СИСТЕМНЫЕ УГРОЗЫ ЦИФРОВЫМ ПРАВАМ ЧЕЛОВЕКА В ЭЛЕКТРОННОМ ПРАВИТЕЛЬСТВЕ: МАССОВАЯ СЛЕЖКА, УТЕЧКИ ПЕРСОНАЛЬНЫХ ДАННЫХ И АЛГОРИТМИЧЕСКАЯ ДИСКРИМИНАЦИЯ

Бутаёрова Мадинабону Шухратжон кизи

Университет мировой экономики и дипломатии

Магистрант факультета международного права

xh2025-70151@uwed.ac.uz, 998 91 701 94 99

Аннотация: В условиях цифровизации государственного управления электронное правительство одновременно выступает инструментом реализации прав граждан и источником новых системных угроз цифровым правам человека. Цель статьи анализ трёх взаимосвязанных угроз. Массовой слежки, утечек персональных данных и алгоритмической дискриминации через призму международных стандартов защиты прав человека. На основе анализа практики Европейского суда по правам человека, Комитета ООН по правам человека и регионального регулирования (GDPR, Регламент ЕС об искусственном интеллекте) выявлены пробелы в имплементации международных норм применительно к государственным цифровым системам. В заключении сформулированы рекомендации по укреплению правовых гарантий транспарентности и подотчётности государства.

Ключевые слова: электронное правительство, массовая слежка, утечка персональных данных, алгоритмическая дискриминация, GDPR, цифровые права человека, искусственный интеллект.

Elektron hukumatda inson raqamli huquqlariga tizimli tahdidlar: ommaviy kuzatuv, shaxsiy ma'lumotlarning sizib chiqishi va algoritmik kamsitish

Butayorova Madinabona Shuhratjon qizi

Jahon iqtisodiyoti va diplomatiya universiteti

Xalqaro huquq fakulteti magistranti
xh2025-70151@uwed.ac.uz, 998 91 701 94 99

Annotatsiya: Davlat boshqaruvining raqamlashtirilishi sharoitida elektron hukumat bir vaqtning o'zida fuqarolar huquqlarini amalga oshirish vositasi va raqamli inson huquqlariga yangi tizimli tahdidlar manbai bo'lib xizmat qilmoqda. Tadqiqotning maqsadi — xalqaro inson huquqlari standartlari nuqtai nazaridan uch o'zaro bog'liq tahdidni, ommaviy kuzatuvni, shaxsiy ma'lumotlarning sizib chiqishini va algoritmik kamsitishni tahlil qilishdan iborat. Yevropa inson huquqlari sudi, BMT Inson huquqlari qo'mitasi amaliyoti hamda mintaqaviy tartibga solish (GDPR, sun'iy intellekt bo'yicha YEI Reglamenti) tahlili asosida davlat raqamli tizimlariga nisbatan xalqaro me'yorlarni amalga oshirishdagi bo'shliqlar aniqlangan. Yakunda davlatning shaffoflik va hisobdorlik bo'yicha huquqiy kafolatlarini mustahkamlash yuzasidan tavsiyalar ishlab chiqilgan.

Kalit so'zlar: elektron hukumat, ommaviy kuzatuv, shaxsiy ma'lumotlarning sizib chiqishi, algoritmik kamsitish, GDPR, raqamli inson huquqlari, sun'iy intellekt.

Systemic Threats to Digital Human Rights in E-Government: Mass Surveillance, Personal Data Breaches, and Algorithmic Discrimination

Butayorova Madinabonu Shuhratjon kizi
University of World Economy and Diplomacy
Master of International Law
xh2025-70151@uwed.ac.uz, 998 91 701 94 99

Abstract: As public administration undergoes digitalisation, e-government simultaneously serves as an instrument for realising citizens' rights and a source of new systemic threats to digital human rights. This article aims to analyse three interrelated threats mass surveillance, personal data breaches, and algorithmic discrimination through the lens of international human rights standards. Drawing on the case law of the European Court of Human Rights, the UN Human Rights Committee, and regional regulation (the GDPR and the EU Artificial Intelligence

Act), the study identifies gaps in the implementation of international norms with respect to state digital systems. The conclusion proposes recommendations for strengthening legal guarantees of transparency and state accountability.

Key words: e-government, mass surveillance, personal data breach, algorithmic discrimination, GDPR, digital human rights, artificial intelligence.

