

Обеспечение информационной безопасности как гарантия прав человека



А.В. Туликов

аспирант кафедры теории и истории права Национального исследовательского университета «Высшая школа экономики». Адрес: 101000, Российская Федерация, Москва, ул. Мясницкая, 20. E-mail: alex.amissa@yandex.ru



Аннотация

Статья посвящена актуальной проблеме соотношения информационной безопасности и прав человека. В России понятие «информационная безопасность», как правило, раскрывается через «состояние защищенности жизненно важных интересов личности, общества и государства». В США и Европейском Союзе определение «информационная безопасность» связывается с правовыми принципами конфиденциальности, целостности и доступности информации и информационных систем. Реализация данных принципов позволяет обеспечить баланс интересов различных участников правоотношений, выступая, таким образом, гарантией прав человека. Влияние современных технологий проявляется прежде всего в сфере личных прав, среди которых особое место занимает право на неприкосновенность частной жизни. С одной стороны, в качестве гарантий права на неприкосновенность частной жизни выступают меры, непосредственно направленные на защиту данного права. С другой стороны, при установлении ограничений права на неприкосновенность частной жизни соответствующие гарантии должны предупреждать возможные злоупотребления. В дополнение к принципам конфиденциальности, целостности и доступности выработаны специальные правовые принципы защиты права на неприкосновенность частной жизни. Основными механизмами защиты права на неприкосновенность частной жизни, которые находят выражение в данных принципах, являются согласие субъекта персональных данных на обработку персональных данных и его уведомление о такой обработке. В то же время с развитием интернет-технологий данные механизмы оказываются недостаточными для соблюдения права человека на неприкосновенность частной жизни. Развитие гарантий данного права осуществляется путем создания дополнительных механизмов защиты конфиденциальности, которые выражены в предъявлении специфических требований в сфере сбора и обработки личной информации. Совершенствование технологий также приводит к появлению новых угроз национальной безопасности и информационной безопасности государства как одной из ее составляющих. Необходимость их защиты становится основанием для ограничения права на неприкосновенность частной жизни. Соразмерность ограничений целям их установления выступает гарантией прав человека и информационной безопасности личности. В государствах с демократическими правовыми режимами, как правило, установлен приоритет прав человека перед обеспечением национальной безопасности.



Ключевые слова

права человека, информационная безопасность, правовые принципы, ограничение прав, угрозы безопасности, неприкосновенность частной жизни.

Библиографическое описание: Туликов А.В. Обеспечение информационной безопасности как гарантия прав человека // Право. Журнал Высшей школы экономики. 2015. № 2. С. 50–60.

JEL: K19, УДК: 342.76

Права человека представляют собой фундамент современного правового государства. На постиндустриальном этапе развития защита прав человека приобретает особый характер. Совершенствование информационно-коммуникационных технологий сопровождается расширением возможностей их недобросовестного использования, которое создает угрозы информационной безопасности и может приводить к нарушениям прав человека. В связи с этим возникает проблема соотношения информационной безопасности и прав человека, прежде всего, права на неприкосновенность частной жизни, исследованию которой и посвящена настоящая статья.

В России понятия «безопасность», «информационная безопасность» и «национальная безопасность» раскрываются через «состояние защищенности жизненно важных интересов личности, общества и государств»¹. Информационная безопасность в данном случае определяется как состояние защищенности национальных интересов Российской Федерации в информационной сфере, состоящей из совокупности сбалансированных интересов личности, общества и государства, от внутренних и внешних угроз. Правовая доктрина в целом следует данным положениям².

В отечественной правовой литературе также используется определение «информационной безопасности» через состояние защищенности информационной сферы, при котором невозможна реализация известных угроз в отношении составляющих ее элементов³. При этом понятие «информационная безопасность» рассматривается как более общая категория по отношению к понятию «защита информации», в котором акцент делается на комплексе мероприятий и действий, направленных на обеспечение безопасности информации⁴. В данном случае речь идет о состоянии защищенности информации, а не интересов личности, общества и государства.

В правовой доктрине США и Европейского Союза определение «информационной безопасности» осуществляется через перечисления конкретных элементов информационной сферы, на защиту которых она направлена⁵, и связывается с правовыми принципами конфиденциальности, целостности и доступности информации и информационных систем⁶.

