Научная статья
УДК 34:342.721:004:004.8
EDN: https://elibrary.ru/drgddj
DOI: https://doi.org/10.21202/jdtl.2023.36

Технология распознавания лиц и обеспечение безопасности биометрических данных: компаративный анализ моделей правового регулирования

Дана Утеген ✉

Университет КАЗГЮУ имени М. С. Нарикбаева
г. Астана, Республика Казахстан

Бауржан Жанатович Рахметов

Университет КАЗГЮУ имени М. С. Нарикбаева
г. Астана, Республика Казахстан

Ключевые слова

Безопасность,
биометрическая аутентификация,
биометрические данные,
идентификация,
неприкосновенность частной жизни,
персональные данные,
право,
правовое регулирование,
технологии распознавания лиц,
цифровые технологии

Аннотация

Цель: выявление моделей правового регулирования в сфере биометрической идентификации и аутентификации технологией распознавания физических лиц для выработки рекомендаций по повышению информационной безопасности человека и государственно-правовой охраны его права на неприкосновенность частной жизни.

Методы: рискориентированный подход в праве и такие специально-юридические методы познания, как методы сравнительно-правового анализа и юридического прогнозирования, имеют для исследуемой проблематики определяющее значение и позволяют сопоставить применяемые в зарубежных странах и их объединениях модели правового регулирования в сфере биометрической идентификации и аутентификации системами распознавания физических лиц, спрогнозировать возможные риски для безопасности биометрических данных с учетом перспективы дальнейшего распространения современной технологии распознавания лиц, сформулировать рекомендации по правовой охране биометрических данных.

✉ Контактное лицо

Результаты: предложены пути дальнейшего совершенствования законодательства Республики Казахстан и иных стран, находящихся в процессе развития правового регулирования биометрических данных, в части определения допустимых критериев использования технологии распознавания лиц, разработки категоризации биометрических систем с высоким и низким уровнем риска (по примеру опыта регулирования искусственного интеллекта в Европейском союзе), необходимости введения системы запретов массовой и неизбирательной слежки за человеком с помощью систем видеонаблюдения и др.

Научная новизна: заключается в выявлении положительного зарубежного передового опыта по развитию правового регулирования в сфере распознавания физических лиц на основе биометрии (Европейский союз, Соединенные Штаты Америки, Соединенное Королевство Великобритании, Северная Ирландия), который может быть использован для дальнейшего совершенствования национального законодательства в целях создания наиболее эффективных механизмов правовой защиты персональных данных, включая биометрическую информацию.

Практическая значимость: основанное на рискориентированном подходе и компаративистском анализе исследование позволяет выработать меры по усилению правовой охраны биометрических данных, обеспечению эффективной защиты гражданских прав и свобод на неприкосновенность частной жизни на основе прогноза дальнейшего распространения современной технологии распознавания лиц.

Для цитирования

Утеген, Д., Рахметов, Б. Ж. (2023). Технология распознавания лиц и обеспечение безопасности биометрических данных: компаративный анализ моделей правового регулирования. *Journal of Digital Technologies and Law*, *1*(3), 825–844. https://doi.org/10.21202/jdtl.2023.36

Содержание

Введение

Большинство развитых государств вкладывают значительные финансовые средства для использования технологии распознавания лиц. Это технология, которая сравнивает и анализирует два или более изображений лиц, идентифицирует их при помощи биометрических данных и определяет, кому принадлежат данные на основе

имеющихся баз[1] (Gill, 1997). Биометрические данные, используемые для распознавания лица, хранятся в системе биометрической аутентификации (Sarabdeen, 2022). Система биометрической аутентификации – это информационная система, позволяющая идентифицировать человека на основе некоторых его основных физиологических и поведенческих характеристик[2]. К примерам биометрических признаков можно отнести отпечатки пальцев, лицо, радужную оболочку, отпечаток ладони, сетчатку, геометрию руки, голос, подпись и походку[3]. В ее основе содержатся аппаратные системы сбора данных, интегрирующие программные компоненты, позволяющие с помощью математических алгоритмов выполнять анализ данных и идентифицировать личность человека[4].

Рассматривая различные группы правовых отношений в правоприменительной и правоохранительной деятельности органов исполнительной власти, выбранных в данной работе для сравнительного анализа государств, в реализации которых применимы технологии распознавания лиц, следует выделить следующие объекты, отнесенные к уязвимым:

1) категория объекта, уязвимого в террористическом отношении;
2) особо важные государственные объекты;
3) стратегические объекты отраслей экономики, имеющих стратегическое значение;
4) опасные производственные объекты;
5) объекты массового скопления людей и др.

Наиболее часто технология распознавания лиц используется правоохранительными органами для идентификации подозреваемых в совершении преступлений лиц. Анализ и идентификация происходят путем получения фото, видеоизображений, водительских прав, видеозаписи с камер общественного наблюдения, изображения из социальных сетей и др.[5] Несмотря на то, что системы распознавания лиц применяются, в частности, для охраны правопорядка и обеспечения общественной безопасности, зачастую граждане находятся под наблюдением, даже не подозревая об этом, потому как уведомление о наблюдении отсутствует. Использование системы распознавания лиц силовыми структурами было отмечено критическими замечаниями и высказываниями о предвзятости, дискриминации и отсутствии прозрачности данных систем.

Международное сообщество в целом поддерживает инициативу по обеспечению безопасности при помощи цифровых технологий. Согласно Резолюции Совета Безопасности Организации Объединенных Наций (далее – ООН), государства-члены призывают активно предпринимать действия по противодействию угрозе терроризма

---

1 Все про технологию распознавания лиц. *Www.cloudav.ru*. https://www.cloudav.ru/mediacenter/technology/facial-recognition-technology/ ; TAdviser – портал выбора технологий и поставщиков. (2020). *TAdviser.ru*. https://www.tadviser.ru/index.php/

2 QUII. (2018). Biometric Recognition: definition, challenge and opportunities of biometric recognition systems. *IQUII*. https://medium.com/iquii/biometric-recognition-definition-challenge-and-opportunities-of-biometric-recognition-systems-d063c7b58209

3 Jain, A. (2008). Biometric authentication. *Scholarpedia*, *3*(6), 3716. https://doi.org/10.4249/scholarpedia.3716

4 *Там же*, *2*.

5 Резолюции Совета Безопасности OOHS/RES/2396(2017). https://www.un.org/securitycouncil/ru/content/sres23962017

и мер в области предупреждения преступности[6]. В связи с участившейся практикой, связанной с мошенничеством, фальсификацией и подделкой документов, удостоверяющих личность, рекомендации органа ООН, отвечающего за обеспечение международного мира и безопасности, государствам касались внедрения систем биометрической идентификации данных в целях наблюдения за террористами или лицами, подозреваемыми в террористической деятельности[7].

