Научная статья
УДК 34:004:341:57.087.1:316.642.4
EDN: https://elibrary.ru/joupzt
DOI: https://doi.org/10.21202/jdtl.2025.5

Поведенческая биометрия в Европейском союзе: правовые вызовы и технологические перспективы

Бауржан Рахметов ✉

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

Казбек Хайзабеков

Падуанский университет, Падуя, Италия

Ключевые слова

Европейский союз, законодательство, защита данных, искусственный интеллект, конфиденциальность, поведенческая биометрия, право, правовое регулирование, распознавание лиц, цифровые технологии

Аннотация

Цель: изучение исторического развития законодательства Европейского союза в области поведенческой биометрии, выявление особенностей европейского подхода к регулированию поведенческой биометрии, а также оценка его преимуществ и недостатков.

Методы: общенаучные методы анализа и сравнения с акцентом на изучение юридических текстов, таких как директивы, регламенты и конвенции. Для обеспечения всестороннего понимания проблемы авторы также рассматривают технические аспекты поведенческой биометрии, что позволяет провести комплексный анализ как правовых норм, так и технологических процессов, лежащих в их основе.

Результаты: нормативная правовая база Европейского союза в области биометрии недостаточно четко разграничивает технологии поведенческой и физической биометрии. Это приводит к неоднозначности в понимании рисков и возможностей, связанных с использованием поведенческой биометрии. Авторы подчеркивают, что отсутствие конкретики в законодательстве создает значительные трудности для регулирующих органов, разработчиков технологий и конечных пользователей.

Научная новизна: заключается в том, что она представляет собой первое комплексное исследование исторического развития законодательства Европейского союза в области поведенческой биометрии. В статье раскрываются ключевые характеристики европейского подхода, его сильные и слабые стороны, а также проводится сравнительный анализ с опытом регулирования в Соединенных Штатах. В исследовании детально раскрываются ключевые аспекты, требующие дальнейшего законодательного урегулирования: от четкой дефиниции

✉ Контактное лицо

© Рахметов Б., Хайзабеков К., 2025

Статья находится в открытом доступе и распространяется в соответствии с лицензией Creative Commons «Attribution» («Атрибуция») 4.0 Всемирная (CC BY 4.0) (https://creativecommons.org/licenses/by/4.0/deed.ru), позволяющей неограниченно использовать, распространять и воспроизводить материал при условии, что оригинальная работа упомянута с соблюдением правил цитирования.

поведенческой биометрии до разработки комплексных механизмов обеспечения прозрачности и подотчетности при использовании данных технологий. Учитывая, что поведенческая биометрия является относительно новой и быстро развивающейся технологией, такое исследование имеет важное значение для понимания современных вызовов и перспектив ее регулирования.

Практическая значимость: определяется его многогранным характером и актуальностью для широкого круга специалистов в сфере цифровых технологий: от ученых-правоведов, правоприменителей и законодателей до разработчиков технологий искусственного интеллекта и биометрии.

Для цитирования

Рахметов, Б., Хайзабеков, К. (2025). Поведенческая биометрия в Европейском союзе: правовые вызовы и технологические перспективы. *Journal of Digital Technologies and Law*, *3*(1), 108–124. https://doi.org/10.21202/jdtl.2025.5

Содержание

Введение
1. Эволюция регулирования поведенческой биометрии в Европейском союзе
2. Специфика регулирования поведенческой биометрии в Европейском союзе
   2.1. Особенности подхода Европейского союза к регулированию поведенческой биометрии
   2.2. Преимущества и недостатки подхода Европейского союза к регулированию поведенческой биометрии
3. Сравнительный анализ подходов к регулированию поведенческой биометрии Европейского союза и опыта Соединенных Штатов Америки
Заключение
Список литературы

Введение

Регулирование поведенческой биометрии в Европейском союзе (далее – ЕС) свидетельствует о важности защиты данных и конфиденциальности в условиях быстро меняющегося технологического ландшафта. Биометрия, которая использует физические, физиологические и поведенческие характеристики для идентификации людей, привлекает все больше внимания по мере роста проблем конфиденциальности во всем мире. С момента принятия Конвенции 1981 г. о защите физических лиц в связи с автоматической обработкой персональных данных (Конвенция 108) ЕС постоянно обновляет свое законодательство в области защиты персональных данных. Ключевые документы, такие как Директива 95/46/ЕС и Общий регламент по защите данных (GDPR), помогли Европейскому союзу установить общемировой стандарт защиты персональных данных, особенно в такой чувствительной области, как биометрические данные. Недавние новшества, например, Закон ЕС об

искусственном интеллекте 2024 г. (EU AI Act), еще больше расширили сферу действия этих стандартов, в частности, в отношении использования поведенческой биометрии и искусственного интеллекта в таких чувствительных областях, как безопасность и конфиденциальность.

Несмотря на эти достижения, регулирование поведенческой биометрии сопряжено с различными трудностями, например, в том, что касается различий между физическими и поведенческими данными. Подход ЕС к регулированию биометрических данных оказал значительное влияние на законы о конфиденциальности во всем мире, однако он подвергается критике за отсутствие ясности и конкретики в определенных областях. В настоящей статье рассматривается эволюция нормативных актов ЕС по поведенческой биометрии, анализируются ключевые законодательные акты, их влияние на защиту данных и проблемы в этой области. Авторы также сравнивают подход ЕС к регулированию с подходом Соединенных Штатов, где отсутствие национального законодательства привело к менее всеобъемлющему регулированию биометрических данных.