¹ См.: Доктрина информационной безопасности Российской Федерации, утв. Президентом Российской Федерации от 9 сентября 2000 г. № Пр-1895 // Российская газета. 2000. 28 сентября; Стратегия национальной безопасности Российской Федерации до 2020 года, утв. Указом Президента Российской Федерации от 12 мая 2009 г. № 537 // СЗ РФ. 2009. № 20. Ст. 2444.

² См.: Полякова Т.А. Правовое обеспечение информационной безопасности при построении информационного общества в России: дис... д-ра юрид. наук. М., 2008. С. 112; Лопатин В.Н. Информационная безопасность России: дис... д-ра юрид. наук. М., 2003. С. 91.

³ Речь может идти о таких элементах как информация, информационная инфраструктура, субъекты и система регулирования информационных отношений и т.д. См.: Соколов М.С. Информационная безопасность. К вопросу о содержании понятия «информационная безопасность» // Закон и право. 2011. № 5. С. 9–14; Стрельцов А.А. Теоретические и методологические основы правового обеспечения информационной безопасности России: дис... д-ра юрид. наук. М., 2005. С. 70.

⁴ См.: Швецова Т.В. Информационная безопасность, безопасность информации, защита информации: соотношение понятий // Вестник Московского университета МВД России. 2007. № 2. С. 43–45.

⁵ В данном случае информационная безопасность может предусматривать защиту информационных объектов, которые охватывают не только собственно информацию, но также компьютерное программное обеспечение, технические средства, сети и инфраструктуру, обеспечивающую информационные системы. См.: Information Security and Privacy: a Practical Guide for Global Executives, Lawyers, and Technologists. Shaw T. (ed.). Chicago: American Bar Association, 2011. P. 17.

⁶ См.: Grama J. Legal Issues in Information Security. Sudbury: Jones and Bartlett Publishers, 2010. P. 4. Указанные принципы впервые были сформулированы в таких международных стандартах, как ISO/IEC. ISO/IEC 27002: Code of Practice for Information Security Management 2005, ГОСТ Р ИСО/МЭК 13335-

Реализация данных принципов позволяет обеспечить баланс интересов различных участников правоотношений, выступая, таким образом, гарантией прав человека в сфере обеспечения информационной безопасности.

При соблюдении принципа конфиденциальности ознакомление с конфиденциальной информацией, ее обработка и предъявление требования о ее предоставлении допускаются только для лица, которое обладает правом доступа к такой информации. Роль принципа конфиденциальности заключается в предотвращении вреда, который может быть причинен общественным отношениям в результате неправомерного предоставления и распространения информации, сохраняемой в тайне в силу ее значения для безопасности личности, общества или государства. Данному принципу соответствует своего рода право «таить» информацию, т.е. сохранять ее в тайне, ограничивать доступ третьих лиц к ней, контролировать ее целевое использование.

В отличие от конфиденциальности обеспечение целостности информации стало актуальным в процессе развития компьютерных технологий и появления возможностей несанкционированного доступа к информации с целью внесения в нее изменений или уничтожения. Лицо, которое обладает информацией или правом доступа к информации, вправе требовать обеспечения ее целостности, а также в ряде случаев целостности носителя информации, т.е. сохранения их в оригинальном, неизменном виде, обеспечения невмешательства в структуру (форму) и содержание информации. Данный принцип направлен на обеспечение подлинности информации, которая позволяет сохранять между участниками общественных отношений необходимый уровень доверия и уверенности в том, что они имеют дело с оригинальной информацией и ее источником, а не с подделкой или модификацией.

Принцип доступности играет важную роль в формировании гарантий права человека на доступ к информации. Данный принцип направлен на предотвращение ограничения и создание условий доступа к социально-значимой информации, прежде всего при взаимодействии человека с органами власти, а также к иной информации, предоставления которой он вправе требовать. Этот принцип лежит в основе реализации мер по обеспечению доступа к информации о деятельности государственных органов и органов местного самоуправления, экологической информации, в том числе путем размещения информации на официальных сайтах органов и организаций.

Влияние современных информационно-коммуникационных технологий проявляется прежде всего в сфере личных прав, среди которых особое место занимает право на неприкосновенность частной жизни. Следует согласиться с утверждением, что «без информационной безопасности не может быть неприкосновенности частной жизни»⁷. Поэтому обеспечение информационной безопасности личности составляет основу правовой защиты неприкосновенности частной жизни. С развитием технологий существенно увеличиваются объемы и скорость обмена информацией, расширяется спектр возможных способов ее сбора, обработки, предоставления и распространения. В результате вред, который может быть причинен индивиду путем раскрытия определенной информации или в связи с сохранением ее в тайне, также возрастает. Данные процессы

1-2006 «Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий», где они изложены в техническом контексте. В правовой доктрине США и Европейского Союза они обретают правовое содержание и рассматриваются как правовые принципы.

