



Observatoire ARGA

ARGA Atlas

**ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ, СУДЕБНЫЕ СИСТЕМЫ И СПРАВЕДЛИВЫЙ
ПРОЦЕСС:
АВТОМАТИЗАЦИЯ РЕШЕНИЙ КАК НОВЫЙ РИСК ДЛЯ ПРАВОСУДИЯ**

Авторы:

Сергей Храбрых — президент ARGА, PhD,

Наталия Цмакалова

Организация: Observatoire ARGА, ARGА 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, 2 мая 2026

Цель документа

Настоящий доклад подготовлен с целью анализа того, каким образом системы искусственного интеллекта и иные автоматизированные инструменты используются в судебной и правоохранительной деятельности и какие правовые риски возникают при их применении. Особое внимание уделяется влиянию алгоритмических моделей на право на справедливое судебное разбирательство, презумпцию невиновности, право на эффективную защиту и принцип независимой оценки доказательств.

Практическая задача документа состоит в выявлении ситуаций, в которых автоматизированные оценки, прогнозные модели, системы анализа данных, цифровая фильтрация информации и алгоритмические рекомендации начинают фактически влиять на процессуальные решения. Это может затрагивать вопросы предварительного заключения, оценки риска, распределения дел, анализа доказательств, миграционных процедур, финансового мониторинга и иных сфер, где решения напрямую затрагивают права человека.

Для ARGА данная тема имеет стратегическое значение, поскольку в международных делах, связанных с экстрадицией, розыском, санкциями, комплаенсом и финансовыми расследованиями, цифровые системы всё чаще используются как источник выводов о риске, благонадёжности, вероятности правонарушения или необходимости применения ограничительных мер. При недостаточной прозрачности такие инструменты способны усиливать ошибки и затруднять эффективную правовую защиту.

Настоящий доклад рассматривает применение искусственного интеллекта как часть более широкой проблемы соотношения технологической эффективности и процессуальных гарантий. Его цель состоит в разработке практического подхода, пригодного для адвокатов, судов, регуляторов, правозащитных организаций и специалистов по комплаенсу.

ОГЛАВЛЕНИЕ

Executive Summary

Context & Problem Statement / Почему эта тема имеет правовое и международное значение

Legal Framework / Нормативная и институциональная рамка

Mechanisms of Practice / Abuse / Ключевые механизмы практики, злоупотребления или конфликта

Case Patterns / Типовые сценарии и модели применения

Risk Assessment / Основные риски и правовые уязвимости

Institutional Gaps / Институциональные ограничения и системные слабости

Practical Guidance / Практические рекомендации и модель правового действия

Policy Recommendations / Рекомендации по правовому и институциональному подходу

Conclusion / Заключение

Приложение А. Терминология

Официальные источники

Executive Summary

Искусственный интеллект и автоматизированные системы анализа данных всё активнее внедряются в судебную, правоохранительную и административную практику. Они используются для прогнозирования рисков, сортировки дел, выявления подозрительных операций, анализа документов, оценки вероятности повторного правонарушения и формирования рекомендаций для должностных лиц.

Такие технологии способны повышать скорость обработки информации и выявлять сложные взаимосвязи в больших массивах данных. Одновременно они создают новые правовые риски. Алгоритмические модели могут опираться на неполные или предвзятые данные, использовать непрозрачные критерии и воспроизводить ошибки, которые трудно обнаружить и оспорить.

Особое значение имеет то обстоятельство, что формально решение принимает человек, однако фактически существенное влияние на его выводы может оказывать автоматизированная система. В результате алгоритмическая рекомендация начинает восприниматься как объективная и нейтральная, хотя она является продуктом конкретной модели, обученной на ограниченном наборе данных и встроенной в определённые институциональные предпосылки.

Основной вывод настоящего доклада состоит в том, что использование искусственного интеллекта в сфере правосудия должно рассматриваться не только как технологический вопрос, но и как проблема соблюдения фундаментальных процессуальных гарантий. Любая система, влияющая на принятие решений, затрагивающих права человека, должна подлежать проверке с точки зрения законности, прозрачности, объяснимости, соразмерности и возможности эффективного оспаривания.

