



ФИЛОСОФИЯ

Известия Саратовского университета. Новая серия. Серия: Философия. Психология. Педагогика. 2026. Т. 26, вып. 1. С. 4–8

Izvestiya of Saratov University. Philosophy. Psychology. Pedagogy, 2026, vol. 26, iss. 1, pp. 4–8
<https://phpp.sgu.ru> <https://doi.org/10.18500/1819-7671-2026-26-1-4-8>

EDN: BVSAJ

Научная статья
УДК 004:[1:316]

Цифровой контроль и проблема свободы в информационном обществе

А. Л. Крайнов

Саратовский государственный университет генетики, биотехнологии и инженерии имени Н. И. Вавилова, Россия, 410012, г. Саратов, проспект им. Петра Столыпина, зд. 4, стр. 3

Крайнов Андрей Леонидович, кандидат философских наук, доцент кафедры социально-гуманитарных наук, krainoval@vavilovsar.ru, <https://orcid.org/0000-0002-2129-0065>

Аннотация. Введение. Статья посвящена проблеме цифрового контроля как инструмента принуждения и манипуляции гражданами, лишаящими их свободы и личного пространства. Использование цифровых технологий не только способствует коммуникации и реализации бизнес-процессов, но и является источником постоянного сбора информации о всех действиях пользователей цифровой среды. **Теоретический анализ.** В процессе исследования определены три уровня цифрового контроля: начальный, базовый и тотальный, отличающихся степенью воздействия на человека. На каждом из этих уровней осуществляется слежка за гражданами с помощью различных информационных технологий с целью оценить их лояльность по отношению к государству и выявить противоправное поведение. В качестве примера тотального уровня цифрового контроля показана китайская система социального кредита. **Заключение.** Развитие цифровых технологий неминуемо ведет к увеличению степени цифрового контроля и уменьшению свободы человека. Этот процесс сопровождается полной зависимостью последнего от цифрового мониторинга и лишением личного пространства. Задача человечества заключается в сохранении баланса между цифровым контролем и свободой, чтобы не допустить цифрового рабства и трансформации человека в постчеловека посредством постепенной киборгизации.

Ключевые слова: цифровой контроль, цифровизация, цифровой тоталитаризм, информационное общество, цифровое рабство, цифровая свобода

Для цитирования: Крайнов А. Л. Цифровой контроль и проблема свободы в информационном обществе // Известия Саратовского университета. Новая серия. Серия: Философия. Психология. Педагогика. 2026. Т. 26, вып. 1. С. 4–8. <https://doi.org/10.18500/1819-7671-2026-26-1-4-8>, EDN: BVSAJ

Статья опубликована на условиях лицензии Creative Commons Attribution 4.0 International (CC-BY 4.0)

Article

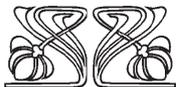
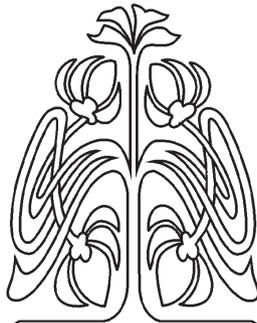
Digital control and the problem of freedom in the information society

A. L. Kraynov

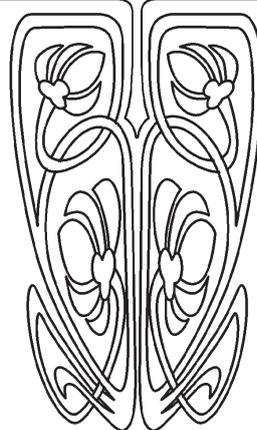
Saratov State University of Genetics, Biotechnology and Engineering named after N. I. Vavilov, building 4, block 3 Peter Stolypin Avenue, Saratov 410012, Russia

Andrey L. Kraynov, krainoval@vavilovsar.ru, <https://orcid.org/0000-0002-2129-0065>

Abstract. Introduction. This article examines the problem of digital control as a tool for coercion and manipulation of citizens, depriving them of freedom and personal space. The use of digital