Введение: Цифровизация государственного управления привела к формированию электронного правительства как новой институциональной модели, в которой государство выступает одновременно гарантом прав граждан и оператором масштабных цифровых систем, аккумулирующих персональные данные миллионов пользователей. Эта двойственная роль порождает специфическое противоречие: инструменты, создаваемые для повышения эффективности и доступности государственных услуг, могут одновременно становиться источником нарушений цифровых прав человека. В научной литературе к числу наиболее значимых системных угроз, возникающих в данном контексте, принято относить массовую слежку, утечки персональных данных из государственных информационных систем и алгоритмическую дискриминацию при автоматизированном принятии решений. Каждая из них опирается на одну и ту же структурную предпосылку избыточную централизацию персональных данных в руках государств и требует самостоятельного международно-правового анализа.

Актуальность. По мере расширения систем электронного правительства цифровых удостоверений личности, единых государственных реестров, платформ межведомственного обмена данными и автоматизированных систем принятия решений возрастает и масштаб потенциальных нарушений цифровых прав. Международно-правовая доктрина пока не выработала единого комплексного подхода к оценке ответственности государства за подобные нарушения, а региональные и универсальные механизмы защиты прав человека применяют разрозненные,

не всегда согласованные критерии. Актуальность настоящего исследования обусловлена необходимостью систематизации международных стандартов, применимых к трём рассматриваемым угрозам, и оценки эффективности их имплементации на практике.

Материалы и методы. В работе использованы международные договоры и резолюции органов ООН, прецедентная практика Европейского суда по правам человека, региональное законодательство Европейского союза (GDPR, Регламент об искусственном интеллекте), а также материалы судебной практики национальных судов (Нидерланды, Австралия, Кения, США). Применялись методы сравнительно-правового анализа, системного анализа и обобщения правоприменительной практики.

Основная часть: Результаты исследования.

В международно-правовой доктрине массовую слежку, утечки персональных данных и алгоритмическую дискриминацию принято рассматривать не как отдельные инциденты, а как системные явления, поскольку они способны структурно трансформировать баланс между публичной властью и индивидуальной свободой. Как отмечает Дэвид Лайон, один из ведущих исследователей surveillance studies1, современное государство постепенно превращается в “надзорное общество”, в котором наблюдение становится имманентной чертой повседневного управления. Применительно к электронному правительству эта тенденция приобретает особое измерение. Технологии, разработанные для удобства граждан, создают инфраструктуру, потенциально пригодную для тотального контроля.

Массовая слежка в системах электронного правительства.

Массовая слежка представляет собой широкомасштабный сбор, хранение и анализ данных о гражданах со стороны государственных органов

1David Lyon. The Culture of Surveillance: Watching as a Way of Life. — Cambridge: Polity Press, 2018. — 248 p.

без индивидуализированного подозрения в отношении конкретных лиц. В условиях электронного правительства подобная практика становится технически доступной благодаря централизации государственных реестров, цифровых идентификационных систем и межведомственной интеграции информационных ресурсов. Принципиальное отличие данного явления от традиционного надзора состоит в его неизбирательном характере: объектом наблюдения становится не отдельный подозреваемый, а вся совокупность граждан, взаимодействующих с государственными системами. Особую остроту проблема приобрела после разоблачений Эдварда Сноудена в 2013 году[2], продемонстрировавших масштаб глобального наблюдения, осуществлявшегося в рамках программ PRISM[3] и основанного на сотрудничестве спецслужб союзных государств в формате альянса “Пяти глаз”[4]. Значительная часть перехваченных данных была получена именно через государственные цифровые инфраструктуры, что подчёркивает уязвимость систем электронного правительства перед злоупотреблением собранной информацией.

С доктринальной точки зрения массовая слежка вступает в противоречие с концепцией информационного самоопределения, впервые сформулированной Федеральным конституционным судом Германии в решении по делу о переписи населения 1983 года[5]. Комитет ООН по правам человека в Замечании общего порядка № 16 (1988) разъяснил, что понятие

2The Guardian. Edward Snowden NSA files: secret surveillance and our revelations so far Режим доступа: https://www.theguardian.com/world/2013/aug/21/edward-snowden-nsa-files-revelations

3The Guardian. NSA Prism program taps in to user data of Apple, Google and others https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

4Central Intelligence Agency (CIA). Ask Molly: Five Eyes https://www.cia.gov/stories/story/ask-molly-five-eyes/

5Federal Constitutional Court of Germany. Judgment of 15 December 1983 (Volkszählungsurteil), BVerfGE https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/1983/12/rs19831215_1bvr020983.html