Context & Problem Statement / Почему эта тема имеет правовое и международное значение

Использование искусственного интеллекта в судебной и административной деятельности уже перестало быть теоретической перспективой. Алгоритмические системы применяются для распределения дел, анализа судебной практики, выявления подозрительных операций, оценки вероятности нарушения закона, автоматической сортировки документов и формирования рекомендаций для должностных лиц. В ряде случаев такие инструменты оказывают непосредственное влияние на решения, затрагивающие свободу, имущество, деловую репутацию и иные фундаментальные права.

Особое значение имеет применение автоматизированных систем в уголовном судопроизводстве, миграционных процедурах, финансовом мониторинге, санкционном комплаенсе и международном правовом сотрудничестве. Алгоритмические модели могут использоваться для оценки риска повторного правонарушения, определения уровня угрозы, выявления связей между лицами и транзакциями, а также для приоритизации дел. Если результаты такой обработки принимаются без достаточной проверки, технологический инструмент фактически превращается в источник правовых последствий.

Проблема заключается не в самом использовании технологий, а в том, что автоматизированные выводы часто воспринимаются как более объективные, чем человеческая оценка. На практике алгоритмы зависят от качества исходных данных, методологии обучения, выбранных параметров и целей разработчиков. Ошибки, статистические перекосы и скрытые допущения могут приводить к систематическому воспроизведению неточных или предвзятых результатов.

Значение данной темы носит международный характер. Государства, международные организации, банки, платформы и частные аналитические компании всё активнее внедряют алгоритмические инструменты. Их выводы используются в делах об экстрадиции, предоставлении убежища, санкциях, блокировке активов, банковских ограничениях и оценке комплаенс-рисков. В результате лицо может столкнуться с серьёзными последствиями, не имея полной информации о том, каким образом был сформирован соответствующий вывод.

Для ARGА данная тема имеет особое значение, поскольку эффективная защита в трансграничных делах требует способности анализировать не только правовые аргументы, но

и технические механизмы, влияющие на принятие решений. В условиях расширяющегося применения искусственного интеллекта право на справедливый процесс всё в большей степени зависит от прозрачности и проверяемости алгоритмических систем.

Legal Framework / Нормативная и институциональная рамка

Правовое регулирование применения искусственного интеллекта в сфере правосудия формируется на пересечении норм о правах человека, процессуальных гарантиях, защите персональных данных, административном праве и специальных актов, посвящённых регулированию цифровых технологий.

Ключевое значение имеют положения Европейской конвенции о защите прав человека и основных свобод. Статья 6 закрепляет право на справедливое судебное разбирательство, включая право на независимое и беспристрастное рассмотрение дела, равенство сторон и возможность эффективного оспаривания доказательств. Статья 8 защищает право на уважение частной жизни, а статья 13 гарантирует эффективное средство правовой защиты. В случаях, когда автоматизированные системы затрагивают имущественные интересы, применяется также статья 1 Протокола № 1.

На уровне Европейского союза существенное значение имеют Общий регламент по защите данных (GDPR), Закон об искусственном интеллекте (AI Act), а также отраслевые акты, регулирующие цифровые системы в государственном и частном секторах. Особое значение имеют положения о прозрачности, качестве данных, человеческом контроле и требованиях к системам высокого риска.

Дополнительную роль играют документы Совета Европы, рекомендации Европейской комиссии по эффективности правосудия (CEPEJ), материалы Организации экономического сотрудничества и развития, а также принципы Организации Объединённых Наций, касающиеся применения цифровых технологий с соблюдением прав человека.

На национальном уровне применяются нормы уголовного, административного, гражданского и процессуального законодательства, регулирующие допустимость доказательств, пределы использования автоматизированных систем, требования к мотивировке решений и порядок судебного контроля.

Наряду с государственным регулированием важную роль играют внутренние процедуры банков, платформ, аналитических компаний и иных частных субъектов, использующих алгоритмические модели для оценки риска и принятия решений. Хотя такие процедуры формально носят частноправовой характер, их последствия могут непосредственно затрагивать основные права лиц.