НАУЧНЫЙ
ОТДЕЛ





technologies not only facilitates communication and business processes but also serves as a source of continuous collecting information about all actions of digital users. **Theoretical analysis.** The study identified three levels of digital control: initial, basic, and total, each one with varying degrees of impact on individuals. At each level, citizens are monitored using various information technologies to assess their loyalty to the state and identify unlawful behavior. China's social credit system is used as an example of a total level of digital control. **Conclusion.** The development of digital technologies inevitably leads to an increase in digital control and a decrease in human freedom. This process is accompanied by the latter's complete dependence on digital monitoring and the deprivation of personal space. Humanity's task is to maintain a balance between digital control and freedom to prevent digital slavery and the transformation of humans into posthumans through gradual cyborgization.

Keywords: digital control, digitalization, digital totalitarianism, information society, digital slavery, digital freedom

For citation: Kraynov A. L. Digital control and the problem of freedom in the information society. *Izvestiya of Saratov University. Philosophy. Psychology. Pedagogy*, 2026, vol. 26, iss. 1, pp. 4–8 (in Russian). <https://doi.org/10.18500/1819-7671-2026-26-1-4-8>, EDN: BVSAJB

This is an open access article distributed under the terms of Creative Commons Attribution 4.0 International License (CC-BY 4.0)

Введение

Актуальность исследования обусловлена всевозрастающей ролью информационных цифровых технологий в жизни человека. Прочно укоренившиеся в личном и социальном бытии, они не только способствуют коммуникации и облегчают доступ к информационным ресурсам, но непрерывно следят за всеми действиями индивида и общества. Цифровой контроль, осуществляющийся за человеком с помощью всевозможных гаджетов, не только обогащает маркетинговые базы данных, способствуя лучшей таргетированности рекламных кампаний, но вторгается в личное пространство человека посредством прямого видеонаблюдения, основанного на системе распознавания лиц, и чипирования.

Значимость исследуемой проблемы связана с зависимостью человека от коммуникационной техники (ярким проявлением которой является номофобия), с одной стороны, и постоянной угрозы утраты личной свободы при взаимодействии с данной техникой, с другой.

Цель исследования – определить грань между цифровой свободой и цифровым рабством в современном мире.

Новизна исследования продиктована последними тенденциями информационного общества в сфере цифрового контроля.

Материалы исследования могут быть использованы при подготовке курсов по социальной философии.

Теоретический анализ

Под цифровым контролем принято понимать практику применения цифровых технологий и данных для управления различными процессами и поведением людей. С развитием

цифровизации значимость цифрового контроля только возрастает. Цифровой контроль может проявляться на институциональном и техническом уровнях. В первом случае государство и иные социальные институты являются инициаторами реализации цифрового контроля как средства мониторинга за гражданами в целом и персоналом в частности. Во втором случае цифровой контроль осуществляется с помощью различных цифровых технических средств и приложений, с которыми непосредственно работает человек, собирающими данные о всех проводимых в них операциях и отправляющими их на сервера различных компаний.

Если рассматривать данное явление с организационной точки зрения, то очевидны множество плюсов данной практики, один из которых, по мнению Ю. Глуховской, заключается в безопасности производственного процесса: различные датчики измерения температуры тела, артериального давления и наличия алкоголя в крови сотрудника на проходной снижают производственные риски и повысят эффективность труда¹. Институт развития Интернета (АНО «ИРИ») публикует на своем сайте статью, рассматривающую цифровой контроль в большей степени как инструмент мониторинга и слежки за персоналом². Согласно приведенным аналитическим данным, к методам цифровой слежки за сотрудниками прибегает треть работодателей по всему миру. С одной стороны, данная практика призвана повысить производительность

¹ Глуховская Ю. Цифровой контроль // Новостной портал РБК (РосБизнесКонсалтинг). 2 июня 2020 г. URL: <https://plus.rbc.ru/news/5ed515e97a8aa9b1a19459e0> (дата обращения: 14.10.2025).

