УДК 340.132.1:004.65

Кривогин Максим Сергеевич

аспирант Национального исследовательского университета «Высшая школа экономики»

ПРЕДПОСЫЛКИ ФОРМИРОВАНИЯ СПЕЦИАЛЬНОЙ ПРАВОВОЙ ЗАЩИТЫ БИОМЕТРИЧЕСКИХ ПЕРСОНАЛЬНЫХ ДАННЫХ

Аннотация:
В статье рассматриваются предпосылки возникновения специального правового регулирования биометрических персональных данных. Исходя из анализа законодательства в сфере персональных данных отдельных стран, делается вывод о влиянии политического режима на уровень защиты специальных сведений о физических лицах. Выявлена зависимость между годом принятия закона о персональных данных и выделением биометрических персональных данных в обособленную категорию.

Ключевые слова:
биометрические персональные данные, неприкосновенность частной жизни, Россия, зарубежные страны, авторитарный политический режим, тоталитарный политический режим.

Krivogin Maxim Sergeyevich

PhD student, National Research University – Higher School of Economics

PREMISES OF ESTABLISHMENT OF SPECIAL LEGAL PROTECTION OF BIOMETRIC PERSONAL DATA

Summary:
The article deals with the premises of the special legal regulation of biometric personal data. Based on the analysis of legislation in the field of personal data protection in some countries, it is concluded that any political regime makes an impact on the level of protection of special information about persons. The author considers the dependence between the year of adoption of data protection law and distinguishing of biometric personal data as a particular category.

Keywords:
biometric personal data, privacy, Russia, foreign countries, authoritarian political regime, totalitarian political regime.

Несмотря на то что использование биометрических характеристик, в частности отпечатков пальцев, для идентификации человека практикуется достаточно давно, применение информационных технологий актуализирует данную проблему и выводит ее на новый уровень. Во многом это связано с тем, что информационные технологии позволяют с высокой степенью точности соотнести биометрические данные личности с информацией о ней, которая накапливается в государственных органах либо в частных организациях. Также сбор биометрической информации может быть дистанционным и скрытым, когда гражданин не ставится в известность о собираемых о нем сведениях. В связи с этим те права, которые гарантированы законодательством в сфере защиты персональных данных, например доступ субъекта к своим персональным данным, возможность получения информации об операторе персональных данных, не всегда могут быть реализованы. Использование биометрических персональных данных также затрагивает более широкую проблему – анонимность в публичных местах и ее связь с неприкосновенностью частной жизни. Поэтому для многих стран в связи с появлением биометрической идентификации существенным оказался вопрос о целесообразности применения обособленного правового регулирования такого вида сведений.

Многие европейские страны рассматривают возможность использования биометрической идентификации с большой осторожностью, связывая применение биометрических технологий с усиливающимся с каждым годом надзором за обществом, что в свою очередь рассматривается отдельными исследователями в качестве предпосылки к становлению авторитарного [1, p. 106] или тоталитарного [2, p. 54] политического режима. Другие авторы придают большую значимость не только информации, которой обладает государство демократического типа, соблюдающее правовые нормы, но также и тому факту, насколько информация является избыточной и какие последствия могут наступить для населения страны, если доступ к таким данным получат сторонники тоталитаризма [3, p. 280].

Аналогично регулированию специальных категорий персональных данных существенное влияние на признание биометрической информации в качестве категории персональных данных с повышенной правовой защитой оказывает политический режим. Те страны, которые определенное время в своей истории находились под влиянием тоталитарных или авторитарных режимов, а затем отвергли его, перейдя к демократическому, в большей мере стремятся предоставить дополнительные гарантии субъектам персональных данных.

Например, страны, воевавшие на стороне Германии во Второй мировой войне, а также большинство государств, оккупированных странами «оси», относят биометрическую информацию к чувствительным категориям персональных данных. К таким странам относятся: Австрия, Босния и Герцеговина, Италия, Македония, Румыния, Украина, Черногория, Чехия, Эстония [4]. Несмотря на то что в законодательстве некоторых стран, например Болгарии и Польши [5], в целом не упоминаются биометрические данные в качестве общей категории, отдельные их виды, например генетические, также могут относиться к специальным категориям.

