УДК 347.97

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В ПРАВОСУДИИ И ЕГО ВЛИЯНИЕ НА ГАРАНТИИ ФУНДАМЕНТАЛЬНЫХ ПРАВ И СВОБОД ЧЕЛОВЕКА

Юлия РЕПИНА,
кандидат экономических наук, доцент

АННОТАЦИЯ

В статье проведено теоретическое исследование влияния на гарантии фундаментальных прав и свобод человека использования искусственного интеллекта в правосудии. Исследование выявляет возможные проблемы и направления их решения. Одним из самых опасных негативных последствий для гарантии таких прав является угроза защиты персональных данных. Рассмотрена система, состоящая из семи принципов «конфиденциальности по замыслу», внедрение которой способно обезопасить персональные данные. Предоставлена позиция Европейского суда по правам человека касательно защиты персональных данных. Приведены европейские и украинские нормативные акты, регулирующие вопросы защиты персональных данных.

Ключевые слова: искусственный интеллект, правосудие, фундаментальные права человека, «конфиденциальность по замыслу», защита персональных данных.

ARTIFICAL INTELLIGENCE IN JUSTICE AND ITS IMPACT ON FUNDAMENTAL HUMAN RIGHTS AND FREEDOMS

Yuliia RIEPINA,
Candidate of Economic Sciences, Associate Professor

SUMMARY

In the article the theoretical research is providing of the impact on the guarantee of fundamental human rights and freedoms using artificial intelligence in justice. The research identifies possible problems and directions for their solution. One of the most dangerous negative consequences for guaranteeing such rights, the article calls a threat to the protection of personal data. It is considered a system consisting of seven principles, "privacy-by- design", the creation of which is able to protect personal data. The position of the European Court of Human Rights regarding the protection of personal data is given. The European and Ukrainian regulations governing the protection of personal data are presented.

Key words: artificial intelligence, justice, fundamental human rights, "privacy-by-design", protection of personal data.

Постановка проблемы. Развитие информационных технологий (далее – ИТ) – это объективная реальность, с которой надо считаться. Как правило, появление новых ИТ способствует росту эффективности в той области, в которой они применяются. Одной из перспективных технологий, которая постепенно внедряется, в том числе, в сферу права является искусственный интеллект (далее – ИИ).

Европейская комиссия по эффективности правосудия Совета Европы (далее – CEPEJ) в декабре 2018 г. приняла Европейскую хартию этического использования ИИ в судебных системах и смежных областях (European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment) (далее – Хартия) [1]. В этом документе ИИ определяется как набор научных методов, теорий и технологий, нацеленных на воспроизведение при помощи машины когнитивных способностей человеческого мозга.

Актуальность темы исследования. Внедрение ИИ в правосудие требует соблюдения четко определенных условий, поэтому принципы эффективного использования ИИ в правосудии, провозглашенные Хартией, – это сущностные характеристики, которые отвечают за правильное функционирование судебной системы и без которых она не реализует свое предназначение.

Состояние исследования. Внедрение достижений процесса информатизации общества в деятельность органов государственной власти привлекает внимание ученых и практиков, вопросы взаимодействия ИТ, ИИ и правосудия, то есть междисциплинарные темы для научных исследований, вызывающие интерес не только у правоведов, но и у философов, экономистов, историков, специалистов в области компьютерных наук, социальных коммуникаций. Отдельные вопросы применения ИТ в правосудии были предметом исследований А.В. Брынцева, Н.В. Кушаковой-Костицкой, А.Ю. Каламайко, В.С. Петренко, М.Я. Швец и ряда других украинских юристов-ученых. Стоит отметить отсутствие фундаментальных разработок перспектив и проблем использования ИИ в правосудии в отечественной правовой науке при имеющемся запросе практики и общества в целом на такие исследования.

Целью и задачей статьи является исследование проблем и способов их разрешения при использовании ИИ в правосудии для гарантии фундаментальных прав и свобод человека.