произвольное вмешательство шире понятия незаконное, вмешательство может иметь законодательное основание, но всё же нарушать статью 17 Международного пакта о гражданских и политических правах, если оно несоразмерно преследуемой цели. Данное разъяснение имеет принципиальное значение для оценки государственных программ слежения, которые, как правило, формально предусмотрены законом, однако не соответствуют критерию пропорциональности. Резолюция Генеральной Ассамблеи ООН 68/167 “Право на неприкосновенность частной жизни в цифровую эпоху” (2013)[6] закрепила принцип, согласно которому права, существующие офлайн, должны сохранять равную защиту онлайн. На региональном уровне практика Европейского суда по правам человека выработала ключевые критерии допустимости мер наблюдения: в деле “Класс и другие против Германии” (1978)[7] Суд признал, что тайное наблюдение само по себе может нарушать статью 8 Европейской конвенции при отсутствии надлежащих гарантий против злоупотреблений, а в деле “Роман Захаров против России” (2015)[8] Большая палата констатировала системное нарушение данной статьи в связи с отсутствием судебного контроля над перехватом коммуникаций. Наиболее радикальным примером применения технологий массового наблюдения в государственном управлении остаётся система социального кредита, реализуемая в Китае с

6Организация Объединённых Наций. Генеральная Ассамблея. Резолюция 68/167 «Право на неприкосновенность частной жизни в цифровую эпоху», принятая 18 декабря 2013 г. Документ ООН A/RES/68/ New York: United Nations, 2014. — Режим доступа: https://digitallibrary.un.org/record/764407

7European Court of Human Rights. Case of Klass and Others v. Germany (Application no. 5029/71): Judgment of 6 September 1978 Strasbourg: Council of Europe, 1978. — Режим доступа: https://hudoc.echr.coe.int/eng?i=001-57510

8European Court of Human Rights. Case of Roman Zakharov v. Russia (Application no. 47143/06): Grand Chamber Judgment of 4 December 2015 Strasbourg: Council of Europe, 2015. — Режим доступа: https://hudoc.echr.coe.int/eng?i=001-159324

2014 года[9], в рамках которой цифровые профили граждан используются для принятия решений о доступе к услугам, трудоустройству и передвижению. Значимым доктринальным вкладом является также концепция охлаждающего эффекта (chilling effect) осознание возможного наблюдения само по себе способно ограничивать свободу выражения мнений, что было отмечено ещё в деле “Харман против Великобритании” (1989)[10] и подтверждено Большой палатой ЕСПЧ в деле “Big Brother Watch против Великобритании” (2021)[11], где было указано, что режим массового перехвата данных должен сопровождаться независимым надзором на всех стадиях — от авторизации до уничтожения собранных сведений.

Утечки персональных данных из государственных информационных систем.

Масштаб проблемы иллюстрируется резонансными инцидентами. В 2015 году утечка из Управления кадровой службы США скомпрометировала данные свыше 21 миллиона государственных служащих, включая результаты проверок допуска к секретным сведениям и биометрические данные[12]. В 2017–2018 годах была выявлена уязвимость биометрической системы идентификации Aadhaar в Индии, охватывающей свыше 1,3 млрд граждан:

9State Council of the People's Republic of China. Planning Outline for the Construction of a Social Credit System (2014–2020), issued on 14 June 2014 [Электронный ресурс]. — Beijing: State Council of the PRC, 2014. https://www.gov.cn/zhengce/content/2014-06/27/content_8913.htm

10European Commission of Human Rights. Case of Hewitt and Harman v. the United Kingdom (Application no. 12175/86): Report adopted on 9 May 1989 [Электронный ресурс]. Strasbourg: Council of Europe, 1989. https://hudoc.echr.coe.int/eng?i=001-45372

11European Court of Human Rights. Case of Big Brother Watch and Others v. the United Kingdom (Applications nos. 58170/13, 62322/14, 24960/15): Judgment of 25 May 2021 Strasbourg: ECHR, 2021. — Режим доступа: https://hudoc.echr.coe.int/eng?i=001-210077

12United States Office of Personnel Management. Cybersecurity Resource Center: Cybersecurity Incidents Washington, D.C.: U.S. Office of Personnel Management, 2015. — Режим доступа: https://www.opm.gov/cybersecurity/cybersecurity-incidents/

доступ к персональным данным можно было получить за незначительную плату через несанкционированные порталы13.

С позиций международного права государство несёт как негативные, так и позитивные обязательства по защите персональных данных. Концепция позитивных обязательств была последовательно разработана в практике Применительно к государственным информационным системам это означает обязанность имплементировать надлежащие технические и организационные меры защиты.

