УДК 342.7

ПРАВОВЫЕ ПРОБЛЕМЫ ИСПОЛЬЗОВАНИЯ ТЕХНОЛОГИЙ РАСПОЗНАВАНИЯ ЛИЦ

О. Н. Толочко

Белорусский государственный университет,
ул. Ленинградская 8, 220030, г. Минск, Беларусь, o.tolochko@mail.ru

Аннотация: Целью статьи является анализ и разрешение некоторых правовых проблем, возникающих в процессе использования государственными органами и коммерческими структурами технологий распознавания лиц. По мнению автора, зарубежный опыт использования таких технологий свидетельствует о довольно высоких рисках нарушения прав и законных интересов граждан, в связи с чем обоснована целесообразность совершенствования законодательства, регулирующего сбор, обработку и использование биометрических данных.

Ключевые слова: технологии распознавания лиц; биометрическая аутентификация; правовое регулирование; персональные данные; права и свободы граждан.

LEGAL ISSUES IN USING FACE RECOGNITION TECHNOLOGIES

O. N. Tolochko

Belarusian State University,
Leningradskaya st. 8, 220030, Minsk, Belarus, o.tolochko@mail.ru

Abstract: The purpose of the article is to analyze and resolve some legal problems that arise in the process of using facial recognition technologies by government agencies and commercial structures. According to the author, foreign experience in the use of such technologies indicates fairly high risks of violating the rights and legitimate interests of citizens, and therefore the expediency of improving legislation regulating the collection, processing and use of biometric data is justified.

Keywords: facial recognition technologies; biometric authentication; legal regulation; personal data; rights and freedoms of citizens.

Цифровая трансформация приносит с собой новые для правовой системы проблемы. Нейросети и другие IT-технологии, с одной стороны, открывают колоссальные технические возможности, но с другой – несут в себе серьёзные риски, прежде всего для прав и свобод человека. Ответы на возникающие вопросы нарабатываются международной практикой, однако

говорить о том, что человечество взяло под контроль новые цифровые технологии, по всей вероятности, пока преждевременно. К числу таких рисковых инструментом следует отнести цифровые технологии распознавания лиц.

Под технологиями распознавания лиц понимаются алгоритмы, которые могут сравнивать 2 или более изображений лиц, идентифицировать их при помощи биометрических данных и определять, кому принадлежат эти данные на основе имеющихся баз биометрических данных, хранящихся в особой системе (базе данных) биометрической аутентификации [1]. Система биометрической аутентификации – это информационная система, позволяющая идентифицировать человека на основе некоторых его основных физиологических и поведенческих характеристик, таких как отпечатки пальцев, лицо, радужная оболочка глаз, отпечаток ладони, сетчатка, геометрия руки, голос, подпись, походка [2].

Технологии распознавания лиц могут применяться различными субъектами, – например, правоохранительными органами для идентификации подозреваемых в совершении преступлений лиц. Однако порядок использования систем распознавания лиц должен быть тщательно регламентирован, поскольку в противном случае высок риск превышения полномочий таких органов и распространение наблюдения на неопределённо широкий круг лиц, что может нарушать право на частную жизнь и на защиту от незаконного вмешательства в неё. Использование технологий распознавания лиц часто подвергается критике со стороны правоведов и общественных деятелей в связи с предвзятостью, дискриминацией и отсутствием прозрачности самих технологий.

К настоящему времени накопилась довольно богатая зарубежная практика рассмотрения юридических дел, связанных с процессами обработки, хранения и использования биометрических данных [3]. Анализ и обобщение такой практики обусловили введение в ряде государств специальных ограничений на использование технологий биометрического распознавания, особенно тех, которые обеспечивают массовое наблюдение в общественных местах [4].

Так, в Калифорнии (США) в 2019 г. был введён мораторий на использование технологий распознавания лиц полицией посредством использования нательных камер. В последующем был введён аналогичный запрет и для частных компаний [5]. Кроме того, принятый закон требует, чтобы результат распознавания лиц не был единственным доказательством при решении вопроса об аресте лица, а подкреплялся также и другими доказательствами.

Закон о конфиденциальности биометрической информации штата Иллинойс (США) [6] запрещает обмен, передачу без согласия лица, торговлю

или извлечение финансовой выгоды от продажи биометрических данных. Ограничения, как указано в самом Законе, обусловлены защитой неприкосновенности частной жизни, недопущения предвзятости и дискриминации граждан по цвету кожи и расовой принадлежности.

Использование технологий распознавания лиц ограничивается также по законодательству Великобритании. Предпосылкой к принятию ограничительных мер стало использование полицией указанных технологий для идентификации и поиска людей в общественных местах, что, вероятно, не вполне сообразуется со свободой слова и правом на мирные собрания. Согласно Акту о защите данных 2018 г. [7], биометрические и медицинские данные являются чувствительными данными, поэтому их сбор и обработка должны осуществляться только после получения явного согласия лица. Также должно контролироваться использование технологий, анализирующих эмоции: взгляд, настроение, движение лица, походку, сердцебиение. Использование этих данных является гораздо более рискованным, нежели работа с традиционными биометрическими технологии распознавания лиц, поскольку системы распознавания эмоций в сравнении с ними гораздо менее точны.

Консультативный комитет, созданный в соответствии с положениями Конвенции Совета Европы о защите частных лиц в отношении автоматизированной обработки данных личного характера 1981 г. [8], в 2021 г. выступил с инициативой запрета технологий распознавания лиц, если они используются исключительно для определения цвета кожи, религиозных или иных убеждений, пола, расового или этнического происхождения, возраста, состояния здоровья или социального статуса человека [9].