Изложение основного материала. Первым принципом Хартия называет принцип уважения фундаментальных прав, согласно которому должна быть обеспечена гарантия соответствия инструментов и сервисов ИИ правам человека и основополагающим свободам (прежде всего, тем, которые провозглашены Европейской конвенцией о защите

прав человека и основополагающих свобод и Конвенцией о защите персональных данных) [1].

В настоящее время гарантия фундаментальных прав и свобод человека является условием развития современного правового государства. Согласно Конституции Украины [2] права и свободы человека, а также их гарантии определяют содержание и направленность деятельности государства.

Права человека в отечественной юридической науке понимаются как определяющие основы правового статуса личности, которые являются основополагающими и принадлежат человеку от рождения, естественными и неотъемлемыми, без которых невозможно существование человека как полноценного общественного существа [3].

Часто такие права называют фундаментальными, то есть основными, главными [4]. При длительном эволюционном процессе выявления, обоснования, описания, поиска средств для защиты этих прав проявились их характерные особенности, такие как неделимость (не реализуются по отдельности), взаимозависимость (отсутствует иерархия), взаимосвязанность (возможность реализации одного из них зависит от возможности реализации всех остальных) и универсальность (принадлежность каждому человеку независимо от территориальных, национальных, религиозных, половых, социальных, возрастных или каких-либо еще особенностей человека).

М. Макдугалл утверждает, что права человека, основанные на принципах свободы, равенства и справедливости и имеющие универсальный характер, закрепляются в национальных конституциях [5]. Н.И. Козюбра видит обязанность государства в обеспечении этих прав посредством установления средств и процедур их реализации и защиты [6].

Обращаясь к Конституции Украины, отмечаем, что Глава 2 полностью посвящена правам, свободам и обязанностям человека и гражданина. Так, в Основном Законе Украины провозглашаются права на жизнь, свободу и личную неприкосновенность, свободу мысли, слова, вероисповедания, эффективное средство юридической защиты, справедливый суд и др., являющиеся общепризнанными в международном праве фундаментальными правами человека.

В XX веке права человека нашли свое отражение в многочисленных международных актах, в частности Общей декларации прав человека 1948 г., Конвенции о защите прав человека и основополагающих свобод 1950 г. [7] (далее – ЕКПЧ), Международном пакте о гражданских и политических правах 1966 г., Международном пакте об экономических, социальных и культурных правах 1966 г.

Появление ИТ вызвало необходимость разработать правила обеспечения защиты каждого лица посредством охраны персональных данных, в 1970-х гг. Комитет Министров Совета Европы принял ряд резолюций о защите персональных данных со ссылкой на статью 8 ЕКПЧ «Право на уважение частной и семейной жизни» [8, с. 17], в 1981 г. была открыта для подписания Конвенция о защите персональных данных [9] (Украина ее ратифицировала 6 июля 2010 г., датой вступления в действие стало 1 января 2011 г.).

Конвенция о защите персональных данных имела целью обеспечить каждому лицу соблюдение его прав и основных свобод, в частности его права на неприкосновенность частной жизни в связи с автоматизированной обработкой его персональных данных. С учетом цели были определены основные принципы защиты данных, которыми стали принцип качества, особенных категорий, безопасности данных, дополнительных гарантий для субъекта данных, санкций и средств правовой защиты, расширения защиты. Так, персональные данные, которые свидетельствуют о расовой принадлежности, политических, религиозных и других убеждениях, а также данные, касающиеся здоровья или интимной жизни, не могут поддаваться автоматической обработке, если внутреннее законодательство не обеспечивает соответствующие гарантии. Это правило применяется и к персональным данным, которые касаются осуждения в уголовном порядке.

При дальнейшем рассмотрения проблемы вызывает интерес предложенная Энн Кавукян (бывшим комиссаром по информации и конфиденциальности в канадской провинции Онтарио) система из семи принципов «конфиденциальности по замыслу» (“privacy-by-design”), соблюдение которых способно привести к созданию универсальной структуры для самой сильной защиты персональных данных, доступной в современных условиях [10].