⁷ Information Security and Privacy: A Practical Guide for Global Executives, Lawyers and Technologists. P. 23.

углубляют противоречия, которые вызваны противопоставлением принципов конфиденциальности и доступности, права сохранять информацию в тайне и права доступа к такой информации. Такие противоречия возникают как в частноправовых, так и в публично-правовых отношениях.

В частноправовых отношениях соответствующие противоречия выражены в том, что для поддержки свободы выражения, свободы договора и предпринимательской деятельности в условиях автоматизации бизнес-процессов, внедрения компьютерных и интернет-сервисов необходимо расширение возможностей доступа к личной информации и ее последующего использования для коммерческих и иных организаций. В то же время рост неблагоприятных последствий для личности в связи с подобным использованием личной информации требует ограничения доступа к ней третьих лиц, контроля ее использования и создания дополнительных механизмов защиты права на неприкосновенность частной жизни.

В публично-правовых отношениях все чаще используются специализированные государственные информационные системы, для полноценного функционирования которых необходимо расширение полномочий органов власти в сфере обработки в автоматизированном режиме различного рода личной информации. Данные процессы наряду с мерами, которые предпринимаются для обеспечения национальной безопасности, приводят к формированию в законодательстве ограничений права на неприкосновенность частной жизни. При этом предотвращение незаконного вмешательства в частную жизнь и злоупотреблений со стороны органов власти становится одним из приоритетных направлений обеспечения информационной безопасности личности⁸.

С одной стороны, в качестве гарантий права на неприкосновенность частной жизни выступают меры по обеспечению информационной безопасности, непосредственно направленные на защиту данного права. При этом выработка соответствующих мер осуществляется путем конкретизации правовых принципов конфиденциальности, целостности и доступности с учетом существа права на неприкосновенность частной жизни и его возможных нарушений.

С другой стороны, при установлении ограничений права на неприкосновенность частной жизни соответствующие гарантии должны предупреждать возможные злоупотребления такими ограничениями, приводящие к угрозам информационной безопасности личности. Как справедливо отмечается в отечественной правовой доктрине «панaceей от таких злоупотреблений... служит принцип соразмерности и выводимая из него формула о запрете чрезмерных ограничений. Этот запрет (в процессе законодательной и правоприменительной деятельности) означает, что допустимые по Конституции и международным документам о правах человека ограничения должны по содержанию и объему соответствовать целям вводимых ограничений и могут применяться только для защиты иных равнозначных правовых ценностей»⁹.

В дополнение к принципам конфиденциальности, целостности и доступности в правовой доктрине выработаны специальные правовые принципы защиты права на

⁸ В публично-правовых отношениях происходят и обратные процессы, когда в условиях формирования электронного государства к органам власти предъявляются дополнительные требования в отношении открытости и доступности информации об их деятельности и создания гарантий права на доступ к информации. Данному праву противостоит необходимость сохранения определенных категорий информации в целях обеспечения национальной безопасности, которая выражается в форме придания такой информации правового режима государственной или служебной тайны.

⁹ Права человека: учебник для вузов / отв. ред. Е.А. Лукашева. М.: НОРМА, 2001. С. 301.

неприкосновенность частной жизни¹⁰, в которых определяются пределы и условия осуществления данного права. В связи с принципом конфиденциальности такие специальные правовые принципы определяют возможность сбора персональных данных только законными и добросовестными средствами и для конкретно определенных целей при условии предварительного уведомления или согласия субъекта персональных данных, обеспечения их защиты от таких рисков как потеря или несанкционированный доступ, уничтожение, использование, изменение или раскрытие данных. Наряду с принципом целостности применяется принцип, при соблюдении которого персональные данные должны соответствовать целям их использования и в соответствии с такими целями должны быть точными, полными и актуальными. Принцип доступности дополняется принципами, которые создают условия для доступа субъекта персональных данных к информации о наличии у оператора и характере обрабатываемых им персональных данных такого субъекта, основных целях их использования, личности и месте нахождения оператора данных, а также наделяют субъектов персональных данных дополнительными правами, включая возможность уничтожения, исправления, дополнения или изменения своих персональных данных. Данные принципы в настоящее время отражены как в национальном¹¹, так и в международном праве¹².

