

КИБЕРПРЕСТУПНОСТЬ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

CYBERPRESSURE AND INFORMATION SECURITY

УДК 34:004.8

DOI dx.doi.org/10.24866/1813-3274/2018-3/55-68

Р. И. Дремлюга¹

Дальневосточный федеральный университет, г. Владивосток, Россия

E-mail: dremluga.ri@dvfu.ru

А. С. Кошель²

Дальневосточный федеральный университет, г. Владивосток, Россия

E-mail: koshel.as@dvfu.ru

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ КАК СОЦИАЛЬНЫЙ РЕГУЛЯТОР: ЗА И ПРОТИВ³

Аннотация. Цифровизация влияет не только на общественные отношения, но и грозит замещением права, как регулятора отношений, на новые формы регулирования. Это означает, что в ближайшем будущем под влиянием цифровизации программный код (алгоритмы) может выполнять регуляторную функцию. Анализ процессов цифровизации позволяет прогнозировать изменение механизма правообразования и композиции существующей модели социального регулирования, коррекцию границ известных социальных регуляторов и образование в ней ниши, которую займёт программный код. По факту регулирующий алгоритм – это программный код, автоматически контролирующий или влияющий на поведение людей. Новые методы технологий искусственного интеллекта (например, глубокое машинное

¹ Роман Игоревич Дремлюга, кандидат юридических наук, доцент Юридической школы Дальневосточного федерального университета, Владивосток, Россия.

² Алексей Сергеевич Кошель, кандидат политических наук, доцент кафедры конституционного и административного права Юридической школы Дальневосточного федерального университета, Владивосток, Россия.

Для цитирования: Дремлюга Р. И., Кошель А. С. Искусственный интеллект как социальный регулятор: за и против // Азиатско-Тихоокеанский регион: экономика, политика и право. 2018. № 3. С. 55–68.

³ Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18-29-16129.

обучение) позволяют выявить неочевидные зависимости, недоступные для обнаружения человеком или обычными техническими методами. Интеллектуальные системы будут и должны внедряться в регулирование общественных отношений. Это эффективней как с экономической, так и с точки зрения достижения желаемого результата.

Поведенческие нормы, обеспечиваемые с помощью автоматизированной системы, могут быть простым, фиксированным (но перепрограммируемым) стандартом поведения, который вносится оператором системы. На уровне сбора и мониторинга информации система может работать как простой регистратор нарушений правил поведения. Такие компьютерные программы используют технологию искусственного интеллекта и посредством анализа истории предыдущих ситуаций и сравнения полученных взаимосвязей обучаются для выявления нарушений, совершаемых в настоящий момент.

Несмотря на очевидные преимущества использования компьютерных программ для регулирования поведения общества, некоторые их свойства и побочные эффекты использования систем порождают вопросы в сфере права. Во-первых, подобные системы могут с большой вероятностью из общедоступных фактов о человеке выявлять характеристики, не являющиеся общедоступными и даже личными. Во-вторых, так как системы зачастую обучаются на решениях или информации, созданных людьми, они могут унаследовать человеческие заблуждения. В-третьих, серьезным вызовом является вопрос кибербезопасности подобных систем.

Ключевые слова: искусственный интеллект, цифровая экономика, алгоритмическое регулирование, программный код, социальные регуляторы, правотворчество, правоприменение, интеллектуальные системы, кибербезопасность систем.

