Федеральное государственное автономное образовательное
учреждение высшего образования
**«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ
«ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»**

На правах рукописи

Туликов Алексей Викторович

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ПРАВА ЧЕЛОВЕКА В УСЛОВИЯХ ПОСТИНДУСТРИАЛЬНОГО РАЗВИТИЯ (ТЕОРЕТИКО-ПРАВОВОЙ АНАЛИЗ)

Специальность
12.00.01 – Теория и история права и государства;
история учений о праве и государстве

Диссертация на соискание ученой степени
кандидата юридических наук

Научный руководитель:
доктор юридических наук, доцент
Ирина Юрьевна Богдановская

Москва – 2017

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Актуальность темы исследования. На современном этапе развития в обществе происходят изменения, обусловленные внедрением информационных и коммуникационных технологий. Они упрощают обработку информации, ускоряют информационный обмен и делают его массовым. Их использование способствует распространению средств цифровых коммуникаций и формированию глобального информационного пространства. Основу социального прогресса составляет деятельность, связанная с созданием, обработкой и реализацией информации, представленной в цифровой форме. Практически каждая область жизни общества получает свой цифровой аналог.

В изменяющихся социальных условиях особую актуальность приобретает теоретико-правовое исследование развития прав человека. Преобразования в информационной сфере обусловливают формирование общеправовых тенденций, в соответствии с которыми осуществляется выработка новых стандартов прав человека, их закрепление в национальном праве. Происходящие процессы приводят к необходимости осмысления ряда фундаментальных вопросов развития прав человека в цифровой среде, имеющих общетеоретическое значение.

В современном обществе права человека сталкиваются с вызовами, обусловленными развитием информационных и коммуникационных технологий. Свободное и безопасное существование личности, общества и государства зависит от защищенности информационной сферы их взаимодействия от внешних и внутренних угроз. В Доктрине информационной безопасности Российской Федерации обеспечение и защита прав человека относятся к первоочередной области национальных интересов в информационной сфере, реализация которых направлена на «формирование безопасной среды оборота достоверной информации и устойчивой к различным видам воздействия информационной

инфраструктуры» [1] . Информационная безопасность как феномен постиндустриального периода приобретает междисциплинарный характер, что обусловливает теоретико-правовую значимость анализа ее соотношения с правами человека.

В условиях развития информационных и коммуникационных технологий проблема соотношения информационной безопасности и прав человека обостряется. Ее решение предполагает новый взгляд на теоретико-правовые основы информационной безопасности, пути достижения соразмерности и соблюдения баланса интересов при ее обеспечении. Данная проблема выходит за рамки отдельных отраслей права и требует фундаментальной разработки на общетеоретическом уровне.

Степень научной разработанности проблемы и теоретическая основа исследования. Правовая наука восприняла концепции общественного развития, разработанные в социальных и экономических науках такими учеными, как Д. Белл, П. Дракер, М. Маклюэн, Й. Масуда, Ф. Махлуп, О. Тоффлер, Ф. Феррароттти, и др. Наряду с концепцией постиндустриального общества также используются концепции информационного общества и общества знания, каждая из которых характеризуется своими признакам. Однако, как пишет один из основоположников данных теорий Д. Белл, «даже если все соответствующие признаки имеются в наличии, подобные понятия либо односторонни, либо порождены модным поветрием и ради него искажают суть явления»[2].

Развитию прав человека в современном обществе посвящены труды отечественных ученых-юристов Н.С. Бондаря, Н.В. Варламовой, А.Н. Головистиковой, Л.Ю. Грудцыной, В.А. Карташкина, А.П. Коробова, М.А. Краснова, Л.Е. Лаптевой, Е.А. Лукашевой, А.В. Малько, Г.И. Муромцева, Т.М. Пряхиной, С.В. Пчелинцева, И.Г. Шаблинского и др. В зарубежной правовой

---

[1] Указ Президента Российской Федерации от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СЗ РФ. 2016. № 50. Ст. 7074.

[2] Белл Д. Грядущее постиндустриальное общество. Опыт социального прогнозирования / Пер. с англ. Изд. 2-е, испр. и доп. М.: Academia, 2004. CLXX, 788 с. С. CXLV–CXLVI.