Основными механизмами защиты права на неприкосновенность частной жизни, которые находят выражение в соответствующих правовых принципах, являются согласие субъекта персональных данных на обработку персональных данных и его уведомление о такой обработке. При этом конфиденциальность личной информации обеспечивается путем предоставления доступа или возможности сбора и обработки такой информации только тем лицам, которые получили соответствующее согласие ее обладателя. Если доступ или возможности сбора и обработки предоставляются на основании закона, то обязательным является уведомление об обработке персональных данных их обладателя. Уведомление также обязательно при иных случаях, определенных субъектом персональных данных или установленных законодательством, например, при нарушении конфиденциальности или целостности персональных данных. Указанные механизмы предоставляют субъекту персональных данных правовые возможности контроля за их использованием и, соответственно, гарантии неприкосновенности его частной жизни.

В то же время с развитием сети Интернет и интернет-сервисов, созданием массивных коллекций информации (известных как «Большие данные»¹³) и развитием облачных тех-

¹⁰ Данные правовые принципы были сформированы на базе так называемых, Справедливых информационных принципов, разработанных ОЭСР в 1980 г. См.: OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data // URL: <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm> (дата обращения: 26.04. 2015)

¹¹ Например, они содержатся в Акте Канады о защите личной информации и электронных документов 2000 г. (PIPEDA) и национальном законодательстве государств-членов Европейского Союза. Они также получили отражение в Федеральном законе от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (СЗ РФ. 2006 г. № 31 (часть I). Ст. 3451). В данном Федеральном законе изложение принципов близко к подходу, принятому в Директиве 95/46/ЕС Европейского Парламента и Совета Европейского Союза о защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных

¹² См. напр.: Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных от 28 января 1981 г. // Бюллетень международных договоров. 2014. № 4. С. 13–21.

¹³ См., например: Cumbley R., Church P. Is “Big Data” Creepy? // Computer Law and Security Review. 2013. № 29. P. 601–609.

нологий¹⁴ данные механизмы оказываются недостаточными для соблюдения права человека на неприкосновенность частной жизни. Фактически пользователь постепенно утрачивает контроль над использованием своих персональных данных. Так, при использовании облачных технологий процесс передачи и обработки данных становится для пользователя неопределенным и на практике может заключаться в дроблении информации и ее размещении на серверах, расположенных в различных национальных юрисдикциях.

Кроме того, большинство пользователей дает согласие на обработку их персональных данных, должным образом не ознакомившись с его условиями, не понимая правовых последствий такого согласия и не предвидя последующего использования своей личной информации¹⁵. В результате механизм получения согласия пользователя на обработку его личной информации становится слабой, по существу, формальной гарантией, не обеспечивающей конфиденциальности личной информации и реальной защиты права на неприкосновенность частной жизни.

Для современной электронной коммерции предварительное согласие и последующее уведомление субъекта персональных данных, равно как правовые ограничения применения облачных технологий создают препятствия развитию бизнеса и внедрению инноваций. В связи с этим ограничения свободы предпринимательской деятельности в Интернете, обусловленные использованием традиционных механизмов защиты права на неприкосновенность частной жизни, становятся избыточными.

Развитие гарантий данного права осуществляется путем создания дополнительных по отношению к согласию субъекта персональных данных и его уведомлению механизмов защиты конфиденциальности, которые выражены в предъявлении специфических требований к лицам, осуществляющим сбор и обработку личной информации. Такие требования могут заключаться в установлении специального правового режима так называемых чувствительных данных, ограничении сбора определенной личной информации в цифровой форме, в том числе геолокационных и биометрических данных, ограничении автоматического принятия юридически значимых решений. Формой правовой защиты персональных данных также является ограничение их передачи в национальные юрисдикции, где не обеспечиваются необходимые гарантии права на неприкосновенность частной жизни. Одновременно возрастают требования к технической защите персональных данных для предотвращения неавторизованного доступа к данным, устранению последствий их раскрытия или компрометации.