² Цифровой контроль за сотрудниками (использование технологий мониторинга на рабочем месте) // Официальный сайт российской автономной некоммерческой организации Институт развития Интернета (ИРИ). 7 августа 2023 г. URL: <https://ири.рф/news/tsifrovoy-kontrol-za-sotrudnikami-ispolzovanie-tekhnologiy-monitoringa-na-rabochem-meste/> (дата обращения: 14.10.2025).



труда, так как фиксируется время нецелевого использования рабочего пространства (от кликанья мышкой не на те программы до низкой активности сотрудника в целом), с другой стороны, подобный цифровой контроль зачастую приводит к снижению качества производства, психологическому дискомфорту персонала и утрате доверия к руководству.

Согласно Д. А. Руцину, цифровой контроль представляет собой манипулирование цифровыми коммуникациями со стороны властей. Государство дозирует доступность инструментов цифровой коммуникации для населения, ограничивая использование одних Интернет-сервисов в пользу других. В качестве страны с самым несвободным Интернетом автор приводит Китай, а максимальная свобода в цифровом пространстве отмечается им в Исландии [1, с. 525–526]. Анализируя систему цифрового контроля над гражданами на примере Москвы, И. В. Юшков выделяет две ее части: физическую и виртуальную. Первая представлена техническими устройствами видеонаблюдения с системой распознавания лиц и идентификации личности, а вторая – работой государственных органов в виртуальной среде с целью мониторинга противоправных действий [2]. Задача цифрового контроля, по его мнению, заключается в контроле общества. Таким образом, проблема цифрового контроля всегда сопряжена с проблемой свободы не только в цифровой среде, но и в обществе в целом.

Если анализировать феномен цифрового контроля в философском аспекте, то он связан с понятиями «цифровой тоталитаризм» и «цифровое рабство», так как не просто выступает мониторингом социальной сферы, но лишает человека личного пространства и свободы, превращая его в винтик цифрового общества и подчиняя ряду требований цифровой культуры, главным из которых выступает полная цифровая идентичность. В целом можно выделить три уровня цифрового контроля в зависимости от реализуемой им степени цифрового рабства: начальный, базовый и тотальный.

Начальный уровень цифрового контроля связан с понятием цифрового следа как совокупности всей деятельности человека в сети Интернет. Эта информация никуда не исчезает, но хранится на серверах тех компаний, чьи сервисами человек пользуется. Любые цифро-

вые гаджеты собирают информацию о своем владельце, эта опция зачастую включена в них по умолчанию. Потом данная информация анализируется маркетинговыми службами компаний с целью выявления предпочтений клиента, исправления ошибок в приложениях и трансляции ему контекстной рекламы. Также начальный уровень цифрового контроля проявляется в необходимости формирования пользователем сети своей цифровой идентичности. В цифровом обществе невозможно что-либо сделать, не будучи зарегистрированным во множестве связанных друг с другом сервисов, особенно если речь идет о получении государственных услуг и финансовых операциях. Банки и ритейлеры знают о нас все: от продуктов и вещей, которые мы покупаем, до точного времени нашей активности и наиболее частых маршрутах. Включенная геолокация, участие в программах лояльности, скидках и акциях являются эффективными инструментами начального уровня цифрового контроля.

Базовый уровень цифрового контроля связан с использованием системы видеонаблюдения за обществом. К нему относятся камеры видеонаблюдения нарушений, как ПДД, так и с системой распознавания лиц, также данный контроль включает в себя использование биометрии в качестве кода доступа к данным и различным объектам. Этот уровень цифрового контроля способствует реализации социального контроля и самоконтроля, предотвращая многие правонарушения, и активно используется как на государственном, так и частном уровнях.