Таким образом, применение искусственного интеллекта в сфере правосудия и связанных процедур подчиняется не только техническим стандартам, но и фундаментальным принципам законности, прозрачности, объяснимости, соразмерности и эффективной судебной защиты.

Mechanisms of Practice / Abuse / Key Mechanisms of Practice, Abuse or Conflict

Искусственный интеллект используется в правовых и административных системах в различных формах. В одних случаях алгоритмы выполняют вспомогательную функцию, помогая анализировать большие массивы данных и структурировать документы. В других случаях они формируют рекомендации, которые оказывают существенное влияние на итоговое решение. Чем выше степень зависимости должностного лица от автоматизированного вывода, тем значительнее правовые риски.

Одним из основных механизмов является алгоритмическая оценка риска. Такие модели применяются для прогнозирования вероятности повторного правонарушения, уклонения от правосудия, нарушения миграционного режима, подозрительных финансовых операций или иных событий. Полученный показатель риска может влиять на решение о мере пресечения, уровне контроля, проведении дополнительной проверки или применении ограничительных мер.

Другим механизмом является автоматизированная сортировка и приоритизация дел. Системы могут определять, какие материалы требуют повышенного внимания, какие заявления должны быть рассмотрены в первую очередь и какие документы подлежат дополнительной проверке. Хотя формально такие инструменты оптимизируют работу, они способны влиять на фактическое распределение ресурсов и интенсивность контроля.

Существенную роль играет использование искусственного интеллекта для анализа документов и выявления закономерностей. Алгоритмы могут сопоставлять тексты, извлекать ключевые сведения, обнаруживать связи между лицами и событиями и формировать краткие аналитические выводы. При недостаточной проверке существует риск, что промежуточные выводы будут восприниматься как установленные факты.

Особое значение имеет интеграция алгоритмических систем в частные процедуры банков, платформ и аналитических компаний. Оценка клиента, транзакции или проекта может основываться на автоматизированной модели, результаты которой используются для блокировки операций, отказа в обслуживании или передачи информации в компетентные органы.

Потенциальное злоупотребление возникает тогда, когда алгоритмические выводы принимаются без раскрытия методологии, без возможности проверить исходные данные и без эффективного механизма оспаривания. В таких условиях автоматизированная система становится непрозрачным фактором, влияющим на решения, затрагивающие фундаментальные права и законные интересы лица.

Case Patterns / Типовые сценарии и модели применения

Одним из наиболее распространённых сценариев является использование алгоритмической оценки риска при принятии решений о мере пресечения, освобождении из-под стражи или определении уровня процессуального контроля. Суд или иной орган может учитывать автоматизированный показатель вероятности повторного правонарушения или уклонения от правосудия. Если методология такой оценки не раскрывается и не подвергается критическому анализу, алгоритмический вывод начинает оказывать влияние, сопоставимое с самостоятельным доказательством.

Другой типовой сценарий связан с миграционными и убежищными процедурами. Автоматизированные системы могут использоваться для сортировки заявлений, выявления предполагаемых несоответствий в документах и определения дел, требующих углублённой проверки. Ошибки в исходных данных или некорректные критерии оценки могут приводить к задержкам, отказам и иным неблагоприятным последствиям.

В сфере финансового мониторинга и санкционного комплаенса алгоритмы применяются для выявления подозрительных транзакций, связей между лицами и признаков повышенного риска. На основании таких выводов могут блокироваться операции, ограничиваться доступ к активам и инициироваться дополнительные проверки. При отсутствии прозрачности лицу нередко затруднительно понять причины ограничений и представить адресные возражения.

Отдельный сценарий касается анализа цифровых доказательств. Искусственный интеллект может использоваться для обработки переписки, контрактов, банковских данных, материалов уголовного дела и иных массивов информации. Хотя такие инструменты ускоряют работу, они не исключают необходимости самостоятельной юридической оценки и проверки достоверности выводов.