В Европейском Союзе право на неприкосновенность частной жизни рассматривается как фундаментальное право¹⁶. Его защита гарантируется ст. 8 Европейской конвенции о защите прав человека и основных свобод 1950 г. (далее — Конвенция 1950 г.)¹⁷ и конституциями государств-членов ЕС. Приоритет полного контроля личности над его

¹⁴ См., например: *King N.J., Raja V.T. Protecting the Privacy and Security of Sensitive Customer Data in the Cloud // Computer Law and Security Review. 2012. № 28. P. 308–319; Ryan P., Falvey S. Trust in the Clouds // Computer Law and Security Review. 2012. № 28. P. 513–521.*

¹⁵ См., напр.: *McDonald A.M., Cranor L.F. The Cost of Reading Privacy Policies // I/S: A Journal of Law and Policy for the Information Society. 2008. Vol. 4. P.560.* В данной статье указывается на 244 часа в год, которое нужно было бы потратить пользователям, чтобы ознакомиться со всеми политиками конфиденциальности на сайтах, которые они посещают в течение года, — это чуть больше половины времени, проводимого в сети Интернет.

¹⁶ См. например: *Communication of the European Commission, Strategy for the Effective Implementation of the Charter of Fundamental Rights by the European Union, COM (2010) 573/4, Brussels, 19.10.2010 // URL: http://ec.europa.eu/justice/news/intro/doc/com_2010_573_en.pdf (дата обращения: 26.04. 2015)*

¹⁷ *СЗ РФ, 2001. № 2. Ст. 163.*

персональными данными перед традиционными демократическими свободами (свободой предпринимательской деятельности и свободой слова) лежит в основе нескольких поколений национальных законов в сфере защиты неприкосновенности частной жизни, нормативных правовых актов ЕС и решений Европейского суда по правам человека¹⁸.

В отличие от ЕС в США, где в меньшей степени проявляется патерналистская функция государства, специальные требования в области обработки персональных данных установлены только в наиболее чувствительных сферах¹⁹. В остальных сферах государство отдает приоритет саморегулированию, в основе которого лежат свобода предпринимательской деятельности, свобода договора, свобода слова и печати²⁰. Государство воздействует на общественные отношения путем издания различного рода рекомендаций и политических заявлений²¹.

Несмотря на различия между вышеприведенными подходами, следует также отметить тенденцию к их сближению. Так, в ЕС Директива о защите данных 95/46/ЕС запрещает передачу персональных данных пользователей-резидентов в государства, не входящие в Европейское экономическое сообщество. Исключением является «передача персональных данных в третьи страны, которые обеспечивают адекватный уровень защиты». Признается, что в США такая защита обеспечивается, хотя и имеются исключения. Так, передача персональных данных из ЕС в США допускается, только если оператор является членом Соглашения о безопасной гавани²² или согласился с иными договорными условиями, которые были установлены, чтобы обеспечить адекватную защиту персональных данных.

Развитие технологий приводит к появлению угроз национальной безопасности и информационной безопасности государства как одной из ее составляющих. Необходи-

¹⁸ См., например: Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González. Case C-131/12. В данном деле фактически было признано «право быть забытым», которое предоставило пользователям из ЕС правовую возможность требовать удаления из поисковых запросов определенной информации о своем прошлом. См. также: General Data Protection Regulation (GDPR); European Parliament Legislative Resolution of March 12, 2014 on the Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation) // URL: <http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0212&language=EN> (дата обращения: 26.04.2015). В этих документах, в частности, планируется предусмотреть «право быть забытым», а также урегулировать некоторые другие аспекты использования персональных данных в цифровых сетях.

¹⁹ Например, в США такими сферами являются сбор данных с помощью онлайн-сервисов о детях младше 13 лет, финансовыми институтами о их клиентах, бюро кредитных историй о клиентах и медицинскими работниками о пациентах, а также некоторые другие области, в которых приняты специальные законы. См.: Children's Online Privacy Protection Act (1998), Gramm-Leach-Bliley Act (1999), Fair Credit Report Act of 1992, Health Insurance Portability and Accountability Act (HIPAA) (1996), Electronic Communications Privacy Act (1986), Family and Educational Privacy Act (1974), Video Privacy Protection Act (1988), Telephone Customers Protection Act (1994), Drivers Privacy Protection Act (1994), Privacy Act (1974).

²⁰ См.: Crounse S. The Fair Information Principles: A Comparison of U.S. and Canadian Privacy Policy as Applied to the Private Sector. NY: Rochester Institute of Technology, ProQuest, UMI Dissertations Publishing. 2009. 174 p.

²¹ Защита неприкосновенности частной жизни также может осуществляться в соответствии с законодательством о защите прав потребителей с учетом решений Федеральной торговой комиссии и законодательством штатов в сфере деликтов применительно к правонарушениям, связанным с причинением конкретного имущественного вреда.