Тотальный цифровой контроль выступает гипотетической моделью развития техники и является предметом острых философских дискуссий. На этом уровне обсуждаются проблемы технологической сингулярности и постчеловечества, трансгуманизма и чипирования человека, восстания машин и киборгизации. Сегодня существуют технико-технологические предпосылки для осуществления данного уровня цифрового контроля, реализующиеся в Китае в виде системы социального кредита. Миллионы повсеместно установленных видеочкамер с модулями распознаванием лиц и сканирования тела ежесекундно оценивают поведение граждан КНР на предмет лояльности к государству. При законопослушном поведении количество кредитных единиц возрастает, что дает гражданину ряд пре-



имущества и поощрений (кредиты по низкой процентной ставке, возможность устроить ребенка в престижный детский сад и т.п.), в противном случае количество кредитов уменьшается, и человек экономически загоняется в тупик, выход из которого возможен только при изменении принципов мышления и поведения. Весь процесс происходит полностью в автоматическом режиме с участием технологий искусственного интеллекта, который и выносит решения о начислении/списании кредитных баллов.

По мнению Р. Ф. Мустафина с соавторами, китайская модель цифрового контроля существенно ограничивает права граждан, так как противоречит не только Международному пакту о гражданских и политических правах, но и Конституции КНР, без достаточных оснований собирая обо всех информацию и заранее вынося вердикт о возможной будущей виновности того или иного человека. Причем баллы доверия передаются по наследству детям и с рождения определяют их как законопослушных граждан или потенциальных нарушителей без права реабилитации [3, с. 90–92]. Согласно В. А. Эпштейну, Е. В. Чистякову, с 2020 г. система социального кредита стала еще и карательным инструментом государства, наказывая скрывших факт посещения зон на земном шаре с высоким уровнем Covid-19 [4, с. 95]. Искусственный интеллект постоянно анализирует все действия граждан КНР в реальном и виртуальном мирах и на основе полученных данных решает их дальнейшую судьбу, тем самым устранив понятия свободы и личного пространства из жизни китайцев.

Заключение

Анализ феномена цифрового контроля позволяет заключить, что любое совершенствование его технологий лишает человека части свободного жизненного пространства. Этот процесс сопровождается, по мнению А. С. Линникова, вступлением в противоречие с правами и свободами человека и гражданина, превращая человека из субъекта права в объект цифрового контроля и управления [5, с. 291–292]. Развитие цифровизации успешно борется с анонимностью, приватностью, конфиденциальностью и неприкосновенностью частной жизни, стирая всякие грани между частным и публичным,

под предлогом профилактики девиантного поведения. В цифровом обществе не место аналоговой или обычной (физической) свободе, которая предполагает полную независимость от наблюдателя, выбор деятельности, право не быть порабощенным или заключенным, а также право на личную неприкосновенность и свободу передвижения. В нем может существовать только свобода цифровая, под которой следует понимать беспрепятственное осуществление цифровых коммуникаций и операций в любой точке пространства. Именно для реализации цифровой свободы нужны базовые станции сотовой связи стандартов 5G (20 Гбит/с) и 6G (1 Тбит/с), спутники глобальной системы связи (например, Starlink), чипирование головного мозга с подключением к сети Интернет и искусственному интеллекту (проекты Neuralink и Нейронет).

Как отмечает Ю. И. Соколов, современный человек целенаправленно идет к вырождению, вследствие его добровольного слияния с машиной и сознательному отвержению природы (то есть всего естественного) [8]. Превращая себя в киборга, человек трансформируется в пост-человека, утрачивая приоритет естественного над искусственным. Киборг априори не может быть свободным, так как развитие техники исторически (с первой промышленной революции) лишает человека свободы, полностью подчиняя себе. Киборг постоянно будет объектом тотального цифрового контроля, будет зависеть от качества имплантированных в него технических устройств, нуждаться в своевременном обслуживании их или замене, поручив свое существование (жизнью такое назвать нельзя) компаниям-разработчикам.

Таким образом, вопрос о реализации цифрового контроля представляет собой проблему баланса между уровнем цифрового контроля и степенью обычной свободы. Тотальный цифровой контроль приведет к полному отсутствию физической свободы и цифровому рабству, а начальный уровень позволит максимально уединиться и почувствовать себя относительно ненаблюдаемым. Главная проблема заключается в том, что ученое человечество до сих пор ориентируется на сциентистскую научную парадигму, восхваляющую научно-технический прогресс и все блага, которые он способен дать. Работа над совершенствованием цифровых тех-



нологий на основе искусственного интеллекта, одновременно осуществляющаяся учеными всего мира, и планомерное их внедрение в повседневность ведет не только к становлению эпохи тотального цифрового контроля, но и к эпохе постчеловечества.

