ВИЗУАЛЬНЫЕ ПЕРСОНАЛЬНЫЕ ДАННЫЕ И ИХ ЗАЩИТА

А. С. Русакович,
аспирант Белорусского государственного университета
М. С. Абламейко,
кандидат юридических наук, доцент,
доцент кафедры конституционного права юридического факультета,
Белорусский государственный университет

В условиях экспоненциального развития технологий в сфере цифровой трансформации общества человечество могут ожидать драматические изменения. Среди распространяемых новых технологий самыми сложными и многофункциональными являются технологии интеллектуального видеонаблюдения.

В Республике Беларусь процессы функционирования систем видеонаблюдения носят системный, централизованный характер, конечная цель которых создание в соответствии с Указом Президента Республики Беларусь от 25 мая 2017 года № 187 «О республиканской системе мониторинга общественной безопасности» системы мониторинга по единым техническим стандартам целью которой является повышение уровня общественной безопасности [3]. Она объединяет на одной платформе локальные системы видеонаблюдения, специальные детекторы, каналы связи, центр обработки данных, а также иные системы и информационные ресурсы. При этом, обработка и хранение информации в системе мониторинга осуществляются посредством программной платформы и аппаратного комплекса республиканского центра обработки данных.

Использование технологий видеонаблюдения может дать человеку огромные возможности, однако с ними же могут возникнуть риски и угрозы, когда технологические решения могут привести к глобальным негативным последствиям. Распознавание лиц можно использовать не только как инструмент для идентификации людей и отслеживания их местоположения, но и для получения информации об их социальной активности, например, о том, с кем и где они проводят время. При этом если у человека есть профиль в социальных сетях (база его снимков разного возраста), то точность распознавания повышается в разы. Ни один из изобретенных человечеством механизмов наблюдения не несет в себе такой опасности, как технология распознавания лиц. Это недостающий элемент уже опасной инфраструктуры наблюдения за людьми.

С целью ограничения неконтролируемого использования персональных данных о человеке и их защиты государства принимают специальные законы, решающие вопросы обработки персональных данных. В странах поразному решают вопрос защиты персональных данных. Некоторые подробно регулируют вопросы использования персональных данных любыми компаниями (Европейский союз, Российская Федерация и др.), другие закрепляют минимальный набор обязанностей и точечно решают вопросы защиты персональных данных [1].

Как показывает практика единого понятия персональных данных не закреплено — каждое государство раскрывает его значение самостоятельно. На международном уровне, например, персональные данные были определены в Конвенции Совета Европы о защите частных лиц в отношении автоматизированной обработки данных личного характера, согласно которой термин «данные личного характера» обозначает любую информацию, относящуюся к физическому лицу, идентифицированному или которое может быть идентифицировано [2]. Конвенция стала основой для развития законодательства членов Совета Европы, которые понимают «персональные данные» максимально широко. По состоянию на ноябрь 2021 года Республика Беларусь не является участником данной Конвенции.

В таких условиях наука должна содействовать оперативному исследованию юридических и технических проблем развития и использования систем искусственного интеллекта и предложить сбалансированные решения как содействующие распространению новых технологий, так и обеспечивающие их надежность и безопасность. Выгодное с экономической точки зрения вовлечение технологий искусственного интеллекта в общественные процессы не должно привести к ущемлению интересов граждан и обрушению морально-нравственных норм, сформированных человечеством.

1. Персональные данные. Правовые аспекты

Конституционные основы защиты персональных данных создают статьи 28 (гарантирует право на защиту гражданина от незаконного вмешательства в его личную жизнь, в том числе от посягательства на тайну его корреспонденции, телефонных и иных сообщении , на его честь и достоинство) и статья 34, часть 3 (пользование информацией может быть ограничено законодательством в целях защиты чести, достоинства, личной и семейной жизни граждан и полного осуществления ими своих прав) Конституции Республики Беларусь.

В Законе Республики Беларусь от 10 июля 2008 года № 455-З «Об информации, информатизации и защите информации» закреплено, что персональные данные – это основные и дополнительные персональные сведения о физическом лице, которые в соответствии с законодательными актами Республики Беларусь подлежат внесению в регистр населения, а также иная информация, позволяющая идентифицировать такое лицо [4]. Таким образом, Законом определены лишь базовые положения, направленные на создание механизма защиты персональных данных. Однако детальный порядок работы с персональными данными, их сбор, обработка, хранение законодательными актами не определен.