²² Соглашение регулирует стандарты трансатлантического обмена данными таких компаний, как Google, Microsoft и Facebook.

димось защиты данных ценностей становится основанием для ограничения права на неприкосновенность частной жизни. Соразмерность ограничений целям их установления выступает гарантией прав человека и информационной безопасности личности. Государство всегда более оперативно реагирует на возможности, которые предоставляют новые информационно-коммуникационные технологии для защиты публичных, нежели частных интересов. Это обусловлено тем, что устойчивость функционирования институтов публичной власти, сохранение правопорядка является необходимой предпосылкой соблюдения прав человека.

Большинство государств отреагировало на возросшие в последнее время угрозы национальной безопасности путем расширения полномочий органов власти по доступу к личной информации, ее сбору и обработке, которые в настоящее время не ограничены какими-то отдельными категориями информации. При этом в различных государствах подходы к обеспечению соразмерности принимаемых мер по обеспечению национальной безопасности также могут отличаться.

В государствах с демократическими правовыми режимами, как правило, установлен приоритет прав человека перед обеспечением национальной безопасности²³. Такой приоритет выражается в том, что меры по обеспечению национальной безопасности, связанные со сбором и обработкой соответствующей информации, принимаются при соблюдении специальной процедуры, которая обеспечивает их соразмерность возникающим угрозам. В основе данного подхода лежат положения Конвенции 1950 г.²⁴, в которой определены условия ограничения права человека на неприкосновенность частной жизни — «установление ограничения только законом» и «необходимость в демократическом обществе». Ограничение должно соответствовать целям его установления. Это позволяет не только определить целесообразность или обоснованность установления или применения подобного ограничения, но также оценить возможность эффективного достижения тех же целей в отсутствии ограничения права или его меньшем ограничении.

Для своевременного выявления фактов несоразмерности ограничений прав человека угрозам информационной безопасности и последствиям их проявления могут быть созданы специализированные государственные органы и уполномоченные по правам человека, подконтрольные представительной власти²⁵. Как отмечают в зарубежной литературе, «обеспечение неприкосновенности частной жизни не должно ограничиваться тем, что законодатели, судьи и государственные служащие уделяют ей достаточно внимания. Они также должны обеспечить постоянный контроль, чтобы убедиться, что неприкосновенность частной жизни может играть важную роль в качестве противовеса перед лицом новых угрожающих событий»²⁶. В связи с этим Европейский суд по правам человека указывает, что «надзор за мерами наблюдения может осуществляться на трех этапах: когда наблюдение санкционировано, во время его проведения и после того, как

²³ См., например: *Goncalves M.E., Jesus I.A.* Security Policies and the Weakening of Personal Data Protection in the European Union // *Computer Law and Security Review*. 2013. № 29. P. 255–263.

²⁴ СЗ РФ. 2001. № 2. Ст. 163.

²⁵ Такие органы созданы во многих государствах-членах ЕС. Примером также является Канадский комиссар по неприкосновенности частной жизни (Canadian Privacy Commissioner), который подотчетен Парламенту и рассматривается как основной защитник прав на неприкосновенность частной жизни граждан Канады.

²⁶ *Coudert F.* When Video Cameras Watch and Screen: Privacy Implications of Pattern Recognition Technologies // *Computer Law and Security Review* 26 (2010). P. 381.

оно закончилось. В процессе надзора ценности демократического общества должны соблюдаться как можно более добросовестно...»²⁷.

Чем меньше значение демократических ценностей в политическом режиме, тем большую роль играет обеспечение национальной безопасности для сохранения существующего порядка управления государством, следствием которого является установление различных ограничений прав человека, включая право на неприкосновенность частной жизни. Согласно позиции Европейского суда по правам человека, выраженной в деле «Класс и другие против Германии», «право тайного наблюдения за гражданами, которое характерно для полицейского государства, терпимо в соответствии с Конвенцией только тогда, когда оно строго необходимо для сохранения демократических институтов»; государства «не могут во имя борьбы против шпионажа и терроризма предпринимать любые действия, которые они считают подходящими»²⁸.