Также существенное значение имеет использование алгоритмов в частных решениях банков, платформ и иных организаций. Автоматизированная оценка может привести к закрытию счёта, отказу в обслуживании, ограничению операций или сохранению негативного профиля даже после устранения первоначальных вопросов.

Во всех перечисленных ситуациях общий риск заключается в том, что технологическая рекомендация постепенно приобретает статус фактического основания решения, хотя сама по себе она представляет лишь инструмент анализа, зависящий от качества данных, выбранной модели и институционального контекста.

Risk Assessment / Основные риски и правовые уязвимости

Основной риск заключается в непрозрачности алгоритмических моделей. Лицо, в отношении которого применяется автоматизированная оценка, зачастую не имеет доступа к информации о том, какие данные использовались, какие критерии были применены и каким образом был сформирован итоговый вывод. Это затрудняет эффективное оспаривание и ограничивает право на защиту.

Второй существенный риск связан с качеством исходных данных. Неполные, устаревшие, ошибочные или статистически несбалансированные данные могут приводить к неточным результатам и систематическому воспроизведению предвзятых выводов.

Третья уязвимость состоит в чрезмерном доверии к автоматизированным выводам. Судьи, должностные лица, банки и платформы могут воспринимать алгоритмические рекомендации как объективные и нейтральные, не уделяя достаточного внимания ограничениям модели и возможным альтернативным объяснениям.

Четвёртый риск связан с трансформацией вероятностной оценки в фактическое основание для ограничений. Система может указывать лишь на статистически повышенную вероятность определённого события, однако на практике такой вывод способен привести к реальным правовым последствиям, включая отказ в обслуживании, усиленный контроль, ограничение доступа к активам или неблагоприятное процессуальное решение.

Пятый риск заключается в сохранении негативного алгоритмического профиля. Даже после исправления ошибок или устранения первоначальных обстоятельств автоматизированные системы и внутренние базы данных могут продолжать учитывать прежние оценки, влияя на будущие решения.

Шестой риск состоит в правовой неопределённости. Судебная и административная практика, касающаяся допустимости, объяснимости и процессуальной оценки алгоритмических выводов, продолжает формироваться. Это повышает значение квалифицированного правового и технического анализа в каждом конкретном деле.

Institutional Gaps / Институциональные ограничения и системные слабости

Одной из ключевых системных слабостей является опережающее развитие технологий по сравнению с правовыми механизмами контроля. Алгоритмические системы внедряются

быстрее, чем формируются единые стандарты их проверки, раскрытия методологии и процессуального использования.

Существенным ограничением является недостаточная техническая подготовка многих участников правовой системы. Судьи, адвокаты, регуляторы и должностные лица не всегда располагают достаточными знаниями для оценки качества данных, статистических моделей и ограничений конкретных алгоритмов.

Другой проблемой остаётся зависимость от частных разработчиков и поставщиков технологий. Методологии, программные решения и критерии оценки риска нередко являются закрытыми, а доступ к информации о внутренней логике системы ограничен коммерческой тайной или договорными ограничениями.

Сохраняется и информационная асимметрия. Орган, использующий алгоритмическую систему, может обладать значительно большим объёмом данных и технических сведений, чем лицо, чьи права затрагиваются соответствующим решением.

Дополнительной слабостью является ограниченная способность системы к исправлению ошибок. Даже после выявления некорректных данных или необоснованных выводов обновление информации и восстановление правового статуса могут происходить с существенной задержкой.

В совокупности эти факторы создают ситуацию, в которой автоматизированные инструменты способны оказывать значительное влияние на правовые решения при отсутствии полностью сформированных гарантий прозрачности, проверяемости и эффективного судебного контроля.

Practical Guidance / Практические рекомендации и модель правового действия

Первым практическим шагом является установление факта использования автоматизированной системы. В делах, где выводы о риске, благонадёжности, подозрительности или вероятности определённого поведения играют существенную роль, необходимо выяснить, использовались ли алгоритмические инструменты и какое влияние они оказали на итоговое решение.

