

Научная статья
УДК 340.004.8

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ТЕХНОЛОГИЙ РАСПОЗНАВАНИЯ ЛИЦ: ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ

Людмила Александровна Киселева¹, Александр Сергеевич Шайдуров²

^{1,2} Уральский государственный лесотехнический университет,
Екатеринбург, Россия

¹ kisevala@m.usfeu.ru

² shaydurov-01@mail.ru

Аннотация. Авторы обращаются к проблемам, связанным с внедрением технологий распознавания лиц. Дается анализ преимуществ и недостатков данных технологий с точки зрения правового регулирования. На основе анализа действующего российского законодательства и международного опыта предложены пути решения проблем.

Ключевые слова: технологии распознавания лиц, правовое регулирование, права человека, общественный контроль, персональные данные

Для цитирования: Киселева Л. А., Шайдуров А. С. Правовое регулирование технологий распознавания лиц: проблемы и перспективы // Эффективный ответ на современные вызовы с учетом взаимодействия человека и природы, человека и технологий = Effective reaction to modern challenges of the interaction between human and nature, human and technologies : материалы XVI Международной научно-технической конференции. Екатеринбург : УГЛТУ, 2025. С. 640–646.

Original article

LEGAL REGULATION FACE RECOGNITION TECHNOLOGIES: PROBLEMS AND PROSPECTS

Lyudmila A. Kiseleva¹, Alexander S. Shaidurov²

^{1,2} Ural State Forest Engineering University, Ekaterinburg, Russia

¹ kisevala@m.usfeu.ru

² shaydurov-01@mail.ru

Abstract. The authors address the problems associated with the introduction of facial recognition technologies. The advantages and disadvantages of these technologies are analyzed from the point of view of legal regulation. Based on the

analysis of current Russian legislation and international experience, ways to solve problems are proposed.

Keywords: face recognition technologies, legal regulation, human rights, public control, personal data

For citation: Kiseleva L. A., Shaidurov A. S. (2025) Pravovoe regulirovanie texnologij raspoznavaniya lic: problemy i perspektivy [Legal regulation face recognition technologies: problems and prospects]. Effektivnyi otvet na sovremennye vyzovy s uchetom vzaimodeistviya cheloveka i prirody, cheloveka i tekhnologii [Effective reaction to modern challenges of the interaction between human and nature, human and technologies] : proceedings of the XVI International Scientific and Technical Conference. Ekaterinburg : USFEU, 2025. P. 640–646. (In Russ).

Технологии распознавания лиц (далее – ТРЛ) находят применение в самых разных сферах: от обеспечения безопасности до персонализации услуг. Однако широкое распространение таких технологий порождает серьезные опасения относительно соблюдения права на неприкосновенность частной жизни, гарантированного Конституцией РФ [1]. Массовый сбор и анализ биометрических данных граждан без должного правового регулирования создает риски нарушения конституционных прав.

В условиях активного внедрения технологий распознавания лиц в России необходимо найти баланс между потенциалом технологии и правами человека и разработать эффективные правовые и этические механизмы, которые обеспечат ответственное использование данных технологий в соответствии с принципами демократического общества.

Надо отметить, что технологии распознавания лиц обладают значительным потенциалом. Во-первых, способствуют повышению уровня безопасности, помогая правоохранительным органам в борьбе с преступностью, при раскрытии преступлений, розыске преступников и пропавших без вести, в предотвращении терактов. Так, по данным МВД России, в 2021 г. в Москве с помощью систем распознавания лиц было раскрыто 6,8 тыс. преступлений [2].

Во-вторых, они способны упростить и ускорить процессы идентификации личности, что актуально для таких сфер, как транспортная безопасность (аэропорты, вокзалы), банковская сфера, система доступа к различным объектам. Например, Сбербанк с 2018 г. активно внедряет технологии распознавания лиц для идентификации клиентов в отделениях и мобильном приложении [3].

В-третьих, технологии открывают новые возможности для развития инновационных технологий и сервисов в различных отраслях экономики: от персонализированной рекламы и услуг до совершенствования систем здравоохранения и образования.