Таким образом, в условиях развития технологий обеспечение информационной безопасности выступает одной из важнейших гарантий прав человека. В основе таких гарантий лежит соблюдение принципов конфиденциальности, целостности и доступности информации и информационных систем. Для обеспечения информационной безопасности личности осуществляется выработка специальных правовых принципов защиты права на неприкосновенность частной жизни, а также дополнительных механизмов его защиты, связанных с установлением специфических требований в сфере сбора и обработки личной информации. При обеспечении национальной безопасности и информационной безопасности государства как одной из ее составляющих важнейшей гарантий прав человека выступает соблюдение принципа соразмерности при их ограничении. Реализация данных принципов и механизмов защиты прав человека при обеспечении информационной безопасности может принимать различные формы, которые зависят от правовых традиций и политического режима государства.



Библиография

- Лопатин В.Н. Информационная безопасность России: дис... д-ра юрид. наук. М., 2003. 433 с.
- Полякова Т.А. Правовое обеспечение информационной безопасности при построении информационного общества в России: дис... д-ра юрид. наук. М., 2008. 437 с.
- Права человека: учебник для вузов / отв. ред. Е.А. Лукашева. М.: НОРМА, 2001. 573 с.
- Соколов М.С. Информационная безопасность. К вопросу о содержании понятия «информационная безопасность» // Закон и право. 2011. № 5. С. 9–14.
- Стрельцов А.А. Теоретические и методологические основы правового обеспечения информационной безопасности России: дис... д-ра юрид. наук. М.: РГБ, 2005. 371 с.
- Швецова Т.В. Информационная безопасность, безопасность информации, защита информации: соотношение понятий // Вестник Московского университета МВД России. 2007. № 2. С. 43–45.
- Cumbley R., Church P. Is «Big Data» Creepy? // Computer Law and Security Review. 2013. № 29. P. 601–609.
- Coudert F. When Video Cameras Watch and Screen: Privacy Implications of Pattern Recognition Technologies // Computer Law and Security Review. 2010. № 26. P. 377–384.
- Crounse S. The Fair Information Principles: A Comparison of U.S. and Canadian Privacy Policy as Applied to the Private Sector. N.Y.: Rochester Institute of Technology, UMI Dissertations Publishing, 2009. 174 p.

²⁷ Klass and Others v. Germany, § 56, Series A, № 28.

²⁸ Ibidem.

- Grama J. Legal Issues in Information Security. Sudbury: Jones and Bartlett Publishers, 2010. 526 p.
- Goncalves M.E., Jesus I.A. Security policies and the weakening of personal data protection in the European Union // Computer Law and Security Review. 2013. № 29. P. 255–263.
- Information Security and Privacy: a Practical Guide for Global Executives, Lawyers and Technologists. T. Shaw, ed. Chicago: American Bar Association, 2011. 395 p.
- King N.J., Raja V.T. Protecting the Privacy and Security of Sensitive Customer Data in the Cloud // Computer Law and Security Review. 2012. № 28. P. 308–319.
- McDonald A.M., Cranor L.F. The Cost of Reading Privacy Policies // Journal of Law and Policy for the Information Society. 2008. Vol. 4. P. 540–565.
- Ryan P., Falvey S. Trust in the Clouds // Computer Law and Security Review. 2012. № 28. P. 513–521.
- Silver D. National Security and Transparency: The Legal Frameworks and Factors Federal Courts Use to Balance Competing Democratic Values. PhD Diss. Chapel Hill, 2009. 313 p.

Information Security as a Guarantee for Human Rights



Alexey Tulikov

Postgraduate Student, Department of History and Theory of Law, Law Faculty. Address: 20 Myasnitskaya Str., Moscow, 101000, Russian Federation. E-mail: alex.amissa@yandex.ru



Abstract

The article features a topical issue of the correlation between information security and human rights. The Russian concept of information security is interpreted as a state of safety for the vital interests of a person, society and state. In the US and EU, the definition to information security is associated with the principles of confidentiality, integrity and accessibility to information or information systems. Implementing both principles allows ensuring a balance of interests for various participants of legal relations and hence providing guarantee of human rights in the area of information security. The influence of modern technologies is evident primarily in personal rights in which the right to privacy makes a special domain. On the one hand, the measures to ensure information security targeting the protection of the right guarantee the right of privacy. On the other hand, when restricting the right to privacy, appropriate guarantees should prevent possible abuses with such restrictions which cause the threats to information security of a person. Besides the confidentiality, integrity and accessibility principles, special legal principles were developed to determine the limits and terms to implement the right to privacy. The major mechanisms to protect the right to privacy in the principles are the consent for personal data processing and the notification of it. At the same time, with the development of Internet technologies, such mechanisms are insufficient to respect the right to privacy. The development of guarantees for the right is implemented by creating additional mechanisms of protection and confidentiality expressed in special requirements to collecting and processing personal information. Modern technologies lead to new threats to national security and state information security. The need to protect such concepts is a reason to restrict the right to privacy. The balance between such restrictions and aims serves as a guarantee of human rights and personal information security. The states with democratic legal regimes tend to stipulate the priority of human rights to national security. The less is the significance of democratic values in a political regime, a greater role is given to ensuring national security to protect the existing model of state governance. It leads to setting various restrictions to human rights including the right to privacy.