Первый принцип звучит так: «предупреждение, а не исправление». Подход «конфиденциальности по замыслу» характеризуется скорее превентивными, чем корректирующими средствами. Он предвидит и предотвращает вмешательство в частную жизнь даже до того, как оно произошло. «Конфиденциальность по замыслу» не ждет, пока риски вмешательства в частную жизнь проявятся, при этом не предлагает средства для устранения нарушений конфиденциальности после того, как они произошли, ведь целью является предотвращение их возникновения. Таким образом, «конфиденциальность по замыслу» работает до появления негативного, угрожающего ей факта, а не после.

Вторым принципом системы является «конфиденциальность по умолчанию». «Конфиденциальность по замыслу» стремится достичь максимальной степени конфиденциальности, обеспечивая автоматическую защиту персональных данных в любых информационных системах или бизнес-деятельности (действий нет, а конфиденциальность сохраняется). От лица не требуются какие-либо действия для защиты его данных, ведь защита данных встроена в систему по умолчанию.

Данный принцип поддерживает FIPs (“Fair Information Practices” – это общее название набора стандартов государственных баз использования персональных данных и решения вопросов конфиденциальности и защиты [11]) путем спецификации цели сбора, использования, хранения, предоставления персональных данных, ограничений при сборе персональных данных, минимизации сбора количества персональных дан-

ных, а также лимитирования использования, хранения, предоставления персональных данных.

Если назначение использования персональных данных неясно, должна быть соблюдена презумпция конфиденциальности, а также должно применяться крайне осторожное, предусмотрительное отношение к таким данным, как настройки по умолчанию, обеспечивающие максимальную защиту конфиденциальности.

Третьим принципом называется «конфиденциальность, встроенная в дизайн». «Конфиденциальность по замыслу» встраивается в дизайн и архитектуру информационных систем и бизнес-деятельности, а не прикрепляется в качестве дополнения к ним позже. В результате конфиденциальность является важным компонентом их основных функций, неотъемлемой частью системы без ущерба для ее функциональности. Конфиденциальность внедряется системно, учитывая принятые стандарты и структуры, поддающиеся внешним проверкам и контролю, а также везде, где это возможно, следует тщательно изучать последствия и риски использования персональных данных для конфиденциальности и все меры, принятые для снижения негативного воздействия, включая рассмотрение альтернативных приемов.

«Встроенная конфиденциальность» может влиять на целостный функционал системы, поэтому такое влияние стоит минимизировать, но в то же время она не должна страдать от действий пользователя, неправильной конфигурации или ошибки.

Четвертый принцип звучит так: «полная функциональность – беспроигрышный результат, а не нулевой». «Конфиденциальность по замыслу» стремится соответствовать всему комплексу правовых задач, избегая дихотомий вроде конфиденциальности и безопасности путем демонстрирования возможности соблюдения и того, и другого условия. По своему характеру она позволяет поддерживать полную функциональность в достижении реальных, практических, выгодных нескольким сторонам результатов. Когда конфиденциальность встраивается в уже существующую технологию, процесс или систему, необходимо не допустить нарушений полной функциональности, но при этом максимально оптимизировать все требования. Защита персональных данных часто противопоставляется другим правовым интересам, целям проектирования и техническим возможностям, позиционируясь некоей нулевой суммой. В то же время «конфиденциальность по замыслу» отвергает такой подход, охватывая правовые, не связанные с ограничением приватности цели, а новаторским способом приспосабливает их как некую положительную сумму.

Все интересы и цели должны быть четко записаны, желаемые функции должны быть точно сформулированы и согласованы, а компромиссы – отклонены как зачастую ненужные в пользу поиска такого решения, которое обеспечит многофункциональность.