Roman I. Dremluga¹

Far Eastern Federal University, Vladivostok, Russia

E-mail: dremluga.ri@dvfu.ru

Alexey S. Koshel²

Far Eastern Federal University, Vladivostok, Russia

E-mail: koshel.as@dvfu.ru

**ARTIFICIAL INTELLIGENCE AS A SOCIAL REGULATOR:
PROS AND CONS³**

Abstract. Digitalization affects not only public relations; it also threatens to replace law by new forms of regulation. It means that in the near future, under the influence of digitalization, the program code (algorithms) can perform a regulatory function. The analysis of digitalization processes allows predicting changes in the mechanism of law formation and composition. It would be reflected in the change of the existing model of social regulation, the correction of the boundaries of well-known social regulators and the formation of a niche in it that the program code will occupy. In fact, the regulatory algorithm is a program code that automatically controls or influences the behavior of people. New methods of artificial intelligence technologies (for example, deep machine learning) make it possible to identify non-obvious dependencies inaccessible to humans or conventional technical methods. Intellectual systems will and should be implemented in the regulation of social relations. This is more effective both economically and in terms of achieving the desired result. The behavioral norms controlled by an automated system can be a simple, fixed (but reprogrammable) standard of behavior that is entered by the system operator. At the level of information collection and monitoring, the system can operate as a simple recorder of violations of the rules of conduct. Such computer programs use artificial intelligence technology and by analyzing the history of previous situations and comparing the relationships obtained, they are trained to identify violations committed at the moment. Despite the obvious advantages of using computer programs to regulate the behavior of society, some of their properties and side effects of using systems raise questions in the field of law. Firstly, such systems are likely to reveal characteristics that are not publicly available or even personal from the publicly available facts about a

¹ Roman I. Dremluga, candidate of legal Sciences, associate Professor of the Law school of the Far Eastern Federal University, Vladivostok, Russia.

² Alexey S. Koshel, candidate of political Sciences, associate Professor of the Department of constitutional and administrative law, Law school of the Far Eastern Federal University, Vladivostok, Russia.

For citing: Dremluga R. I., Koshel A. S. Artificial intelligence as a social regulator: pros and cons // Asia-Pacific RIM: Economic, Politics, Law. 2018. № 3. P. 55–68.

³ The reported study was funded by RFBR according to the research project № 18-29-16129.

person. Secondly, since systems are often trained on solutions or information created by people, they can inherit human delusions. Third, the cybersecurity of such systems is a serious challenge.

Keywords: artificial intelligence, digital economy, algorithmic regulation, program code, social regulators, lawmaking, law enforcement, intellectual systems, cybersecurity systems.

В последние годы мы можем наблюдать стремительную цифровизацию России и всего мира. Прежде всего это относится к экономической сфере. Президент Российской Федерации В.В. Путин не раз подчёркивал важность развития в нашем государстве сектора цифровой экономики [8]. Важным шагом в этом направлении было принятие федеральной программы «Цифровая экономика Российской Федерации» [1]. В тексте программы подчёркивается, что «цифровая экономика представляет собой хозяйственную деятельность, ключевым фактором производства в которой являются данные в цифровой форме...» [1]. Клаус Шваб, который является основателем и бессменным президентом экономического форума в Давосе, в своем бестселлере «Технологии Четвёртой промышленной революции» заявляет о беспрецедентном проникновении цифровых технологий во все сферы жизни, скорость которого (проникновения) только увеличивается [7]. Отдельно автор выделяет технологию искусственного интеллекта, говоря о том, что «искусственный интеллект уже перестраивает цифровую экономику и вскоре изменит экономику материального мира» [7].

Прогресс в области технологий является движущим фактором развития экономики и общества. Абсурдно было бы предполагать, что этот прогресс не затронет государственную и правовую сферы. Тренды цифровизации влияют как на практику правоприменения и профессиональную среду юристов, так и на само право.

Необходимо отметить, что влияние цифровизации на право в целом носит обширный характер. Как справедливо отмечают российские авторы, «цифровизация оказывает заметное воздействие на право не только как на систему общеобязательных правил поведения, установленных государством, но и как на процесс и результат его деятельности, правовой порядок с реальными правоотношениями, действиями субъектов права и видами юридической деятельности. Она становится важным фактором, обуславливающим динамику права» [11, с. 10].

Цифровизация влечёт за собой возникновение новых общественных отношений, которые до этого момента не существовали. Ряд учёных акцентируют внимание на возможном появлении новых субъектов права, например, системах искусственного интеллекта, которые обладают автономией воли и интеллекта [25]. Другие исследователи отмечают возникновение общественных отношений, складыва-

ющихся по поводу «нетипичных объектов – информации, цифровых технологий (финтех, регтех и др.), создаваемых посредством применения новых цифровых сущностей (криптовалюты) и объектов материального мира, а также связанных с использованием и оборотом того и другого» [11, с. 10].

Цифровизация влияет не только на общественные отношения, но и грозит замишением права, как регулятора отношений, на новые формы регулирования. Некоторые авторы небезосновательно полагают, что технологии могут не только помочь праву выполнять его функции, но и «потеснить», заменить его [11, с. 10]. По факту это уже происходит, например, блокчейн технология [18] по сути выполняет регуляторную функцию при осуществлении сделки или осуществлении платежа без участия права и даже вопреки ему¹. Есть обоснованные прогнозы, что технология блокчейн оставит без работы нотариусов [9].

