NB: Административное право и практика администрирования
Правильная ссылка на статью:
Якунина А.В. Защита неприкосновенности частной жизни в условиях развития цифровых коммуникаций // NB: Административное право и практика администрирования. 2024. № 2. DOI: 10.7256/2306-9945.2024.2.70695 EDN: EPDVQZ URL: https://nbpublish.com/library_read_article.php?id=70695

Защита неприкосновенности частной жизни в условиях развития цифровых коммуникаций

Якунина Анастасия Владимировна

аспирант, кафедра государственного и административного права, Самарский национальный исследовательский университет имени академика С.П. Королева

443086, Россия, Самарская область, г. Самара, шоссе Московское, 34

yakunina@urlife.pro

Статья из рубрики "Публичное право: новые проблемы и реалии"

DOI:

10.7256/2306-9945.2024.2.70695

EDN:

EPDVQZ

Дата направления статьи в редакцию:

09-05-2024

Аннотация: В данной статье рассматривается влияние технологического прогресса на обеспечение и защиту неприкосновенности частной жизни в условиях расширения цифровых коммуникаций. Уровень ожиданий конкретного общества относительно состояния неприкосновенности частной жизни служит эталоном, стимулирующим либо ослабляющим действия по совершенствованию национального законодательства. Чувствительное отношение к восприятию технологий, основанное на здравом смысле, позволит избежать явных нарушений соразмерности и поддерживать баланс между частными и публичными интересами в обществе. В статье автор проводит анализ влияния цифровых технологий на приватную жизнь в условиях расширения государственной поддержки данной сферы на примере самых влиятельных корпораций Palantir Technologies Inc. и Cambridge Analytica, и предлагает эффективные меры по обеспечению защиты личных данных в современном цифровом мире. В рамках подготовки настоящей статьи был использован комплекс методов, включая сравнительно-правовой метод, системный анализ, историко-правовой метод и эмпирические методы для анализа практической реализации правовых норм. Научная

новизна исследования определяется комплексным и всесторонним анализом влияния цифровых технологий на неприкосновенность частной жизни, поскольку применяемые информационные технологии дают большую возможность как для сознательного, так и для неосознанного нарушения прав и свобод. Кроме того, в настоящей статье рассматриваются этические и правовые аспекты использования личных данных граждан и даются рекомендации по улучшению конфиденциальности в цифровую эпоху. В связи с этим вопрос неприкосновенности частной жизни в контексте эволюции цифровых коммуникаций приобретает особую актуальность. В заключение статьи обсуждается важность баланса публичных и частных интересов в сфере цифровых технологий и защиты данных и предлагаются пути решения этой сложной проблемы в интересах всех заинтересованных сторон.

Ключевые слова:

неприкосновенность частной жизни, конфиденциальность, персональные данные, цифровизация, Palantir Technologies, Cambridge Analytica, защита данных, transparency report, оценка воздействия, цифровые коммуникации

Право человека на неприкосновенность частной жизни закреплено нормативно с середины XX века и получило подтверждение в международных документах, включая Всеобщую декларацию прав человека (статья 12), Конвенцию о защите прав человека и основных свобод (статья 8), Конвенцию о правах ребенка (статья 16), Международную конвенцию о защите прав всех трудящихся-мигрантов и членов их семей (статья 14), Конвенцию СНГ о правах и основных свободах человека (статья 9), а также множество других международных договоров и региональных соглашений о правах человека [1, с. 13-19]. Этот процесс стал важным шагом в признании данного права международным сообществом.

Анализ актов международного права позволяет сделать вывод, что право человека на неприкосновенность частной жизни относится к категории основных прав и свобод человека, признаваемых по рождению [2, 103-105]. Любое вмешательство со стороны других лиц должно быть определено законом и подвергнуто критической оценке его необходимости и соразмерности.

Уровень ожиданий конкретного общества относительно состояния неприкосновенности частной жизни служит эталоном, стимулирующим либо ослабляющим действия по совершенствованию национального законодательства. Чувствительное отношение к восприятию технологий, основанное на здравом смысле, позволит избежать явных нарушений соразмерности и поддерживать баланс между частными и публичными интересами в обществе.