Пятым принципом объявляется «комплексная безопасность – защита жизненного цикла». «Конфиденциальность по замыслу» встраивается в систему до получения первого фрагмента персональных данных и работает в течение всего жизненного цикла задействованных данных как сильная мера безопасности, необходимая для обеспечения защиты таких данных от начала до конца периода работы с ними. Итак, гарантируется, что все данные надежно сохраняются, а затем надежно и своевременно удаляются, обеспечивается непрерывное и безопасное управление их жизненным циклом.

Защита персональных данных должна быть постоянной. Принципы безопасности здесь актуальны, потому что без сильной безопасности нет конфиденциальности, что является существенным условием. Так, субъекты доступа к персональным данным, требующим защиты, должны взять на себя ответственность за их безопасность (согласно степени чувствительности) на весь жизненный цикл таких данных в соответствии со стандартами, разработанными авторитетными органами. Применяемые стандарты безопасности должны обеспечивать конфиденциальность, целостность и доступность персональных данных на весь их жизненный цикл, в том числе методы безопасного уничтожения, соответствующее шифрование, а также строгие методы контроля доступа и протоколирования.

Шестой принцип звучит так: «видимость и прозрачность». «Конфиденциальность по замыслу» стремится убедить все заинтересованные стороны в том, что независимо от задействованной бизнес-практики или технологии, она фактически работает в соответствии с установленными намерениями и целями, а также подлежит независимой верификации. Ее компоненты и операции остаются видимыми и прозрачными как для пользователей, так и для провайдеров. Помни, доверяй, но проверяй!

Видимость и прозрачность важны для установления ответственности и доверия. Этот принцип хорошо подходит для полного раскрытия FIP, но в целях контроля особый акцент стоит сделать на подотчетности, открытости и согласованности.

Седьмой принцип звучит так: «уважение конфиденциальности пользователя». Прежде всего «конфиденциальность по замыслу» требует, чтобы создатели и операторы руководствовались интересами частных лиц, предлагая строгие настройки конфиденциальности, соответствующие уведомления, а также расширение возможностей пользователя. Результатом является ориентированный на пользователя продукт.

Наилучшие результаты «конфиденциальность по замыслу» обычно имеет тогда, когда она разрабатывается с учетом интересов и потребностей отдельных пользователей, которые в наибольшей степени заинтересованы в управлении своими личными данными.

Предоставление субъектам данных возможности играть активную роль в управлении собственными данными может быть единственной наиболее эффективной проверкой на предмет упущений и злоупотреблений по отношению к конфиденциальности и личным данным. Уважение конфиденциальности пользователя поддерживает FIP, что предполагает согласие, точность, доступ и согласованность.

Так, для сбора, использования или раскрытия персональных данных требуется свободное и четкое разрешение, если иное не предусмотрено законом. При этом чем выше чувствительность данных, тем четче и конкретнее требуется согласие. Позднее согласие может быть отозвано. Персональные данные должны быть точными, полными и актуальными для того, чтобы указанные цели были достигнуты. Каждому лицу должен быть обеспечен доступ к его персональным данным, а также информирование об их использовании и раскрытии. Организации должны создать механизмы подачи жалоб и возмещения ущерба, а также довести до общественности информацию о них, в том числе о доступе к следующему уровню апелляции.

Результатом соблюдения этого принципа является создание не человеко-машинных интерфейсов (“human-machine interfaces”), а человеко-ориентированных (“human-centered”), пользователе-ориентированных (“user-centric”) и удобных пользователю (“user-friendly”) интерфейсов.

Европейский суд по правам человека (далее – ЕСПЧ) неоднократно постановлял, что сбор и хранение персональных данных полицией или органами национальной безопасности предполагают вмешательство в право, гарантированное статьей 8 ЕКПЧ, но в то же время ЕСПЧ вынес много решений, касающихся оправдания такого вмешательства, например дело «Б.Б. против Франции» [12] (ЕСПЧ решил, что включение лица, осужденного за совершение преступления на сексуальной почве, в национальную базу данных судебных решений попало под действие статьи 8 ЕКПЧ, но с учетом того, что были реализованы достаточные гарантии защиты данных, такие как право субъекта персональных данных обращаться с запросом об их изъятии, ограниченность срока их хранения и ограниченный доступ к ним, между конкурирующими частными и общественными интересами был соблюден справедливый баланс, поэтому Суд пришел к выводу, что нарушения статьи 8 ЕКПЧ не было).

