and Justice: New UNESCO-IAP Guidelines on Digital Evidence Collection.
2. https://www.unesco.org/en/articles/balancing-privacy-and-justice-new-un esco-iap-guidelines-digital-evidence-collection#:~:text=As%20digital%2 0platforms%20increasingly%20store,the%20respect%20of%20fundamen tal%20rights
3. Beyond bits, bytes and borders : how we untangle digital evidence dilemmas in Central Asia. https://www.osce.org/blog/590168#:~:text=There%20are%20also%20legi timate%20human,This%20is%20why%20a%20delicate
4. Доказательства из социальных сетей. https://ksip.ru/events/dokazatelstva-iz-sotsialnykh-setey/
5. ЕСПЧ: слежение за электронной перепиской служащего является нарушениемего права на частную жизнь. https://www.coe.int/ru/web/portal/-/echr-monitoring-an-employee-s-electr onic-communications-amounted-to-a-breach-of-his-right-to-private-life

pISSN:2349-5707 Volume:13,Issue 4, April -2026 eISSN:2349-5715

6. Is revision of the council of Europe guidelines on electronic evidence already needed? https://utrechtlawreview.org/articles/10.36633/ulr.525
7. Дело Riley v. California, 573 U.S. 373 (2014). https://supreme.justia.com/cases/federal/us/573/373/
8. Можно ли считать доказательством по делу информацию из социальных сетей. https://www.spot.uz/ru/2019/10/29/social/ Ш.М. Мирзиёев подписал закон о цифровых доказательствах. https://uz.kursiv.media/2024-11-22/mirziyoev-podpisal-zakon-o-czifrovy h-dokazatelstvah
9. Скриншоты и переписка - теперь доказательства в суде Узбекистана. https://upl.uz/obshestvo/46817-news
10. Можно ли считать доказательствами сообщения в соцсетях? https://delo-press.ru/journals/law/protsessualnye-aspekty/45605-mozhno- li-schitat-dokazatelstvami-soobshcheniya-v-sotssetyakh/