Это означает, что в ближайшем будущем под влиянием цифровизации программный код (алгоритмы) может выполнять регуляторную функцию. Такое регулирование в зарубежной литературе называется «алгоритмическим регулированием» [27]. Как отмечают российские исследователи, «анализ процессов цифровизации позволяет прогнозировать изменение механизма правообразования и композиции существующей модели социального регулирования, коррекцию границ известных социальных регуляторов и образование в ней ниши, которую займет программный код» [11, с. 10].

По факту регулирующий алгоритм – это программный код, автоматически контролирующий или влияющий на поведение людей. Попытки внедрения программного кода для регулирования общественных отношений предпринимались и раньше, но наибольшее распространение такие разработки получили с развитием технологий искусственного интеллекта и машинного обучения [26].

В свете тотальной цифровизации всё чаще общественные отношения осуществляются посредством цифровых технологий. Следовательно, проще регулировать поведение субъектов отношений с помощью программного кода, так как можно легко написать и обучить (если речь об искусственном интеллекте) компьютерную программу, которая автоматически вмешается в случае нежелательного поведения, заблокирует возможность субъекта для повторения подобного, повлияет на его поведение в будущем и т.д.

Регулирование может исходить как от государства, так и от субъектов общественных отношений (физические и юридические лица). Например, Facebook (крупнейшая социальная сеть) в автоматическом режиме (с помощью программного кода) борется против нарушений прав ребёнка, нарушения интеллектуальных прав, публикации сообщений, провоцирующих межнациональную рознь, и т.д. То есть алгоритм

¹ Во многих странах блокчейн и блокчейн-платежи не признаются государством.

сам принимает решение о том, что материал, опубликованный пользователем Facebook, нарушает права ребёнка. Лишь в случае, если пользователь не согласен с принятым решением, к разрешению спорной ситуации подключаются люди.

В Великобритании и России уже сегодня применяются элементы непосредственного участия граждан в правотворческом процессе. Так, к примеру, правотворческая инициатива в закрытой британской социальной сети Jolistics проходит премодерацию самими же участниками социальной сети и, при получении необходимого числа одобрений участников социальной сети, направляется члену Палаты общин, который вправе реализовать её посредством права законодательной инициативы [6]. Одним из предлагаемых О.А. Антоновой и др. исследователями элементов демократизации и расширения применения права народной законодательной инициативы является использование поддержки выдвижения Народного законопроекта посредством SMS-сообщений [3; 4]. Однако, по мнению профессора права Университета Пенсильвании К. Коглианиса, использование современных технологий само по себе не может оказать заметное влияние на участие граждан в процессе нормотворчества, взамен того, наоборот, может оказать негативное воздействие на процесс нормотворчества [12].

Интеллектуальные системы регулирования с помощью программного кода могут выполнять три ключевых функции:

- Автоматическое формирование правил;
- Автоматический сбор и анализ информации о поведении субъектов;
- Выявление нарушений и применение санкций.

Поведенческие нормы, обеспечиваемые с помощью автоматизированной системы, могут быть простым, фиксированным (но перепрограммируемым) стандартом поведения, который вносится оператором системы. Примером такой простой формы алгоритмического вмешательства, где правила устанавливаются оператором, является использование защиты паролем, когда система автоматически проверяет надёжность пароля и заставляет пользователя его изменить, если пароль не достаточно надёжный. Правила установления пароля при этом заранее определены оператором (например, минимальное количество символов). Альтернативно, поведенческий стандарт может быть адаптивным и подстраиваться под достижение какой-либо фиксированной, всеобъемлющей (но перепрограммируемой) цели. Такие системы часто называют «сложными» или «интеллектуальными», например, интеллектуальные транспортные системы, которые эффективно учатся определять наиболее надёжного предиктора потока трафика, применяя при этом процессы машинного обучения, к постоянно обновляемым в режиме реального времени данным о трафике.

Интеллектуальные системы уже участвуют в формировании правовых норм. Например, согласно описанию в функционал новой системы, разработанной для обеспечения законодательной деятельности в Российской Федерации, входят [2]:

автоматизированная подготовка документов, долгосрочное, среднесрочное и краткосрочное планирование; семантическая обработка протоколов заседаний и автоматическая регистрация решений из протоколов; интегрированная нормативно-справочная подсистема; генерация шаблонов размещаемых документов в системе с учётом зарегистрированных учётных данных; возможность оперативного уведомления участников законотворческой деятельности об изменениях с объектами законотворчества; автоматический контроль размещаемых документов и реквизитов.