Помимо целей обеспечения безопасности, следует также отметить влияние пандемии COVID-19, поспособствовавшей ускорению применения систем распознавания лиц в борьбе с распространением инфекции и контроля за перемещением граждан в период карантинных ограничений. Алгоритмы систем распознавания лиц применялись для контроля за перемещением граждан, ношением масок, измерения температуры тела в целях управления мерами обеспечения общественного здравоохранения (Chen & Wang, 2023; Johnson et al., 2022; Shore, 2022).

В этой связи представляет интерес опыт правового регулирования стран, которые на данном этапе активно применяют систему биометрических баз данных, нацеленную на упрощение процедур уголовного расследования и контроля за перемещением на границах.

1. Соединенные Штаты Америки: внедрение и регулирование технологии распознавания лиц

На примере Соединенных Штатов Америки стоит сразу отметить практику использования камер с функцией распознавания лиц в контексте контртеррористических мер после событий 11 сентября 2001 г. На основании принятого Конгрессом США Закона о защите государственных границ были внедрены биометрические удостоверения личности[8]. С 2004 г. в стране была введена система снятия отпечатков пальцев и включения в базу изображения лиц, прибывающих в Америку. Проверка биометрических данных лиц по государственным базам данных направлена на выявление подозреваемых в терроризме лиц, разыскиваемых преступников или нарушивших ранее иммиграционное законодательство США. Таким образом, меньше чем за полгода была собрана биометрическая база данных более пяти миллионов человек. Кроме того, органы безопасности США приняли меры в отношении 3800 иностранцев на основании информации, полученной в ходе процесса биометрического скрининга при посещении США[9]. Меры были связаны с задержанием подозреваемых лиц на основании ордера об аресте, отказе в приеме на границе либо возвращении в страну последнего пребывания.

---

6 *Там же*.

7 Резолюция 2396 (2017), принятая Советом Безопасности на его 8148-м заседании 21 декабря 2017 года. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N17/460/27/PDF/N1746027.pdf?OpenElement

8 Markey, E. J. (2021, June 15). Text: S.2052 – 117th Congress (2021–2022): Facial Recognition and Biometric Technology Moratorium Act of 2021. https://www.congress.gov/bill/117th-congress/senate-bill/2052/text

9 Federal Register, Vol. 73, Iss. 245. (2008, December 19). https://www.govinfo.gov/content/pkg/FR-2008-12-19/html/E8-30095.htm

Однако трагические события, связанные с террористическим актом 2001 г., не повлияли не возникновение, а лишь способствовали развитию уже существовавшей ранее системы идентификации по отпечаткам пальцев.

В США и других развитых странах в 1960–1970-х гг. системы распознавания лиц и анализа выражения лица начали разрабатываться в исследовательских лабораториях, финансируемых Министерством обороны и разведывательными службами. В 1990 г. были созданы новые компании для коммерциализации технологии, которые искали рынки сбыта, в особенности среди учреждений, использующих собственные компьютерные сети, таких как финансовая индустрия, бизнес, крупномасштабные системы идентификации, паспортные службы, государственные департаменты, правоохранительные и пенитенциарные системы (Schweber, 2014). В 1999 г. Федеральное бюро расследований США разработало и внедрило автоматизированные системы идентификации отпечатков пальцев. Данная система объединяет записи отпечатков пальцев, собранных федеральными правоохранительными органами. Она предоставляет возможности автоматизированного поиска отпечатков пальцев, электронного хранения изображений и электронного обмена отпечатками пальцев. В 2008 г. данная система обрабатывала в среднем более 63 000 отпечатков пальцев в день, 91 % из которых сканируются в систему в цифровом виде, остальная часть может храниться на бумажном носителе[10].

За последние годы в практике США накопилось достаточное количество дел, связанных с рассмотрением процессов обработки, хранения и использования биометрических данных (Stepney, 2019). В этой связи наиболее важным представляются изучение и анализ отдельных решений для формирования данной категории проблемных вопросов с целью совершенствования законодательства Республики Казахстан.

В 2021 г. в США было рассмотрено дело Роберта Уильямса, чернокожего мужчины, который был арестован в 2020 г. за кражу часов из магазина в городе Детройт (штат Мичиган). Несмотря на то, что он не посещал данный магазин уже несколько лет, его задержали в присутствии двух его дочерей по подозрению в краже имущества. В случае Уильямса департамент полиции Детройта использовал технологию распознавания лиц, чтобы идентифицировать подозреваемого по изображению с камер наблюдения. Таким образом, была применена база данных изображений водительских прав департамента полиции штата Мичиган. Однако при идентификации произошла погрешность в идентификации лица, повлиявшая на последствия в виде задержания под стражей невиновного лица в течение 30 часов[11].

К сожалению, данный случай не является единственным – практика привлечения невиновных лиц участилась (Bowyer, 2004). В связи с применением технологии распознавания лиц было проведено исследование Национального института стандартов и технологий США[12]. Данное исследование выявило, что при идентификации

---

10 FIRS IAFIS (Federal Bureau of Investigation). https://www.fbi.gov/how-we-can-help-you/need-an-fbi-service-or-more-information/freedom-of-informationprivacy-act/department-of-justice-fbi-privacy-impact-assessments/firs-iafis

11 Harwell, D. (2021, April 13). Wrongfully Arrested Man Sues Detroit Police over False Facial Recognition Match. *Washington Post*. https://www.washingtonpost.com/technology/2021/04/13/facial-recognition-false-arrest-lawsuit/

12 NIST (National Institute of Standards and Technology) (2000). https://www.nist.gov/

лица чаще всего происходит дискриминация по цвету кожи. Также технология распознавания лиц обширно применялась правоохранительными органами для идентификации лиц при проведении митингов и демонстраций, расследования мелких правонарушений и ареста людей без каких-либо доказательств вины (Buresh, 2021). В результате постоянно возрастает количество людей, которые стали жертвами нерегулируемой системы наблюдения и мониторинга[13].

В итоге после ряда последствий обнаружения погрешностей при идентификации лиц гражданским обществом США и международными неправительственными организациями были сформированы петиции с призывом к массовому запрету технологий биометрического распознавания, обеспечивающих массовое и дискриминационное наблюдение[14]. В некоторых штатах США был инициирован Мораторий по запрету применения технологии распознавания лиц. В последующем в США был предложен к принятию законопроект о распознавании лиц, ограничивающий применение данной технологии и ее неэтичного использования[15]. В данном документе содержится перечень ограничений по части применения технологии распознавания лиц. К таким ограничениям отнесены:

– иммиграционный контроль,
– мирные протесты,
– установление личности подозреваемого в совершении преступления.

Согласно законопроекту, правоохранительным органам выставлено требование по осуществлению тестирования системы распознавания лиц и предоставлению ежегодных отчетов об эффективности практики их применения. Одним из важных критериев является удаление из баз данных изображений несовершеннолетних лиц, оправданных или освобожденных без предъявления обвинений[16].

Несмотря на то, что большинство штатов инициировало внедрение и регулирование технологии распознавания лиц, следует отметить опыт штата Калифорния, который стал первым штатом в США, запретившим использование технологии распознавания лиц правоохранительными органами. В последующем практика Калифорнии повлияла на введение запрета на использование технологии распознавания лиц не только для правоохранительных органов, но и для частных организаций[17].