литературе данная проблема рассмотрена в работах американских ученых-юристов А. Барака, В.С. Джексона, Г. Штейнера и др., европейских – К. Васака, Дж. Махоней, А. Мильне, Дж. Никель и др.

Правовые аспекты влияния информационных и коммуникационных технологий на развитие современного общества были исследованы еще в трудах А.Б. Венгерова. В дальнейшем теоретическое осмысление влияния информационных и коммуникационных технологий на права человека получило развитие в трудах таких российских ученых, как О.А. Городов, В.А. Дозорцев, П.У. Кузнецов, В.Н. Монахов, В.П. Мозолин, В.Б. Наумов, И.М. Рассолов, А.А. Тедеев, и др. В европейской правовой науке правам человека в условиях развития сети Интернет и цифровых технологий посвящены труды Дж. Зиккарди, Дж. Кристофферсена, А. Сааренпа, П. Хустинкса и др., в американской правовой науке – Дж.П. Барлоу, Дж. Бойла, Т.С. Ву, Дж.Л. Голдсмита, Дж. Грама, Д.Р. Джонсона, Л. Лессига, Г.Г. Перритта, Д.Г. Поста, Дж.П. Трахтмана, И.Т. Харди, Дж. Хуггеса и др.

Исходными для исследования аксиологических аспектов развития правовых явлений в современном обществе являлись положения, разработанные в трудах С.С. Алексеева и В.С. Нерсесянца. Исследования правовых ценностей продолжились в трудах А.Н. Бабенко, Ю.Ю. Витютнева, В.Д. Зорькина, В.А. Карташкина, О.В. Мартышина. В зарубежной правовой доктрине проблемы правовых ценностей в условиях перехода к постиндустриальному обществу были исследованы Ж.-Л. Бержелем, Р. Дворкиным, Г. Кельзеном, Н. Луманом, Н. Неновски, Ф. Хайеком.

Существенный вклад в исследование теоретико-правовых аспектов обеспечения информационной безопасности Российской Федерации внесли такие ученые, как В.Н. Лопатин, Т.А. Полякова, А.А. Стрельцов, А.П. Фисун, и др. Обеспечение информационной безопасности с позиции отраслей права представлены в работах отечественных ученых Г.В. Алексеева, И.Л. Бачило, Ю.В. Волкова, А.С. Жарова, А.К. Жаровой, Д.А. Калмыкова, В.П. Кириленко, А.В. Крутских, А.В. Кубышкина, А.В. Нестерова, О.А. Федотова,

А.А. Чеботаревой, Е.В. Янина и др. Различные правовые аспекты обеспечения информационной безопасности личности, общества, государства исследованы в трудах С.А. Буданова, С.Н. Головина, Ю.А. Журавлева, Л.А. Коврижных, Д.Г. Коровяковского, Н.А. Полянской, А.А. Тамодлина и др.

Правовые проблемы информационной безопасности в контексте обеспечения неприкосновенности частной жизни, противодействия киберпреступности исследованы в трудах таких зарубежных ученых-юристов, как И. Боухадана, Г. Гринлиф, М. Колумбик, Д. Исом, С.Калланан, Г. Кристоу, А. Митракас, С. Нельсон, У. Пагало, Дж. Симек, Т. Тропина, Т. Шоу, и др.

На сегодняшний день теоретико-правовая проблема соотношения прав человека и информационной безопасности в отечественной юридической литературе исследована недостаточно. В ее разработке особое значение приобретает анализ с общетеоретических позиций правовых категорий, принципов и положений в области обеспечения информационной безопасности, их влияния на права человека в условиях цифровой среды. Данные вопросы связаны с признанием обеспечения информационной безопасности одной из ключевых гарантий прав человека.

Объектом исследования являются информационная безопасность и права человека в постиндустриальный период.

Предметом диссертации выступают теоретико-правовые аспекты соотношения информационной безопасности и прав человека в условиях развития информационных и коммуникационных технологий.

Цель исследования заключается в выявлении и разрешении теоретических проблем развития института прав человека в связи с обеспечением информационной безопасности в современном обществе.

Задачи исследования:

анализ особенностей развития института прав человека в новых социальных условиях;

исследование правовых аспектов идентичности личности в цифровой среде;

анализ правовых подходов к обеспечению цифрового равенства;

аксиологический анализ информационной свободы и информационной безопасности как правовых ценностей постиндустриального периода;

определение информационной безопасности как правовой категории и обобщение правовых принципов ее обеспечения;

анализ проблемы соразмерности и соблюдения баланса интересов при обеспечении информационной безопасности.