1. Эволюция регулирования поведенческой биометрии в Европейском союзе

Чтобы получить более полное представление о том, как биометрия регулируется в ЕС, важно понимать контекст и условия, которые способствовали появлению и внедрению ее правовой базы (Carrigan & Coglianese, 2011). В связи со стремительным развитием электронной обработки данных в 1960-х и 1970-х гг. возникла острая необходимость в усилении мер по защите конфиденциальности, особенно при автоматическом сборе персональных данных. Это нашло отклик в ЕС и привело к принятию Конвенции 108 и Директивы 95/46/ЕС (De Hert, 2013). Эти документы стали первыми юридически обязательными международными нормативными актами, регулирующими защиту данных, в том числе биометрических.

Конвенция 108, подписанная 28 января 1981 г., обязала страны ЕС внести ряд конкретных изменений в свое внутреннее законодательство, руководствуясь такими принципами, как справедливый и законный сбор и автоматическая обработка данных и наличие конкретных, явных и законных целей для хранения таких данных; запрещение использовать данные в иных целях и хранить их дольше, чем необходимо. Эти принципы также включают адекватность, актуальность данных и отсутствие их избыточности. Как правило, в соответствии с положениями Конвенции 108 ответственность за управление обработкой персональных данных несут контролирующие органы[1].

В настоящее время действует обновленная версия этого документа, известная как Конвенция 108+. Статья 6 этой Конвенции предусматривает, что обработка биометрических данных для идентификации личности разрешена при условии наличия соответствующих гарантий защиты от рисков, которые угрожают интересам, правам и основным свободам человека, включая риск дискриминации. В то же время биометрические данные, используемые для однозначной идентификации, относятся к категории конфиденциальных данных, поэтому их обработка должна

[1] Convention 108 and Protocols: Background. (n.d.). Council of Europe Portal. https://clck.ru/3Ge8xN

сопровождаться определенными гарантиями. Для этого требуются: отдельное или совместное согласие субъекта данных; закон, определяющий цели, методы и конкретные условия, при которых может осуществляться обработка данных; меры конфиденциальности, основанные на анализе рисков, и меры предосторожности в области безопасности[2].

Директива 95/46/ЕС, принятая 24 октября 1995 г., также стала важным документом в области регулирования биометрии. Основное внимание было уделено защите основных прав и свобод человека при обработке данных в странах ЕС и свободному перемещению таких данных. Основная ответственность за защиту данных лежит на надзорных органах каждого отдельного государства, принявшего Директиву 95/46/ЕС. Это независимые органы, которые уполномочены давать рекомендации по административным мерам и нормативным актам, а также возбуждать судебные разбирательства в случае обнаружения нарушений требований по защите данных. Хотя в Директиве 95/46/ЕС не упоминается конкретно обработка биометрических данных, в соответствии с ее ст. 29 была создана Рабочая группа для проведения консультаций и представления мнений по вопросам функционирования и регулирования биометрических данных[3]. Так, в 2003 г. был издан «Рабочий документ по биометрии», в котором рассматривается применение положений Директивы 95/46/ЕС к биометрическим технологиям[4]. В 2012 г. Рабочая группа также опубликовала заключение по изменениям в рекомендациях, касающихся принципов и путей повышения конфиденциальности и защиты данных в биометрических приложениях[5].

Несмотря на это, на сегодняшний день Директива 95/46/ЕС считается утратившей силу в связи с ее заменой Общим регламентом по защите данных (GDPR), который положил начало новому этапу развития регулирования персональных данных. Регламент был принят в 2016 г. и вступил в силу в 2018 г. Как и Директива 95/94/ЕС, он распространяется на все страны ЕС, но не требует от них изменения своего внутреннего законодательства. Все организации как внутри ЕС, так и за его пределами должны соблюдать требования Общего регламента. Между тем Регламент требует, чтобы организации, базирующиеся за пределами ЕС и предоставляющие товары или услуги, отслеживающие поведение, обрабатывающие и хранящие данные граждан ЕС, идентифицировали своих представителей в ЕС. В свою очередь, контролеры и обработчики данных также имеют определенные обязательства. Контролеры всегда должны помнить о соблюдении мер, необходимых для эффективной защиты данных; они должны обрабатывать только те данные, которые входят в сферу их обязанностей, и не предоставлять доступ к ним никому, кроме тех, кто обязан их обрабатывать (Nguyen, 2018).

---

2 Convention 108 +. (2018). Council of Europe. https://clck.ru/3Ge94r

3 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data. (1995). Official Journal of the European Union. https://clck.ru/3Ge97y

4 Working Document on Biometrics. (2003). The Working Party. https://clck.ru/3Ge9AL

5 Opinion on Developments in Biometric Technologies. (2012). The Working Party. https://clck.ru/3Ge9D4

В языке регулирующих органов термин «биометрические данные» впервые появился с введением GDPR. Статья 4 определяет биометрические данные как «персональные данные, полученные в результате специальной технической обработки, относящиеся к физическим, физиологическим или поведенческим характеристикам физического лица»[6]. Стоит отметить, что Общий регламент по защите данных предусматривает категорию специальных данных, требующих более высокого уровня защиты, которая включает и биометрические данные. В соответствии со ст. 9, обработка биометрических данных, целью которой является определение личности, состояния здоровья, сексуальной жизни и ориентации, строго запрещена, за исключением определенных условий. Например, явно выраженное согласие субъекта персональных данных позволяет обойти этот запрет[7] (Meden et al., 2021).