---

13 Rauenzahn, B., Chung, J., & Kaufman, A. (2021, March 20). Facing Bias in Facial Recognition Technology. *The Regulatory Review*. https://www.theregreview.org/2021/03/20/saturday-seminar-facing-bias-in-facial-recognition-technology/#:~:text=According%20to%20the%20researchers%2C%20facial

14 The Computer Got It Wrong: Why We're Taking the Detroit Police to Court over a Faulty Face Recognition "Match". (2021, April 13). *American Civil Liberties Union*. https://www.aclu.org/news/privacy-technology/the-computer-got-it-wrong-why-were-taking-the-detroit-police-to-court-over-a-faulty-face-recognition-match

15 Paul, K. (2019, May 15). San Francisco Is First US City to Ban Police Use of Facial Recognition Tech. *The Guardian*. https://www.theguardian.com/us-news/2019/may/14/san-francisco-facial-recognition-police-ban

16 Ban Biometric Surveillance. *Access Now*. https://www.accessnow.org/ban-biometric-surveillance/

17 California Law Enforcement Prohibited from Using Facial Recognition Technology in Body Cameras under Ting Bill Signed by the Governor. Assemblymember Phil Ting Representing the 19th California Assembly District. https://a19.asmdc.org/press-releases/20191008-california-law-enforcement-prohibited-using-facial-recognition-technology

На примере Калифорнии по применению ограничительных мер использования технологии распознавания лиц правоохранительными органами были включены основания по части предоставления ордера на обыск и требование по приведению достаточных доказательств совершения преступления. Кроме того, ограничительные меры правоохранительных органов касались использования технологии распознавания лиц во время протестов и митингов для идентификации участников в целях недопущения нарушений гражданских свобод и прав человека. Данный законопроект получил широкую поддержку со стороны международных неправительственных организаций по контролю за деятельностью правительства, групп по защите гражданских свобод, а также самих же представителей правоохранительных органов[18]. Особой поддержкой со стороны крупных компаний, таких как IBM, Amazon и Microsoft, стало решение о приостановлении продажи инструментов распознавания лиц правительствам[19].

В результате принятый закон о распознавании лиц запрещает, чтобы совпадение было единственным доказательством, устанавливающим достаточные основания для ареста, как наиболее адекватная мера защиты, предотвращающая ошибки в постановлении о привлечении к ответственности (Gates, 2002).

Также в штате Иллинойс был принят закон о регулировании систем распознавания лиц, к примеру Закон о приватности биометрической информации Иллинойса[20] (Zuo et al., 2019). В данном законе прописаны положения о запрете на обмен, передачу без согласия, торговлю или извлечение финансовой выгоды от продажи биометрических данных[21] (Hill et al., 2022).

На основании проведенного анализа в различных штатах США следует отметить некоторую фрагментарность подходов. Так как не все штаты ограничили применение камер с функцией распознавания лиц, большинство штатов приняли законы, регулирующие ограничение применения таких камер правоохранительными органами[22]. Не все граждане и иностранные граждане, проживающие на территории США, могут рассчитывать на безопасность в случаях погрешности при идентификации. Данный законопроект лишь обеспечивает базовую защиту для американцев, позволяя гражданскому обществу продвигать инициативы по ограничению бесконтрольного применения данных систем.

По мнению авторов законопроекта, сформированный подход по ограничению применения функции распознавания лиц и регулированию сбора и обработки данных

---

18 В США ограничат использование полицией систем распознавания лиц. (2022, September 30). *ForkLog*. https://forklog.com/news/v-ssha-ogranichat-ispolzovanie-politsiej-sistem-raspoznavaniya-lits

19 Муравьев, Д. (2020, June 19). Почему IT-компании отказались от технологии распознавания лиц и при чем тут протесты в Америке. *Теплица социальных технологий*. https://te-st.ru/2020/06/19/why-it-companies-against-facial-recognition/

20 740 ILCS 14/ Biometric Information Privacy Act. *Www.ilga.gov*. www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57

21 Приближается крайний срок подачи иска в многомиллионном урегулировании процесса со Snapchat. (2022, October 13). *Chicago24online*. https://chicago24online.com/news/priblizhaetsya-krajnij-srok-podachi-iska-v-mnogomillionnom-uregulirovanii-processa-so-snapchat/ ; Thornley v. Clearview AI, Inc., No. 20-3249 (7th Cir. 2021). *Justia Law*. https://law.justia.com/cases/federal/appellate-courts/ca7/20-3249/20-3249-2021-01-14.html

22 Face Off: Law Enforcement Use of Face Recognition Technology. (2018, February 23). *Electronic Frontier Foundation*. https://www.eff.org/wp/law-enforcement-use-face-recognition

позволит снизить вероятность злоупотребления мониторингом в дискриминационном характере, а также обеспечит меры по защите неприкосновенности частной жизни[23].

Тем самым следует сделать вывод, что технологии распознавания лиц и наблюдения допускают погрешности, способствуют дискриминации, в особенности в тех случаях, когда правоохранительные органы продолжают принимать решения об аресте и задержании лиц без дополнительных способов расследования преступлений (Givens et al., 2004). В случае принятия ограничительных мер система распознавания лиц будет использоваться лишь в необходимых и оправданных целях, а также ограничит широкие дискреционные полномочия правоохранительных органов (Nissenbaum, 2004). К тому же усилит право на возможность удаления информации о себе в случае оправдательного приговора. Инициатива законодателей по ограничению системы распознавания лиц также обусловлена защитой неприкосновенности частной жизни, недопущения предвзятости и дискриминации граждан по цвету кожи и расовой принадлежности.

2. Европейский союз: рискориентированный подход в правовом регулировании

Рассматривая практику Европейского союза (далее – ЕС), следует обратить внимание на принятие законодательства, ограничивающего использование систем распознания лиц в реальном времени. Кроме злоупотреблений со стороны правоохранительных органов в части задержания ряда граждан без явных на то оснований, выяснилось, что инструменты применения искусственного интеллекта и систем распознавания лиц могут быть использованы для слежки за мигрантами, религиозными группами или представителями меньшинств[24]. Выработанная позиция представителей европейского парламента ассоциирует методы слежки с опасностью для неприкосновенности частной жизни и гражданских свобод, а также способствующей проявлению предвзятости и дискриминационных технологий.

Предпосылками к принятию ограничительных мер стала обширная практика использования полицией технологии автоматического распознавания лиц для поиска людей в общественных местах. Технологии распознавания лиц, установленные на уличных камерах в целях обеспечения общественной безопасности, вызывали возмущения со стороны активистов, гражданского общества, которые в свою очередь требовали отчет о реальных фактах предотвращения преступлений при помощи установления наблюдения (Кутейников и др., 2022). В высказанных протестах правозащитным сообществом подчеркивались свобода слова и право на мирные собрания, которые являются важнейшими гражданскими свободами. Подчеркнуто, что использование правительством системы распознавания лиц препятствует выражению мнения, наносит ущерб целым сообществам и нарушает индивидуальные свободы[25].