Положение о технической и криптографической защите информации в Республике Беларусь, утвержденное Указом Президента от 16 апреля 2013 года № 196 «О некоторых мерах по совершенствованию защиты информации» также охватывает персональные данные в контексте собственников (владельцев) информационных систем, которые осуществляют сбор, анализ и хранение информации о частной жизни физического лица, электронных документов и др.

Кроме этого, в ноябре вступает в силу Закон от 07 мая 2021 года № 99-З «О защите персональных данных», который вносит определенную ясность в данную сферу [5]. Так, он дает право субъекту персональных данных узнать, где находятся его данные. Для этого необходимо написать письменное заявление и занести его в соответствующие органы. Гражданин вправе знакомиться со своими персональными данными, требовать их изменений. Категории персональных данных и их правовой режим также определены в соответствии с нормативным правовым актом: какие из них могут быть общедоступными, а какие подлежат дополнительной защите (например, биометрия или сведения о судимости). Можно будет также требовать удаления своих данных, если их собрали или обработали без оснований или «они не являются необходимыми для заявленной цели их сбора» [1].

В данном Законе дается следующее определение: персональные данные – любая информация, относящаяся к идентифицированному физическому лицу или физическому лицу, которое может быть идентифицировано.

В свою очередь, физическое лицо, которое может быть идентифицировано, – физическое лицо, которое может быть прямо или косвенно определено, в частности через фамилию, собственное имя, отчество, дату рождения, идентификационный номер либо через один или несколько признаков, характерных для его физической, психологической, умственной, экономической,

культурной или социальной идентичности. Преимущество нового определения заключается в том, что оно четко описывает основные признаки персональных данных и позволяет относить к таким данным информацию, косвенно идентифицирующую субъектов персональных данных.

Законом определяются следующие виды персональных данных [5]:

– общедоступные персональные данные – персональные данные, распространенные самим субъектом персональных данных либо с его согласия или распространенные в соответствии с требованиями законодательных актов;

– специальные персональные данные – персональные данные, касающиеся расовой либо национальной принадлежности, политических взглядов, членства в профессиональных союзах, религиозных или других убеждений, здоровья или половой жизни, привлечения к административной или уголовной ответственности, а также биометрические и генетические персональные данные;

– генетические персональные данные – информация, относящаяся к наследуемым либо приобретенным генетическим характеристикам человека, которая содержит уникальные данные о его физиологии либо здоровье и может быть выявлена, в частности, при исследовании его биологического образца;

– биометрические персональные данные – информация, характеризующая физиологические и биологические особенности человека, которая используется для его уникальной идентификации (отпечатки пальцев рук, ладоней, радужная оболочка глаза, характеристики лица и его изображение и другое).

Таким образом, изображение человека и характеристики лица можно отнести к визуальным персональным данным.

2. Защита визуальных персональных данных. Технические аспекты

Применение систем видеонаблюдения возможно, как с идентификацией человека, так и без нее. В первом случае вопрос о вмешательстве в частную жизнь не возникает, так как происходит лишь общий мониторинг ситуации, поведения конкретного объекта, без использования метода распознавания лица и установления личности человека. Вместе с тем, все чаще при функционировании «умных городов» стоит вопрос именно о применении метода распознавания лиц, так при обеспечении общественной безопасности наряду с выявлением инцидента стоит вопрос определения лица виновного в произошедшем. Также, следует отметить, что во многих странах имеются базы

данных граждан, включающие цифровой фотопортрет и иные персональные данные.

Таким образом, при использовании систем видеонаблюдения с применением искусственного интеллекта возможным становится полная идентификация лица, включающая как основные, так и дополнительные персональные данные. С одной стороны, применение подобных систем действительно приводит к положительной динамике сокращения преступности, предотвращения крупных аварий, профилактике, раскрытия, пресечения преступлений, правонарушений, борьбе с терроризмом и незаконной миграцией и т.д., с другой стороны, далеко не каждое общество отдельно взятой страны готово к тотальному контролю со стороны государства и небезосновательно видит в этом посягательство на тайну частной жизни. В основном недовольство людей сконцентрировано на полной идентификации человека.