Наконец, Закон ЕС об искусственном интеллекте, принятый в марте 2024 г., является на сегодняшний день самым последним и актуальным нормативным актом, который также применяется к биометрии. В настоящее время искусственный интеллект оказывает огромное влияние на развитие биометрических технологий. В сочетании с биометрией системы искусственного интеллекта способствуют снижению количества человеческих ошибок и ускорению принятия решений (Rawat et al., 2023). Таким образом, Закон ЕС об искусственном интеллекте включает в себя несколько ключевых положений, направленных на регулирование биометрии, включая поведенческую биометрию. Отметим, что этот документ охватывает следующие аспекты, связанные с биометрией: биометрические данные; системы распознавания эмоций, биометрической категоризации, удаленной биометрической идентификации, удаленной биометрической идентификации в режиме реального времени и более удаленной биометрической идентификации[8]. Среди них к поведенческой биометрии относятся системы распознавания эмоций и удаленной биометрической идентификации в режиме реального времени (Xefteris et al., 2016; Alsaadi, 2021; Revett, 2008). Система распознавания эмоций предназначена для обработки таких характеристик, как направление взгляда, настроение, мимика и выражение лица, походка и сердцебиение. В связи с этим Закон ЕС об искусственном интеллекте вводит запрет на использование технологий распознавания эмоций на рабочем месте и в школах, на предиктивную полицейскую деятельность, если она основана на профилировании человека и оценке личностных характеристик, а также на ИИ, который предполагает манипулирование поведением людей или их уязвимостями. Что касается систем удаленной биометрической идентификации в режиме реального времени, то эта технология может быть использована при соблюдении строгих мер предосторожности и ограничений[9].

---

6 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation). (2016). Official Journal of the European Union. https://clck.ru/3Ge9Gn

7 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation). (2016). Official Journal of the European Union. https://clck.ru/3Ge9Gn

8 Santalu, N. (2023). Biometrics Under the EU AI Act. The International Association of Privacy Professionals. https://clck.ru/3Ge9Jz

9 Holistic AI Team. (2024). Prohibited AI Practices Under the EU AI Act. https://clck.ru/3Ge9Lf

2. Специфика регулирования поведенческой биометрии в Европейском союзе

2.1. Особенности подхода Европейского союза к регулированию поведенческой биометрии

Подход, который характеризует регулирование биометрии в ЕС, можно рассматривать как рискориентированный. Законодательство в области поведенческой биометрии сопровождается жесткими ограничительными мерами, направленными на защиту частной жизни и гражданских свобод, а также на борьбу с предвзятостью и дискриминирующими технологиями. Сбор, обработка и хранение поведенческих данных сопровождаются более высоким уровнем риска, особенно по сравнению с другими типами персональных данных (Rezaee, 2025). Дело в том, что точность анализа таких данных не позволяет полностью определить личность человека, а лишь выявляет специфические закономерности, связанные с его характером и привычками. Важно учитывать, что такие факторы, как высокий уровень стресса или физическое состояние, не позволяют поведенческим биометрическим данным точно оценить поведение человека. В свою очередь, более точное профилирование характерного поведения требует сбора значительного объема поведенческих данных. Кроме того, поскольку сбор поведенческих данных постоянно продолжается, возникает необходимость в хранении значительных объемов такой информации, что также создает дополнительные риски для конфиденциальности данных[10] (Sharma & Elmiligi, 2022).

Поведенческая биометрия – это относительно новая технология, которая сегодня активно набирает обороты, но по-прежнему сопряжена с определенными проблемами и рисками. Чтобы смягчить их, GDPR обязывает получать согласие субъектов данных на обработку и сбор их биометрических данных, в том числе поведенческих. Ранее GDPR уже классифицировал биометрические данные как чувствительные. Однако недавно принятый Закон ЕС об ИИ расширил систему классификации, добавив такие уровни риска, как неприемлемый, высокий, ограниченный, низкий или минимальный. Чтобы определить уровень риска, важно выяснить природу и масштабы применения ИИ (Arcila, 2024). Категория неприемлемого риска, которая запрещает использование ИИ, включает такие системы ИИ, которые предполагают социальную оценку, основанную на поведении или личных качествах, и манипулирование поведением или уязвимостями людей. Использование удаленной биометрической идентификации в режиме реального времени также запрещено, за исключением случаев, когда эта технология может помочь в поиске пропавших людей, предотвращении опасных для жизни ситуаций, включая прогнозируемые теракты, и выявлении подозреваемых в совершении преступлений. Система распознавания эмоций относится к категории ограниченного риска, но ее применение запрещено в учебных заведениях и на рабочих местах, за исключением медицинских оснований и соображений безопасности[11].

---

[10] Makhani, F. (2022). Beyond Fingerprints: Exploring Behavioral Biometrics For Secure Identity Verification. VikingCloud. https://clck.ru/3Ge9SS

[11] High-Level Summary of the AI Act. (2024). Future of Life Institute. https://clck.ru/3Ge9UK

2.2. Преимущества и недостатки подхода Европейского союза к регулированию поведенческой биометрии

Одним из преимуществ подхода ЕС является то, что его опыт регулирования значительно повлиял на другие страны, которые создают и развивают свое собственное законодательство о защите данных и биометрии. В работе (Greenleaf, 2012) на основании изучения 39 неевропейских стран было показано, что в законодательстве 33 из них имеется значительное сходство с Конвенцией 108. Причина этого, в частности, заключается в том, что страны таким образом демонстрируют свое стремление присоединиться к европейскому законодательству о защите частной жизни. В целом желание присоединиться к Конвенции 108 выразили Аргентина, Кабо-Верде, Маврикий, Марокко, Мексика, Сенегал, Тунис и Уругвай[12].