---

23 Turner, N. L, & Chin, C. (2022, April 7). Police Surveillance and Facial Recognition: Why Data Privacy Is an Imperative for Communities of Color. *Brookings*. https://www.brookings.edu/research/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color/

24 Обзор решений ЕСПЧ за сентябрь 2018 года (2018, 14 сентября). Помощь для желающих обратиться в Европейский суд по правам человека в Страсбурге. https://european-court-help.ru/obzor-reshenii-espch-za-sentiabr-2018-goda/ ; Face off Report. (2018). *Big Brother Watch*. bigbrotherwatch.org.uk/campaigns/stop-facial-recognition/report/

25 Guariglia, Paige Collings, & Matthew. (2022, September 26). Ban Government Use of Face Recognition in the UK. *Electronic Frontier Foundation*. https://www.eff.org/deeplinks/2022/09/ban-government-use-face-recognition-uk

Примечательным делом, рассмотренным высоким судом в Кардиффе, был иск Эда Бриджеса при поддержке правозащитной организации Liberty. Бриджес заявил, что использование полицией технологии распознавания лиц во время его похода в магазин, а затем на мирной акции протеста против торговли оружием нарушает его право на неприкосновенность частной жизни и участие в мирных собраниях.

В постановлении высокого суда в Кардиффе было отмечено, что, несмотря на то, что система массового наблюдения нарушает права на частную жизнь тех, кого сканируют камеры наблюдения, судьи пришли к выводу, что, автоматизированное распознавание лиц несет в себе законные основания[26] (Бегишев, Хисамова, 2018).

В 2022 г. законодательные инициативы в Соединенном Королевстве Великобритании и Северной Ирландии (далее – Великобритания) об ограничении систем распознавания лиц были пересмотрены[27]. Согласно Акту о защите данных Великобритании от 2018 г., обозначено, что биометрические и медицинские данные являются чувствительными данными, соответственно, сбор или обработка этих данных должны осуществляться только после получения явного согласия[28]. Управление комиссара по информации Великобритании также выступило с уведомлением о проведении расследования в отношении тех организаций, которые внедряют системы распознавания лиц, несущих риск использования алгоритма анализа эмоций.

Технологии анализа эмоций обрабатывают такие данные, как отслеживание взгляда, анализ настроения, движения лица, анализ походки, сердцебиение, выражение лица[29] (Бегишев, Хисамова, 2018).

Анализ эмоций предполагает сбор, хранение и обработку целого ряда персональных данных, включая подсознательные поведенческие или эмоциональные реакции. Такое использование данных гораздо более рискованно, чем традиционные биометрические технологии, которые используются для идентификации лица (Sprokkereef, 2007).

Возникшие проблемы применения систем идентификации повлияли на проведение тщательного анализа правового регулирования биометрических систем аутентификации в Европейском союзе. В апреле 2021 г. Европейский орган по надзору за защитой данных, проанализировав текущие риски и опасения по части применения систем с функцией распознавания лиц, призвал запретить использование искусственного интеллекта для автоматического определения лиц в общественных местах. Аналогичным образом, в январе 2021 г. Совет Европы призвал к строгому регулированию технологий и отметил в своем новом руководстве, что технологии распознавания лиц должны быть запрещены, если они используются исключительно

---

26 Bowcott, O. (2019, September 4). Police Use of Facial Recognition Is Legal, Cardiff High Court Rules. *The Guardian*. https://www.theguardian.com/technology/2019/sep/04/police-use-of-facial-recognition-is-legal-cardiff-high-court-rules

27 Каминский, Б. (2022, 27 июля). В Британии потребовали запретить распознавание лиц в магазинах. *ForkLog*. https://forklog.com/news/v-britanii-potrebovali-zapretit-raspoznavanie-lits-v-magazinah

28 Data Protection Act. "Data Protection Act 2018. (2018). *Legislation.gov.uk*. https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

29 "Immature Biometric Technologies Could Be Discriminating against People" says ICO in Warning to Organisations. (2022, October 27). *Ico.org.uk*. https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/10/immature-biometric-technologies-could-be-discriminating-against-people-says-ico-in-warning-to-organisations/

для определения цвета кожи, религиозных или иных убеждений, пола, расового или этнического происхождения, возраста, состояния здоровья или социального статуса человека. Группы гражданских свобод также призвали ЕС запретить биометрическое наблюдение на основании несоответствия правам человека[30].

Европейская комиссия включила в Закон ЕС об искусственном интеллекте ограничения использования системы распознавания лиц в общественных местах и для частных компаний, тем не менее оставила возможность применения в исключительных целях для правоохранительных органов. Органы обеспечения безопасности могут использовать эту технологию в таких случаях, как поиск пропавших детей, предотвращение террористических атак или обнаружение вооруженных и опасных преступников.

Законопроект ЕС об искусственном интеллекте, представленный в апреле 2021 г., направлен на ограничение использования биометрических систем идентификации, включая технологию распознавания лиц. В рамках проекта предлагается ввести новые требования, регулирующие применение технологии в зависимости от критериев – «высокого риска» или «низкого риска»[31].

К системам высокого риска искусственного интеллекта будут отнесены:

– критически важные объекты, которые могут подвергнуть риску жизнь и здоровье граждан;

– биометрическая идентификация и категоризация физических лиц;

– образование и профессиональная подготовка (например, подсчет баллов на экзаменах);

– компоненты безопасности продукции (например, применение искусственного интеллекта в роботизированной хирургии);

– трудоустройство, управление персоналом и доступ к самозанятости (например, программное обеспечение для сортировки резюме при приеме на работу);

– доступ к основным частным и государственным услугам и льготам (система кредитования по баллам, ограничивающая граждан в возможности получить кредит);

– данные правоохранительных органов;

– данные миграционных и пограничных служб (проверка подлинности проездных документов);

– данные институтов отправления правосудия и демократических процессов (применение закона к конкретному набору доказательств)[32].

Системы высокого риска будут запрещены для использования без цели или должны будут соответствовать строгим правилам надзорных органов, также применяться в серьезных случаях обеспечения безопасности. Широкий спектр технологий распознавания лиц, используемых в правоохранительных целях, при пограничном контроле, в общественных местах, образовательных учреждениях, общественном транспорте, может быть разрешен только при условии оценки соответствия и соблюдения требований безопасности (Sprokkereef, 2007). Технологии

30 *Там же, 20*.

31 Каспарянц, Д. (2021, 7 октября). Стандартизация искусственного интеллекта в ЕС. *Научно-технический центр ФГУП "ГРЧЦ"*. https://rdc.grfc.ru/2021/10/ai-standards/

32 Europe fit for the Digital Age: Commission proposes new rules and actions for excellence and trust in Artificial Intelligence. (2021, April 21). *European Commission*. https://ec.europa.eu/commission/presscorner/detail/en/ip_21_1682

распознавания лиц, используемые по категории низкого риска, будут ограничены критериями прозрачности и требований к правилам хранения и обработки информации[33].

