

☞ ТЕОРИЯ КОНСТИТУЦИИ ☞

Дата поступления рукописи в редакцию: 08.06.2026 г.

DOI: 10.24412/2076-1503-2026-7-110-116

Дата принятия рукописи в печать: 03.08.2026 г.

КИРИЛЛОВА Татьяна Константиновна,

доктор юридических наук, профессор кафедры гражданского права Санкт-Петербургского государственного университета аэрокосмического приборостроения,

e-mail: tania.kirillova@gmail.com@yandex.ru

СОСНОВСКИЙ Евгений Сергеевич,

преподаватель кафедры публичного права Санкт-Петербургского государственного университета аэрокосмического приборостроения,

e-mail: jacksos730@gmail.com

**ЭВОЛЮЦИЯ КОНСТИТУЦИОННЫХ ГАРАНТИЙ ПРАВА НА НЕПРИКОСНОВЕННОСТЬ
ЧАСТНОЙ ЖИЗНИ В ЦИФРОВУЮ ЭПОХУ**

Аннотация. В статье исследуется трансформация конституционных гарантий права на неприкосновенность частной жизни в условиях цифровизации общественных отношений, развития технологий больших данных, искусственного интеллекта, биометрической идентификации и платформенной экономики. Обосновывается, что классическое понимание частной жизни как сферы, защищенной преимущественно от физического вторжения государства или иных лиц, в цифровую эпоху дополняется информационным, алгоритмическим и инфраструктурным измерениями. Автор анализирует соотношение права на неприкосновенность частной жизни, тайны переписки, защиты персональных данных, цифровой автономии личности и конституционного принципа достоинства человека. Делается вывод о необходимости перехода от формальной модели согласия на обработку данных к модели конституционно ориентированных гарантий, включающих минимизацию данных, прозрачность алгоритмических решений, эффективный судебный контроль, независимый надзор и специальные механизмы защиты от цифрового профилирования.

Ключевые слова: Конституция, частная жизнь, персональные данные, цифровые права, цифровой конституционализм, искусственный интеллект, биометрия, алгоритмическое профилирование, достоинство личности, информационная безопасность.

KIRILLOVA Tatiana Konstantinovna,

Doctor of Law, Professor of the Department of Public Law, St. Petersburg State University of Aerospace Instrumentation

SOSNOVSKY Evgeny Sergeevich,

Lecturer at the St. Petersburg State University of Aerospace Instrumentation

**THE EVOLUTION OF CONSTITUTIONAL GUARANTEES OF THE RIGHT TO PRIVACY IN THE
DIGITAL AGE**

Annotation. The article examines the transformation of constitutional guarantees of the right to privacy under the conditions of digitalization, big data technologies, artificial intelligence, biometric identification and platform economy. It is argued that the classical understanding of privacy as a sphere protected mainly from physical intrusion by the state or private actors is supplemented in the digital age by informational, algorithmic and infrastructural dimensions. The author analyzes the relationship between the right to privacy, secrecy of correspondence, personal data protection, digital autonomy and the constitutional principle of human dignity. The article concludes that it is necessary to move from a formal consent-based model of data processing to a constitutionally

oriented system of guarantees, including data minimization, transparency of algorithmic decision-making, effective judicial control, independent supervision and special mechanisms of protection against digital profiling.

Key words: *Constitution, privacy, personal data, digital rights, digital constitutionalism, artificial intelligence, biometrics, algorithmic profiling, human dignity, information security.*

Право на неприкосновенность частной жизни относится к числу фундаментальных конституционных прав, непосредственно связанных с достоинством личности, свободой индивидуального самоопределения и пределами вмешательства публичной власти в сферу личной автономии. В российской конституционной модели данное право выражено прежде всего в положениях статей 23 и 24 Конституции Российской Федерации, закрепляющих право каждого на неприкосновенность частной жизни, личную и семейную тайну, защиту чести и доброго имени, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, а также запрет сбора, хранения, использования и распространения информации о частной жизни лица без его согласия.

Однако цифровая эпоха изменила саму природу угроз частной жизни. Если в классической конституционно-правовой парадигме основным риском выступало прямое вторжение – обыск, прослушивание, опубликование сведений личного характера, то в современном обществе угроза часто возникает незаметно: через постоянный сбор метаданных, поведенческую аналитику, биометрическую идентификацию, автоматизированное принятие решений, трансграничную передачу данных, использование предиктивных алгоритмов. Частная жизнь оказывается затронутой даже тогда, когда отдельный пользователь формально согласился с условиями цифрового сервиса, но фактически не способен осознать объем, цели и последствия обработки своих данных.