В других государствах, которые также подверглись тоталитарному или авторитарному влиянию, может и не существовать дополнительной защиты в рамках отнесения биометрической информации к специальным категориям персональных данных. Однако, несмотря на это, для обработки такой информации могут применяться дополнительные требования. Например, во Франции, Португалии, Люксембурге, Латвии, Словении, Грузии, Македонии и Черногории для осуществления оператором обработки биометрических персональных данных существует необходимость 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 неизбыточности 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. Например, если доступ к лаборатории, осуществляющей исследования ядовитых веществ, происходит на основе сканирования отпечатков пальцев либо сетчатки глаза, то обработка персональных данных считается допустимой, когда получено согласие субъекта, так как необходимость защиты указанных веществ и возможный общественный ущерб от неправомерного доступа к ним являются значительными, контроль на основе обычных персональных данных не всегда может обеспечить необходимый уровень безопасности. В то же время использование таких систем для контроля доступа в магазин бытовой химии не может считаться оправданным, поскольку без ущерба для безопасности могут быть применены иные меры охраны.

Приведенный выше пример представляет собой тот случай, когда государство стремится ограничить накопление и использование персональных данных не только государственными органами, но также и коммерческими организациями. В то же время, ограничивая использование частными лицами некоторых категорий персональных данных, государство также ограничивает себя, поскольку отдельные силовые структуры могут получить доступ к такой информации, где проблематичен контроль за соблюдением правил обработки персональных данных и высока возможность тайного их накопления и использования.

Если рассматривать историю изменения законодательства в сфере защиты персональных данных в странах ЕС применительно к биометрической информации, то можно отметить существование тенденции включения биометрической информации в специальные категории персональных данных для стран, в которых законодательство о защите персональных данных было принято до 2001 г. В данном случае государства, имея длительно функционирующую по времени систему защиты персональных данных, более склонны к адаптации вновь возникающих угроз к уже устоявшимся категориям персональных данных, нежели чем к разработке новых категорий и переосмыслению отдельных аспектов регулирования. Это достигается либо путем отнесения биометрической информации к специальным (чувствительным) категориям персональных данных в рамках принятия поправок к законодательству, либо посредством разъяснений уполномоченного органа в сфере защиты персональных данных [7, с. 66].

Противоположная модель регулирования биометрических персональных данных применяется в других странах, где комплексное законодательство о защите персональных данных было принято после терактов 2001 г. в США, ставших толчком для ускоренного развития технологий, предназначенных для биометрической идентификации. В данном случае у стран отсутствуют как функционирующие модели регулирования персональных данных, так и судебная практика в этой сфере. Поэтому при построении системы регулирования персональных данных «с чистого листа» государства не сталкиваются с необходимостью адаптации новых моделей регулирования к уже действующим нормам и более свободно могут вводить новые категории персональных данных в законодательство. К таким странам можно отнести Италию (2003) [8], Словению (2004) [9], Россию (2006) [10], Черногорию (2008) [11], Грузию (2011) [12], Словакию (2013) [13], Казахстан (2013) [14], где помимо специальных персональных данных также существует дополнительное правовое регулирование и для биометрических категорий. При этом, несмотря на то что в результате введения новой категории персональных данных многие страны сталкиваются с проблемами их

регулирования (например, отнесение обычной фотографии или подписи на документе к биометрическим персональным данным), ни одно государство не стало делать шаг назад и исключать такие нормы из законодательства. Это обусловлено тем, что одновременно с совершением попыток обеспечения неприкосновенности частной жизни граждан от только возникающих угроз не всегда достаточно ясен сам предмет правового регулирования в этой сфере. Именно поэтому ученые, занимающиеся проблемами защиты персональных данных, призывают подходить к вопросу о включении в законодательство новых категорий персональных данных либо исключении существующих со всей тщательностью [15, p. 200]. Необходимо определить, насколько обособленное регулирование будет соответствовать объективной необходимости, действующему законодательству, а также учитывать социальные условия конкретной страны.