Вне зависимости от представленных проектов регулирования искусственного интеллекта в Европе до сих пор существуют серьезные опасения касательно применения такого рода категоризации и регулирования без надлежащего общественного контроля. Большинство из государств – участников ЕС все же выступают за более строгие правила, включая полный запрет на использование таких технологий. В частности, система удаленной биометрической идентификации и технология распознавания лиц отнесены к системам высокого риска (Firc, 2023). Одним из главных требований обозначен четкий запрет на применение в общественных местах в правоохранительных целях.

3. Республика Казахстан: на пути к регулированию биометрических данных

В Республике Казахстане отмечается тенденция к применению опыта зарубежных стран по биометрической аутентификации в различных сферах, таких как государственные, банковские, медицинские, правоохранительные, образовательные и др.

В действующее законодательство о защите персональных данных был внесен ряд поправок[34], включено определение биометрических данных, утверждены правила процессов обработки и хранения биометрических данных при оказании государственных услуг. В положениях данных правил указаны процессы обработки биометрических данных при оказании государственных услуг, сбор которых осуществляется на добровольной основе, и собранная информация может быть в любой момент удалена из базы данных по письменному заявлению субъекта данных[35].

В соответствии с Законом «О персональных данных и их защите», понятие биометрических данных определено в качестве категории персональных данных, которые характеризуют физиологические и биологические особенности субъекта, на основе которых можно установить его личность[36].

Понятие определяет принадлежность биометрических данных к персональным данным, а процесс идентификации биометрических данных квалифицируется как «биометрическая аутентификация». Согласно Закону об информатизации,

---

[33] Филипова, И. А. (2022). *Правовое регулирование искусственного интеллекта*: учебное пособие (2-е изд., обновл. и доп.). Нижний Новгород: Нижегородский госуниверситет. https://www.researchgate.net/publication/359194516_Legal_Regulation_of_Artificial_Intelligence/citation/download ; Madiega, T., & Mildebrath, H. (2021, September). *In-Depth Analysis*. https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_EN.pdf

[34] О персональных данных и их защите. *ИПС "Әділет"*. https://adilet.zan.kz/rus/docs/Z1300000094/z13094.htm

[35] Правила сбора, обработки и хранения биометрических данных физических лиц для их биометрической аутентификации при оказании государственных услуг. *ИПС "Әділет"*. https://adilet.zan.kz/rus/docs/V2000021547#z14

[36] *Там же*, 22.

биометрическая аутентификация определена как комплекс мер, идентифицирующих личность на основании физиологических и биологических неизменных признаков[37].

Кроме указанных определений, в Республике Казахстане принят Закон о дактилоскопической и геномной регистрации. Цели закона обусловлены требованиями по обязательному сбору отпечатков пальцев для создания единой базы биометрических данных. База отпечатков данных будет применяться при пограничном контроле, мерам по противодействию терроризму, раскрытию уголовных преступлений, обеспечению правопорядка и безопасности[38].

По части процессов обработки данных также в 2022 г. была разработана Программа развития национальной платежной системы в Республике Казахстан до 2025 г.[39] В данной программе предусмотрено введение биометрической аутентификации при платежных операциях, в рамках инициативы ее реализации указано, что она нацелена на повышение обеспечения безопасности персональных данных за счет внедрения механизма получения цифрового согласия со стороны субъектов на обработку данных. В результате субъект должен видеть процедуру своего обращения за получением государственной услуги, цели обращения и с возможностью предоставления или отзыва согласия на доступ к его данным[40].

Кроме процедур повсеместного применения биометрических данных, в Программе развития Алматы до 2025 и 2030 гг. заявлено об установке камер видеонаблюдения с функцией распознавания лиц[41]. На 2027 г. запланировано расширение систем видеонаблюдения путем установки камер на всех уязвимых в террористическом плане объектах и во дворах многоквартирных жилых комплексов[42]. Актуальность установки камер наблюдения возросла после массовых беспорядков, произошедших в январе 2022 г., когда в нескольких крупных городах Республики Казахстан, в особенности в Алматы, правоохранительные органы и безопасности не могли контролировать массовые беспорядки, мародерство и нарушения общественного порядка[43].

Инициативы по установке видеокамер с функцией распознавания лиц определены законопроектом о регулировании цифровых технологий, согласно которому были

---

37 Закон Республики Казахстан № 418-V от 24 ноября 2015 г. «Об информатизации» (с изменениями и дополнениями по состоянию на 03.09.2022). *Информационная система ПАРАГРАФ*. https://online.zakon.kz/document/?doc_id=33885902

38 Раисова, З. (2021, 6 января). Обязательная дактилоскопия казахстанцев: зачем она нужна и как это работает? *CABAR.asia*. https://cabar.asia/ru/zachem-vvoditsya-obyazatelnaya-daktiloskopiya-kazahstantsev

39 Об утверждении Национального плана развития Республики Казахстан до 2025 года и признании утратившими силу некоторых указов Президента Республики Казахстан: Указ Президента Республики Казахстан № 636 от 15 февраля 2018 г. *ИПС "Әділет"*. https://adilet.zan.kz/rus/docs/U1800000636

40 Об утверждении Программы создания Национальной платформы цифровой биометрической идентификации на 2021–2024 годы (2021). *Открытые НПА*. https://legalacts.egov.kz/npa/view?id=13895562

41 *Программа развития Алматы до 2030 г. социально ориентирована*. (2022, 28 июня). https://www.gov.kz/memleket/entities/almaty/press/news/details/394216?lang=ru

42 Алхабаев, Ш. (2022, 12 сентября). Систему распознавания лиц внедрят в Алматы. *Tengrinews.kz*. https://tengrinews.kz/kazakhstan_news/sistemu-raspoznavaniya-lits-vnedryat-v-almatyi-477602

43 Казахстан: жертвы январских протестов не находят правосудия. (2022, May 9). *Human Rights Watch*. https://www.hrw.org/ru/news/2022/05/09/kazakhstan-no-justice-january-protest-victims

внесены поправки и изменения в действующий Закон об информатизации[44]. В целях обеспечения национальной безопасности и общественного правопорядка планируется внедрение национальной системы видеомониторинга как совокупности программных и технических средств, осуществляющих сбор, обработку и хранение базы видеоизображений[45].

Между тем проанализированные документы и нормативные правовые акты, касающиеся защиты персональных данных в Республике Казахстан, на данный момент лишь частично соответствуют международным стандартам защиты прав человека. Кроме того, наличие законов не дает весомую гарантию их защиты. Отдельного внимания требуют правила сбора, обработки, хранения биометрических данных[46].

Применение камер с функцией распознавания лиц и сбор отпечатков пальцев граждан может допустить вмешательство в частную жизнь. Поэтому при правовом регулировании биометрических данных следует тщательно изучить международный опыт государств, которые уже реализуют практику сбора биометрических данных, во избежание рисков, связанных с утечкой персональных данных (Raissova & Mukhamejanova, 2021).