В научной литературе последних лет эта трансформация описывается через категории цифрового конституционализма, информационного капитализма, алгоритмической власти и «капитализма наблюдения» [6; 8; 15]. В российской доктрине подчеркивается, что цифровизация требует переосмысления традиционных правовых конструкций, поскольку информационная среда становится не внешним объектом регулирования, а условием реализации большинства прав и свобод [2; 3]. В этом смысле право на частную жизнь перестает быть только «негативным» правом, защищающим человека от вмешательства. Оно приобретает позитивное содержание: государство обязано формировать

институциональные, процессуальные и технологические гарантии, позволяющие человеку сохранять контроль над цифровым образом собственной личности.

Цель настоящей статьи – выявить основные направления эволюции конституционных гарантий права на неприкосновенность частной жизни в цифровую эпоху.

Для достижения указанной цели поставлены следующие задачи: раскрыть конституционно-правовую природу права на частную жизнь; определить специфику цифровых угроз данному праву; проанализировать развитие зарубежных и российских подходов к защите персональных данных и цифровой автономии; сформулировать предложения по укреплению конституционных гарантий неприкосновенности частной жизни в условиях алгоритмизации.

Методологическую основу исследования составили формально-юридический, сравнительно-правовой, системный, историко-правовой и доктринальный методы. Особое значение имел сравнительно-правовой анализ, поскольку право на частную жизнь в цифровой среде развивается под влиянием международных стандартов, практики конституционных и наднациональных судов, а также европейской модели защиты персональных данных.

Право на неприкосновенность частной жизни в конституционном праве традиционно рассматривается как сложное субъективное право, включающее несколько взаимосвязанных элементов: личную автономию, семейную тайну, тайну коммуникаций, защиту персональных данных, контроль над распространением сведений о себе, а также возможность свободно формировать индивидуальную идентичность. В российской доктрине подчеркивается, что это право имеет комплексный характер и связано не только с запретом произвольного вмешательства, но и с обязанностью государства обеспечивать юридические механизмы охраны частной сферы [1].

В цифровой среде особое значение приобретает информационный аспект частной жизни. Данные о человеке становятся самостоятельным ресурсом, который используется государством, бизнесом, цифровыми платформами, работодателями, банками, страховыми организациями и иными

субъектами. При этом даже отдельные, на первый взгляд нейтральные сведения – геолокация, история поисковых запросов, сведения о покупках, активность в социальных сетях – при объединении позволяют формировать детализированный профиль личности. Именно поэтому современная защита частной жизни не может ограничиваться охраной интимной или семейной тайны. Она должна охватывать весь процесс обращения с данными: сбор, хранение, сопоставление, анализ, передачу, удаление и использование в автоматизированных решениях.

В европейской правовой традиции данная логика получила развитие через автономное признание права на защиту персональных данных. Общий регламент Европейского союза о защите данных 2016 г. сформировал модель, основанную на принципах законности, добросовестности, прозрачности, ограничения целей обработки, минимизации данных, точности, ограничения срока хранения, целостности и конфиденциальности [4]. Хотя нормативные правовые акты не включаются в список литературы настоящей статьи, сам факт влияния европейской модели очевиден: защита данных стала рассматриваться не как техническая отрасль регулирования, а как элемент конституционной архитектуры современного общества.

О. Лински обоснованно отмечает, что защита персональных данных в европейском праве связана не только с приватностью в узком смысле, но и с распределением власти между индивидом, государством и организациями, обладающими информационными ресурсами [5]. Этот вывод имеет универсальное значение: в цифровую эпоху тот, кто контролирует данные, получает возможность воздействовать на поведение человека, оценивать его надежность, прогнозировать предпочтения и ограничивать доступ к социальным благам. Следовательно, конституционная гарантия частной жизни должна пониматься как гарантия против информационной асимметрии и произвольной цифровой власти.

Исторически право на частную жизнь было ориентировано на защиту пространства, коммуникаций и репутации. В цифровую эпоху данная триада дополняется категорией цифровой автономии. Под цифровой автономией следует понимать способность лица самостоятельно определять пределы раскрытия информации о себе, понимать последствия цифрового взаимодействия, возражать против неправомерной обработки данных и требовать объяснения значимых автоматизированных решений.