Keywords

human rights, information security, legal principles, rights limitations, security threats, privacy.

Citation: Tulikov A.V. (2015) Information Security as a Guarantee for Human Rights. *Pravo. Zhurnal Vysshey shkoly ekonomiki*, no 2, pp. 50–60 (in Russian).



References

- Coudert F. (2010) When Video Cameras Watch and Screen: Privacy Implications of Pattern Recognition Technologies. *Computer Law and Security Review*, no 26, pp. 377–384.
- Crounse S. (2009) *The Fair Information Principles: A Comparison of U.S. and Canadian Privacy Policy as Applied to the Private Sector*. N.Y.: Rochester Institute of Technology, ProQuest, UMI Dissertations Publishing, 174 p.
- Cumbley R., Church P. (2013) Is “Big Data” Creepy? *Computer Law and Security Review*, no 29, pp. 601–609.
- Grama J. (2010) *Legal Issues in Information Security*. Sudbury: Jones and Bartlett Publishers, 526 p.
- Goncalves M.E., Jesus I.A. (2013) Security policies and the weakening of personal data protection in the European Union. *Computer Law and Security Review*, no 29, pp. 255–263.
- King N.J., Raja V.T. (2012) Protecting the Privacy and Security of Sensitive Customer Data in the Cloud. *Computer Law and Security Review*, no 28, pp. 308–319.
- Lopatin V.N. (2003) Informatsionnaya bezopasnost' Rossii (*Diss. Doct. Jurid. Nauk*) [Information Security of Russia (Doctor of juridical sciences dissertation)]. Moscow, 433 p. (in Russian)
- Lukasheva E.A. (ed.) (2001) *Prava cheloveka. Uchebnik dlya vuzov* [Human Rights. Textbook]. Moscow: Norma, 573 p. (in Russian)
- McDonald A.M., Cranor L.F. (2008) The Cost of Reading Privacy Policies. *A Journal of Law and Policy for the Information Society*, vol. 4, pp. 540–565.
- Polyakova T.A. (2008) *Pravovoe obespechenie informatsionnoy bezopasnosti pri postroenii informatsionnogo obshchestva v Rossii (Diss. Doct. Jurid. Nauk)* [Ensuring Legal Guarantees to Information Security in Russian Information Society (Doctor of juridical sciences dissertation)]. Moscow, 437 p. (in Russian)
- Ryan P., Falvey S. (2012) Trust in the Clouds. *Computer Law and Security Review*, no 28, pp. 513–521.
- Shaw T. (ed.) (2011) *Information Security and Privacy: a Practical Guide for Global Executives, Lawyers and Technologists*. Chicago: American Bar Association, 395 p.
- Shvetsova T.V. (2007) Informatsionnaya bezopasnost', bezopasnost' informatsii, zashchita informatsii: sootnoshenie ponyatiy [Information Security, Security of Information, Protection of Information: Correlation of Concepts] *Vestnik Moskovskogo universiteta MVD*, no 2, pp. 43–45 (in Russian)
- Silver D. (2009) *National Security and Transparency: The Legal Frameworks and Factors Federal Courts Use to Balance Competing Democratic Values (PhD Diss.)*. Chapel Hill: University of North Carolina, 313 p.
- Sokolov M.S. (2011) Informatsionnaya bezopasnost'. K voprosu o sodержanii ponyatiya «informatsionnaya bezopasnost'» [Information Security. On the Concept of Information Security]. *Zakon i pravo*, no 5, pp. 9–14 (in Russian).
- Strel'tsov A.A. (2005) *Teoreticheskie i metodologicheskie osnovy pravovogo obespecheniya informatsionnoy bezopasnosti Rossii (Diss. Doct. Jurid. Nauk)* [Theoretical and Methodological Fundamentals of Legal Guarantees for Information Security of Russia (Doctor of juridical sciences dissertation)]. Moscow, 371 p. (in Russian)