Методологическая и теоретическая основа исследования. Методологической основой настоящего исследования являются общенаучные методы познания, такие как системный метод, методы формальной логики, аксиологический, диалектический методы. Кроме того, в работе применялись следующие специальные методы исследования правовых явлений: сравнительно-правовой метод, формально-юридический метод, историко-правовой метод.

В качестве теоретической основы настоящего диссертационного исследования были использованы труды ведущих ученых в области теории права и государства, прав человека, а также ученых и специалистов в области национальной безопасности и информационной безопасности как ее составляющей, содержащие теоретические выводы, научные концепции и гипотезы.

Правовую базу исследования составляют положения теории права и государства и отраслевых правовых наук. При проведении исследования использовались положения отечественного и зарубежного законодательства, международных правовых актов, а также судебная практика российских судов, судов зарубежных государств, Европейского суда по правам человека и Суда справедливости Европейского союза.

Научная новизна диссертационного исследования заключается в том, что в диссертации впервые соотношение информационной безопасности и прав человека рассматривается с применением аксиологического метода, обосновано значение информационной свободы и информационной безопасности как правовых ценностей постиндустриального периода.

Вводится в оборот новый понятийный аппарат: с общетеоретических позиций развиваются понятия «цифровые права», «цифровая идентичность» «цифровое равенство», формулируется определение информационной безопасности как правовой категории.

Впервые обобщаются правовые принципы, которые лежат в основе правового регулирования в области обеспечения информационной безопасности и соблюдения баланса интересов личности, общества и государства.

Новизна научной работы также проявляется в теоретико-правовом анализе технологической нейтральности и технологической зависимости правового регулирования при обеспечении правового равенства в постиндустриальном обществе, соотношения права и технологий при осуществлении и защите прав человека.

Основные научные положения, выносимые на защиту.

1. Установлено, что в постиндустриальный период происходит формирование новой группы прав человека – цифровых прав, осуществление которых связано с использованием информации, представленной в цифровой форме. Развитие цифровых прав происходит в условиях различных национальных моделей правового регулирования. Их выбор зависит от соотношения информационного патернализма и свободы информации, признаваемого в национальном праве.

2. Вводится правовое определение цифровой идентичности, под которой понимается уникальная совокупность информации о личности, представленной в цифровой форме, с использованием которой индивиды вступают в правоотношения, осуществляют права и обязанности. Определено, что правовое регулирование в цифровой среде основано на подходе, при котором допускается отличие цифровой идентичности от реальной.

3. Установлено, что цифровое равенство является новым этапом в развитии правового равенства и заключается в равных возможностях индивидов при осуществлении их прав с использованием информационных и коммуникационных технологий. Цифровое равенство обеспечивается на основе принципа сетевой

нейтральности и принципа доступности. Выявлена тенденция повышения технологической зависимости правового регулирования при обеспечении цифрового равенства.

4. Выявлено, что существующий конфликт между информационной свободой и информационной безопасностью как правовыми ценностями постиндустриального периода может быть решен исходя из их соотношения в системе правовых ценностей. В правовом государстве они взаимозависимы, их соотношение исключает доминирование одной ценности над другой. При достижении баланса между ними обеспечивается осуществление и защита прав человека как высшей правовой ценности.

5. Правовая категория «информационная безопасность» развивается с общетеоретических позиций и определяется как состояние защищенности прав человека в информационной сфере. Установлено возрастание роли правовых принципов, связанных с обеспечением конфиденциальности, целостности и доступности информации, при правовом регулировании в области обеспечения информационной безопасности.

6. Установлено, что обеспечение информационной безопасности представляет собой гарантию прав человека. В ходе ее развития изменяется соотношение права и технологий и повышается значение технических способов защиты прав человека. Установлено, что технические нормы при обеспечении информационной безопасности не заменяют, но дополняют правовое регулирование. Доказана универсальность подхода к достижению баланса интересов личности, общества и государства при обеспечении информационной безопасности на основе правового принципа соразмерности.