В Европейском Союзе 27 апреля 2016 г. был принят (вступил в действие 25 мая 2018 г.) Общий регламент защиты данных, или Новые правила защиты персональных данных (“General Data Protection Regulation”, далее – GDRP) [13]. Его предназначение заключается в усилении и унификации защиты персональных данных всех лиц в ЕС. Среди главных принципов документа провозглашаются принцип законности, справедливости и прозрачности, достижения конкретных целей, минимизации использования данных, точности, ограничения хранения данных, целостности и конфиденциальности/безопасности, подотчетности. Важно, что GDRP обязаны использовать и лица, обрабатывающие данные (они отвечают за непосредственную обработку данных), и лица, собирающие данные (они определяют цель и значение обработки персональных данных).

Именно в этом документе отдельно определяются «чувствительные данные» (“sensitive data”) введением понятия «специальные категории персональных данных» (“special categories of personal data”). К ним относятся данные, раскрывающие расовое и этническое происхождение, политические взгляды, религиозные и философские убеждения, принадлежность к профессиональным объединениям, генетические данные, биометрические данные, позволяющие идентифицировать определенное лицо, сведения о состоянии здоровья, сексуальной ориентации (пункты 13, 14, 15 статьи 4, статья 9, вступление, пункты 51–56 GDRP).

Для регулирования подобных отношений в Украине 1 июня 2010 г. Был принят Закон Украины «О защите персональных данных» [14], который распространяется на деятельность по обработке персональных данных, осуществляемой полностью или частично с применением автоматизированных средств, а также на обработку персональных данных, которые находятся в картотеке или предназначены к внесению в картотеку с применением неавтоматизированных средств. Стоит отметить, что в Украине уже с 1994 г. действует Закон Украины «О защите информации в информационно-телекоммуникационных системах» [15], которым регулируются отношения в сфере защиты информации в информационных, телекоммуникационных и информационно-телекоммуникационных системах.

Несомненно, обработка судебных решений и данных должна проводиться с четкими целями, совместимыми с правами и свободами, а также гарантированными ЕКПЧ и Конвенцией о защите персональных данных.

При использовании инструментов ИИ при юридическом споре, помощи при принятии судебного решения или предоставлении рекомендаций общественности необходимо обеспечить соблюдение (не нарушение) гарантий права на доступ к правосудию и права на справедливый суд (равенство прав и соблюдение состязательности процесса). Кроме этого, обязательным является надлежащее соблюдение принципов верховенства права и независимости судьи в процессе принятия решения.

По мнению экспертов (например, [1]), преимущества стоит предоставлять таким типам программных разработок, как «разработки этические по замыслу (“ethical-by-design”), когда этический выбор по инерции делается разработчиками программы, поэтому не остается пользователю, и «разработки, ориентированные на права человека» (“human-rights-by-design”). Это означает, что на отдельных этапах проектирования и машинного обучения программы интегрируются правила, которые запрещают прямое или непрямое нарушение защищенных конвенциями фундаментальных прав.

Вопросы этичности и неэтичности являются широко дискутируемыми, но акцент стоит сместить на проблему разработки возможных средств защиты [16].

Выводы. В Украине разработана и утверждена «Национальная стратегия в сфере прав человека», одним из направлений которой определено обеспечение права на справедливый суд, а также создана и функционирует экспертная группа по правам человека при Министерстве юстиции Украины. Совет судей Украины в мае 2018 г. в своем Решении «О мерах по разработке и организации мероприятий по обеспечению независимости

судов и судей» № 22 отметил необходимость совместных действий судебной, исполнительной и законодательной ветвей власти.