На уровне сбора и мониторинга информации система может работать как простой регистратор нарушений правил поведения. Например, автоматизированные системы определения скорости транспортного средства, которые используют камеры контроля скорости для обеспечения в реальном времени идентификации транспортных средств, которые превышают предписанные ограничения скорости.

Примером сложной системы выявления являются компьютерные программы обнаружения мошенничества с кредитными картами, которые используют методы машинного обучения для профилирования кредитных моделей расходов. Подобные системы нацелены на обнаружение подозрительных транзакций и, в случае их совершения, они автоматически блокируют транзакцию и(или) информируют держателя карты.

Такие компьютерные программы используют технологию искусственного интеллекта и посредством анализа истории предыдущих ситуаций и сравнения полученных взаимосвязей обучаются для выявления нарушений, совершаемых в настоящий момент.

Кроме того, интеллектуальные системы могут выявлять правонарушения до их совершения. Подобные системы не являются лишь научной разработкой [13] и давно используются правоохранительными органами различных стран [28]. Например, одной из первых разработок в сфере искусственного интеллекта для прогнозирования преступности является программное обеспечение PredPol, разработанное учёными из Калифорнийского университета. Данная интеллектуальная система используется по всей территории США, а в тестовом режиме – в столице Уругвая Монтевидео, британском графстве Кент и японской префектуре Канагава. Система выдаёт информацию, состоящую из трёх переменных: тип, время и место неблагоприятного события. Используя отчёты о преступности за широкие промежутки времени (годы и даже десятилетия), алгоритм определяет районы, где самый высокий уровень вероятности потенциальных преступлений [16].

Имея достаточно большое количество данных о желательном или нежелательном поведении, можно легко обучить искусственный интеллект выявлять с достаточно большой долей вероятности подобное поведение в будущем [17].

Некоторые системы могут автоматически принимать решение о применении санкций или других методов управления поведением человека без необходимости вмешательства посторонних лиц. Подобные компьютерные программы также могут

работать в опережающем режиме, основываясь на алгоритмически определённых прогнозах будущего поведения кандидата. Такой принцип давно используется в интеллектуальных системах, оценивающих возможность выдачи кредита, страховое покрытие и кадровый потенциал при трудоустройстве [20].

Самыми «печально известными» системами, которые автоматически применяют санкции к нарушителям, являются разработки военного назначения. Например, на границе между Северной и Южной Кореей используется интеллектуальное вооружение, которое автоматически открывает огонь по лицам, пересекающим границу [23], подобные системы планируется использовать и на границе Турции с Сирией [29]*. Чаще такие подобные предиктивные системы просто блокируют возможность завершения противоправной операции и её повторения.

Авторы, анализирующие системы «алгоритмического регулирования», выделяют четыре основные характеристики, необходимые для их функционирования:

- глубокое понимание желаемого результата;
- измерение в реальном времени для определения, если этот результат достигается;
- прописанные алгоритмы (то есть набор правил), которые вносят коррективы на основе новых данных;
- периодический, более глубокий анализ правильности и эффективности самих алгоритмов [21].

Внедрение компьютерных систем для регулирования поведения граждан имеет несомненные преимущества, которые стали ещё более очевидны при широком распространении систем искусственного интеллекта. Во-первых, использовать такие системы гораздо дешевле, чем содержать штат сотрудников, регистрирующих, анализирующих и принимающих решение о реакции на правонарушение. Во-вторых, такие системы, за некоторым исключением, гораздо объективней человека. В-третьих, искусственный интеллект гораздо эффективней, так как может работать 24 часа в сутки 7 дней в неделю с большей точностью.

Кроме того, благодаря использованию алгоритмов машинного обучения, сетевой коммуникационной инфраструктуре и облачным вычислениям, можно отслеживать и вмешиваться в поведение не только одного пользователя, но и всего населения, проживающего на каком-либо значительном географическом пространстве. Такая система может в режиме реального времени воздействовать на поведение и менять своё представление о поведении людей. Подобные разработки гораздо лучше анализируют взаимосвязи, прогнозируют будущие правонарушения и выявляют общие тенденции. Следует отметить, что новые методы технологий искусственного

* Для получения дополнительной информации о платформе стабилизированного оружия ASELSAN см.: www.aselsan.com.tr.