Конвенция 108+, которая заменила Конвенцию 108 в 2018 г., также стала влиятельным ориентиром в мировой практике регулирования защиты данных. Помимо государств – членов ЕС, обновленный протокол подписали Великобритания (в то время являвшаяся членом ЕС), Уругвай, Кабо-Верде, Маврикий, Мексика, Сенегал и Тунис. Кроме того, Аргентина, Буркина-Фасо и Марокко также присоединились к Конвенции 108+[13]. Тем не менее именно GDPR служит основным ориентиром для регулирования защиты данных во всем мире. К 2020 г. законы, аналогичные GDPR, были приняты в таких странах, как Бразилия, Канада и Южная Корея (Chen et al., 2022). Многие африканские страны, включая Танзанию, Эсватини, Руанду, Уганду и Нигерию, ввели ряд новых правил защиты данных, основанных на тех же принципах, что и GDPR[14]. Стоит отметить, что требования GDPR относятся не только к странам, но и к организациям по всему миру. Поскольку европейское законодательство требует строгих гарантий защиты данных, организациям, деятельность которых распространяется на граждан Европы, пришлось внести существенные изменения в соответствии с GDPR (Li et al., 2019; Chen et al., 2022).

Подход ЕС к регулированию биометрии, включая поведенческую биометрию, отличается высокой степенью защиты данных и конфиденциальности. Согласно ст. 9 GDPR, биометрические данные классифицируются как конфиденциальные данные, требующие особой защиты и соблюдения требований конфиденциальности. Это означает, что, как правило, обработка таких данных разрешена только при строгом соблюдении определенных условий. Например, необходимо получить явно выраженное согласие субъекта данных – физического лица, чьи данные используются. Кроме того, GDPR предоставляет субъектам данных право изучать информацию, хранящуюся в организациях, и отзывать свое согласие на сбор данных организациями. Организации, осуществляющие сбор и обработку данных граждан Европы, обязаны выразить заинтересованность в сборе личной информации, обосновать причины обладания этой информацией и представить субъектам данных информацию о себе. В целом по требованиям GDPR организации должны ограничивать обработку данных,

12 Chart of Signatures and Ratifications of Treaty 108. (n.d.). Council of Europe. https://clck.ru/3Ge9a5

13 Baker, J. (2018). What Does the Newly Signed ‘Convention 108+’ Mean for UK Adequacy? The International Association of Privacy Professionals. https://clck.ru/3Ge9ch

14 Wu, J., & Hayward, M. (2023). International Impact of the GDPR Felt Five Years on. Pinsent Masons. https://clck.ru/3Ge9gi

а также владение и передачу данных между платформами, предоставляя соответствующие средства защиты и удаления данных по истечении установленного периода. Очевидно, что подход GDPR можно считать ориентированным на пользователя. Это положительно влияет на индивидуальную ответственность, снижает риски безопасности и способствует усилению мер по обеспечению конфиденциальности (Aseri, 2020).

За нарушение вышеуказанных правил использования биометрических данных предусмотрены суровые санкции. Как правило, существует два уровня административных штрафов за несоблюдение GDPR: 1) до 10 млн евро или 2 % от годового глобального оборота, в зависимости от того, какая из этих сумм больше; 2) до 20 млн евро или 4 % от годового оборота, в зависимости от того, какая из этих сумм больше. Размер штрафа определяется конкретными положениями GDPR. Меньшая сумма назначается, если нарушена безопасность данных, а большая – если нарушены права граждан на неприкосновенность частной жизни. Например, в соответствии с практикой применения GDPR Ирландская комиссия по защите данных в 2023 г. оштрафовала Meta[15] на 1,2 млрд евро за передачу личной информации европейских пользователей в США без надлежащих механизмов защиты данных. До этого под санкции также попали такие компании, как Amazon, TikTok, WhatsApp, Google и др.[16]

Наиболее существенными недостатками европейского подхода являются несовершенство классификации и отсутствие конкретики в некоторых аспектах. В частности, европейские регулирующие органы не учитывают тот факт, что разные типы биометрии используют разные типы данных; только поведенческая биометрия собирает такие данные, как динамика нажатия клавиш, движения мыши, ввод данных с сенсорного экрана, движения глаз, жесты и походка (Eberz et al., 2017; Cheung & Vhaduri, 2020). Вместо этого европейское законодательство содержит лишь общие толкования и руководящие принципы, касающиеся физических, психологических и поведенческих особенностей. Этот недостаток можно проследить как в прошлом, имея в виду Конвенцию 108 и Директиву 95/46/ЕС, так и в настоящее время, в Конвенции 108+, GDPR и Законе ЕС об искусственном интеллекте. Дело в том, что динамичный характер поведенческих данных, который не позволяет прогнозировать, моделировать или получать их так же легко, как физические данные, делает их неподходящими для действующих правил ЕС, которые охватывают только физическую биометрию. Компании и финансовые учреждения в ЕС, которые уже приступили к последовательному внедрению поведенческой биометрии, по-прежнему руководствуются правилами сбора физических данных[17] (Kindt, 2018).

Проблема неопределенности также очевидна в других важных положениях нормативных актов, касающихся использования биометрических данных. Например, в GDPR не проводится существенного различия между основными сравнительными функциями биометрических технологий, в частности между верификацией и идентификацией. Верификация предполагает использование

---

15 Мета – организация признана экстремистской, ее деятельность запрещена на территории Российской Федерации.

16 20 Biggest GDPR Fines So Far. (2024). Data Privacy Manager. https://clck.ru/3Ge9me

17 Özal, M. (2020). 'Behavioral Biometrics': A Brief Introduction from the Perspective of Data Protection Law. CiTiP Blog. https://clck.ru/3Ge9pA

биометрических данных в соотношении «один к одному» (1 : 1), а идентификация – «один ко многим» (1 : n). Стоит отметить, что, по мнению Совета Европы и национальных органов по надзору за защитой данных, функция верификации более безопасна, чем метод идентификации, поскольку не требует использования базы данных. Напротив, использование биометрической идентификации требует обширного сбора и хранения биометрической информации в базах данных. Кроме того, следует отметить, что биометрическая идентификация сопряжена с дополнительными рисками из-за вероятностного сопоставления, что отрицательно сказывается на уровне точности. Соответственно, европейские регулирующие органы должны объективно учитывать относительные риски, связанные как с верификацией, так и с идентификацией, при введении соответствующих правил применения этих двух основных функций биометрических технологий[18].