Формально многие цифровые сервисы основываются на согласии пользователя.

Однако современная научная литература убедительно показывает ограниченность модели «информированного согласия» в условиях сложных платформенных экосистем [9; 10]. Пользователь редко обладает реальной возможностью прочитать и оценить многостраничные правила обработки данных, отказаться от навязанных условий или использовать альтернативный сервис без потери доступа к общественно значимым коммуникационным инфраструктурам. В результате согласие часто превращается в юридическую фикцию, прикрывающую дисбаланс власти между субъектом данных и оператором цифровой платформы.

Н. Ричардс подчеркивает, что приватность важна не только для защиты секретов, но и для свободы мысли, интеллектуального развития, политического участия и человеческого достоинства [10]. Данный подход особенно значим для конституционного права: без защищенной частной сферы невозможно свободное формирование убеждений, критика власти, участие в политической жизни и реализация иных основных прав. Таким образом, неприкосновенность частной жизни является не изолированным субъективным правом, а условием функционирования демократического правопорядка.

В цифровую эпоху конституционная гарантия частной жизни должна защищать человека не только от раскрытия интимной информации, но и от скрытого манипулирования. Исследования в области философии и права технологий показывают, что цифровые архитектуры способны подталкивать пользователя к определенному поведению, используя персонализированные стимулы, поведенческие паттерны и уязвимости внимания [12]. Если подобное воздействие осуществляется непрозрачно и на основе глубокого профилирования, оно затрагивает не только приватность, но и свободу воли.

Категория цифрового конституционализма получила широкое распространение в зарубежной литературе последних лет. Г. Де Грегорио рассматривает цифровой конституционализм как процесс переосмысления прав и пределов власти в алгоритмическом обществе, где значительная часть регулятивных функций фактически осуществляется частными цифровыми платформами [6]. Э. Челесте связывает цифровой конституционализм с попытками закрепления фундаментальных прав пользователей интернета, включая право на приватность, доступ к информации, защиту от цензуры и недискриминацию в цифровой среде [7].

Данный подход имеет принципиальное значение для конституционного права.

Традиционная теория основных прав исходит из вертикальной модели: государство как носитель публичной власти обязано воздерживаться от необоснованного вмешательства в права человека. Однако в цифровой среде значительная часть вмешательств осуществляется частными субъектами, которые не всегда обладают формальным статусом публичной власти, но фактически контролируют инфраструктуру коммуникации, доступ к информации, видимость контента, цифровую репутацию и возможности экономического участия.

Ю. Коэн характеризует современный информационный капитализм как систему, в которой правовые конструкции собственности, договора, интеллектуальных прав и защиты данных формируют новые режимы власти над информационными потоками [8]. Это означает, что конституционные гарантии частной жизни должны быть направлены не только против произвола государства, но и против чрезмерной концентрации информационной власти у частных корпораций. Иначе право на частную жизнь будет сохранять формальную значимость, но терять реальную эффективность.

В российском праве данная проблема проявляется в необходимости согласования конституционных гарантий частной жизни с развитием цифровых государственных сервисов, биометрических систем, электронного документооборота, цифровых платформ занятости, финансовых технологий и систем видеонаблюдения. С одной стороны, цифровизация повышает доступность государственных и коммерческих услуг. С другой стороны, она увеличивает объем обрабатываемых данных и создает риски централизации сведений о гражданах. Поэтому конституционно допустимая цифровизация должна отвечать критериям необходимости, соразмерности, правовой определенности и подотчетности.

Персональные данные являются ключевым юридическим инструментом защиты частной жизни в цифровую эпоху. При этом важно подчеркнуть: защита персональных данных не сводится к защите конфиденциальной информации. Многие персональные данные могут быть общедоступными или не иметь очевидно интимного характера, однако их автоматизированная обработка способна привести к существенным последствиям для человека. Например, сведения о поведении пользователя в сети могут использоваться для кредитного скоринга, таргетированной политической рекламы, оценки трудовой дисциплины или страховых рисков.

Современная доктрина защиты данных

исходит из того, что вред может возникать не только из-за утечки информации, но и из-за неправомерных выводов, сделанных на ее основе. С. Вахтер и Б. Миттельштадт предложили концепцию «права на разумные выводы», указывая, что регулирование должно охватывать не только исходные данные, но и производные профили, прогнозы и оценки, влияющие на положение человека [13]. Это особенно важно для конституционного права, поскольку алгоритмический вывод может стать основанием для ограничения возможностей лица без открытого обвинения, понятной процедуры и эффективного средства защиты.