интеллекта (например, глубокое машинное обучение) позволяют выявить неочевидные зависимости, недоступные для обнаружения человеком или обычными техническими методами [14].

Несмотря на очевидные преимущества использования компьютерных программ для регулирования поведения общества, некоторые их свойства и побочные эффекты использования систем порождают вопросы в сфере права. Во-первых, подобные системы могут с большой вероятностью из общедоступных фактов о человеке выявлять характеристики, не являющиеся общедоступными и даже личными. Вот несколько небольших примеров. Одна из интеллектуальных систем может с высокой степенью достоверности установить сексуальную ориентацию по фотографии человека [19]. Другая способна распознать политические убеждения и уровень интеллекта [15]. Такая функциональность систем может привести к возможности дискриминации политической оппозиции, сексуальных меньшинств и других групп, причастность к которым ранее можно было установить только при явном желании лица. Получается, что благая цель профилактики правонарушений может обернуться тотальным контролем не только поведения, но и внутренних убеждений и предпочтений.

Во-вторых, так как системы зачастую обучаются на решениях или информации, созданных людьми, они могут унаследовать человеческие заблуждения. Пожалуй, самым известным примером является американская система, помогающая судьям оценить риск повторного совершения правонарушения. Система обучалась на выборке случаев повторного совершения преступлений за достаточно большой промежуток времени и в результате чаще выдавала высокий риск для «чернокожих» преступников. Некоторые исследования показали, что система действительно чаще ошибалась в пользу белых преступников [30].

Так как интеллектуальная система зачастую учится на уже существующей информации, она наследует все предубеждения тех лиц, которые эту информацию формировали. Например, если мы проектируем систему выявления правонарушений и берём информацию о предыдущих правонарушениях, мы должны делать поправку на то, что полиция больше времени проводит в неблагополучных районах и, следовательно, оттуда получает наибольшее количество выявленных правонарушений. Кроме того, у лиц, проживающих в этих районах, нет денег на квалифицированную юридическую помощь и больше вероятность попасть в списки правонарушителей. Получается замкнутый круг: интеллектуальная система будет всё больше внимания уделять неблагополучным районам и выявлять там правонарушителей, что ещё больше увеличит рейтинг «неблагополучности» и заставит выявлять правонарушителей в этих районах.

В-третьих, серьёзным вызовом является вопрос кибербезопасности подобных систем. В настоящее время хакеры являются достаточно серьёзной угрозой мировой стабильности. Если допустить возможность, что они смогут вмешиваться в во-

просы правотворчества и правоприменения, то угроза в разы возрастает. В мире не существует программ, в которых нет уязвимостей. Средний для отрасли информационных технологий показатель примерно 1–25 ошибок на 1000 строк кода в готовом программном обеспечении, разрабатывавшемся с использованием разных методик. Каждая ошибка – это потенциальная уязвимость [5]. Говоря простым языком, уязвимости есть в любых программах, и вопрос только в оценке рисков. В случае, когда некорректная работа регулирующей системы может подорвать доверие к государству в целом, потенциальные риски достаточно высоки.

Подводя итоги, следует отметить, что бессмысленно сопротивляться прогрессу. Интеллектуальные системы будут и должны внедряться в регулирование общественных отношений. Это эффективней как с экономической, так и с точки зрения достижения желаемого результата. Несмотря на явные преимущества, такие системы должны внедряться с большой осторожностью, принимая во внимание последующие негативные эффекты.

СПИСОК ЛИТЕРАТУРЫ

1. Об утверждении программы «Цифровая экономика Российской Федерации»: распоряжение Правительства Российской Федерации от 28 июля 2017 г. № 1632-р // Собрание законодательства Российской Федерации. – 2017. – 7 авг., № 32. – Ст. 5138.
2. Перечни законопроектов и проектов постановлений [Электронный ресурс] // Система обеспечения законодательной деятельности. – Режим доступа: <http://sozd.duma.gov.ru/>.
3. Антонова, О. А. Законодательная инициатива граждан как форма участия в управлении делами общества и государства // Вестник Прикамского социального института. – 2018. – № 2 (80). – С. 6–13.
4. Дворников, Д. В. Концепция электронного опроса избирателей при сборе подписей в поддержку выдвижения кандидатов в депутаты (на выборные должности) (sms-выдвижение) / Д. В. Дворников, В. В. Красинский, А. С. Пучнин // Вестник Тамбовского университета. Сер. : Гуманитарные науки. – 2010. – № 9 (89). – С. 250–255.
5. Дик, Д. И. Оценка уровня безопасности информационной системы на основе анализа количества ошибок в программном коде / Д. И. Дик, В. М. Солодовников // Вестник Курганского государственного университета. Сер.: Технические науки. – 2015. – № 3 (37). – С. 32–35.
6. Жожина, М. О демократизации законодательного процесса в Российской Федерации / М. Жожина, Н. В. Михайлова // Этносоциум и межнациональная культура. – 2017. – № 3 (105). – С. 9–14.