Технологический прогресс создает новые возможности для человека, общества и государства, но также порождает множество проблем, угроз и рисков [3, с. 118-119]. Тревожной тенденцией является все более активное использование информационно-коммуникационных технологий государственными и негосударственными субъектами, а также смешанными (коммерческими организациями с государственным участием) группами, в собственных интересах. Крупные IT-корпорации многомерны и сочетают в себе принудительные и подрывные меры с использованием как обычных, так и нетрадиционных способов, и тактик, для достижения своих целей. На сегодняшний день,

основная проблема в том, что гражданам зачастую неизвестно какие продукты и программное обеспечение используются компаниями для работы с их данными, а также какие именно данные обрабатываются подобными организациями и какие меры предосторожности предусмотрены для защиты персональных данных и предотвращения их неправомерного использования. Частная компания, имея доступ к большому количеству данных о человеке, отклоняет запросы на прозрачность, так называемый «transparency report», по причине защиты коммерческих интересов. Полученные такими компаниями данные используются в собственных экономических интересах для рекламы, скрытого наблюдения, дифференцированного ценообразования, влияния на выборы, целенаправленной дезинформации, прогнозирования настроений на инвестиционных рынках, управления корпоративными рисками и пр. Применяемые информационные технологии дают большую возможность как для сознательного, так и для неосознанного нарушения права на неприкосновенность частной жизни.

В связи с этим вопрос неприкосновенности частной жизни в контексте эволюции цифровых коммуникаций приобретает особую актуальность.

В большинстве стран мира разработка и внедрение цифровых технологий является вопросом внутренней политики государства, что, в свою очередь, находит отражение в государственных программах долгосрочного развития. Подобные государственные программы применяются в Японии (Smart Japan ICT Strategy), Канаде (Pan-Canadian Artificial Intelligence Strategy), Великобритании (UK Digital Strategy 2017), Франции (AI for Humanity), Индии (AI Garage), России (Цифровая экономика Российской Федерации) и многих других странах. В свою очередь данные программы требуют принятия соответствующих правовых актов и увеличения финансовой поддержки научно-технической сферы [4, с. 76-82]. В то же время цифровые технологии зачастую настолько важны для граждан, что их неправомерное использование сопряжено с серьезным риском нарушения неприкосновенности частной жизни и других основных прав, и свобод. Различные типы массовой слежки, мониторинг в Интернете и меры по сбору данных, такие как история просмотров в браузере; история покупок; история поиска; местоположение; финансовые данные; данные о состоянии здоровья и другая личная информация поступают в банки данных, затрагивая интересы каждого человека [5]. В связи с этим возникает обеспокоенность по поводу угроз нарушения права на неприкосновенность частной жизни, особенно в условиях расширения государственной поддержки цифровых технологий и укрепления тотального контроля над деятельностью человека как в Интернете, так и в реальной жизни. Это подчеркивает необходимость разработки эффективной международной системы защиты прав и свобод личности в сети.

Персональные данные граждан нужны не только государству. Коммерческие организации постоянно собирают данные в своих интересах. Они утверждают, что это делается для увеличения качества обслуживания клиентов, но эта информация может быть использована и вопреки интересам граждан. Так, например, существуют опасения, что Amazon Echo записывает разговоры, Apple передает данные о пользователях спецслужбам, а Google продает данные своих пользователей. В связи с этим крупные технологические компании подвергаются тщательной проверке за использование неэтичных методов в работе с конфиденциальными данными пользователей. Обладая огромными человеческими и финансовыми ресурсами, крупные корпорации создали технологические монополии и постепенно стали доминировать на научно-техническом рынке, установив тем самым широкое экономическое влияние. Однако из-за недобросовестного отношения к конфиденциальности пользовательских данных эти организации часто становятся участниками судебных разбирательств, что в какой-то

степени отражает смещение баланса между частными и публичными интересами.

