Секция «Административное право»

Применение принципа неизбыточности при обработке биометрических персональных данных

Научный руководитель – Терещенко Людмила Константиновна

Кривогин Максим Сергеевич

Аспирант

Национальный исследовательский университет «Высшая школа экономики», Факультет права, Москва, Россия

E-mail: mkrivogin@yandex.ru

Информационные технологии с каждым годом позволяют получать и обрабатывать все большее количество информации о физических лицах. В одних случаях это упрощает реализацию прав граждан, например, на свободу слова, поиск и передачу информации. В других случаях, наоборот, ограничивает право на неприкосновенность частной жизни. Применение биометрических технологий для сбора информации о гражданах зачастую заставляет государства вводить дополнительные ограничения на их использование.

В большинстве случаев особое законодательное регулирование биометрических персональных данных обусловлено их свойствами. Биометрические персональные данные являются уникальными по своей природе (ДНК, отпечатки пальцев) и относятся лишь к определенному человеку, что позволяет осуществлять их дальнейшее использование для идентификации физических лиц. Такая информация, а также содержащие ее материальные носители, становятся доступны для сбора и анализа другим лицам в процессе повседневной активности гражданина, независимо от его воли, что дает возможность производить накопление и обработку таких сведений скрытно, без уведомления субъекта персональных данных. Использование биометрических данных в криминалистических целях, их распространённость и сложность доказывания невиновности в случае обнаружения на месте преступления отпечатков пальцев или биологического материала подозреваемого также говорит о чувствительности данных сведений [1].

Учитывая приведенные свойства биотермической информации, а также правовую практику Европейского суда по правам человека в данной сфере, где хранение информации о ДНК и отпечатках пальцев граждан, которые не совершали противоправных действий, было признанно нарушением права на неприкосновенность частной жизни [7], особую значимость приобретают положения законодательства о персональных данных, направленные на ограничение возможности обработки данного вида сведений.

Основными критериями легитимности осуществления обработки персональных данных в рамках ФЗ РФ «О персональных данных» являются: наличие согласия субъекта, которое должно быть информированным, конкретными и сознательным, а также соблюдение принципов обработки персональных данных (ограничение обработки достижением цели, запрет объединения баз персональных данных, неизбыточность по отношению к целям обработки, точность и актуальность персональных данных).

Принцип неизбыточности персональных данных, который достаточно часто применяется в судебной практике для определения законности обработки персональных данных [3], не всегда может быть однозначно применен для защиты биометрических сведений, поскольку он направлен на учет «количественной», а не «качественной» избыточности персональных данных. Например, данный принцип позволяет ограничить количество собираемых сведений о сотруднике при его приеме на работу, однако при его применении не учитывается вид персональных данных (обычные или биометрические), поэтому в РФ отсутствуют какие-либо законодательные ограничения на использования контроля доступа в помещение работодателя по отпечаткам пальцев или сетчатке глаза.

Схожая позиция содержится и в правовой практике Российской Федерации, где суды, в спорах о законности обработки биометрических персональных данных, обращают внимание исключительно на наличие или отсутствие согласия гражданина [4]. В результате этого не происходит учета чувствительности данной информации, создаются предпосылки для ее распространения, что в условиях постоянного развития информационных технологий в данной сфере ведет к существенному ограничению прав субъекта персональных данных [2].

В то же время, в законодательстве отдельных стран Европейского Союза существует более рациональный подход к регулированию обработки биометрических персональных данных, который позволяет обеспечить как право на неприкосновенность частной жизни субъекта персональных данных, так и интересы компаний коммерческих организаций и государственных органов.

Достаточно интересным является подход Словении, где происходит введение нескольких критериев, позволяющих оператору осуществлять обработку биометрических персональных данных, в число которых входит необходимость охраны безопасности предприятия, защиты конфиденциальной информации, а также невозможность использования других средств для осуществления данных целей [5].

В других странах, например, во Франции, Португалии, Латвии для осуществления оператором обработки биометрических персональных данных, необходимо получить предварительное согласие национального органа по защите персональных данных [6]. В данном случае, для обеспечения надлежащей защиты личной информации частного лица, происходит частичное изменение ролей оператора и органа по защите персональных данных. Последний, вместо стандартного осуществления контроля над адекватностью соблюдения оператором принципа не избыточности персональных данных по отношению к целям обработки ex-post, производит оценивание ex-ante. Критерии такой оценки, во многом сводятся к возможности или невозможности использования оператором иных, более нейтральных технологий, для соответствующих целей.

Введение в российское законодательство требования обязательной оценки оператором возможности использования других средств перед осуществлением обработки биометрической информации позволит обеспечить надлежащее применение принципа неизбыточности персональных данных и гарантировать высокий уровень охраны прав субъектов персональных данных.

Источники и литература

1) Горелишвии Д. Постатейный комментарий к проекту закона «О персональных данных» // URL: https://goo.gl/px3xRg (дата обращения 16.02.2017)

2) Интернет видит все // URL: https://www.gazeta.ru/tech/2016/04/29_a_8204579.shtml (дата обращения 16.02.2017)

3) Савельев А.И. Электронная коммерция в России и за рубежом: правовое регулирование. 2-е изд. М.: Статут, 2016 // СПС «КонсультантПлюс».

4) Постановление Шарьинского районного суда, г. Кострома, дело № 5-124/2013 от 18 марта 2013 года

5) Data protection act of Slovenia No. 001-22-148/04 // URL: http://haa.su/I2w/ (дата обращения: 19.02.2017).

6) Data protection laws of the world // URL: https://www.dlapiperdataprotection.com/ (дата обращения: 18.02.2017).

7) S. and Marper v. the United Kingdom / URL: http://www.bailii.org/eu/cases/ECHR/2008/1581.html (дата обращения: 15.02.17)