7. Клаус, Ш. Технологии Четвертой промышленной революции / Ш. Клаус. – М. : ЭКСМО, 2018. – 320 с.
8. Латухина, К. Владимир Путин: Внедрить цифровые технологии во все сферы жизни [Электронный ресурс] // Российская газета. – 2017. – 4 июня. – Режим доступа: <https://rg.ru/2017/06/04/reg-szfo/vladimir-putin-vnedrit-cifrovye-tehnologii-vo-vse-sfery-zhizni.html>.
9. Радченко, И. В. Вытеснит ли технология «блокчейн» нотариуса // Нотариальный вестникъ. – 2017. – № 8. – С. 42–44.
10. Унижаев, Н. В. Проблемы использования технологии блокчейн в цифровой экономике // Альманах мировой науки. – 2018. – № 3 (23). – С. 211–215.
11. Хабриева, Т. Я. Право перед вызовами цифровой реальности // Журнал российского права. – 2018. – № 9 (261). – С. 5–16.
12. Coglianese, C. The Internet and citizen participation in rulemaking // A Journal of law and policy. – 2005. – Vol. 1, iss. 1. – P. 33–57.
13. Deshmukh, S. S. Prediction of crime hot spots using spatiotemporal ordinary kriging / S. S. Deshmukh, B. Annappa // Studies in Computational Intelligence. – 2019. – Vol. 771. – P. 683–691.
14. Big Data. Bigger Dilemmas : A critical review / H. Ekbia, M. Mattioli, I. Kouper [et al.] // Journal of the Association for Information Science and Technology. – 2015. – Vol. 68. – P. 1523–1545.
15. Face-reading AI will be able to detect your politics and IQ, professor says [Электронный ресурс] // The Guardian. – 2017. – 12 September. – Режим доступа: <https://www.theguardian.com/technology/2017/sep/12/artificial-intelligence-face-recognition-michal-kosinski>.
16. Nevett, J. The real minority report: Police trial AI to predict and prevent crimes before they happen [Электронный ресурс] // Daily Star. – 2018. – January 29. – Режим доступа: <https://www.dailystar.co.uk/news/world-news/677796/artificial-intelligence-japan-kanagawa-police-predict-minority-report-2020-olympics>.
17. Miller, A. What do we worry about when we worry about price discrimination? The law and ethics of using personal information for pricing // Journal of Technology Law and Policy. – 2014. – Vol. 19. – P. 41–95.
18. Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system [Электронный ресурс]. – Режим доступа: <https://bitcoin.org/bitcoin.pdf>.
19. New AI can guess whether you're gay or straight from a photograph [Электронный ресурс]. – Режим доступа: <https://www.theguardian.com/technology/2017/sep/07/new-artificial-intelligence-can-tell-whether-youre-gay-or-straight-from-a-photograph>.
20. O’Neil, C. Weapons of math destruction: how big data increases inequality and threatens democracy / C. O’Neil. – New York : Allen Lane, 2016. – 259 p.