Особую озабоченность вызывает растущее влияние технологических компаний, активно ищущих сотрудничества с правительством и в конечном итоге проникающих в государственную систему через оказание технической поддержки информационных ресурсов органов государственной власти, тем самым влияя на их работу. В качестве примера можно привести одну из самых влиятельных корпораций в современном цифровом мире Palantir Technologies Inc. (далее по тексту – Palantir, Palantir Technologies) – компания по интеграции и аналитике данных, продукты которой часто используются службами национальной безопасности и правоохранительными органами по всему миру.

Услуги Palantir, включая её платформу Gotham, используются полицией по всей Америке, и иногда эти соглашения становятся частью непубличных договоренностей. Например, в 2012 году Департамент полиции Нового Орлеана и компания Palantir Technologies заключили соглашение о предоставлении Palantir программного обеспечения для отслеживания связей между гражданами и ранее выявленными членами банд в рамках программы по предотвращению преступности. Полиция смогла проанализировать их криминальное прошлое и активность в социальных сетях и спрогнозировать вероятность совершения преступлений ими или против них и членов их семей. При этом официально нигде не упоминалось о сотрудничестве полиции и Palantir, в связи с чем, вопросы об источниках финансирования упомянутой выше программы, соответствии использования системы наблюдения нормам этики и законодательству остались без ответа. Полагаем, что ответ должен лежать в законодательных нормах, направленных на достижение баланса между частными и публичными интересами, путем создания механизмов, гарантирующих право на неприкосновенность частной жизни, наряду с гарантиями, сохраняющими право на поиск, получение и свободное распространение информации.

Очевидно, что Palantir Technologies использовал Новый Орлеан в качестве полигона для тестирования своей технологии прогнозирования полицейской деятельности, чтобы в дальнейшем иметь возможность заключать многомиллионные контракты с силовыми ведомствами по всему миру.

Известно, что спустя более десяти лет после того, как компания Palantir начала работать в Новом Орлеане, она запатентовала по крайней мере одну систему прогнозирования преступности и начала предоставлять спецслужбам других стран аналогичное программное обеспечение для определения склонности граждан к совершению террористических атак.

С одной стороны, меры по сокрытию подробностей соглашения между представителями власти и частной компанией можно было оправдать снижением преступности, если бы предложенные технологии прогнозирования существенно повлияли на уровень преступности в Новом Орлеане. Однако, если верить статистике, представленной Федеральным бюро расследований (FBI), на уровне преступности это существенно не отразилось, и даже замечен рост уровня преступности с 2016 года:

уровень преступности в Новом Орлеане, Лос-Анджелес, в 2015 году составил 949,56 на 100 000 населения, что на 2,5% меньше, чем в 2014 году;

уровень преступности в Новом Орлеане, Лос-Анджелес, в 2016 году составил 1069,72 на 100 000 населения, что на 12,65% больше, чем в 2015 году;

уровень преступности в Новом Орлеане, Лос-Анджелес, в 2017 году составил 1121,41 на 100 000 населения, что на 4,83% больше, чем в 2016 году;

уровень преступности в Новом Орлеане, Лос-Анджелес, в 2018 году составил 1163,3 на 100 000 населения, что на 3,74% больше, чем в 2017 году.

Таким образом, говорить о благоприятном исходе использования технологий слежения нельзя, поскольку в результате «эксперимента» компания Palantir Technologies получила доступ к личной информации американских граждан, при этом сами граждане не были защищены от совершаемых в отношении них и их близких преступлений.

Это не первый случай, когда стало известно об использовании Правительством США технологий Palantir. По крайней мере, с 2009 года компания оказывает поддержку Пентагону в обнаружении самодельных взрывных устройств в Афганистане и Ираке в рамках совместной программы оценки рисков. Поскольку проект осуществлялся в период ведения военных действий, компании не пришлось беспокоиться о нарушениях гражданских свобод, которые неизбежно возникают при использовании технологий предотвращения преступности даже в военное время [6].

Сегодня компания Palantir занимается цифровым профилированием и активно сотрудничает с Миграционной и таможенной службой США (ICE), для облегчения депортации мигрантов, одновременно обрабатывая широкий спектр данных: гражданство, информацию о заявлении на получение убежища, расовое или этническое происхождение, политические взгляды, религию и философские убеждения, членство в профсоюзах, сведения о доходах, сексуальную жизнь и сексуальную ориентацию, сведения о судимости и многое другое. Полученные данные периодически используются для нарушения декларируемых прав и свобод человека. Например, известны два случая 2017 и 2019 года, когда ICE применило технологии Palantir для проведения рейдов и облегчения ареста мигрантов, что привело к массовому нарушению гражданских прав и к разлучению детей с их семьями.