Однако наряду с преимуществами технологии распознавания лиц несут в себе и ряд существенных рисков.

Без должного правового регулирования и общественного контроля внедрение технологий может привести к нарушению прав и свобод граждан, в первую очередь, к нарушению права на неприкосновенность частной жизни. Массовый сбор биометрических данных без согласия граждан, создание баз данных, содержащих информацию о миллионах людей, отсутствие прозрачности в использовании ТРЛ – все это создает риски для неправомерного использования этих данных. Правозащитники выражают обеспокоенность относительно того, что недостаточный контроль за системами распознавания лиц может привести к нарушению прав человека [4].

Кроме того, особую опасность представляет возможность ошибок в работе алгоритмов распознавания лиц, что может привести к негативным последствиям для невинных людей. Исследования показывают, что точность алгоритмов технологий распознавания лиц может варьироваться в зависимости от расы, пола, возраста и других факторов, что создает риск дискриминации [5].

Конституция Российской Федерации гарантирует право на неприкосновенность частной жизни (статья 23) и защиту персональных данных (статья 24) [1], однако нормы, регулирующие непосредственно использование технологий распознавания лиц, в российском законодательстве отсутствуют.

В настоящее время использование указанных технологий регламентируется отдельными положениями ряда законов, в частности, Федерального закона «О персональных данных» от 27.07.2006 № 152-ФЗ [6], Федерального закона «Об оперативно-розыскной деятельности» от 12.08.1995 № 144-ФЗ [7], Федерального закона «О полиции» от 07.02.2011 № 3-ФЗ [8], а также подзаконных нормативно-правовых актов. Так, согласно статье 6 Федерального закона «Об оперативно-розыскной деятельности», использование ТРЛ в рамках оперативно-розыскной деятельности допускается только на основании судебного решения [7].

Однако в отношении использования технологий распознавания лиц в других сферах, например, для безопасности в общественных местах или в коммерческих целях, четких правовых норм не существует, что создает лазейки для злоупотреблений.

Можно выделить следующие пробелы в законодательстве:

1. Недостаточно четко определены цели, для достижения которых допустимо использование технологий распознавания лиц;
2. Не регламентированы условия и порядок сбора, обработки и хранения биометрических данных граждан;
3. Не установлены гарантии прав человека и гражданина при незаконном использовании данных технологий [9].

Для того, чтобы технологии распознавания лиц не нарушали прав и свобод человека, необходим комплекс мер, направленных на обеспечение их сбалансированного и этичного использования в России.

На основе анализа действующего российского законодательства и международного опыта предлагаем следующие пути решения проблем:

1. Совершенствование законодательства.

Необходимо разработать и принять специальный закон, регулирующий использование технологии распознавания лиц, в котором должны быть четко определены:

- цели, для достижения которых допустимо использование ТРЛ;
- условия и порядок сбора, обработки, хранения и использования биометрических данных;
- права и обязанности операторов систем ТРЛ;
- порядок получения согласия граждан на сбор и обработку их биометрических данных;
- ответственность должностных лиц за нарушение законодательства в сфере ТРЛ.

При этом важно привести российское законодательство в соответствие с международными стандартами в области прав человека, приняв во внимание Общие рекомендации № 31 Комитета министров Совета Европы государствам-членам о защите данных при использовании биометрических данных правоохранительными органами [10].

2. Внедрение технических решений.

Необходимо стимулировать разработку и внедрение более точных и непредвзятых алгоритмов распознавания лиц, которые минимизируют риски ошибок и дискриминацию. Одним из подходов к решению этой проблемы является Federated Learning, который позволяет обучать алгоритмы на распределенных наборах данных без необходимости их централизованного хранения [11].

Важным направлением работы является также разработка и внедрение систем анонимизации и шифрования биометрических данных, чтобы их невозможно было использовать для идентификации конкретного человека без его согласия. Например, технология дифференциальной приватности позволяет добавлять в данные небольшой объем шума, что делает невозможной идентификацию отдельных людей, но при этом сохраняет возможность использования данных для статистического анализа [12].

3. Общественный контроль и повышение осведомленности граждан.