Распознавание изображений с учетом конфиденциальности подразумевает изменение определенного содержимого, например, лиц, в изображении или видеопотоке, чтобы сделать такое содержимое неузнаваемым.

У каждого человека уникальное строение лица. Специальное программное обеспечение может проанализировать его и сравнить с информацией в базе данных для последующей идентификации. Существуют системы, которые используют для анализа фотографии миллионов пользователей сети Интернет, в том числе из популярных социальных сетей, таких как Facebook, Instagram, Twitter и YouTube. Нынешний уровень развития алгоритмов уже не позволяет скрыться от распознавания человеку в очках и кепке, только если он будет постоянно смотреть вниз, тем самым скрывая лицо от камер [8].

Технологически системы иногда могут сильно отличаться в плане распознавания лиц, но все они имеют общие принципы работы. Для начала выделяется лицо человека, будь он один или находясь в толпе. Лицо лучше всего обнаруживается в тот момент, когда человек смотрит прямо в камеру, однако современные технологические достижения позволяют также распознавать лицо и в тех ситуациях, когда человек не смотрит прямо в нее. Затем фиксируется фотография лица и начинается ее анализ [7]. Большинство решений для распознавания лиц использует 2D-изображения вместо объемных 3D-изображений, поскольку они могут более просто сопоставлять 2D-фото с общедоступными фотографиями или фотографиями, имеющимися в базе данных.

Каждое лицо состоит из различимых узловых точек. Программы для распознавания лиц анализируют эти точки, такие как расстояние между глазами

или форма скул. После этого анализ лица превращается в математическую формулу. Черты лица преобразуются в цифровой код - отпечаток лица (faceprint) [9]. Далее код сравнивается с базой данных отпечатков лиц. В этой базе данных имеются фотографии с идентификаторами, которые можно сравнивать. Затем технология определяет соответствия полученных данных тому, что представлено в базе данных. Результатом этого становится идентификация человека с предоставлением дополнительной информации начиная с ФИО, места жительства, работы гражданина, его идентификационного или страховой номер, заканчивая данными о поведении, передвижении, взглядах, предпочтениях, убеждениях конкретного лица, его IP адресе, рекламном профиле.

Существует много работ как защитить лицо человека от нежелательного распознавания. В работе [9] представлен алгоритм защиты лиц путем деидентификации т.е. затемнения деталей лица с помощью цифровой модификации видеоизображений. Более сложные методы модификации требуют идентификации определенных лиц или контрольных точек на изображении. Анализ экспериментальных исследований показал, что предсказание модели распознавания лиц напрямую зависит от расположения таких точек лица на входном изображении. Кроме того, было обнаружено, что верхняя часть лица является более полезной для распознавания, чем нижняя. Тип модификации ограничен сложностью, точностью и скоростью доступных в настоящее время алгоритмов обработки изображений, а также качеством данных и деталей, необходимых для работы системы.

В статье [6] нами предложен подход, который позволяет защитить от несанкционированной идентификации любого человека с помощью технологии распознавания лиц путем добавления в исходное изображение лица комбинации пикселей (меток), которые воспринимаются алгоритмами машинного обучения как характерные для изображаемого объекта шаблоны и приводит к искажению распознавания. Оценка качества распознавания проводилась с помощью нейросетевого метода на уже измененных изображениях. Было выявлено что, если использовать замаскированные изображения для обучения метода распознавания лиц, то такие изображения приводят к появлению функциональной модели с менее точной идентификацией. Таким образом внесение изменений на уровне пикселей позволяет снизить правильность распознавания на 25%, а в некоторых случаях и на 30%.

С целью увеличения стойкости к различного рода мерам, нацеленным на выявление искажений на изображениях было принято решение

использовать частотные алгоритмы, где перед добавлением в изображение комбинации пикселей происходят некоторые преобразования (зашумление, фильтрация и др.).

Также следует отметить, что технология многоуровневого включения требует выполнения индивидуальных условий для избегания так называемой проблемы выхода значений пикселей из возможных пределов (0, 255) [6]. Если не учитывать этот факт, то появляются яркие точки и линии, которые визуально отличают исходное изображение от измененного.