21. O'Reilly, T. Open data and algorithmic regulation // *Beyond transparency: open data and the future of civic innovation* / ed. By B. Goldstein, D. Dyson. – San Francisco : Code for America Press, 2013. – P. 289–300.
22. Pagallo, U. Algo-rhythms and the beat of the legal drum // *Philosophy and Technology*. – 2018. – Vol. 3, iss. 14. – P. 507–524.
23. Parkin, S. Killer Robots: The soldiers that never sleep [Электронный ресурс] // BBC. – 2015. – July 16. – Режим доступа: <http://www.bbc.com/future/story/20150715-killer-robots-the-soldiers-that-never-sleep>.
24. Super aEgis II [Электронный ресурс]. – Режим доступа: http://www.doda.am.com/eng/sub2/menu2_1_4.php.
25. Solaiman, S. M. Legal personality of robots, corporations, idols and chimpanzees: a quest for legitimacy // *Artificial Intelligence and Law*. – 2017. – Vol. 25, iss. 2. – P. 155–179.
26. Bryson, J. J. Of, for, and by the people: the legal lacuna of synthetic persons / J. J. Bryson, M. E. Diamantis, T. D. Grant // *Artificial Intelligence and Law*. – 2017. – Vol. 25, iss. 3. – P. 273–291.
27. Yeung, K. Algorithmic regulation: A critical interrogation // *Regulation and Governance*. – 2018. – Vol. 12, iss. 4. – P. 505–523.
28. Yi Shu Ng. China is using AI to predict who will commit crime next. July 24, 2017 [Электронный ресурс]. – Режим доступа: <https://mashable.com/2017/07/24/china-ai-crime-minority-report/#QKYhs4z.qqqR>.
29. Şafak, Y. Turkey starts building automatic shooting gun towers at Syrian border. May 30, 2016 [Электронный ресурс]. – Режим доступа: <http://www.yenisafak.com/en/news/turkey-starts-building-automatic-shooting-gun-towers-at-syrian-border-2473487>.
30. Zone of ethics. Propublica. 2016 [Электронный ресурс]. – Режим доступа: <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>.

REFERENCES

1. On approval of the program «Digital economy of the Russian Federation»: The decree of the Russian Federation Government from July 28, 2017 No. 1632-p. *Collection of legislation of the Russian Federation*, 2017, August 8, no. 32, pp. 5138. (In Russian).
2. *Legislative Support System. Lists of Draft Laws and Draft Resolutions*. Available at: http://ppr.ru/projects/?id_4=8 (accessed 17 July 2018). (In Russian).
3. Antonova O.A. Zakonodatel'naya initsiativa grazhdan kak forma uchastiya v upravlenii delami obshchestva i gosudarstva [The Legislative initiative of citizens as a form of participation in the management of the Affairs of society and state]. *Vestnik Prikam'skogo sotsial'nogo instituta*, 2018, no. 2 (80), pp. 6–13.

4. Dvornikov D.V., Krasinskii V.V., Puchnin A.S. Kontsepsiya elektronnoogo oprosa izbiratelei pri sbore podpisei v podderzhku vydvizheniya kandidatov v deputaty (na vybornye dolzhnosti) (sms-vydvizhenie) [The Concept of the electronic survey of voters during the collection of signatures in support of nomination of candidates (for elected office) (sms-extension)]. *Vestnik Tambovskogo universiteta. Series: Gumanitarnye nauki*, 2010, no. 9 (89), pp. 250–255.

5. Dick D.I., Solodovnikov V.M. Otsenka urovnya bezopasnosti informatsionnoi sistemy na osnove analiza kolichestva oshibok v programmnom kode [Evaluation of the level of security of the information system based on the analysis of the number of errors in the code]. *Vestnik Kurganskogo gosudarstvennogo universiteta. Series: Tekhnicheskie nauki*, 2015, no. 3 (37), pp. 32–35.

6. Zhozhina M., Mikhailova N. O demokratizatsii zakonodatel'nogo protsessa v Rossiiskoi Federatsii [On democratization of the legislative process in the Russian Federation]. *Etnosotsium i mezhnatsional'naya kul'tura*, 2017, no. 3 (105), pp. 9–14.

7. Klaus Sh. *Tekhnologii Chetvertoi promyshlennoi revolyutsii* [Technologies of the Fourth industrial revolution]. Moscow: EKSMO Publ., 2018, pp. 89–95.

8. Latukhina K. Vladimir Putin: Vnedrit' tsifrovyte tekhnologii vo vse sfery zhizni [Vladimir Putin: To introduce digital technologies in all spheres of life]. *Rossiiskaya gazeta*, 2017, June 4. Available at: <https://rg.ru/2017/06/04/reg-szfo/vladimir-putin-vnedrit-cifrovyte-tehnologii-vo-vse-sfery-zhizni.html> (accessed 19 July 2018).

9. Radchenko I.V. Vytesnit li tekhnologiya «blokchein» notariusa [Will the blockchain technology Displace the notary]. *Notarial'nyi vestnik*, 2017, no. 8, pp. 42–44.