Вторым шагом является запрос информации о применённой модели. По возможности следует получать сведения о типе системы, источниках данных, критериях оценки, используемой методологии и степени участия человека в принятии окончательного решения.

Третьим шагом является проверка качества исходных данных. Необходимо установить, являются ли использованные сведения актуальными, полными и корректными, а также исключить ошибки в идентификации лиц, транзакций, документов и событий.

Четвёртым шагом является критическая оценка выводов модели. Алгоритмическая рекомендация должна рассматриваться как аналитический инструмент, а не как самостоятельное доказательство. Следует анализировать допущения модели, статистические ограничения и возможные альтернативные объяснения.

Пятым шагом является привлечение независимых специалистов. В сложных делах целесообразно использовать экспертов в области анализа данных, цифровых технологий и статистики для проверки корректности выводов.

Шестым шагом является формирование процессуальной позиции, основанной на принципах прозрачности, объяснимости, законности, соразмерности и права на эффективное оспаривание. Если алгоритмический вывод существенно влияет на права лица, защита должна

добиваться его полноценной проверки и надлежащей оценки судом или компетентным органом.

Policy Recommendations / Рекомендации по правовому и институциональному подходу

Использование искусственного интеллекта в правосудии должно основываться на принципе, согласно которому окончательное решение всегда принимается человеком, несущим полную юридическую ответственность за его содержание и последствия. Автоматизированные системы могут служить вспомогательным инструментом, но не должны подменять независимую оценку доказательств и обстоятельств дела.

Необходимо обеспечивать достаточную прозрачность алгоритмических моделей. Лица, чьи права затрагиваются соответствующими выводами, должны иметь возможность получить информацию о характере используемой системы, типах данных, общих критериях оценки и степени влияния алгоритма на принятое решение.

Следует устанавливать единые стандарты проверки качества данных, используемых для обучения и функционирования моделей. Ошибочные, устаревшие или несбалансированные данные не должны становиться основанием для решений, ограничивающих права и законные интересы.

Суды и регуляторы должны оценивать алгоритмические выводы как доказательственный материал, подлежащий полноценной проверке, а не как автоматически достоверный результат технического процесса. Необходим анализ методологии, ограничений модели и возможных альтернативных объяснений.

Особое значение имеет развитие эффективных процедур исправления ошибок и восстановления статуса. Если автоматизированная система сформировала необоснованный вывод, лицо должно иметь реальную возможность добиться корректировки данных, пересмотра оценки и устранения последствий.

Правовое регулирование должно обеспечивать баланс между использованием технологий для повышения эффективности и сохранением фундаментальных процессуальных гарантий. Скорость обработки данных не может рассматриваться как самостоятельное основание для снижения стандартов справедливого процесса.

Автоматизированные выводы, базы данных и оценка риска в правоприменении: минимальные процессуальные гарантии при использовании ИИ и алгоритмов

Расширение применения алгоритмов, скоринговых моделей и цифровых баз данных в судебных, следственных, регуляторных и квазипубличных процедурах меняет архитектуру доказывания и принятия решений. На практике автоматизированный вывод («высокий риск», «подозрительная активность», «совпадение по базе», «вероятная связь», «аномальный паттерн») нередко становится триггером реальных правовых последствий: розыск и задержание, арест и блокировка активов, отказ в услуге или доступе, миграционные ограничения, усиление процессуальных мер контроля, инициирование проверки или обвинительного сценария. Ключевой риск состоит в том, что вероятностный машинный вывод начинает восприниматься как установленный факт, а источник ошибки смещается в «чёрный ящик» данных, настроек и модели; при этом цифровая среда ускоряет распространение ошибки, а «цифровой след» подозрения живёт дольше, чем память о ручном решении. Практически важно различать (а) допустимость, (б) доказательственный вес и (в) достаточность в совокупности автоматизированных материалов: алгоритмический результат может быть допустимым как повод для проверки или как один из элементов общей картины,

но иметь сниженный доказательственный вес и, как правило, сам по себе не является достаточным основанием для неблагоприятной меры без независимых, проверяемых подтверждений.