Таким образом, отнесение определенных типов информации к специальным категориям персональных данных, а также введение в законодательство дополнительных видов персональных данных не является произвольным, такое регулирование обусловлено историческими событиями, происходившими в государстве, влиянием политического режима, а также пониманием права на неприкосновенность частной жизни в рамках отдельной страны. Все европейские страны, которые подверглись оккупации войсками нацистской Германии, а также воевали на ее стороне, в той или иной форме отражают в законодательстве биометрические данные, распространяя на них режим персональных данных.

Ссылки:

1. Yue Liu N. Bio-Privacy: Privacy Regulations and the Challenge of Biometrics. New York, 2012. 354 p.
2. Staples W. Encyclopedia of Privacy. Cambridge, 2006. 512 p.
3. Mordini E. Second Generation Biometrics: The Ethical, Legal and Social Context. Berlin, 2012. 402 p.
4. Data protection laws of the world [Электронный ресурс]. URL: https://www.dlapiperdataprotection.com/ (дата обращения: 18.07.2016).
5. Global data privacy [Электронный ресурс]. URL: http://www.nortonrosefulbright.com/files/global-data-privacy-directory-52687.pdf (дата обращения: 18.07.2016).
6. Data protection laws of the world.
7. Ивановский В.П. Теоретические проблемы правовой защиты частной жизни в связи с использованием информационных технологий : дис. … канд. юрид. наук. М., 1998. 168 с.
8. Personal Data Protection Code – Legislative Decree no. 196 of 30 June 2003 [Электронный ресурс]. URL: http://194.242.234.211/documents/10160/2012405/Personal+Data+Protection+Code+-+Legislat.+Decree+no.196+of+30+June+2003.pdf (дата обращения: 22.08.2016).
9. Personal Data Protection Act of the Republic of Slovenia No. 001-22-148/04 [Электронный ресурс]. URL: https://www.coe.int/t/dghl/standardsetting/dataprotection/National%20laws/SLOVENIA_DP_LAW.pdf (дата обращения: 19.07.2016).
10. О персональных данных : федер. закон от 27 июля 2006 г. № 152-ФЗ // СЗ РФ. № 31. Ст. 3451.
11. Personal Data Protection Law 79/08 (Montenegro) [Электронный ресурс]. URL: http://www.azlp.me/images/stories/Zakon/personaldataprotectionlaweng.pdf (дата обращения: 19.07.2016).
12. Law of Georgia on Personal Data Protection № 141. December 28, 2011 [Электронный ресурс]. URL: https://www.coe.int/t/dghl/standardsetting/dataprotection/National%20laws/Georgia%20(Law%20of...)%20on%20Personal%20Data%20Protection%20as%20amended%2014%2005%202013.pdf (дата обращения: 19.07.2016).
13. Act No. 428/2002 Coll. on Protection of Personal Data (Slovak Republic) [Электронный ресурс]. URL: http://ec.europa.eu/justice/policies/privacy/docs/implementation/slovakia_428_02_en.pdf (дата обращения: 19.07.2016).
14. О персональных данных и их защите [Электронный ресурс] : закон Республики Казахстан от 21 мая 2013 г. № 94-V. URL: http://online.zakon.kz/Document/?doc_id=31396226 (дата обращения: 19.07.2016).
15. McCullagh K. Data Sensitivity: Proposals for Resolving the Conundrum // Journal of International Commercial Law and Technology. 2007. Vol. 2, issue 4. P. 197–201.

References:

Data protection laws of the world 2016, viewed 18 July 2016, <https://www.dlapiperdataprotection.com/>.

Global data privacy 2016, viewed 18 July 2016, <http://www.nortonrosefulbright.com/files/global-data-privacy-directory-52687.pdf>.

Ivanovskiy, VP 1998, *Theoretical problems of legal protection of privacy in connection with the use of information technology*: PhD thesis, Moscow, 168 p., (in Russian).

McCullagh, K 2007, 'Data Sensitivity: Proposals for Resolving the Conundrum', *Journal of International Commercial Law and Technology,* vol. 2, issue 4, pp. 197-201.

Mordini, E 2012, *Second Generation Biometrics: The Ethical, Legal and Social Context,* Berlin, 402 p.

Staples, W 2006, *Encyclopedia of Privacy,* Cambridge, 512 p.

Yue Liu, N 2012, *Bio-Privacy: Privacy Regulations and the Challenge of Biometrics,* New York, 354 p.