Необходимо обеспечить прозрачность в использовании технологий распознавания лиц со стороны государственных органов и частных компаний. Граждане имеют право знать, где, как и с какой целью используются их биометрические данные. Важно повышать уровень осведомленности

населения о данных технологиях, их преимуществах и рисках, а также о правах граждан в этой сфере.

Необходимо развитие механизмов общественного контроля за использованием технологий распознавания лиц, в том числе с участием институтов гражданского общества и правозащитных организаций.

Подводя итоги, можно сказать, что технологии распознавания лиц обладают огромным потенциалом, но их внедрение в России требует взвешенного подхода. Необходимо устранить пробелы в правовом регулировании и стимулировать разработку и внедрение более точных и непредвзятых алгоритмов распознавания лиц, которые сведут к минимуму ошибки и дискриминацию.

Список источников

1. Конституция Российской Федерации (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ, от 04.03.2020 № 1-ФКЗ) // Собрание законодательства РФ : [сайт]. 2014. № 31. URL: <http://szrf.pravo.gov.ru/list.html#editions=e100&divid=100000&volume=1002014031000> (дата обращения: 13.08.2024).

2. В Москве камеры с распознаванием лиц помогли раскрыть более 6,8 тыс. преступлений за 2021 г. ТАСС : [сайт]. 2022. URL: <https://tass.ru/obschestvo/13552205> (дата обращения: 23.08.2024).

3. Сбербанк начал использовать биометрию для выдачи кредитов // T Adviser : [сайт]. URL: [https://www.tadviser.ru/index.php/Проект:Сбербанк_РФ_\(система_идентификации_клиентов\)](https://www.tadviser.ru/index.php/Проект:Сбербанк_РФ_(система_идентификации_клиентов)) (дата обращения: 28.08.2024).

4. Как работает распознавание лиц и можно ли обмануть эту систему // РБК Тренды : [сайт]. 2021. URL: https://trends.rbc.ru/trends/industry/6050ac809a794712e5ef39b7#card_6050ac809a794712e5ef39b7_6 (дата обращения: 25.09.2024).

5. Buolamwini J., Gebru T. Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification // Proceedings of Machine Learning Research. 2018. Vol. 81. P. 77–91.

6. О персональных данных : Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 14.07.2022) // Собрание законодательства РФ : [сайт]. 2006. № 31. Ч. 1. Ст. 3451. URL: <http://szrf.pravo.gov.ru/list.html#editions=e100&divid=100000&volume=1002006031000&page=1&sort=position&limit=50&nd=107&volid=1002006031000> (дата обращения: 25.09.2024).

7. Об оперативно-розыскной деятельности : Федеральный закон от 12.08.1995 № 144-ФЗ (ред. от 11.06.2022) // Собрание законодательства РФ : [сайт]. 1995. № 33. Ст. 3349. URL: <http://szrf.pravo.gov.ru/list.html#editions=>

e100&divid=100000&volume=1001995033000&page=1&sort=position&limit=50&nd=106&volid=1001995033000 (дата обращения: 29.09.2024).

8. О полиции : Федеральный закон от 07.02.2011 № 3-ФЗ (ред. от 14.07.2022) // Собрание законодательства РФ : [сайт]. 2011. № 7. Ст. 900. URL: <http://szrf.pravo.gov.ru/list.html#editions=e100&divid=100000&volume=1002011007000&page=1&sort=position&limit=50&nd=3&volid=1002011007000> (дата обращения: 29.09.2024).

9. Этические аспекты искусственного интеллекта // UNESCO : [сайт]. URL: <https://www.unesco.org/ru/artificial-intelligence/recommendation-ethics> (дата обращения: 03.09.2024).

10. Защита персональных данных: Комитет министров обновил рекомендацию, касающуюся профилирования // Совет Европы : [сайт]. URL: <https://www.coe.int/ru/web/portal/-/data-protection-committee-of-ministers-updates-recommendation-on-profiling> (дата обращения: 20.08.2024).

11. Advances and open problems in federated learning / P. Kairouz, H. B. McMahan, B. Avent [et al.] // Foundations and Trends in Machine Learning. 2021. Vol. 14. Issue 1–2. P. 1–210.