Список литературы

1. Руцин Д. А. Проблемы цифрового контроля в современном мире // Война и мир в Отечественной и мировой истории : материалы Международной научной конференции : в 2 т. Посвящается 75-летию Победы в Великой Отечественной войне. СПб., 2020. С. 525–529. EDN: QGYVMF
2. Юшков И. В. Развитие цифровой системы контроля над обществом в России // Власть. 2021. Т. 29, № 5. С. 53–57. <https://doi.org/10.31171/vlast.v29i5.8532>
3. Мустафин Р. Ф., Мустафина С. А., Абазов И. В. Цифровой контроль в Китае как средство ограничения гражданских прав // Кубанское агентство судебной информации PRO-SUD-123.RU: юридический сетевой электронный научный журнал. 2018. № 4 (7). С. 85–93. EDN: YTEVJZ
4. Эпштейн В. А., Чистякова Е. В. Система социального кредита КНР как область применения технологии искусственного интеллекта // Современные востоковедческие исследования. 2020. № 27. С. 193–196. EDN: OPLUML
5. Линников А. С. Цифровой правовой контроль как новая цивилистическая категория // Вестник Пермского университета: юридические науки. 2024. № 2 (64). С. 289–310. <https://doi.org/10.17072/1995-4190-2024-64-289-310>
6. Соколов Ю. И. Риски человека в цифровую эпоху // Проблемы анализа риска. 2021. Т. 18, № 2. С. 72–87. <https://doi.org/10.32686/1812-5220-2021-18-2-72-87>

References

1. Rushchin D. A. Problems of digital control in the modern world. In: *Voyna i mir v Otechestvennoy i mirovoy istorii: materialy mezhdunarodnoy nauchnoy konferentsii: v 2 t. Posvyashchaetsya 75-letiyu Pobedy v Velikoy Otechestvennoy voyne* [War and Peace in National and World History. Proceedings of the International scientific conference: in 2 vols. Dedicated to the 75th Anniversary of Victory in the Great Patriotic War]. St. Petersburg, 2020, pp. 525–529 (in Russian). EDN: QGYVMF
2. Yushkov I. V. Development of a digital system of control over society in Russia. *Vlast' [Power]*, 2021, vol. 29, no. 5, pp. 53–57 (in Russian). <https://doi.org/10.31171/vlast.v29i5.8532>
3. Mustafin R. F., Mustafina S. A., Abazov I. V. Digital control in China as a means of restricting civil rights. *Kubanskoe agentstvo sudebnoy informatsii PRO-SUD-123.RU: Yuridicheskiy setevoy elektronnyi nauchnyi zhurnal* [Kuban Agency of Judicial Information PRO-SUD-123.RU: Legal online electronic scientific journal], 2018, no. 4 (7), pp. 85–93 (in Russian). EDN: YTEVJZ
4. Epshteyn V. A., Chistyakova E. V. PRC social credit system as a field of application artificial intelligence technologies. *Sovremennye vostokovedcheskie issledovaniya* [Modern Oriental Studies], 2020, no. 27, pp. 193–196 (in Russian). EDN: OPLUML
5. Linnikov A. S. Digital legal control as a new civil category. *Vestnik Permskogo universiteta: yuridicheskie nauki* [Perm University Herald: Juridical Sciences], 2024, no. 2 (64), pp. 289–310 (in Russian). <https://doi.org/10.17072/1995-4190-2024-64-289-310>
6. Sokolov Yu. I. Human risks in the digital age. *Problemy analiza riska* [Issues of Risk Analysis], 2021, vol. 18, no. 2, pp. 72–87 (in Russian). <https://doi.org/10.32686/1812-5220-2021-18-2-72-87>

Поступила в редакцию 25.09.2025; одобрена после рецензирования 23.10.2025; принята к публикации 15.11.2025
The article was submitted 25.09.2025; approved after reviewing 23.10.2025; accepted for publication 15.11.2025