В работе правоохранительных органов, в процессе обработки биометрических данных рекомендуется придерживаться предложенных способов применения технологий распознавания лиц в правоприменительной и правоохранительной деятельности, исключающих или существенно снижающих возможность нарушения неприкосновенности частной жизни, прав и свобод человека:

Применение системы распознавания лиц должно быть соответствующим законной цели и оправданно необходимым.

Применение системы распознавания лиц должно иметь открытый и транспарентный характер, что включает отчетность перед гражданами в виде статистических данных, представление материалов о раскрытии преступлений при помощи технологии распознавания лиц.

Возможность для обращения в уполномоченные органы при наличии жалоб и обращений, а также получения интересующей информации.

Наличие четких правил, политики и процедур сохранности биометрических данных и процессов их обработки.

Соблюдение правил по минимизации сбора биометрических данных.

Ограничение доступа третьих лиц, не имеющих отношения к процессу обработки и наблюдения.

Соответствие требованиям законов и мерам безопасности для защиты от несанкционированного доступа и использования биометрических данных.

На регулярной основе проведение плановых и внеплановых проверок для обеспечения качества защиты биометрических данных и исключения от неправомерного использования, и предоставления доступа к ним.

---

44 О проекте Закона Республики Казахстан «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам регулирования цифровых технологий»: Постановление Правительства Республики Казахстан № 1001 от 28.12.2019. *ИПС "Әділет"*. https://adilet.zan.kz/rus/docs/P1900001001

45 Об утверждении Правил функционирования Национальной системы видеомониторинга. *ИПС "Әділет"*. https://adilet.zan.kz/rus/docs/V2000021693

46 Исследование возможных экономических, социальных и правовых последствий закона РК «О дактилоскопической и геномной регистрации». (2021, June 23). *Soros Kazakhstan Foundation*. www.soros.kz/ru/study-of-the-law-of-the-republic-of-kazakhstan-on-fingerprint-and-genomic-registration/

Выводы

В данном исследовании рассмотрен опыт применения технологий распознавания лиц и биометрической идентификации в качестве инструмента обеспечения безопасности. При помощи описания ограничений со стороны государств сформированы подходы к правовому регулированию рассматриваемой сферы, преимуществ и рисков их применения.

В целях недопущения любых нарушений неприкосновенности частной жизни, дискриминации, ограничений прав и свобод со стороны правительства или частных организаций необходимо на основе проанализированного опыта государств, реализовавших национальные проекты по регулированию биометрических данных, выявить гарантии и повышение степени государственно-правовой защиты. Анализ опыта государств продемонстрировал, что принятие соответствующих законов, регулирующих защиту биометрических данных, неизбежно, поскольку действующее законодательство недостаточно отвечает критериям безопасного использования технологии распознавания лиц правительственными и частными организациями.

По итогам проведенного анализа и изученного опыта зарубежных стран следует выделить следующие важные предложения для дальнейшего совершенствования законодательства в Республике Казахстан:

– дополнить действующее законодательство в части определения допустимых критериев использования технологии распознавания лиц;

– внести запрет массовой и неизбирательной слежки за человеком с помощью систем видеонаблюдения;

– запретить использование изображений граждан Республики Казахстан, взятых из общедоступных источников в целях пополнения баз биометрических данных;

– разработать категоризацию биометрических систем с высоким и низким уровнями риска на примере опыта регулирования искусственного интеллекта в Европейском союзе;

– установить запрет на использование системы биометрической идентификации в реальном времени любыми пользователями, кроме правоохранительных органов.

На основе изученного опыта ЕС и США указанные рекомендации могут быть приняты во внимание как в Республике Казахстан, так и в других государствах, находящихся на пути процесса развития и правового регулирования биометрических данных. При применении систем распознавания лиц на практике государственным органам следует способствовать соблюдению принципов прозрачности, законности и необходимости, а также сформировать политику обработки данных третьих лиц.

Список литературы

Бегишев, И. Р., Хисамова, З. И. (2018). Криминологические риски применения искусственного интеллекта. *Всероссийский криминологический журнал*, *12*(6), 767–775. https://doi.org/10.17150/2500-4255.2018.12(6).767-775

Кутейников, Д. Л., Ижаев, О. А., Зенин, С. С. (2022). Неприкосновенность частной жизни в условиях использования систем искусственного интеллекта для удаленной биометрической идентификации личности. *Lex Russica*, *75*(2), 121–131. https://doi.org/10.17803/1729-5920.2022.183.2.121-131

Bowyer, K. W. (2004). Face recognition technology: security versus privacy. *IEEE Technology and Society Magazine*, *23*(1), 9–19. https://doi.org/10.1109/mtas.2004.1273467

Buresh, D. L. (2021). Should Personal Information and Biometric Data Be Protected under a Comprehensive Federal Privacy Statute that Uses the California Consumer Privacy Act and the Illinois Biometric Information Privacy Act as Model Laws?. *Santa Clara High Technology Law Journal*, *38*(1). https://digitalcommons.law.scu.edu/chtlj/vol38/iss1/2

Chen, W., & Wang, M. (2023). Regulating the use of facial recognition technology across borders: A comparative case analysis of the European Union, the United States, and China. *Telecommunications Policy*, *47*(2), 102482. https://doi.org/10.1016/j.telpol.2022.102482

Firc, A., Malinka, K., & Hanáček, P. (2023). Deepfakes as a threat to a speaker and facial recognition: An overview of tools and attack vectors. *Heliyon*, *9*(4), e15090. https://doi.org/10.1016/j.heliyon.2023.e15090

Gates, K. A. (2002). Wanted Dead or Digitized: Facial Recognition Technology and Privacy. *Television & New Media*, *3*(2), 235–238. https://doi.org/10.1177/152747640200300217

Gill, P. (1997). Technostalgia: Making the future past perfect. *Camera Obscura: Feminism, Culture, and Media Studies*, *14*(1–2), 161–179. https://doi.org/10.1215/02705346-14-1-2_40-41-161

Givens, G., Beveridge, J. R., Draper, B. A., Grother, P., & Phillips, P. J. (2004). How features of the human face affect recognition: a statistical comparison of three face recognition algorithms. In *Proceedings of the 2004 IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, 2004. https://doi.org/10.1109/cvpr.2004.1315189

Hill, D., O'Connor, C. D., & Slane, A. (2022). Police use of facial recognition technology: The potential for engaging the public through co-constructed policy-making. *International Journal of Police Science & Management*, *24*(3), 325–335. https://doi.org/10.1177/14613557221089558

Johnson, Th. L., Johnson, N. N., McCurdy, D., & Olajide, M. M. (2022). Facial recognition systems in policing and racial disparities in arrests. *Government Information Quarterly*, *39*(4), 101753. https://doi.org/10.1016/j.giq.2022.101753

Jones, C. (2021). Law Enforcement Use of Facial Recognition: Bias, Disparate Impacts to People of Color, and the Need for Federal Legislation. *NCJL & Tech.*, *22*(4), 777. https://scholarship.law.unc.edu/ncjolt/vol22/iss4/6