12. Dwork C., Roth A. The algorithmic foundations of differential privacy. Foundations and Trends in Theoretical Computer Science. 2013. Vol. 9. Issue 3–4. P. 211–407.

References

1. The Constitution of the Russian Federation (subject to amendments made by the Laws of the Russian Federation on Amendments to the Constitution of the Russian Federation dated 30.12.2008 № 6-FKZ, dated 30.12.2008 № 7-FKZ, dated 05.02.2014 № 2-FKZ, dated 21.07.2014 № 11-FKZ, dated 04.03.2020 № 1-FKZ) // Collection of Legislation of the Russian Federation : [website]. 2014. № 31. URL: <http://szrf.pravo.gov.ru/list.html#editions=e100&divid=100000&volume=1002014031000> (accessed: 13.08.2024).

2. In Moscow, face recognition cameras helped to solve more than 6.8 thousand crimes in 2021. TASS : [website]. 2022. URL: <https://tass.ru/obschestvo/13552205> (accessed: 23.08.2024).

3. Sberbank has started using biometrics to receive reports [Electronic resource] // Tadviser : [website]. URL: [https://www.tadviser.ru/index.php/Проект:Сбербанк_РФ_\(система_идентификации_клиентов\)](https://www.tadviser.ru/index.php/Проект:Сбербанк_РФ_(система_идентификации_клиентов)) (accessed: 28.08.2024).

4. How does facial recognition work and is it possible to deceive this system // RBC Trends : [website]. 2021. URL: https://trends.rbc.ru/trends/industry/6050ac809a794712e5ef39b7#card_6050ac809a794712e5ef39b7_6 (accessed: 25.09.2024).

5. Buolamvini J., Gebu T. Gender shades: differences in the accuracy of intersections in commercial gender classification // Proceedings of research in the

field of machine learning. 2018. Vol. 81. P. 77–91. URL: <http://proceedings.mlr.press/v81/buolamwini18a.html> (accessed: 13.08.2024).

6. On Personal data : Federal Law № 152-FL of 27.07.2006 (as amended on 14.07.2022) // Collection of Legislation of the Russian Federation : [website]. 2006. № 31. P. 1. Art. 3451. URL: <http://szrf.pravo.gov.ru/list.html#editions=e100&divid=100000&volume=1002006031000&page=1&sort=position&limit=50&nd=107&volid=1002006031000> (accessed: 25.09.2024).

7. On Administrative and Executive activities : Federal Law № 144-FL dated 12.08.1995 (as amended on 11.06.2022) // Collection of Legislation of the Russian Federation : [website]. 1995. № 33. Art. 3349. URL: <http://szrf.pravo.gov.ru/list.html#editions=e100&divid=100000&volume=1001995033000&page=1&sort=position&limit=50&nd=106&volid=1001995033000> (accessed: 29.09.2024).

8. On Police : Federal Law № 3-FL dated 17.02.2011 (as amended on 14.07.2022) // Collection of Legislation of the Russian Federation : [website]. 2011. № 7. Art. 900. URL: <http://szrf.pravo.gov.ru/list.html#editions=e100&divid=100000&volume=1002011007000&page=1&sort=position&limit=50&nd=3&volid=1002011007000> (accessed: 29.09.2024).

9. Ethical aspects of artificial intelligence // UNESCO : [website]. URL: <https://www.unesco.org/ru/artificial-intelligence/recommendation-ethics> (accessed: 03.09.2024).

10. Data protection: Committee of Ministers updates recommendation on profiling // The Council of Europe : [website]. URL: <https://www.coe.int/ru/web/portal/-/data-protection-committee-of-ministers-updates-recommendation-on-profiling> (accessed: 20.08.2024).

11. Advances and open problems in federated learning / P. Kairouz, H. B. McMahan, B. Avent [et al.] // Foundations and Trends in Machine Learning. 2021. Vol. 14. Issue 1–2. P. 1–210.

12. Dwork C., Roth A. The algorithmic foundations of differential privacy. Foundations and Trends in Theoretical Computer Science. 2013. Vol. 9. Issue 3–4. P. 211–407.