3. Сравнительный анализ подходов к регулированию поведенческой биометрии Европейского союза и опыта Соединенных Штатов Америки

Чтобы лучше понять систему регулирования поведенческой биометрии в ЕС, будет полезно изучить опыт США и сравнить его с подходом ЕС. Наиболее примечательно, что вместо единого национального законодательства, как в ЕС, в Соединенных Штатах биометрия регулируется на уровне штатов[19].

Во многих штатах, включая Иллинойс, Техас и Арканзас, действуют различные законы, направленные на регулирование биометрии и биометрических данных. Для начала стоит отметить штат Иллинойс, который стал первым штатом, регулирующим сбор, использование и хранение биометрических данных, введя в 2008 г. Закон о конфиденциальности биометрической информации (Biometric Information Privacy Act, BIPA). Согласно этому закону, компании обязаны получать письменное согласие от субъектов данных перед сбором их биометрической информации и ограничивать такие методы, как сканирование сетчатки или радужной оболочки глаза, снятие отпечатков пальцев, образцов голоса, сканирование геометрии лица и кистей рук. Другими словами, другие биологические и поведенческие данные не считаются биометрическими идентификаторами в соответствии с этим законом (Illman, 2017). Аналогичные определения биометрических идентификаторов содержатся в Законе штата Техас от 2009 г. в разделе 503.001[20].

В штате Арканзас принят Закон о биометрических данных, который фокусируется исключительно на биологических параметрах, исключая данные о поведении. Этот нормативный акт определяет биометрические данные как информацию о биологических характеристиках человека, таких как отпечатки пальцев, изображение лица или глаз, ДНК и другие уникальные биологические особенности, используемые для идентификации[21].

---

18 Kindt, E. (2020). A First Attempt at Regulating Biometric Data in the European Union. AI Now Institute. https://clck.ru/3Ge9ti

19 Biometric Data Protection (Privacy – EU, UK and US). (2021). https://clck.ru/3Ge9w2

20 2023 Texas Statutes Business and Commerce Code. https://clck.ru/3GePrv

21 Arkansas Personal Information Protection Act. https://clck.ru/3GeRBo

Различные законы Соединенных Штатов неодинаково интерпретируют биометрические данные. Среди них Закон штата Калифорния о защите прав потребителей (California Consumer Privacy Act, далее – CCPA) от 2018 г., который значительно расширяет понимание биометрических данных. Согласно этому закону, биометрическая информация включает в себя «физиологические, биологические или поведенческие характеристики человека, включая ДНК, которые могут использоваться отдельно или в сочетании с другими данными для установления личности»[22]. Сюда входят не только традиционные биометрические идентификаторы, но и поведенческие паттерны, такие как нажатие клавиш, походка, привычки сна, данные о физических нагрузках и состоянии здоровья, которые могут идентифицировать человека[23]. Примечательно, что в соответствии с CCPA граждане штата имеют больше возможностей для контроля над своими биометрическими данными, включая права на общее раскрытие данных, на запрашивание и удаление информации, а также на «равное обслуживание и расценки» (Ghelardi, 2020).

Кроме того, Закон США о праве на неприкосновенность частной жизни от 2024 г., являющийся преемником Закона США о конфиденциальности и защите данных от 2021 г., направлен на установление четких общенациональных прав и средств защиты данных. Законопроект был внесен в Палату представителей и в Сенат в апреле 2024 г. и месяц спустя был одобрен Подкомитетом по данным, инновациям и торговле. Теперь он должен будет пройти через полный комитет и обе палаты Конгресса, прежде чем вступит в силу в качестве закона. Этот законопроект определяет биометрическую информацию как данные, полученные в результате технологической обработки уникальных биологических, физических или физиологических характеристик, включая отпечатки пальцев, изображение лица и походки и другие характеристики. Важно отметить, что законопроект был разработан по образцу GDPR, действующего в ЕС[24].

По сравнению с законодательством ЕС, американское законодательство менее проработано. Законы принимаются не на федеральном уровне, а на уровне штатов, что указывает на необходимость более комплексного подхода (Neace, 2020). Также становится очевидным, что в этих нормативных актах, как и в нормативных актах ЕС, нет четкого различия между физической и поведенческой биометрией. Хотя в некоторых законах упоминаются поведенческие характеристики, до сих пор нет четкого законодательного определения или регулирования поведенческой биометрии. Следовательно, вопросы, связанные с поведенческой биометрией, остаются недостаточно решенными и требуют дальнейшего законодательного внимания и разработки. Необходимость уделять пристальное внимание поведенческим биометрическим данным, включая такие характеристики, как движения рук и направление взгляда, была также четко сформулирована исполнительной властью в Указе президента Джо Байдена об искусственном интеллекте[25].