В. Харцог и Д. Солов справедливо отмечают, что право информационной безопасности часто реагирует на последствия утечек, но недостаточно эффективно предотвращает системные риски, заложенные в архитектуре сбора и хранения данных [9]. Применительно к конституционным гарантиям это означает необходимость смещения акцента с последующего возмещения вреда на предварительное проектирование безопасных и правомерных цифровых систем. Иными словами, частная жизнь должна защищаться не только судом после нарушения, но и самой архитектурой цифровой среды.

Такой подход близок к идее «privacy by design», предполагающей внедрение гарантий приватности на этапе проектирования технологий. В конституционно-правовом измерении это означает, что государственные информационные системы, системы биометрической идентификации, цифровые платформы публичных услуг и автоматизированные реестры должны создаваться с учетом минимизации данных, разграничения доступа, криптографической защиты, журналирования операций, независимого аудита и возможности оспаривания решений.

Наиболее острые вызовы праву на неприкосновенность частной жизни связаны с использованием искусственного интеллекта и биометрических технологий. Биометрические данные обладают особой чувствительностью, поскольку они непосредственно связаны с телесной и поведенческой идентичностью человека. Пароль можно заменить, но лицо, голос, отпечатки пальцев или рисунок вен заменить практически невозможно. Утечка или неправомерное использование биометрических данных создает долговременный риск для личности.

Алгоритмическое профилирование также меняет характер вмешательства в частную жизнь. Если традиционное вмешательство обычно имело индивидуальный и явный характер, то алгоритмическое воздействие может быть массовым, скрытым и вероятностным. Человек

может не знать, что в отношении него сформирован риск-профиль, что он отнесен к определенной категории потребителей, заемщиков, работников или политически восприимчивых пользователей. При этом такие профили способны влиять на доступ к кредитам, вакансиям, страховым продуктам, информации и социальным возможностям.

К. Юнг в исследовании алгоритмического регулирования показывает, что алгоритмы могут выполнять функции управления поведением, не будучи традиционными правовыми нормами [14]. Именно поэтому конституционное право должно учитывать не только юридические запреты и разрешения, но и технологические механизмы, которые фактически регулируют социальное поведение. Если алгоритм определяет видимость информации, оценивает надежность гражданина или автоматически принимает решение о предоставлении услуги, он становится частью нормативной среды.

Особую опасность представляет сочетание больших данных, искусственного интеллекта и наблюдения. Ш. Зубофф описывает данную модель как экономическую систему извлечения поведенческих данных и прогнозирования поведения пользователей [15]. Независимо от оценки отдельных аспектов этой концепции очевидно, что массовая коммерческая обработка данных способна затрагивать конституционные основы свободы личности. Следовательно, государство не может ограничиваться ролью пассивного наблюдателя за отношениями между пользователем и платформой.

Российская конституционная модель содержит значимый потенциал защиты частной жизни. Статья 23 Конституции Российской Федерации закрепляет общую гарантию неприкосновенности частной жизни, а статья 24 прямо запрещает сбор, хранение, использование и распространение информации о частной жизни лица без его согласия. Тем самым Конституция изначально включает информационное измерение приватности, что позволяет адаптировать ее положения к цифровой эпохе без формального изменения текста.

Развитие отраслевого законодательства о персональных данных, информации, связи, биометрической идентификации, цифровых финансовых технологиях и государственных информационных системах свидетельствует о постепенном усложнении правового регулирования. Вместе с тем конституционно-правовая проблема состоит не только в наличии законов, но и в качестве гарантий. Для права на частную жизнь принципиальна ясность правового основания обработки данных, определенность целей, ограничение объема собираемой

информации, реальная возможность отзыва согласия, независимый контроль и судебная защита.

Российская доктрина цифрового права справедливо указывает, что цифровизация требует межотраслевого подхода, поскольку данные одновременно выступают объектом гражданского оборота, административного управления, информационной безопасности и конституционной защиты [2]. Однако именно конституционное право должно задавать предельные рамки цифровизации. Технологическая эффективность не может рассматриваться как самостоятельное основание для расширения сбора данных. Любое вмешательство в частную жизнь должно быть не только законным, но и необходимым, соразмерным, обоснованным публичной целью и обеспеченным эффективными средствами контроля.