10. Unizhaev N. Problemy ispol'zovaniya tekhnologii blokchein v tsifrovoi ekonomike [In the problems of using blockchain technology in the digital economy]. *Al'manakh mirovoi nauki*, 2018, no. 3 (23), pp. 211–215.

11. Khabrieva T.Ya. Pravo pered vyzovami tsifrovoi real'nosti [Right facing the challenges of the digital reality]. *Zhurnal rossiiskogo prava*, 2018, no. 9 (261), pp. 5–16.

12. Coglianese C. The internet and citizen participation in rulemaking. *A Journal of Law and Policy*, 2005, vol. 1, iss. 1, pp. 33–57.

13. Deshmukh S.S., Annappa B. Prediction of crime hot spots using spatio-temporal ordinary kriging. *Studies in Computational Intelligence*, 2019, vol. 771, pp. 683–691.

14. Ekbia H., Mattioli M., Kouper I. et al. Big Data. Bigger Dilemmas: A Critical Review. *Journal of the Association for Information Science and Technology*, 2015, vol. 68, pp. 1523–1545.

15. *Face-reading AI will be able to detect your politics and IQ, professor says*. Available at: <https://www.theguardian.com/technology/2017/sep/12/artificial-intelligence-face-recognition-michal-kosinski> (accessed 28 July 2018).

16. Nevett J. The Real Minority Report: Police trial AI to predict and prevent crimes before they happen. *Daily Star*, 2018, January 29. Available at: <https://www.dailystar.co.uk/news/world-news/677796/artificial-intelligence-japan-kanagawa-police-predict-minority-report-2020-olympics> (accessed 23 August 2018).
17. Miller A. What Do We Worry About When We Worry About Price Discrimination? The Law and Ethics of Using Personal Information for Pricing. *Journal of Technology Law & Policy*, 2014, vol. 19, pp. 41–95.
18. Nakamoto S. *Bitcoin: A Peer-to-Peer Electronic Cash System*. Available at: <https://bitcoin.org/bitcoin.pdf> (accessed 23 August 2018).
19. *New AI can guess whether you're gay or straight from a photograph*. Available at: <https://www.theguardian.com/technology/2017/sep/07/new-artificial-intelligence-can-tell-whether-youre-gay-or-straight-from-a-photograph> (accessed 23 August 2018).
20. O'Neil C. *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. New York: Allen Lane, 2016. 259 p.
21. O'Reilly T. Open Data and Algorithmic Regulation. In: Goldstein B., Dyson L. (eds). *Beyond Transparency: Open Data and the Future of Civic Innovation*. San Francisco: Code for America Press, 2013, pp. 289–300.
22. Pagallo U. Algo-rhythms and the beat of the legal drum. *Philosophy and Technology*, 2018, vol. 31, iss. 4, pp. 507–524.
23. Parkin S. Killer Robots: The soldiers that never sleep. *BBC*, 2015, July 16. Available at: <http://www.bbc.com/future/story/20150715-killer-robots-the-soldiers-that-never-sleep> (accessed 23 August 2018).
24. *Super aEgis II*. Available at: http://www.dodaam.com/eng/sub2/menu2_1_4.php (accessed 23 August 2018).
25. Solaiman S.M. Legal personality of robots, corporations, idols and chimpanzees: a quest for legitimacy. *Artificial intelligence and law*, 2017, vol. 25, iss. 2, pp. 155–179.
26. Bryson J.J. Diamantis M.T., Grant T.D. Of, for, and by the people: the legal lacuna of synthetic persons. *Artificial Intelligence and Law*, 2017, vol. 25, iss. 3, pp. 273–291.
27. Yeung K. Algorithmic regulation: A critical interrogation. *Regulation and Governance*, 2018, vol. 12, iss. 4, pp. 505–523.
28. Yi Shu Ng. *China is using AI to predict who will commit crime next*. July 24, 2017. Available at: <https://mashable.com/2017/07/24/china-ai-crime-minority-report/#QKYhs4z.qqqR> (accessed 23 August 2018).
29. Şafak Y. *Turkey starts building automatic shooting gun towers at Syrian border. May 30, 2016*. Available at: <http://www.yenisafak.com/en/news/turkey-starts-building-automatic-shooting-gun-towers-at-syrian-border-2473487> (accessed 23 August 2018).
30. *Zone of ethics. Propublica. 2016*. Available at: <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing> (accessed 23 August 2018).