1. Обязательная раскрываемость основания (и фиксация в материалах): право знать, что решение опирается на алгоритм, базу или скоринг. Орган, принимающий решение, должен отразить в процессуальном документе (и при необходимости раскрывать стороне): факт использования автоматизированной системы (модель, скоринг, правило, база совпадений); роль системы (триггер проверки, рекомендация, источник доказательственного материала или фактическое основание меры); какие последствия повлекло использование автоматизации. Смысл гарантии: без знания факта автоматизации и её роли невозможно эффективно оспаривать ошибку, а суду затруднительно корректно оценить допустимость, вес и достаточность материала.

2. Разведение трёх уровней: данные → модель/правило → правовой вывод. Следует методологически отделять первичные данные (записи, документы, логи, реестры) от алгоритмической обработки (признаки, пороги, правила, обученная модель) и от правовой квалификации и меры. В мотивировке должно быть видно, какие факты установлены независимо, а где присутствует вероятностная интерпретация; правовой вывод не должен подменяться формулой «система присвоила высокий риск» безотносительно к индивидуальным обстоятельствам дела.

3. Проверяемое происхождение данных и качество набора данных (управление данными). В материалах должны быть проверяемо обозначены: источник данных; дата и способ получения; наличие журналов доступа и изменений; правила обновления и исправления; показатели полноты и актуальности; известные классы ошибок (дубли, устаревание, неверная идентификация, «слияние» профилей, смещения по географии, языку или транслитерации). Ошибка базы данных не должна автоматически ухудшать правовое положение лица; если происхождение и качество данных непроверяемы, доказательственный вес результата снижается, а требования к независимым подтверждениям возрастают.

4. Прозрачность логики (объяснимость): не «формула», а проверяемый смысл. Не всегда требуется раскрывать исходный код, однако должны быть доступны (и отражены в объёме, достаточном для проверки): описание логики (какие факторы учитываются и как); пороги срабатывания и их значение; ограничения применимости; чувствительность к ошибкам данных. При принятии решения, затрагивающего фундаментальные права, вывод «система показала риск» без раскрытия логики, порогов и ограничений должен оцениваться как материал со сниженным доказательственным весом и не может быть единственным основанием неблагоприятной меры.

5. Калибровка надёжности: частота ошибок и риск ложноположительных выводов. Орган, опирающийся на скоринг или алгоритм, должен быть готов подтвердить известные метрики качества (включая ложноположительные и ложноотрицательные срабатывания), процедуры валидации и мониторинга деградации модели, а при необходимости — процедуры выявления смещений и дискриминационных эффектов. Если показатели ошибок неизвестны или скрыты, корректный подход — рассматривать результат как ориентир для проверки, а не как самостоятельное основание ограничения прав.

6. Индивидуализация и запрет «автоматического решения»: человек отвечает за итог. Даже при использовании ИИ итоговая мера должна быть результатом самостоятельной человеческой оценки с проверкой контекста; недопустима подмена индивидуального решения «порогом системы». Должностное лицо должно обосновать применимость вывода к конкретному лицу с учётом обстоятельств и рассмотреть существенные альтернативные

объяснения и возражения; ссылка лишь на «высокий риск по системе» без независимой оценки фактов не должна признаваться достаточной мотивировкой.

7. Состязательность: доступ к материалам, право на контрпроверку и независимую экспертизу. Для эффективного оспаривания должны обеспечиваться: доступ к минимуму исходных данных и параметров, необходимых для проверки (какие записи, какие совпадения, какие признаки, какой порог); возможность представить независимое заключение; возможность задавать вопросы ответственному представителю о данных, порогах, ошибках, применимости и ограничениях. При наличии ограничений (тайна, безопасность, коммерческая конфиденциальность) допустимы балансирующие процедуры (закрытый доступ эксперта, редакция, закрытое заседание), но не полное устранение возможности проверки.

8. Процедура исправления: право на корректировку данных и снятие «цифрового следа». Должны существовать механизмы исправления неверных записей; отметки о спорности или обжаловании; синхронизации исправлений между системами и копиями; восстановления статуса после опровержения, чтобы риск-профиль не сохранялся неопределённо долго без актуальных оснований.