Безусловно, государство вправе осуществлять юрисдикцию в пределах установленных границ, но с учетом взятых на себя обязательств, касающихся соблюдения прав человека. Защищая права и свободы одной группы лиц, нельзя пренебрегать правами и свободами других.

Лондонская полиция испытывала продукты Palantir Predictive Crime Mapping в течение двенадцати месяцев, с мая 2014 по апрель 2015 года. Позже Palantir выиграл тендер на заключение контракта с национальной службой здравоохранения Великобритании стоимостью 480 миллионов фунтов стерлингов ($579 млн) для переработки системы сбора медицинских данных, выявления закономерности и, в конечном счете, перестройки всей системы, несмотря на противодействие со стороны Британской медицинской ассоциации (BMA), Ассоциации врачей Великобритании, групп пациентов и борцов за конфиденциальность.

В феврале 2017 года, после покупки программного обеспечения у Palantir Technologies, Министерство юстиции Дании представило на общественное обсуждение законопроект, целью которого является обоснование обработки персональных данных населения с использованием программного обеспечения, предоставленного Palantir (для датской полиции и разведки).

В январе 2020 года Palantir расширил географию своего влияния и стал работать с правительствами других стран. За последние годы контракты Palantir с правительствами

по всему миру выросли на 74% с 31 декабря 2018 г. по 30 июня 2020 г. – с $670,6 млн до $1,2 млрд. Отсутствие прозрачности во всех этих контрактах вызывает постоянную озабоченность со стороны общественности. Нельзя быть уверенными, была ли проведена, например, оценка воздействия на защиту персональных данных и оценка воздействия на права человека в отношении продуктов компании Palantir, поскольку сама компания данную информацию не раскрывает.

Последние десять лет происходит непрерывный рост числа компаний, использующих технологический прогресс для расширения своего влияния в общественных и государственных делах. Ярким примером является компания Cambridge Analytica, которая занималась психографическим профилированием американских избирателей, тем самым представляя угрозу для избирательного процесса. Этот пример также следует рассматривать как вызов демократическим институтам в целом.

Скандал между Cambridge Analytica и Facebook (социальная сеть «Facebook» принадлежит транснациональной холдинговой компании Meta, деятельность которой решением суда признана экстремистской и запрещена на территории Российской Федерации) разразился в 2018 году [7], когда Кристофер Уайли директор по исследованиям в Cambridge Analytica и SCL (Strategic Communication Laboratories) Group, выступил в роли разоблачителя компании и дал большое интервью, объяснив, что психографическое профилирование позволило Cambridge Analytica влиять на избирателей, используя данные социальных сетей для создания инструмента «психологической войны».

Cambridge Analytica получила данные около 87 миллионов пользователей Facebook (социальная сеть «Facebook» принадлежит транснациональной холдинговой компании Meta, деятельность которой решением суда признана экстремистской и запрещена на территории Российской Федерации) [8] при помощи приложения «thisisyourdigitallife» для составления профиля личности. Пользователи, загрузившие приложение через социальную сеть, не только отвечали на вопросы о себе, но и давали согласие на доступ к другим данным своего профиля, включая отметки «нравится» и списки контактов. Таким образом, компания получила около пяти тысяч «точек» данных о каждом пользователе и его контактах, тем самым имея возможность моделировать поведение около 230 миллионов человек.

Полученные данные были использованы для создания алгоритмов таргетинга Cambridge Analytica, чтобы предсказать и повлиять на поведение отдельных избирателей на президентских выборах 2016 года.

На сегодняшний день вопрос о реальной степени влияния Cambridge Analytica на волю американских и британских избирателей остается открытым, однако нет сомнений в том, что негативный опыт этой компании в разных странах привлек большое внимание, что говорит о необходимости дальнейшей разработки эффективных средств защиты субъективных прав человека в цифровой среде [9].