Nissenbaum, H. (2004). Privacy as Contextual Integrity. *Washington Law Review*, *79*, 119. https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10

Raissova, G., & Mukhamejanova, D. (2021). Nondiscrimination Policy and Privacy Protection in Case of Genetic Passport for Soldiers. *South Asian Journal of Social Sciences and Humanities*, *2*(3), 140–150. https://doi.org/10.48165/sajssh.2021.2309

Ring T. (2016). Privacy in peril: is facial recognition going too far too fast?, *Biometric Technology Today*, *7–8*, 7–11. https://doi.org/10.1016/S0969-4765(16)30123-0

Sarabdeen, J. (2022, March 11). Protection of the rights of the individual when using facial recognition technology. *Heliyon*, *8*(3), e09086. https://doi.org/10.1016/j.heliyon.2022.e09086

Schweber, H. (2014). Lochner v. New York and the Challenge of Legal Historiography. *Law & Social Inquiry*, *39*(1), 242–274. https://doi.org/10.1111/lsi.12062

Shore, A. (2022). Talking about facial recognition technology: How framing and context influence privacy concerns and support for prohibitive policy. *Telematics and Informatics*, *70*, 101815. https://doi.org/10.1016/j.tele.2022.101815

Sprokkereef, A. (2007, August). Data Protection and the Use of Biometric Data in the EU. In *The Future of Identity in the Information Society* (pp. 277–284). Boston, MA: Springer. https://doi.org/10.1007/978-0-387-79026-8_19

Stepney, Ch. (2019). Actual Harm Means it is too Late: How Rosenbach v. Six Flags Demonstrates Effective Biometric Information Privacy Law. *Loyola of Los Angeles Entertainment Law Review*, *40*(1). https://digitalcommons.lmu.edu/elr/vol40/iss1/2

Zuo, K. J., Saun, T. J., & Forrest, C. R. (2019). Facial Recognition Technology: A Primer for Plastic Surgeons. *Plastic and Reconstructive Surgery*, *143*(6), 1298e–1306e. https://doi.org/10.1097/prs.0000000000005673

Сведения об авторах

Утеген Дана – заместитель директора, старший преподаватель Высшей школы права, Университет КАЗГЮУ имени М. С. Нарикбаева
Адрес: 010000, Республика Казахстан, г. Астана, Коргалжинское шоссе, 8
E-mail: d_utegen@kazguu.kz
ORCID ID: https://orcid.org/0000-0001-5296-7916

Рахметов Бауржан Жанатович – PhD в области политики и международных отношений, ассистент-профессор Международной школы экономики, Университет КАЗГЮУ имени М. С. Нарикбаева
Адрес: 010000, Республика Казахстан, г. Астана, Коргалжинское шоссе, 8
E-mail: b_rakhmetov@kazguu.kz
ORCID ID: https://orcid.org/0000-0003-3948-9977
Web of Science Researcher ID:
https://www.webofscience.com/wos/author/record/32537389
Google Scholar ID: https://scholar.google.com/citations?user=hanfRwoAAAAJ

Вклад авторов

Д. Утеген осуществляла составление черновика рукописи и его критический пересмотр с внесением ценных замечаний интеллектуального содержания; разработку дизайна методологии; проведение сравнительного анализа; сбор литературы; анализ законодательства Соединенных Штатов Америки и Республики Казахстан; подготовку и редактирование текста статьи; формулировку ключевых выводов, предложений и рекомендаций; оформление рукописи.
Б. Ж. Рахметов осуществлял формулирование идеи, исследовательских целей и задач; участие в научном дизайне; анализ и обобщение литературы; анализ законодательства Европейского союза и Республики Казахстан; интерпретацию частных результатов исследования; критический пересмотр и редактирование текста рукописи; интерпретацию общих результатов исследования; утверждение окончательного варианта статьи.

Конфликт интересов

Б. Ж. Рахметов является членом редакционной коллегии журнала, статья прошла рецензирование на общих основаниях.

Финансирование

Исследование не имело спонсорской поддержки.

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.19.61 Правовое регулирование информационной безопасности
Специальность ВАК: 5.1.2 / Публично-правовые (государственно-правовые) науки

История статьи

Дата поступления – 7 ноября 2022 г.
Дата одобрения после рецензирования – 23 апреля 2023 г.
Дата принятия к опубликованию – 15 августа 2023 г.
Дата онлайн-размещения – 20 августа 2023 г.

Research article
DOI: https://doi.org/10.21202/jdtl.2023.36

Facial Recognition Technology and Ensuring Security of Biometric Data: Comparative Analysis of Legal Regulation Models

Dana Utegen ✉

M. Narikbayev KAZGUU University
Astana, Republic of Kazakhstan

Baurzhan Zh. Rakhmetov

M. Narikbayev KAZGUU University
Astana, Republic of Kazakhstan

Keywords

Biometric authentication,
biometric data,
digital technologies,
facial recognition,
technologies,
identification,
law,
legal regulation,
personal data,
privacy,
security

Abstract

Objective: to specify the models of legal regulation in the sphere of biometric identification and authentication with facial recognition technology in order to elaborate recommendations for increasing information security of persons and state-legal protection of their right to privacy.

Methods: risk-oriented approach in law and specific legal methods of cognition, such as comparative-legal analysis and juridical forecasting, are significant for the studied topic and allow comparing the legal regulation models used in foreign countries and their unions in the sphere of biometric identification and authentication with facial recognition systems, forecasting the possible risks for the security of biometric data, taking into account the prospects of further dissemination of the modern facial recognition technology, and to shape recommendations on legal protection of biometric data.

✉ Corresponding author

Results: the ways are proposed to further improve legislation of the Republic of Kazakhstan and other countries currently developing the legal regulation of biometric data, regarding the admissible criteria for using the facial recognition technology, the elaboration of categorization of biometric systems with a high and low risk levels (by the example of the experience of artificial intelligence regulation in the European Union), and the necessity to introduce a system of prohibitions of mass and unselective surveillance of humans with video surveillance systems, etc.

Scientific novelty: consists in identifying a positive advanced foreign experience of developing legal regulation in the sphere of facial recognition based on biometry (European Union, the United States of America, the United Kingdom of Great Britain and Northern Ireland), which can be used for further improvement of the national legislation in order to create more effective mechanisms of legal protection of personal data, including biometric information.

Practical significance: based on risk-oriented approach and comparative analysis, the research allows elaborating measures for enhancing the legal protection of biometric data and ensuring effective protection of civil rights and freedoms by forecasting further expansion of the modern facial recognition technology.