9. Пропорциональность и градуировка последствий. Автоматизированный вывод должен запускать последствия, соразмерные его надёжности и проверяемости: низкая или неизвестная надёжность — только мягкие проверочные меры; более высокая подтверждённая плюс независимые данные — возможность более строгих мер; невозможность проверки при высокой цене ошибки — запрет или существенное ограничение использования. Чем менее прозрачен и менее проверяем результат (данные, метод, показатели ошибок), тем меньший доказательственный вес он должен иметь и тем более ограниченными должны быть правовые последствия.

Отдельно следует учитывать, что риски возникают не только при скоринге и работе с базами, но и при использовании генеративных систем для подготовки процессуальных документов: «галлюцинации» (включая несуществующие ссылки на практику и доктрину) способны превращать текст в источник процессуальной ошибки, а ответственность за проверку источников неизбежно остаётся на представителе и стороне; поэтому в делах, где применялись такие инструменты, особенно важны требования раскрываемости роли автоматизации, верифицируемости каждого фактического и правового утверждения и обеспеченности состязательной контрпроверки.

Итоговая формула

Чтобы использование алгоритмов и цифровых систем оценки риска не подрывало справедливый процесс, органу, принимающему решение, следует одновременно обеспечивать раскрываемость факта автоматизации и её роли с фиксацией этого в процессуальном акте; проверяемое происхождение и качество данных; объяснимость логики, порогов и ограничений применимости; известную либо как минимум оцениваемую ошибочность модели; состязательность и реальную возможность контрпроверки, включая независимую экспертизу; индивидуализированное человеческое решение без подмены мотивировки «порогом системы»; действенный механизм исправления данных и восстановления статуса; пропорциональность последствий уровню неопределённости; явное различие допустимости, доказательственного веса и достаточности автоматизированных материалов в совокупности.

Conclusion / Заключение

Искусственный интеллект и автоматизированные системы анализа данных становятся всё более заметным элементом современной судебной, правоохранительной, административной и финансовой инфраструктуры. Их использование может повышать эффективность обработки информации, ускорять выявление связей между данными и помогать органам власти или частным институтам справляться с большими объёмами материалов.

Однако технологическая эффективность не устраняет требований справедливого процесса. Если автоматизированный вывод влияет на решение о свободе, имуществе, миграционном статусе, банковском обслуживании, доступе к активам или иной значимой правовой сфере, такой вывод должен быть проверяемым, объяснимым и оспоримым.

Главная опасность состоит в том, что алгоритмическая оценка может получить фактический авторитет доказательства без прохождения полноценной процессуальной проверки. В таких условиях лицо оказывается в ситуации, когда неблагоприятное решение принято на основе модели, методология которой неизвестна, исходные данные не раскрыты, а механизм исправления ошибок ограничен.

Для ARGА основной вывод состоит в следующем. Применение искусственного интеллекта в правосудии и смежных процедурах должно рассматриваться как отдельное направление правовой защиты. Защита должна включать анализ источников данных, логики модели, степени человеческого контроля, возможности оспаривания и соответствия автоматизированного вывода базовым гарантиям справедливого процесса.

Технологии могут использоваться в правовой системе только при условии, что они не подменяют независимое судебное мышление и не лишают человека возможности понимать, проверять и оспаривать основания решений, затрагивающих его права.

Приложение А. Терминология

Искусственный интеллект. Программная или техническая система, способная на основе данных формировать выводы, рекомендации, прогнозы или решения, влияющие на последующие действия человека или организации.

Автоматизированная система принятия решений. Система, которая полностью или частично обрабатывает данные и формирует результат, используемый при принятии юридически значимого решения.

Алгоритмическая оценка риска. Модель, присваивающая лицу, операции, делу или событию определённый уровень риска на основе заданных параметров и исходных данных.

Объяснимость. Возможность понять, какие факторы повлияли на результат работы системы и каким образом был сформирован соответствующий вывод.