---

22 California Consumer Privacy Act. https://clck.ru/3GeRFp

23 What is the California Consumer Privacy Act (CCPA)? (2024). TermsFeed. https://clck.ru/3GeAJh

24 Wright, V. (2024). The American Privacy Rights Act (APRA): Everything You Need to Know. BigID. https://clck.ru/3GeALE ; Pınarbaşı, A. T. (2024). The American Privacy Rights Act (APRA): Everything You Need to Know. Didomi. https://clck.ru/3GeANc

25 Brunetti, F. (2024). Behavioral Characteristics as a Biometric: Something to Keep an Eye (Scan) on. The International Association of Privacy Professionals. https://clck.ru/3GeATg

Заключение

Подводя итог, можно сказать, что регулирование поведенческой биометрии в ЕС претерпело значительные изменения, определяемые ключевыми законодательными актами, такими как Конвенция 108, Директива 95/46/ЕС, а совсем недавно – Общим регламентом о защите данных 2018 г. и Законом ЕС об искусственном интеллекте 2024 г. Эти документы заложили прочную основу для защиты персональных данных, особенно биометрических, отнесенных к категории конфиденциальной информации. Введение определения и строгих правил обработки биометрических данных в GDPR установило глобальный стандарт, оказавший влияние не только на европейские страны, но и на правовую практику во всем мире. Однако некоторые проблемы остаются нерешенными, например, проведение различия между физической и поведенческой биометрией и решение сложных задач, связанных с такими биометрическими технологиями, как верификация и идентификация.

Сравнение подхода ЕС с подходом Соединенных Штатов свидетельствует о более всеобъемлющей и унифицированной нормативно-правовой базе ЕС, в отличие от разрозненных законов на уровне штатов в США. Несмотря на то, что США добились прогресса в принятии таких нормативных актов, как Закон штата Иллинойс о конфиденциальности биометрической информации (BIPA) и более поздний Закон о праве на неприкосновенность частной жизни, отсутствие единого национального подхода вызывает обеспокоенность. Например, проблеме поведенческой биометрии в США по-прежнему уделяется недостаточно внимания. Поскольку такие технологии, как искусственный интеллект, продолжают развиваться и их взаимосвязь с биометрическими технологиями становится все более тесной, важно подчеркнуть, что ЕС и США должны усилить свои нормативные акты для защиты персональных данных и для содействия этичному использованию биометрических данных. Однако, учитывая новизну поведенческой биометрии, необходимы также дальнейшие исследования в области правового регулирования персональных данных.

Список литературы

Alsaadi, E. (2021). *Study on Most Popular Behavioral Biometrics, Advantages, Disadvantages and Recent Applications: A Review*. https://doi.org/10.13140/RG.2.2.28802.09926

Arcila, B. B. (2024). AI liability in Europe: How does it complement risk regulation and deal with the problem of human oversight? *Computer Law & Security Review*, *54*, 106012. https://doi.org/10.1016/j.clsr.2024.106012

Aseri, A. (2020). The Implication of the European Union's General Data Protection Regulation (GDPR) on the Global Data Privacy. *Journal of Theoretical and Applied Information Technology*, *98*(4), 692–702.

Carrigan, C., & Coglianese, C. (2011). The Politics of Regulation: From New Institutionalism to New Governance. *Annual Review of Political Science*, *14*(1), 107–129. https://doi.org/10.1146/annurev.polisci.032408.171344

Chen, C., Frey, C. B., & Presidente, G. (2022). Privacy Regulation and Firm Performance: Estimating the GDPR Effect Globally. *Oxford Martin School*.

Cheung, W., & Vhaduri, S. (2020). Continuous Authentication of Wearable Device Users from Heart Rate, Gait, and Breathing Data. *2020 8th IEEE RAS/EMBS International Conference for Biomedical Robotics and Biomechatronics (BioRob)*, 587–592. https://doi.org/10.1109/BioRob49111.2020.9224356

De Hert, P. (2013). Biometrics and the Challenge to Human Rights in Europe. Need for Regulation and Regulatory Distinctions. In: P. Campisi (Eds.), *Security and Privacy in Biometrics* (pp. 369–413). Springer London. https://doi.org/10.1007/978-1-4471-5230-9_15

Eberz, S., Rasmussen, K. B., Lenders, V., & Martinovic, I. (2017). Evaluating Behavioral Biometrics for Continuous Authentication: Challenges and Metrics. *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*, 386–399. https://doi.org/10.1145/3052973.3053032

Ghelardi, E.-M. (2020). Closing the Data Gap: Protecting Biometric Information Under the Biometric Information Privacy Act and the California Consumer Protection Act. *St. John's Law Review*, *94*(3).

Greenleaf, G. (2012). The Influence of European Data Privacy Standards Outside Europe: Implications for Globalization of Convention 108. *International Data Privacy Law*, *2*(2), 68–92. https://doi.org/10.1093/idpl/ips006

Illman, E. J. (2017). Data Privacy Laws Targeting Biometric and Geolocation Technologies. *The Business Lawyer*, *73*(1), 191–198.

Kindt, E. (2018). Having Yes, Using No? About the New Legal Regime for Biometric Data. *Computer Law & Security Review*, *34*(3), 523–538. https://doi.org/10.1016/j.clsr.2017.11.004

Li, H., Yu, L., & He, W. (2019). The Impact of GDPR on Global Technology Development. *Journal of Global Information Technology Management*, *22*(1), 1–6. https://doi.org/10.1080/1097198X.2019.1569186

Meden, B., Rot, P., Terhorst, P., Damer, N., Kuijper, A., Scheirer, W. J., Ross, A., Peer, P., & Struc, V. (2021). Privacy–Enhancing Face Biometrics: A Comprehensive Survey. *IEEE Transactions on Information Forensics and Security*, *16*, 4147–4183. https://doi.org/10.1109/TIFS.2021.3096024

Neace, G. (2020). Biometric Privacy: Blending Employment Law with the Growth of Technology. *UIC Law Review*, *53*(1).

Nguyen, F. Q. (2018). The Standard for Biometric Data Protection. *Journal of Law & Cyber Warfare*, *7*(1), 61–84.