Таким образом, на фоне кризиса доверия к работе органов власти с персональными данными после многочисленных скандалов, связанных с неправомерным использованием данных граждан по всему миру (от Cambridge Analytica до алгоритма A-levels), следовало бы избежать очередного дефицита взаимопонимания в системе «гражданин – общество – государство», введя требования большей прозрачности и применяя более строгие меры регулирования в деятельности технологических гигантов.

При этом важно отметить, что излишняя регламентация может препятствовать развитию инноваций и подорвать экономический потенциал цифрового пространства, поэтому важно обеспечить баланс интересов в данной сфере [10, 678-679].

Необходимо как можно чаще проводить независимый мониторинг соблюдения технологическими компаниями международных и национальных стандартов защиты данных, а также оценивать их влияние на права человека в целом.

Кроме того, на наш взгляд необходимо повысить прозрачность закупочной деятельности технологического сектора государства. Заключение любых контрактов с технологическими компаниями должно основываться на принципах законности, справедливости и прозрачности, а также целостности и конфиденциальности. В случае, если компания получает доступ к персональным данным граждан, должны быть определены цели обработки таких данных, ограничен срок их хранения и установлена строгая подотчетность.

Крайне важно повышение уровня общественного внимания к вопросам сотрудничества государства и технологических компаний. Целесообразно ввести правила, направленные на обеспечение прозрачности данной сферы: государственные органы, имеющие контракты с крупными технологическими компаниями, должны публиковать такие контракты и соглашения о совместном использовании персональных данных и проводить соответствующую оценку воздействия на права человека, которая позволит сопоставить и оценить риски обработки данных и будет содержать план действий по их снижению до приемлемого уровня. Кроме того, создание этических правил сбора и обработки данных может способствовать благоприятной атмосфере для развития бизнеса, а также стимулировать инновации посредством культуры ответственного поведения.

Как с такими компаниями, как Palantir Technologies, так и с любыми другими крупными технологическими компаниями, с которыми сотрудничает государство - должны существовать надежные гарантии защиты прав и свобод человека. Никто не должен жертвовать своими правами на неприкосновенность частной жизни в качестве платы за жизнь в цифровую эпоху.

Библиография

1. Гарчева Л. П. О некоторых рисках нарушения прав человека в условиях цифровизации // Юридические науки. 2022. Т. 8. № 1. С. 13-19.
2. Ромашов П. А. К вопросу о праве на неприкосновенность частной жизни в цифровой век // Пермский юридический альманах. 2019. № 2. С. 103-118.
3. Каирбаева Л. К. Защита персональных данных в международном и европейском праве //Вестник Института законодательства и правовой информации Республики Казахстан». 2020. №5(63). С. 118-124.
4. Сильченко Р. Н. Проблемы защиты прав и свобод человека в условиях применения технологий искусственного интеллекта // Проблемы экономики и юридической практики. 2019. Т. 15. №4. С. 76-82.
5. Шумиленко А.П., Пастухова Л.В. Международное право прав человека. Симферополь: ИТ "АРИАЛ", 2019.
6. Айтуарова А. М. Возвращаясь к научной публикации phd М.Ж. Куликпаевой "международно-правовые основы обеспечения права на частную жизнь в контексте развития цифровых технологий" // Вестник Института законодательства и правовой информации Республики Казахстан. 2023. №1(72). С. 267-275.
7. Hu M. Cambridge Analytica's black box. Big Data & Society. 2020. №7(2). P. 77-91.

8. Костина О. В. Наследование аккаунтов в социальных сетях как средство обеспечения баланса интересов граждан и предпринимателей // Юридическая наука. 2022. №6. С. 53-56.
9. Rowena Rodrigues. Legal and human rights issues of AI: Gaps, challenges and vulnerabilities // Journal of Responsible Technology. 2020. №4. P. 98-113.
10. Богданов Д. Е. Технодетерминизм в частном праве: влияние биопринтинга на развитие концепции защиты права на цифровой образ // Вестник Пермского университета. Юридические науки. 2020. №50. С. 678-704.