Развитие ИТ, появление ИИ в судебной сфере являются неизбежными явлениями, способными оказать положительное влияние на правосудие в целом. Необходимо тесное сотрудничество специалистов в компьютерных областях знаний и представителей юридических профессий.

Для гарантии фундаментальных прав человека ИТ вообще и ИИ в частности должны содержать встроенные в них стандарты, протоколы, процессы, которые не смогут нарушить такие гарантии. Какие бы ИТ не использовались в судебной системе и смежных с нею областях, ее основная функция, а именно правосудие, должна быть реализована.

Список использованной литературы:

1. European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment ; adopted at the 31st plenary meeting of the CEPEJ (Strasbourg, 3–4 December 2018). URL: https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699.

2. Конституция Украины : принята на пятой сессии Верховной Рады Украины 28 июня 1996 г. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр.

3. Юридична енциклопедія : в 6 т. / редкол.: Ю.С. Шемчушенко (голова редкол.) та ін. Київ : Українська енциклопедія, 1998. Т. 4 : Н–П, 2002. 710 с.

4. Ожегов С.И. Словарь русского языка: около 57 000 слов / под ред. Н.Ю. Шведовой. 18-е изд., стереотип. Москва : Русский язык, 1987. 746 с.

5. McDougal M.S., Gerhard B. Human Rights in the United Nations. *Faculty Scholarship Series*. 1964. № 2606. URL: https://digitalcommons.law.yale.edu/fss_papers/2606.

6. Козюбра М.І. Право і людина: лінії взаємозв'язку та тенденції розвитку. *Наукові записки НаУКМА. Юридичні науки*. 2015. Т. 168. С. 3–9.

7. Конвенция о защите прав человека и основополагающих свобод. URL: https://www.echr.coe.int/Documents/Convention_RUS.pdf.

8. Посібник з європейського права у сфері захисту персональних даних. Київ : К.І.С., 2015. 216 с.

9. Конвенция о защите частных лиц в отношении автоматизированной обработки данных личного характера. URL: https://rm.coe.int/1680078c46.

10. Cavoukian A. Privacy by Design. The 7 Foundational Principles. Implementation and Mapping of Fair Information Practices. URL: https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf.

11.Dixon P. A Brief Introduction to Fair Information Practices. URL: https://www.worldprivacyforum.org/2008/01/report-a-brief-introduction-to-fair-information practices.

12. ЄСПЛ, «Б.Б. проти Франції» від 17 грудня 2009 р. № 5335/06. *Посібник з європейського права у сфері захисту персональних даних*. Київ : К.І.С., 2015. С. 157.

13. General Data Protection Regulation (GDRP): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 // OJ L 119/1, 4.5.2016. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF.

14. Про защиту персональных данных : Закон Украины от 1 июня 2010 г. № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17.

15. Про защиту информации в информационно-телекоммуникационных системах : Закон Украины от 5 июля 1994 г. № 80/94-ВР. URL: https://zakon.rada.gov.ua/laws/card/80/94-вр.

16. Leidner J.L., Plachouras V. Ethical by Design: Ethics Best Practices for Natural Language Processing. *Proceeding of the First Workshop on Ethics in Natural Language Processing*. Valencia, Spain. April 4th, 2019. P. 30–40. URL: https://www.aclweb.org.ua/ anthology/W17-1604.

17. Национальная стратегия в сфере прав человека : утверждена Указом Президента Украины от 25 августа 2015 г. № 501/2015. URL: https://zakon.rada.gov.ua/laws/show/501/2015.

18. О мерах по разработке и организации мероприятий по обеспечению независимости судов и судей : Решение ССУ от 18 мая 2018 г. № 22. URL: http://rsu.gov.ua/ua/documents?id=80&page=10&per-page=8.

ИНФОРМАЦИЯ ОБ АВТОРЕ

Репина Юлия Сергеевна – кандидат экономических наук, доцент

INFORMATION ABOUT THE AUTHOR

Riepina Yuliia Sergeevna – Candidate of Economic Sciences, Associate Professor

riepina.yuliya@gmail.com