Разработанный в Европейском Союзе Закон об искусственном интеллекте [10] также ограничивает использование технологий распознавания лиц в общественных местах и для частных компаний, однако оставляет возможность применения правоохранительными органами в исключительных целях (поиск пропавших детей, предотвращение террористических атак или обнаружение вооруженных и опасных преступников). Закон предполагает ограничение использования биометрических систем идентификации, включая технологию распознавания лиц. Закон пока не вступил в силу, это произойдёт не ранее 2026 года, однако большинство государств – участников ЕС в настоящее время выступает за ужесточение регулятивных норм, включая полный запрет на использование таких технологий, в особенности, в общественных местах.

Для Республики Беларусь использование технологий распознавания лиц является довольно новой сферой регулирования. Закон Республики Беларусь «О защите персональных данных» 7 мая 2021 г. № 99-З специальных ограничений на обработку биометрических данных органами правопорядка

не содержит. Действующее законодательство относит биометрические данные к категории «специальных персональных данных» и разрешает их обработку в случаях, если такие данные сделаны общедоступными действиями самого субъекта персональных данных; когда обработка является необходимой для выполнения обязанностей (полномочий), предусмотренных законодательными актами, и если законодательными актами прямо предусматривается обработка таких данных без согласия лица (ч. 2 ст. 8 Закона о защите персональных данных). Такая формулировка, как можно видеть, довольно широка и позволяет использование биометрических данных почти без ограничений. Норма части 3 ст. 8 Закона, согласно которой «обработка специальных персональных данных допускается лишь при условии принятия комплекса мер, направленных на предупреждение рисков, которые могут возникнуть при обработке таких персональных данных для прав и свобод субъектов персональных данных», вряд ли в полной мере может гарантировать защиту таких прав.

В связи с этим представляется целесообразным дополнить Закон о защите персональных данных особой нормой, регулирующей сбор, обработку, хранение и использование биометрических данных, а также использование камер видеонаблюдения с функцией распознавания лиц, с целью недопущения незаконного вмешательства в частную жизнь граждан. В ходе разработки законопроекта важно использовать опыт государств, реализующих сбор, обработку и использование биометрических данных, во избежание рисков, связанных с утечкой и неправомерным использованием таких данных. В практике правоохранительных органов, так же, как и в процессе обработки специальных персональных данных, необходимо исключать или существенно снижать возможность нарушения неприкосновенности частной жизни, прав и свобод граждан. Использование технологий распознавания лиц должно соответствовать строго определённым в Законе целям и иметь транспарентный характер, что включает в себя, в числе прочего, публикацию данных о раскрытии при помощи таких технологий конкретных преступлений.

Необходимо также дополнить действующее законодательство определением допустимых критериев использования технологии распознавания лиц; установить ограничения на массовое и неизбирательное применение систем видеонаблюдения, а также на использование изображений граждан, взятых из общедоступных источников, в целях пополнения баз биометрической аутентификации.

Целесообразно также предусмотреть возможность обращения гражданина в уполномоченные органы для получения интересующей информации о сборе, обработке и использовании его биометрических данных и обеспечить эффективный (лучше всего – судебный) порядок обжалования

незаконных действий должностных лиц. Государственным органам, использующим технологии распознавания лиц, следует неукоснительно соблюдать принципы законности, необходимости и транспарентности.

Такие меры, как представляется, будут способствовать совершенствованию защиты прав и законных интересов граждан, а также, в итоге, повышению доверия и согласия в обществе.

Библиографические ссылки

1. Sarabdeen, J. Protection of the rights of the individual when using facial recognition technology / J. Sarabdeen // Heliyon, 2022 Mar 11;8(3):e09086. URL: https://pubmed.ncbi.nlm.nih.gov/35309394/ (дата обращения 05.03.2024).

2. Biometric Recognition: definition, challenge and opportunities of biometric recognition systems // Medium. URL: https://medium.com/iquii/biometric-recognition-definition-challenge-and-opportunities-of-biometric-recognition-systems-d063c7b58209 (дата обращения 05.03.2024).

3. Stepney, Ch. Actual Harm Means it is too Late: How Rosenbach v. Six Flags Demonstrates Effective Biometric Information Privacy Law / Ch. Stepney // Loyola of Los Angeles Entertainment Law Review. – 2019. – Vol. 40(1). URL: https://digitalcommons.lmu.edu/elr/vol40/iss1/2/ (дата обращения 05.03.2024).

4. Benedict, T.J. The Computer Got It Wrong: Facial Recognition Technology and Establishing Probable Cause to Arrest // Wash. & Lee L. Rev. – 2022. – Vol.79. – Issue 2. – P. 849–898. URL: https://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?article=4773&context=wlulr (дата обращения 05.03.2024).

5. California bill to bans use of facial recognition videos on body cams // OECD.AI Policy Observer. – URL: https://oecd.ai/en/incidents/8279 (дата обращения 05.03.2024).

6. 740 ILCS 14 / Biometric Information Privacy Act // Illinois General Assembly . URL: https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57 (дата обращения 05.03.2024).

7. Data Protection Act 2018 // Legislation.gov.uk. URL: https://www.legislation.gov.uk/ukpga/2018/12/contents (дата обращения 05.03.2024).

8. Конвенция Совета Европы о защите частных лиц в отношении автоматизированной обработки данных личного характера 1981 г. // Совет Европы. URL: https://rm.coe.int/1680078c46 (дата обращения 05.03.2024).

9. Совет Европы призвал ограничить использование технологии распознавания лиц и запретить её бесконтрольное применение. URL: https://d-russia.ru/sovet-evropy-prizval-ogranichit-ispolzovanie-tehnologii-raspoznavanija-lic-i-zapretit-ejo-beskontrolnoe-primenenie.html (дата обращения 05.03.2024).

10. Artificial intelligence act. URL: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf (дата обращения 05.03.2024).