Результаты процедуры рецензирования статьи

В связи с политикой двойного слепого рецензирования личность рецензента не раскрывается.
Со списком рецензентов издательства можно ознакомиться здесь.

РЕЦЕНЗИЯ
на статью на тему «Защита неприкосновенности частной жизни в условиях развития цифровых коммуникаций».

Предмет исследования.
Предложенная на рецензирование статья посвящена актуальным вопросам защиты неприкосновенности частной жизни. Автором обозначено наличие проблемы на основе анализа практики, а также научной литературы. В качестве конкретного предмета исследования выступили мнения ученых, положения законодательства и международных актов, эмпирические данные.
Методология исследования.
Цель исследования прямо в статье не заявлена. При этом она может быть ясно понята из названия и содержания работы. Цель может быть обозначена в качестве рассмотрения и разрешения отдельных проблемных аспектов вопроса о защите неприкосновенности частной жизни в условиях развития цифровых коммуникаций. Исходя из поставленных цели и задач, автором выбрана методологическая основа исследования.
В частности, автором используется совокупность общенаучных методов познания: анализ, синтез, аналогия, дедукция, индукция, другие. В частности, методы анализа и синтеза позволили обобщить и разделить выводы различных научных подходов к предложенной тематике.
Наибольшую роль сыграли специально-юридические методы. В частности, автором активно применялся формально-юридический метод, который позволил провести анализ и осуществить толкование норм действующего законодательства (прежде всего, положений международных актов). Например, следующий вывод автора: «Право человека на неприкосновенность частной жизни закреплено нормативно с середины XX века и получило подтверждение в международных документах, включая Всеобщую декларацию прав человека (статья 12), Конвенцию о защите прав человека и основных свобод (статья 8), Конвенцию о правах ребенка (статья 16), Международную конвенцию о защите прав всех трудящихся-мигрантов и членов их семей (статья 14), Конвенцию СНГ о правах и основных свободах человека (статья 9), а также множество других международных договоров и региональных соглашений о правах человека [1, с. 13-19]. Этот процесс стал важным шагом в признании данного права международным сообществом».
Также положительную роль сыграли эмпирические методы исследования. В частности, автор делает определенные выводы, используя статистические данные. Отметим

следующие рассуждения автора: «если верить статистике, представленной Федеральным бюро расследований (FBI), на уровне преступности это существенно не отразилось, и даже замечен рост уровня преступности с 2016 года: уровень преступности в Новом Орлеане, Лос-Анджелес, в 2015 году составил 949,56 на 100 000 населения, что на 2,5% меньше, чем в 2014 году; уровень преступности в Новом Орлеане, Лос-Анджелес, в 2016 году составил 1069,72 на 100 000 населения, что на 12,65% больше, чем в 2015 году; уровень преступности в Новом Орлеане, Лос-Анджелес, в 2017 году составил 1121,41 на 100 000 населения, что на 4,83% больше, чем в 2016 году; уровень преступности в Новом Орлеане, Лос-Анджелес, в 2018 году составил 1163,3 на 100 000 населения, что на 3,74% больше, чем в 2017 году. Таким образом, говорить о благоприятном исходе использования технологий слежения нельзя, поскольку в результате «эксперимента» компания Palantir Technologies получила доступ к личной информации американских граждан, при этом сами граждане не были защищены от совершаемых в отношении них и их близких преступлений».

Таким образом, выбранная автором методология в полной мере адекватна цели исследования, позволяет изучить все аспекты темы в ее совокупности.

Актуальность.