Таким образом, в Республике Беларусь все острее становится проблема по обеспечению прав граждан по защите неприкосновенности их персональных данных, что обусловлено использованием новых технологии, ростом киберпреступности. Практически единственными инструментами политики по отношению к защите персональных данных в Республике Беларусь являются законодательство, а также изучение технических инструментов деидентификации лиц.

В современных условиях недостаточно проработанным и понятным для простого гражданина является механизм защиты его визуальных персональных данных. Гражданин должен иметь возможность прекратить обработку своих персональных данных, то есть в теории можно вылавливать все свои фотографии в толпе и настаивать, что это хранение и обработка без вашего согласия. Исключениями из данной ситуации являются случаи, когда:

– использование изображения осуществляется в государственных, общественных или иных публичных интересах;

– изображение получено при съемке, которая проводится в местах, открытых для свободного посещения, или на публичных мероприятиях (собраниях, съездах, конференциях, концертах, представлениях, спортивных соревнованиях и подобных мероприятиях);

– гражданин позировал за плату.

В данной работе в дополнение к основным типам персональных данных предложено ввести термин «визуальные персональные данные». Предлагается подход, который поможет обеспечить защиту визуальных персональных данных при обработке моделями распознавания лиц путем внесения изменений в исходное изображение на уровне пикселей.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Абламейко, М.С., Защита визуальных персональных данных: правовые аспекты / М.С. Абламейко // Веб-программирование и интернет-технологии WebConf2021: материалы 5-й Междунар. науч.-практ. конференции, Минск, 18–21 мая 2021 г. / БГУ,

Механико-математический фак. ; [редкол.: И. М. Галкин (отв. ред.) и др.]. – Минск: БГУ, 2021. – 400 с. – Деп. в БГУ 07.05.2021, №005207052021.
2. Конвенция о защите частных лиц в отношении автоматизированной обработки данных личного характера / [Электронный ресурс] // Режим доступа: http://hrlibrary.umn.edu/euro/Rets108.html. -- Дата доступа: 10.11.2021.
3. О республиканской системе мониторинга общественной безопасности [Электронный ресурс]: Указ Президента Респ. Беларусь, 25 мая 2017 г., №187 / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2021. – Режим доступа: https://pravo.by/upload/docs/op/P31700187_1496091600.pdf. – Дата доступа: 10.11.2021.
4. Об информации, информатизации и защите информации [Электронный ресурс]: Закон Респ. Беларусь, 10 ноябр. 2008 г., № 455-З / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2021. – Режим доступа: https://pravo.by/document/?guid=3871&p0=h10800455. – Дата доступа: 10.11.2021.
5. О защите персональных данных [Электронный ресурс]: Закон Респ. Беларусь, 7 мая 2021 г., №99-З / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2021. – Режим доступа: https://pravo.by/document/?guid=12551&p0=H12100099&p1=1&p5=0. – Дата доступа: 10.11.2021.
6. Русакович, А.С., Безопасность данных при распознавании облика лица человека / А.С. Русакович // Шаг в будущее: искусственный интеллект и цифровая экономика. Технологическое лидерство: взгляд за горизонт: материалы IV Международного научного форума. Вып. 4 / Министерство науки и высшего образования Российской Федерации, Государственный университет управления: под общ. ред. П. В. Терелянского: ред. кол. И. В. Лобанов [и др.]. – Москва: ГУУ, 2021. – 328 с.
7. Belhumeur P.N. Eigenfaces vs. fisherfaces: Recognition using class specific linear projection / P.N. Belhumeur, J.P. Hespanha, D.J. Kriegman // IEEE Trans. Pattern Anal. Mach. Intell. – Т. 19, № 7. – P. 711-720, 1997.
8. International Biometrics & Identification Association. Privacy Best Practice Recommendations for Commercial Biometric Use [Electronic resoure]. – Mode of access: https://www.ibia.org/resources/white-papers. – Date of access: 11.11.2021.
9. Newton E., Sweeney L., Malin B. Preserving Privacy by De-identifying Facial Images, Carnegie Mellon University, School of Computer Science, Technical Report, CMU-CS-03-119, pages 1-26, 2003.