For citation

Utegen, D., Rakhmetov, B. (2023). Facial Recognition Technology and Ensuring Security of Biometric Data: Comparative Analysis of Legal Regulation Models. *Journal of Digital Technologies and Law, 1*(3), 825–844. https://doi.org/10.21202/jdtl.2023.36

References

Begishev, I. R., & Khisamova, Z. I. (2018). Criminological risks of using artificial intelligence. *Russian Journal of Criminology*, *12*(6), 767–775. (In Russ.). https://doi.org/10.17150/2500-4255.2018.12(6).767-775

Bowyer, K. W. (2004). Face recognition technology: security versus privacy. *IEEE Technology and Society Magazine*, *23*(1), 9–19. https://doi.org/10.1109/mtas.2004.1273467

Buresh, D. L. (2021). Should Personal Information and Biometric Data Be Protected under a Comprehensive Federal Privacy Statute that Uses the California Consumer Privacy Act and the Illinois Biometric Information Privacy Act as Model Laws? *Santa Clara High Technology Law Journal*, *38*(1). https://digitalcommons.law.scu.edu/chtlj/vol38/iss1/2

Chen, W., & Wang, M. (2023). Regulating the use of facial recognition technology across borders: A comparative case analysis of the European Union, the United States, and China. *Telecommunications Policy*, *47*(2), 102482. https://doi.org/10.1016/j.telpol.2022.102482

Firc, A., Malinka, K., & Hanáček, P. (2023). Deepfakes as a threat to a speaker and facial recognition: An overview of tools and attack vectors. *Heliyon*, *9*(4), e15090. https://doi.org/10.1016/j.heliyon.2023.e15090

Gates, K. A. (2002). Wanted Dead or Digitized: Facial Recognition Technology and Privacy. *Television & New Media*, *3*(2), 235–238. https://doi.org/10.1177/152747640200300217

Gill, P. (1997). Technostalgia: Making the future past perfect. *Camera Obscura: Feminism, Culture, and Media Studies*, *14*(1–2), 161–179. https://doi.org/10.1215/02705346-14-1-2_40-41-161

Givens, G., Beveridge, J. R., Draper, B. A., Grother, P., & Phillips, P. J. (2004). How features of the human face affect recognition: a statistical comparison of three face recognition algorithms. In *Proceedings of the 2004 IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, 2004. https://doi.org/10.1109/cvpr.2004.1315189

Hill, D., O'Connor, C. D., & Slane, A. (2022). Police use of facial recognition technology: The potential for engaging the public through co-constructed policy-making. *International Journal of Police Science & Management*, *24*(3), 325–335. https://doi.org/10.1177/14613557221089558

Johnson, Th. L., Johnson, N. N., McCurdy, D., & Olajide, M. M. (2022).Facial recognition systems in policing and racial disparities in arrests. *Government Information Quarterly*, *39*(4), 101753. https://doi.org/10.1016/j.giq.2022.101753

Jones, C. (2021). Law Enforcement Use of Facial Recognition: Bias, Disparate Impacts to People of Color, and the Need for Federal Legislation. *NCJL & Tech.*, *22*(4), 777. https://scholarship.law.unc.edu/ncjolt/vol22/iss4/6

Kuteynikov, D. L., Izhaev, O. A., Lebedev, V. A., & Zenin, S. S. (2022). Privacy in the realm of Artificial Intelligence Systems Application for Remote Biometric Identification. *Lex Russica*, *75*(2), 121–131. (In Russ.). https://doi.org/10.17803/1729-5920.2022.183.2.121-131

Nissenbaum, H. (2004). Privacy as Contextual Integrity. *Washington Law Review*, *79*, 119. https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10

Raissova, G., & Mukhamejanova, D. (2021). Nondiscrimination Policy and Privacy Protection in Case of Genetic Passport for Soldiers. *South Asian Journal of Social Sciences and Humanities*, *2*(3), 140–150. https://doi.org/10.48165/sajssh.2021.2309

Ring T. (2016) Privacy in peril: is facial recognition going too far too fast?, *Biometric Technology Today*, *7–8*, 7–11. https://doi.org/10.1016/S0969-4765(16)30123-0

Sarabdeen, J. (2022, March 11). Protection of the rights of the individual when using facial recognition technology. *Heliyon*, *8*(3), e09086. https://doi.org/10.1016/j.heliyon.2022.e09086

Schweber, H. (2014). Lochner v. New York and the Challenge of Legal Historiography. *Law & Social Inquiry*, *39*(1), 242–274. https://doi.org/10.1111/lsi.12062

Shore, A. (2022). Talking about facial recognition technology: How framing and context influence privacy concerns and support for prohibitive policy. *Telematics and Informatics*, *70*, 101815. https://doi.org/10.1016/j.tele.2022.101815

Sprokkereef, A. (2007, August). Data Protection and the Use of Biometric Data in the EU. In *The Future of Identity in the Information Society* (pp. 277–284). Boston, MA: Springer. https://doi.org/10.1007/978-0-387-79026-8_19

Stepney, Ch. (2019). Actual Harm Means it is too Late: How Rosenbach v. Six Flags Demonstrates Effective Biometric Information Privacy Law. *Loyola of Los Angeles Entertainment Law Review*, *40*(1). https://digitalcommons.lmu.edu/elr/vol40/iss1/2

Zuo, K. J., Saun, T. J., & Forrest, C. R. (2019).Facial Recognition Technology: A Primer for Plastic Surgeons. *Plastic and Reconstructive Surgery*, *143*(6), 1298e–1306e. https://doi.org/10.1097/prs.0000000000005673

Authors information

Dana Utegen – Deputy Director, Senior Lecturer of KAZGUU Law School, KAZGUU University Astana
Address: 8 Korgalzhinskoye shosse, 010000 Astana, Republic of Kazakhstan
E-mail: d_utegen@kazguu.kz
ORCID ID: https://orcid.org/0000-0001-5296-7916

Baurzhan Zh. Rakhmetov – PhD in Politics and International Relations, Assistant Professor of International School of Economics, KAZGUU University Astana
Address: 8 Korgalzhinskoye shosse, 010000 Astana, Republic of Kazakhstan
E-mail: b_rakhmetov@kazguu.kz
ORCID ID: https://orcid.org/0000-0003-3948-9977
Web of Science Researcher ID:
https://www.webofscience.com/wos/author/record/32537389
Google Scholar ID: https://scholar.google.com/citations?user=hanfRwoAAAAJ

Authors' contributions

Dana Utegen made the manuscript draft and critically reviewed it, inserting valuable comments of intellectual contentя; developed the methodology design; performed comparative analysis; collected literature; analyzed legislation of the United States of America and the Republic of Kazakhstan; prepared and edited the manuscript; formulated the key conclusions, proposals and recommendations; formatted the manuscript.
Baurzhan Zh. Rakhmetov formulated the research idea, goals and tasks; participated in research design; analyzed and summarized literature; analyzed legislation of the European Union and the Republic of Kazakhstan; interpreted the specific research results; critically reviewed and edited the manuscript; interpreted the general research results; approved the final version of the article.

Conflict of interest

Rakhmetov B. Zh. is a member of the Editorial Board of the Journal; the article has been reviewed on general terms.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law
ASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – November 7, 2023
Date of approval – April 23, 2023
Date of acceptance – August 15, 2023
Date of online placement – August 20, 2023