Ключевым международно-правовым инструментом в данной сфере остаётся Общий регламент о защите данных Европейского союза (GDPR)14, оказавший существенное влияние на глобальное регулирование в силу так называемого Брюссельского эффекта стандарты регулирования крупнейшего рынка фактически становятся глобальными ввиду нецелесообразности сегментации бизнес-процессов для разных юрисдикций. Статья 35 GDPR обязывает государственные органы как контролёров данных проводить оценку воздействия на защиту данных (DPIA) для любой масштабной обработки, способной повлечь высокий риск для прав субъектов, а статья 83(4) предусматривает возможность применения штрафов вплоть до 10 млн евро или 2% годового оборота, хотя практика применения этой меры к государственным органам остаётся неоднородной.

Особую опасность представляет утечка биометрических данных, в отличие от паролей, отпечатки пальцев, параметры радужной оболочки и

13The Tribune India. Rs 500, 10 minutes, and you have access to billion Aadhaar details https://www.tribuneindia.com/news/archive/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details-523361

14Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), Article 5 // Official Journal of the European Union. — 2016. — L 119. — P. 1–88. — Режим доступа: https://eur-lex.europa.eu/eli/reg/2016/679/oj

данные распознавания лица обладают свойством неизменяемости скомпрометированный идентификатор невозможно заменить. Рабочая группа по статье 29 в Заключении 3/2012[15] подчеркнула необходимость повышенного уровня защиты биометрических данных ввиду их особой чувствительности, а GDPR отнёс такие данные к специальным категориям (статья 9) с запретом обработки по умолчанию[16].

Алгоритмическая дискриминация при автоматизированном принятии решений.

Алгоритмическая дискриминация возникает, когда автоматизированная система воспроизводит или усиливает социальные предубеждения, встроенные в исторические данные, на которых она обучалась. Исследователь Кэти О'Нил в работе “Оружие математического уничтожения” (2016)[17] обозначила данный феномен как заморозку настоящего, алгоритмы не предвидят будущее, а воспроизводят прошлое, придавая дискриминации видимость объективности.

Наиболее известным примером алгоритмической дискриминации в государственном управлении является дело COMPAS в сфере американского уголовного правосудия, расследование ProPublica (2016)[18] установило, что алгоритм оценки риска рецидива демонстрирует статистически значимую расовую предвзятость. Схожие проблемы выявлены и в практике

15Article 29 Data Protection Working Party. Opinion 3/2012 on developments in biometric technologies (WP193), adopted on 27 April 2012 Brussels: European Commission, 2012.

16Regulation (EU) 2016/679 (GDPR), Article 9 (Processing of special categories of personal data) // Official Journal of the European Union. — 2016. — L 119. — P. 1–88.

17Cathy O'Neil. Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy. — New York: Crown Publishing Group, 2016. — 288 p.

18ProPublica. Machine Bias: There's Software Used Across the Country to Predict Future Criminals. And It's Biased Against Blacks https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

европейских государств, в деле SyRI[19] окружной суд Гааги в 2020 году признал незаконной автоматизированную систему выявления социального мошенничества ввиду отсутствия транспарентности алгоритма и несоразмерного вмешательства в частную жизнь малообеспеченных граждан.

Международное сообщество отреагировало на эти вызовы развитием концепции алгоритмической подотчётности. Статья 22 GDPR предоставляет субъекту данных право не быть объектом исключительно автоматизированного решения, имеющего юридически значимые последствия, включая право на вмешательство человека и право оспорить решение. Значительный вклад в развитие международных стандартов внесли Рекомендация ЮНЕСКО об этике искусственного интеллекта (2021) и Рамочная программа ОЭСР в области политики в сфере ИИ (2019), акцентирующие принципы прозрачности, объяснимости и справедливости алгоритмических систем. Принятый в 2024 году Регламент ЕС об искусственном интеллекте установил для систем ИИ высокого риска, применяемых в государственном управлении, обязательные требования управления рисками, качества обучающих данных и надзора со стороны человека, прямо отнеся к категории высокорискованных системы, используемые для оценки права граждан на социальные услуги. Существенной общей характеристикой всех трёх рассмотренных угроз является их непрозрачность: гражданин, как правило, не осведомлён ни о масштабах ведущегося за ним наблюдения, ни о факте утечки его данных, ни о роли алгоритма в принятии решения, затронувшего его права. Это делает традиционные механизмы правовой защиты судебное обжалование, обращение в надзорный орган практически недоступными для значительного

19District Court of The Hague. NJCM c.s. v. The State of the Netherlands (SyRI case), ECLI:NL:RBDHA:2020:865: Judgment of 5 February 2020 [Электронный ресурс]. — The Hague, 2020.