Одной из проблем остается фрагментарность гарантий при использовании автоматизированных решений. Гражданин должен обладать правом знать, что в отношении него применяется автоматизированная обработка, понимать ее логику в объеме, достаточном для защиты своих прав, требовать пересмотра решения человека и оспаривать неблагоприятные последствия. Без этих элементов защита частной жизни и персональных данных становится неполной, поскольку основное вмешательство происходит не на стадии сбора информации, а на стадии ее интерпретации и применения. Эволюция конституционных гарантий права на неприкосновенность частной жизни в цифровую эпоху может быть представлена в нескольких направлениях.

Первое направление: расширение предмета защиты. Конституционная охрана должна распространяться не только на сведения интимного характера, но и на цифровые следы, метаданные, биометрические параметры, поведенческие профили, алгоритмические выводы и иные производные данные, способные повлиять на правовое или социальное положение человека.

Второе направление: переход от индивидуалистической модели согласия к модели структурной защиты. Согласие остается важным юридическим инструментом, но оно не может быть единственной гарантией. В условиях информационной асимметрии необходимы императивные обязанности операторов данных: минимизация, прозрачность, безопасность, ограничение сроков хранения, запрет несовместимого использования, оценка рисков и независимый аудит.

Третье направление: признание значения

алгоритмической прозрачности. Конституционная гарантия частной жизни требует, чтобы значимые автоматизированные решения не были полностью непрозрачными для человека. Речь не обязательно идет о раскрытии исходного программного кода во всех случаях, но лицо должно понимать критерии, источники данных и последствия профилирования в объеме, позволяющем эффективно защищать свои права.

Четвертое направление: усиление судебного и внесудебного контроля. В цифровой сфере вред часто носит массовый и труднообратимый характер. Поэтому необходимы не только индивидуальные иски, но и административный надзор, коллективные механизмы защиты, специальные процедуры проверки информационных систем, а также возможность оперативного прекращения неправомерной обработки данных.

Пятое направление: конституционализация технологического проектирования. Права человека должны учитываться на стадии разработки цифровых систем. Государственные информационные платформы, системы биометрической идентификации и алгоритмического анализа должны проходить оценку воздействия на права и свободы. Такая оценка должна быть не формальной процедурой, а реальным инструментом выявления рисков дискриминации, чрезмерного наблюдения, утечки данных и ограничения автономии личности.

Шестое направление: развитие гарантий против манипулятивного воздействия. Частная жизнь связана с внутренней свободой человека. Поэтому цифровые практики, основанные на скрытом использовании психологических уязвимостей, микротаргетинге и персонализированном манипулировании, должны оцениваться не только с позиции защиты потребителя или конкуренции, но и с позиции конституционных прав.

Право на неприкосновенность частной жизни в цифровую эпоху переживает глубокую трансформацию. Его классическое содержание – защита личной и семейной тайны, тайны коммуникаций, запрет произвольного вмешательства – сохраняет значение, но уже не исчерпывает современных конституционных задач. Цифровая среда создает новые формы уязвимости: постоянное наблюдение, скрытое профилирование, автоматизированные решения, биометрическую идентификацию, трансграничное движение данных и манипулятивное воздействие на поведение.

В этих условиях конституционные гарантии должны развиваться в направлении защиты цифровой автономии личности. Человек должен

обладать реальным, а не декларативным контролем над данными о себе; иметь возможность понимать и оспаривать автоматизированные решения; быть защищенным от чрезмерного сбора информации и непрозрачного профилирования. Государство, в свою очередь, обязано не только воздерживаться от необоснованного вмешательства, но и создавать правовую, институциональную и технологическую инфраструктуру защиты частной жизни.

Наиболее перспективной представляется модель, соединяющая конституционные принципы достоинства, свободы и соразмерности с современными механизмами защиты данных: минимизацией, прозрачностью, безопасностью по умолчанию, независимым аудитом, оценкой воздействия на права человека и эффективным судебным контролем. Только такая модель способна обеспечить реальность права на неприкосновенность частной жизни в обществе, где личность все чаще существует одновременно в физическом, информационном и алгоритмическом измерениях.

