Секция «Уголовное право и криминология, уголовно-исполнительное право»

# Уголовно-правовая защита биометрических персональных данных

***Алексеева Татьяна Сергеевна***
*Аспирант*
Московский государственный университет имени М.В.Ломоносова, Юридический факультет, Кафедра уголовного права и криминологии, Москва, Россия
*E-mail: alexeyevatatiana@mail.ru*

Определение биометрических персональных данных в Федеральном законе «О персональных данных» содержит два ключевых признака: связь с биологическими и физиологическими характеристиками субъекта персональных данных и использование для установления его личности.

Какие это могут быть данные и почему они важны для уголовного права?

Некоторые ориентиры дают нормативные правовые акты: например, в Федеральном законе от 29.12.2022 № 572-ФЗ и Постановлении Правительства РФ от 30.06.2018 № 772 определено, что в единую информационную систему персональных данных вносятся такие биометрические данные, как изображение лица и запись голоса. В литературе о биометрии в качестве идентификаторов называются отпечатки пальцев, голос, лицо, сетчатка или радужная оболочка глаза, почерк и геометрия руки [6, с. xxii]. Принципиальным признаком биометрических данных в нашем праве является возможность идентификации, хотя в Европейском Регламенте о защите персональных данных, например, предлагается считать фотографии биометрическими данными только при такой идентификации, при которой используются специальные технические средства для установления личности - на такое сужение понятия критически обращается внимание в литературе [1].

В связи с критерием идентификации перечень биометрических данных особенно узок, но их значимость нельзя переоценить: они используются во многих системах безопасности и неразрывно связаны с личностью. Контроль прохода, доступа в информационные системы и гарантии уникальности личности - такие основные функции биометрии называются в доктрине [3]. Какие нормы уголовного закона актуализируются в этой связи? Можно обозначить три ключевые группы, в соответствии с функциями.

Во-первых, следует обратить внимание на контроль физического прохода на определенные объекты. Применительно к ст. 327 УК РФ исследователи обращают внимание на пробельный характер нормы, которая не позволяет рассматривать в качестве документов отпечатки пальцев, изготовленные с помощью фотополимерных технологий [5]. Рассматривая случаи незаконного проникновения на охраняемые объекты, авторы отмечают, что в данном случае следовало бы квалифицировать именно по ст. 327 УК РФ, а не по ст. 137 УК РФ, если бы предмет ст. 327 УК РФ включал физические объекты с биометрическими данными [5].

Неправомерный доступ к компьютерным (информационным) системам - второй аспект; он в целом охвачен диспозицией нормы ст. 272 УК РФ, и практика содержит некоторые примеры использования собственных биометрических данных для доступа к компьютерной информации без надлежащих оснований. Именно так обвиняемая Л.К.В., будучи сотрудником оператора сотовой связи, входила в информационную систему и оформляла сим-карты, что повлекло «модификацию компьютерной информации» [8].

Отдельным вопросом, тем не менее, является также доступ с целью хищения, который связан с соответствующими нормами в 21 главе УК РФ. Преступления могут совершать работники банковской сферы: использовать ложные предлоги для личного приглашения

клиента, проводить биометрическую фотоидентификацию, благодаря чему получать доступ к личному кабинету в интернет-банке. Например, при таких обстоятельствах последующее хищение денежных средств с помощью операций в личном кабинете судом города Пензы квалифицировано как кража с банковского счета [9]. Такую же квалификацию получают действия субъектов, которые подключают к банковскому счету другого лица свои биометрические данные и впоследствии переводят себе с их помощью денежные средства [10], [7].

Второй аспект - использование биометрических данных для доступа к системе - наиболее полно отражен в действующем праве, однако он не проясняет, какой может быть ответственность в случае посягательства только на такие данные - как на основной, а не дополнительный, объект. Если данные, собранные банком для оказания услуг, можно рассматривать как включенные в режим банковской тайны, то какова защита от неправомерного сбора и распространения биометрических данных самих по себе (вне банковской сферы и хищений)?

Стабильность биометрии, представляя собой гарантию повышенной безопасности, в случае утечки влечет наихудшие последствия: неправомерное использование обладателю данных "грозит до конца его жизни" [6, с. 51]. Единственной нормой, которая теоретически могла бы защитить именно гарантии уникальности личности, вне связи с какими-либо иными сферами, представляется ст. 137 УК РФ. Однако в последней в качестве обязательного признака предусмотрено понятие "тайны" - и в литературе встречается критика распространения данной нормы на персональные данные в силу того, что многие из них не соответствуют критерию неизвестности третьим лицам [2, с. 35-36], происходит "отождествление ... институтов" [4, с. 39]. Тем не менее, представляется, что в качестве сведений нужно рассматривать не просто отпечаток пальца, лицо и иные внешние, доступные другим людям, параметры, но такую их запись в информационной системе, которая позволяет беспрепятственно устанавливать личность и защищена от посторонних лиц, что может делать ее предметом для ст. 137 УК РФ.

**Источники и литература**

1) Грибанов А.А. Общий регламент о защите персональных данных (General Data Protection Regulation): идеи для совершенствования российского законодательства // Закон. 2018. № 3. С. 149-162 // СПС КонсультантПлюс.

2) Озерова А.С. Личная и семейная тайна как предмет уголовно-правовой охраны: проблемы судебной практики // Уголовное право. 2022. № 3. С. 30-38.

3) Платонова Н.И., Соловьева-Опошнянская А.Ю. Биометрические персональные данные: возможности и проблемы // Юрист. 2019. № 6. С. 63-67 // СПС КонсультантПлюс.

4) Филатова М.А. Персональные данные как предмет преступного посягательства // Уголовное право. 2021. № 11. С. 35-43.

5) Чукин Д.С., Муфаздалов С.И. Объекты с биометрическими данными как предмет преступления, предусмотренного статьей 327 Уголовного кодекса Российской Федерации // Право в Вооруженных Силах. 2020. № 4. С. 37-42 // СПС КонсультантПлюс.

6) Vacca, John R. Biometric Technologies and Verification Systems. 2007. Elsevier.

7) Приговор Горно-Алтайского городского суда Республики Алтай от 08.09.2022 N 1-427/2022

8) Приговор Ковылкинского районного суда Республики Мордовия от 07.10.2022 по делу № 1-116/2022
9) Приговор Ленинского районного суда города Пензы от 17.01.2020 № 1-21/2020 (1-289/2019)
10) Приговор Октябрьского городского суда Республики Башкортостан от 14.09.2022 по делу № 1-240/2022