числа потенциальных жертв нарушений. Международное право должно реагировать на данный вызов через развитие обязательств о транспарентности, распространяющихся на государственные цифровые системы, что лишь частично реализовано в действующем регулировании.

Заключение: Массовая слежка, утечки персональных данных и алгоритмическая дискриминация представляют собой три взаимосвязанных системных вызова развитию электронного правительства, вытекающих из самой логики цифровизации государственного управления. По результатам исследования сформулированы следующие выводы и рекомендации:

- международным органам следует развивать единые критерии оценки правомерности мер массового наблюдения (законность, необходимость, пропорциональность, независимый надзор), применимые непосредственно к системам электронного правительства;
- государствам, внедряющим централизованные биометрические реестры, необходимо предусматривать обязательную оценку воздействия на защиту данных до запуска системы, а не по факту выявленных утечек;
- применение автоматизированных систем принятия решений в государственном секторе должно сопровождаться правом граждан на объяснение алгоритмического решения и на вмешательство человека, по аналогии со статьёй 22 GDPR;
- развивающимся странам, реализующим стратегии цифровизации государственного управления, целесообразно ориентироваться на международные стандарты прозрачности и подотчётности уже на этапе проектирования цифровых систем (privacy by design), а не адаптировать их постфактум;
- судебная практика, в том числе национальная, должна рассматриваться как самостоятельный и действенный инструмент защиты цифровых прав, о чём свидетельствуют прецеденты по делам SyRI и Robodebt.

Реализация указанных мер позволит государствам, развивающим системы электронного правительства, снизить структурные риски нарушения цифровых прав человека и обеспечить более высокий уровень доверия граждан к процессам цифровизации государственного управления.

Библиография:

1. Международный пакт о гражданских и политических правах 1966 года, ст. 17. (URL: https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights)
2. Всеобщая декларация прав человека 1948 года, ст. 12.
3. Резолюция Генеральной Ассамблеи ООН 68/167 «Право на неприкосновенность частной жизни в цифровую эпоху» от 18 декабря 2013 г. (URL: https://digitallibrary.un.org/record/764407)
4. United Nations Human Rights Committee. General Comment No. 16 (Article 17: Right to privacy), 1988.
5. Regulation (EU) 2016/679 of 27 April 2016 (General Data Protection Regulation) // Official Journal of the European Union. — 2016. — L 119. (URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj)
6. Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) // Official Journal of the European Union. — 2024. — OJ L 2024/1689.
7. European Court of Human Rights. Klass and Others v. Germany, Judgment of 6 September 1978. (URL: https://hudoc.echr.coe.int/eng?i=001-57510)
8. European Court of Human Rights. Roman Zakharov v. Russia, Judgment of 4 December 2015. (URL: https://hudoc.echr.coe.int/eng?i=001-159324)
9. European Court of Human Rights. Big Brother Watch and Others v. the United Kingdom, Judgment of 25 May 2021. (URL: https://hudoc.echr.coe.int/eng?i=001-210077)

10. European Court of Human Rights. X and Y v. the Netherlands, Judgment of 26 March 1985. (URL: https://hudoc.echr.coe.int/eng?i=001-57603)
12. District Court of The Hague. NJCM c.s. v. The State of the Netherlands (SyRI case), ECLI:NL:RBDHA:2020:865, 5 February 2020.
13. Royal Commission into the Robodebt Scheme. Report, 2023. (URL: https://www.royalcommission.gov.au/robodebt/report)
14. Lyon D. The Culture of Surveillance: Watching as a Way of Life. — Cambridge: Polity Press, 2018. — 248 p.
15. Bradford A. The Brussels Effect: How the European Union Rules the World. — New York: Oxford University Press, 2020. — 424 p.
16. O'Neil C. Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy. — New York: Crown Publishing Group, 2016. — 288 p.
18. ProPublica. Machine Bias: There's Software Used Across the Country to Predict Future Criminals. — 23.05.2016. (URL: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing)
19. The Guardian. Edward Snowden NSA files: secret surveillance and our revelations so far. — 21.08.2013. (URL: https://www.theguardian.com/world/2013/aug/21/edward-snowden-nsa-files-revelations)
20. UNESCO. Recommendation on the Ethics of Artificial Intelligence, adopted 23 November 2021. — Paris: UNESCO, 2021.
21. OECD. Recommendation of the Council on Artificial Intelligence (OECD/LEGAL/0449), 2019.
22. The Tribune India. Rs 500, 10 minutes, and you have access to billion Aadhaar details. — 03.01.2018.