Список литературы:

- [1] Авакьян С.А. Конституционное право России: учебный курс: в 2 т. 7-е изд., перераб. и доп. М.: Норма: ИНФРА-М, 2021.
- [2] Цифровое право: учебник / под общ. ред. В.В. Блажеева, М.А. Егоровой. М.: Проспект, 2020.
- [3] Хабриева Т.Я., Черногор Н.Н. Право в условиях цифровой реальности // Журнал российского права. 2018. № 1. С. 85–102.
- [4] Kuner C., Bygrave L.A., Docksey C., Drechsler L. The EU General Data Protection Regulation (GDPR): A Commentary. Oxford: Oxford University Press, 2020.
- [5] Lynskey O. The Foundations of EU Data Protection Law. Oxford: Oxford University Press, 2015.
- [6] De Gregorio G. Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society. Cambridge: Cambridge University Press, 2022.
- [7] Celeste E. Digital Constitutionalism: The Role of Internet Bills of Rights. Abingdon; New York: Routledge, 2022.
- [8] Cohen J.E. Between Truth and Power: The Legal Constructions of Informational Capitalism. Oxford: Oxford University Press, 2019.
- [9] Solove D.J., Hartzog W. Breached! Why Data Security Law Fails and How to Improve It. Oxford: Oxford University Press, 2022.
- [10] Richards N. Why Privacy Matters. Oxford: Oxford University Press, 2021.
- [11] Citron D.K. The Fight for Privacy:

Protecting Dignity, Identity, and Love in the Digital Age. New York: W.W. Norton & Company, 2022.

[12] Susser D., Roessler B., Nissenbaum H. Technology, autonomy, and manipulation // Internet Policy Review. 2019. Vol. 8. № 2.

[13] Wachter S., Mittelstadt B. A Right to Reasonable Inferences: Re-thinking Data Protection Law in the Age of Big Data and AI // Columbia Business Law Review. 2019. № 2. P. 494–620.

[14] Yeung K. Algorithmic regulation: A critical interrogation // Regulation & Governance. 2018. Vol. 12. № 4. P. 505–523.

[15] Zuboff S. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. New York: PublicAffairs, 2019.

References:

[1] Avakyan S.A. Constitutional Law of Russia: training course: in 2 vols. 7th ed., Revised. and additional M.: Norm: INFRA-M, 2021.

[2] Digital law: textbook/under the general. ed. V.V. Blazheeva, M.A. Egorova. M.: Prospect, 2020.

[3] Khabrieva T.Ya., Chernogor N.N. Law in Digital Reality//Journal of Russian Law. 2018. № 1. S. 85-102.

[4] Kuner C., Bygrave L.A., Docksey C., Drechsler L. The EU General Data Protection Regulation (GDPR): A Commentary. Oxford: Oxford University Press, 2020.

[5] Lynskey O. The Foundations of EU Data Protection Law. Oxford: Oxford University Press, 2015.

[6] De Gregorio G. Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society. Cambridge: Cambridge University Press, 2022.

[7] Celeste E. Digital Constitutionalism: The Role of Internet Bills of Rights. Abingdon; New York: Routledge, 2022.

[8] Cohen J.E. Between Truth and Power: The Legal Constructions of Informational Capitalism. Oxford: Oxford University Press, 2019.

[9] Solove D.J., Hartzog W. Breached! Why Data Security Law Fails and How to Improve It. Oxford: Oxford University Press, 2022.

[10] Richards N. Why Privacy Matters. Oxford: Oxford University Press, 2021.

[11] Citron D.K. The Fight for Privacy: Protecting Dignity, Identity, and Love in the Digital Age. New York: W.W. Norton & Company, 2022.

[12] Susser D., Roessler B., Nissenbaum H. Technology, autonomy, and manipulation // Internet Policy Review. 2019. Vol. 8. № 2.

[13] Wachter S., Mittelstadt B. A Right to Reasonable Inferences: Re-thinking Data Protection Law in the Age of Big Data and AI // Columbia Business Law Review. 2019. № 2. P. 494–620.

[14] Yeung K. Algorithmic regulation: A critical interrogation // Regulation & Governance. 2018. Vol. 12. № 4. P. 505–523.

[15] Zuboff S. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. New York: PublicAffairs, 2019.



Юридическое издательство
«ЮРКОМПАНИ»

Издание учебников,
учебных и методических
пособий, монографий,
научных статей.

Профессионально.

В максимально
короткие сроки.

Размещаем
в РИНЦ, E-Library.

ЮРКОМПАНИ

www.law-books.ru