Прозрачность. Доступность информации о характере используемой системы, источниках данных, общих принципах работы и степени влияния на итоговое решение.

Человеческий контроль. Реальная возможность ответственного должностного лица самостоятельно оценить вывод автоматизированной системы, отклонить его и принять собственное мотивированное решение.

Цифровой профиль. Совокупность данных, выводов и оценок, сформированных в отношении лица, операции или объекта на основе автоматизированной обработки информации.

Алгоритмическая предвзятость. Систематическое искажение результата, возникающее из-за качества исходных данных, структуры модели, выбранных критериев или исторически закреплённых неравенств.

Эффективное оспаривание. Возможность лица получить достаточную информацию о неблагоприятном выводе, представить возражения, потребовать проверки и добиться исправления ошибки.

Приложение В. Матрица рисков / полномочий / правовых последствий

Действие	Правовой риск	Юридический предел	Возможные последствия	Практический комментарий
Использование алгоритмической оценки риска	Придание вероятностному выводу значения фактического основания	Риск-оценка не должна заменять индивидуальную судебную или административную проверку	Усиленный контроль, отказ, ограничительная мера, неблагоприятное решение	Необходимо проверять данные, критерии модели и степень влияния вывода на решение
Автоматизированная сортировка дел или заявлений	Неравное распределение внимания и ресурсов	Сортировка не должна приводить к скрытой дискриминации или лишению доступа к рассмотрению	Задержки, приоритетное рассмотрение одних дел и фактическое оттеснение других	Следует анализировать критерии приоритизации и возможность пересмотра
Использование закрытой модели	Невозможность понять основание неблагоприятного вывода	Коммерческая тайна или техническая сложность не должны исключать право на защиту	Ограничение возможности оспаривания, процессуальное неравенство	Нужно добиваться раскрытия хотя бы общих критериев, источников данных и роли модели
Применение ошибочных или устаревших данных	Формирование неверного цифрового профиля	Решения должны основываться на актуальных, точных и проверяемых данных	Неверная классификация, отказ в услуге, ограничение прав	Необходимо требовать исправления данных и пересмотра оценки
Использование алгоритмического вывода в суде	Формальное принятие технического результата как доказательства	Суд должен оценивать методологию, источник данных и альтернативные объяснения	Ошибочные выводы, нарушение равенства сторон, ограничение защиты	Требуется независимая техническая экспертиза и процессуальное оспаривание
Автоматизированная оценка в банковском или комплаенс-контуре	Ограничение доступа к финансовой инфраструктуре без полноценного объяснения	Частная оценка риска не должна превращаться в бессрочное ограничение прав	Блокировка операций, закрытие счёта, сохранение негативного профиля	Следует готовить документированную позицию и добиваться пересмотра
Сохранение негативного цифрового профиля	Продолжение последствий после устранения ошибки	Данные и выводы должны обновляться после изменения обстоятельств	Повторные ограничения, репутационный	Необходимо добиваться удаления или обновления

			ущерб, отказы	новые	устаревших сведений
--	--	--	------------------	-------	------------------------

Данная матрица отражает типовые ситуации, в которых применение искусственного интеллекта и автоматизированных систем может создавать юридически значимые последствия для лица. Её практическая функция состоит в том, чтобы заранее выявлять точки риска, требовать прозрачности и не допускать подмены индивидуальной правовой оценки автоматизированным выводом.

Официальные источники

European Union, Artificial Intelligence Act.

European Union, General Data Protection Regulation (Regulation (EU) 2016/679).

Council of Europe, Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law.

Council of Europe, European Convention on Human Rights.

European Commission for the Efficiency of Justice (CEPEJ), European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their Environment.

Organisation for Economic Co-operation and Development (OECD), OECD Principles on Artificial Intelligence.

United Nations, materials on human rights and digital technologies.

Office of the United Nations High Commissioner for Human Rights (OHCHR), materials on the right to privacy in the digital age.

European Court of Human Rights, case law concerning Article 6 of the European Convention on Human Rights.

European Court of Human Rights, case law concerning Article 8 of the European Convention on Human Rights.