Актуальность заявленной проблематики не вызывает сомнений. Имеется как теоретический, так и практический аспекты значимости предложенной темы. С точки зрения теории тема защиты неприкосновенности частной жизни в условиях развития цифровых коммуникаций сложна и неоднозначна. Сложно спорить с автором в том, что «Технологический прогресс создает новые возможности для человека, общества и государства, но также порождает множество проблем, угроз и рисков [3, с. 118-119]. Тревожной тенденцией является все более активное использование информационно-коммуникационных технологий государственными и негосударственными субъектами, а также смешанными (коммерческими организациями с государственным участием) группами, в собственных интересах. Крупные IT-корпорации многомерны и сочетают в себе принудительные и подрывные меры с использованием как обычных, так и нетрадиционных способов, и тактик, для достижения своих целей. На сегодняшний день, основная проблема в том, что гражданам зачастую неизвестно какие продукты и программное обеспечение используются компаниями для работы с их данными, а также какие именно данные обрабатываются подобными организациями и какие меры предосторожности предусмотрены для защиты персональных данных и предотвращения их неправомерного использования. Частная компания, имея доступ к большому количеству данных о человеке, отклоняет запросы на прозрачность, так называемый «transparency report», по причине защиты коммерческих интересов. Полученные такими компаниями данные используются в собственных экономических интересах для рекламы, скрытого наблюдения, дифференцированного ценообразования, влияния на выборы, целенаправленной дезинформации, прогнозирования настроений на инвестиционных рынках, управления корпоративными рисками и пр. Применяемые информационные технологии дают большую возможность как для сознательного, так и для неосознанного нарушения права на неприкосновенность частной жизни».

Тем самым, научные изыскания в предложенной области стоит только поприветствовать.

Научная новизна.

Научная новизна предложенной статьи не вызывает сомнений. Во-первых, она выражается в конкретных выводах автора. Среди них, например, такой вывод:

«необходимо повысить прозрачность закупочной деятельности технологического сектора государства. Заключение любых контрактов с технологическими компаниями должно основываться на принципах законности, справедливости и прозрачности, а также целостности и конфиденциальности. В случае, если компания получает доступ к

персональным данным граждан, должны быть определены цели обработки таких данных, ограничен срок их хранения и установлена строгая подотчетность».

Указанный и иные теоретические выводы могут быть использованы в дальнейших научных исследованиях.

Во-вторых, автором предложены идеи по совершенствованию действующего законодательства. В частности,

«Целесообразно ввести правила, направленные на обеспечение прозрачности данной сферы: государственные органы, имеющие контракты с крупными технологическими компаниями, должны публиковать такие контракты и соглашения о совместном использовании персональных данных и проводить соответствующую оценку воздействия на права человека, которая позволит сопоставить и оценить риски обработки данных и будет содержать план действий по их снижению до приемлемого уровня. Кроме того, создание этических правил сбора и обработки данных может способствовать благоприятной атмосфере для развития бизнеса, а также стимулировать инновации посредством культуры ответственного поведения».

Приведенный вывод может быть актуален и полезен для правотворческой деятельности.

Таким образом, материалы статьи могут иметь определенных интерес для научного сообщества с точки зрения развития вклада в развитие науки.

Стиль, структура, содержание.

Тематика статьи соответствует специализации журнала «NB: Административное право и практика администрирования», так как она посвящена правовым проблемам, связанным с защитой неприкосновенности частной жизни.

Содержание статьи в полной мере соответствует названию, так как автор рассмотрел заявленные проблемы, достиг цели своего исследования.

Качество представления исследования и его результатов следует признать в полной мере положительным. Из текста статьи прямо следуют предмет, задачи, методология и основные результаты исследования.

Оформление работы в целом соответствует требованиям, предъявляемым к подобного рода работам. Существенных нарушений данных требований не обнаружено.

Библиография.

Следует высоко оценить качество использованной литературы. Автором активно использована литература, представленная авторами из России (Богданов Д.Е., Гарчева Л.П., Костина О.В., Ромашов П.А. и другие).

Таким образом, труды приведенных авторов соответствуют теме исследования, но не обладают признаком достаточности, не способствуют раскрытию различных аспектов темы.

Апелляция к оппонентам.

Автор провел серьезный анализ текущего состояния исследуемой проблемы. Все цитаты ученых сопровождаются авторскими комментариями. То есть автор показывает разные точки зрения на проблему и пытается аргументировать более правильную по его мнению.

Выводы, интерес читательской аудитории.

Выводы в полной мере являются логичными, так как они получены с использованием общепризнанной методологии. Статья может быть интересна читательской аудитории в плане наличия в ней систематизированных позиций автора применительно к заявленным автором вопросам.

На основании изложенного, суммируя все положительные и отрицательные стороны статьи

«Рекомендую опубликовать»