Rawat, Y., Gupta, Y., Khothari, G., Mittal, A., & Rautela, D. (2023). The Role of Artificial Intelligence in Biometrics. *2023 2nd International Conference on Edge Computing and Applications (ICECAA)*, 622–626. https://doi.org/10.1109/ICECAA58104.2023.10212224

Revett, K. (2008). *Behavioral Biometrics: A Remote Access Approach*. Wiley.

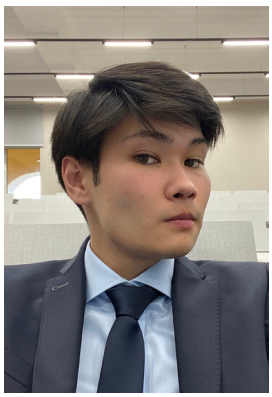
Rezaee, K. (2025). Machine Learning and Facial Recognition for Down Syndrome Detection: A Comprehensive review. *Computers in Human Behavior Reports*, *17*, 100600. https://doi.org/10.1016/j.chbr.2025.100600

Sharma, M., & Elmiligi, H. (2022). Behavioral Biometrics: Past, Present and Future. *Recent Advances in Biometrics*. IntechOpen. https://doi.org/10.5772/intechopen.102841

Xefteris, S., Doulamis, N., Andronikou, V., Varvarigou, T., & Cambourakis, G. (2016). Behavioral Biometrics in Assisted Living: A Methodology for Emotion Recognition. *Engineering, Technology & Applied Science Research*, *6*(4), 1035–1044. https://doi.org/10.48084/etasr.634

Сведения об авторах

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



Хайзабеков Казбек – магистрант в области европеистики и глобальных исследований, кафедра политологии, права и международных исследований, Падуанский университет
Адрес: Италия, 35122, г. Падуя, ул. 8 февраля, 2
E-mail: khaizabekovk@gmail.com
ORCID ID: https://orcid.org/0009-0009-8241-8016
WoS Researcher ID: https://www.webofscience.com/wos/author/record/MIN-4357-2025

Вклад авторов

Авторы внесли равный вклад в разработку концепции, методологии, валидацию, формальный анализ, проведение исследования, подбор источников, написание и редактирование текста, руководство и управление проектом.

Конфликт интересов

Бауржан Рахметов является членом редакционной коллегии данного журнала; статья прошла рецензирование на общих условиях.

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.87 / Международное право
Специальность ВАК: 5.1.5 / Международно-правовые науки

История статьи

Дата поступления – 19 сентября 2024 г.
Дата одобрения после рецензирования – 23 октября 2024 г.
Дата принятия к опубликованию – 25 марта 2025 г.
Дата онлайн-размещения – 30 марта 2025 г.

Research article
UDC 34:004:341:57.087.1:316.642.4
EDN: https://elibrary.ru/joupzt
DOI: https://doi.org/10.21202/jdtl.2025.5

Behavioral Biometrics in the European Union: Legal Challenges and Technological Prospects

Baurzhan Rakhmetov ✉
M. Narikbayev KAZGUU University, Astana, Kazakhstan

Kazbek Khaizabekov
University of Padova, Padova, Italy

Keywords

artificial intelligence,
behavioral biometrics,
data protection,
digital technologies,
European Union,
facial recognition,
law,
legal regulation,
legislation,
privacy

Abstract

Objective: to study the historical development of the European Union legislation on behavioral biometrics; to identify the features of the European approach to the regulation of behavioral biometrics, to assess its advantages and disadvantages.

Methods: general scientific methods of analysis and comparison, with an emphasis on the study of legal texts such as directives, regulations and conventions. To ensure a comprehensive understanding of the issue, the authors also consider the technical aspects of behavioral biometrics, which allows for a comprehensive analysis of both legal norms and the technological processes underlying them.

Results: the research demonstrates that the European Union regulatory legal framework on biometrics does not clearly distinguish between behavioral and physical biometrics technologies. This leads to ambiguity in understanding the risks and opportunities associated with the use of behavioral biometrics. The authors emphasize that the insufficiently specific legislation creates significant difficulties for regulators, technology developers, and end users.

Scientific novelty: the article is the first comprehensive study of the historical development of European Union legislation on behavioral biometrics. The work reveals the key characteristics of the European approach, its strengths and weaknesses, and compares it with the United States' regulatory practice. The study reveals the key aspects that require further regulation: from a clear definition of behavioral biometrics to the development of comprehensive mechanisms to ensure transparency and accountability in the use of these

✉ Corresponding author
© Rakhmetov B., Khaizabekov K., 2025

This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (CC BY 4.0) (https://creativecommons.org/licenses/by/4.0), which permits unrestricted re-use, distribution and reproduction, provided the original article is properly cited.

technologies. Given that behavioral biometrics is a relatively new and rapidly developing technology, the research is important for understanding current challenges and prospects for its regulation.

Practical significance: the research is multifaceted and relevant for experts in digital technologies: legal scholars, law enforcement officers, legislators, and developers of artificial intelligence and biometrics technologies.

For citation

Rakhmetov, B., & Khaizabekov, K. (2025). Behavioral Biometrics in the European Union: Legal Challenges and Technological Prospects. *Journal of Digital Technologies and Law, 3*(1), 108–124. https://doi.org/10.21202/jdtl.2025.5

References

Alsaadi, E. (2021). *Study on Most Popular Behavioral Biometrics, Advantages, Disadvantages and Recent Applications: A Review*. https://doi.org/10.13140/RG.2.2.28802.09926

Arcila, B. B. (2024). AI liability in Europe: How does it complement risk regulation and deal with the problem of human oversight? *Computer Law & Security Review*, *54*, 106012. https://doi.org/10.1016/j.clsr.2024.106012

Aseri, A. (2020). The Implication of the European Union's General Data Protection Regulation (GDPR) on the Global Data Privacy. *Journal of Theoretical and Applied Information Technology*, *98*(4), 692–702.

Carrigan, C., & Coglianese, C. (2011). The Politics of Regulation: From New Institutionalism to New Governance. *Annual Review of Political Science*, *14*(1), 107–129. https://doi.org/10.1146/annurev.polisci.032408.171344

Chen, C., Frey, C. B., & Presidente, G. (2022). Privacy Regulation and Firm Performance: Estimating the GDPR Effect Globally. *Oxford Martin School*.

Cheung, W., & Vhaduri, S. (2020). Continuous Authentication of Wearable Device Users from Heart Rate, Gait, and Breathing Data. *2020 8th IEEE RAS/EMBS International Conference for Biomedical Robotics and Biomechatronics (BioRob)*, 587–592. https://doi.org/10.1109/BioRob49111.2020.9224356

De Hert, P. (2013). Biometrics and the Challenge to Human Rights in Europe. Need for Regulation and Regulatory Distinctions. In: P. Campisi (Eds.), *Security and Privacy in Biometrics* (pp. 369–413). Springer London. https://doi.org/10.1007/978-1-4471-5230-9_15

Eberz, S., Rasmussen, K. B., Lenders, V., & Martinovic, I. (2017). Evaluating Behavioral Biometrics for Continuous Authentication: Challenges and Metrics. *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*, 386–399. https://doi.org/10.1145/3052973.3053032

Ghelardi, E.-M. (2020). Closing the Data Gap: Protecting Biometric Information Under the Biometric Information Privacy Act and the California Consumer Protection Act. *St. John's Law Review*, *94*(3).

Greenleaf, G. (2012). The Influence of European Data Privacy Standards Outside Europe: Implications for Globalization of Convention 108. *International Data Privacy Law*, *2*(2), 68–92. https://doi.org/10.1093/idpl/ips006

Illman, E. J. (2017). Data Privacy Laws Targeting Biometric and Geolocation Technologies. *The Business Lawyer*, *73*(1), 191–198.

Kindt, E. (2018). Having Yes, Using No? About the New Legal Regime for Biometric Data. *Computer Law & Security Review*, *34*(3), 523–538. https://doi.org/10.1016/j.clsr.2017.11.004

Li, H., Yu, L., & He, W. (2019). The Impact of GDPR on Global Technology Development. *Journal of Global Information Technology Management*, *22*(1), 1–6. https://doi.org/10.1080/1097198X.2019.1569186

Meden, B., Rot, P., Terhorst, P., Damer, N., Kuijper, A., Scheirer, W. J., Ross, A., Peer, P., & Struc, V. (2021). Privacy–Enhancing Face Biometrics: A Comprehensive Survey. *IEEE Transactions on Information Forensics and Security*, *16*, 4147–4183. https://doi.org/10.1109/TIFS.2021.3096024

Neace, G. (2020). Biometric Privacy: Blending Employment Law with the Growth of Technology. *UIC Law Review*, *53*(1).

Nguyen, F. Q. (2018). The Standard for Biometric Data Protection. *Journal of Law & Cyber Warfare*, *7*(1), 61–84.

Rawat, Y., Gupta, Y., Khothari, G., Mittal, A., & Rautela, D. (2023). The Role of Artificial Intelligence in Biometrics. *2023 2nd International Conference on Edge Computing and Applications (ICECAA)*, 622–626. https://doi.org/10.1109/ICECAA58104.2023.10212224

Revett, K. (2008). *Behavioral Biometrics: A Remote Access Approach*. Wiley.

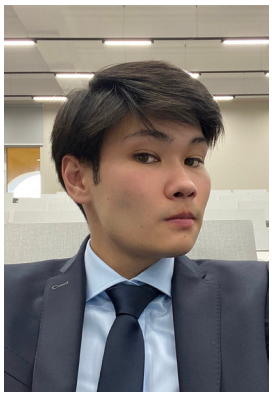
Rezaee, K. (2025). Machine Learning and Facial Recognition for Down Syndrome Detection: A Comprehensive review. *Computers in Human Behavior Reports*, *17*, 100600. https://doi.org/10.1016/j.chbr.2025.100600

Sharma, M., & Elmiligi, H. (2022). Behavioral Biometrics: Past, Present and Future. *Recent Advances in Biometrics*. IntechOpen. https://doi.org/10.5772/intechopen.102841

Xefteris, S., Doulamis, N., Andronikou, V., Varvarigou, T., & Cambourakis, G. (2016). Behavioral Biometrics in Assisted Living: A Methodology for Emotion Recognition. *Engineering, Technology & Applied Science Research*, *6*(4), 1035–1044. https://doi.org/10.48084/etasr.634

Authors information

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



Kazbek Khaizabekov – Master's Student, European and Global Studies, Department of Political Science, Law, and International Studies, University of Padova
Address: Via VIII Febbraio, 2, 35122 Padova PD, Italy
E-mail: khaizabekovk@gmail.com
ORCID ID: https://orcid.org/0009-0009-8241-8016
WoS Researcher ID: https://www.webofscience.com/wos/author/record/MIN-4357-2025

Authors' contributions

The authors have contributed equally into the concept and methodology elaboration, validation, formal analysis, research, selection of sources, text writing and editing, project guidance and management.

Conflict of interest

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

Thematic rubrics

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

Article history

Date of receipt – September 19, 2024
Date of approval – October 23, 2024
Date of acceptance – March 25, 2025
Date of online placement – March 30, 2025