Теоретическая и практическая значимость диссертации состоит в том, что на основе теоретико-правового анализа соотношения информационной безопасности и прав человека формулируются выводы и положения, имеющие важное значение для развития теории права и государства, вводится новый понятийный аппарат, развиваются теоретические положения о правовых ценностях постиндустриального периода, правах человека в условиях цифровой

среды, их осуществлении и защите при обеспечении информационной безопасности личности, общества и государства.

Практическое значение результатов работы заключается в том, что они могут быть использованы в законотворческом процессе, а также при разработке учебно-методической литературы и в образовательном процессе.

Степень достоверности и апробация результатов диссертационного исследования. Материалы исследования и положения, выносимые на защиту, опубликованы в научных рецензируемых изданиях. Основные положения и выводы научного исследования были представлены в докладах автора на заседаниях методологического семинара кафедры теории и истории права факультета права НИУ ВШЭ, на научных конференциях, форумах и семинарах по проблемам информационной безопасности и прав человека в современном обществе: Конференция-семинар «Новые вызовы и угрозы информационной безопасности: правовые проблемы» (Москва, ИГП РАН, 5 – 6 февраля 2016 г.), II Международная научно-практическая конференция «Управление информационной безопасностью в современном обществе» (Москва, НИУ ВШЭ, 3 – 4 июня 2014 г.), ИНФОФОРУМ ЕВРАЗИЯ/СИТИ, IX Евразийский форум информационной безопасности и информационного взаимодействия (Правительство Москвы, 6 – 7 июня 2013 г.), 3-я Международная конференция «Право в цифровую эпоху», (Москва, НИУ ВШЭ, 20 – 21 мая 2013 г.), Конференция-семинар «Демократические институты в условиях развития информационного общества» (Москва, ИГП РАН, 1 – 2 марта 2013 г.), а также в опубликованных по результатам таких мероприятий сборниках материалов.

Структура диссертации: введение, две главы, заключение и список литературы.

ГЛАВА 1. ПРАВА ЧЕЛОВЕКА И ВЫЗОВЫ ПОСТИНДУСТРИАЛЬНОГО ПЕРИОДА

§1. Институт прав человека в условиях развития информационных и коммуникационных технологий

Информационные и коммуникационные технологии способствуют изменениям в обществе. Они характеризуются возрастающей ролью информации и знаний[3], что нашло отражение в таких концепциях, как «информационное общество» и «общество знаний». В настоящее время современное общество переживает следующий этап своего развития, также определяемый как «сетевое общество» или «цифровое общество»[4]. Использование средств цифровых коммуникаций практически во всех сферах общественных отношений приводит к изменению интересов и ценностей, принципов и условий существования людей.

В постиндустриальный период происходит дальнейшее развитие института прав человека. В результате преобразования информационной сферы права человека получают новую среду для их осуществления – цифровую, в том числе онлайновую среду[5], также называемую киберпространством. При этом права человека сталкиваются с такими особенностями киберпространства, которые традиционно выделяются в отечественной и зарубежной юридической литературе[6], как его трансграничный характер, зависимость от технических

---

[3] Информация и знания, по мнению Д.Белла, лежат в основе современного общества. Белл Д. Грядущее постиндустриальное общество Опыт социального прогнозирования. С. CLI.

[4] См. напр.: Banakar R. Normativity in Legal Sociology: Methodological Reflections on Law and Regulation in Late Modernity. Springer International Publishing, 2015. P. 241–264; Castells M. The Rise of the Network Society: The Information Age: Economy, Society and Culture. Wiley, 2000. 624 p.

[5] Под цифровой средой в настоящем исследовании понимается часть информационной сферы, взаимодействие в которой осуществляется с использованием информации, представленной в цифровой форме. Под онлайновой (от англ. on line – «на линии», «на связи») средой в настоящем исследовании понимается область цифровой среды, в которой взаимодействие осуществляется с использованием подключенных к сети Интернет технических средств.

[6] См., напр.: Федотов М.А. Конституционные ответы на вызовы киберпространства // Lex Russica. 2016. № 3. С. 164–182; Рассолов И.М. Право и киберпространство. М.: Московское

средств[7] и технических норм, деятельности различного рода информационных посредников[8]. Влияние цифровой среды на права человека становится междисциплинарной, фундаментальной проблемой, требующей общетеоретического осмысления.

В отечественной и зарубежной юридической литературе дается различная оценка развития института прав человека в условиях цифровой среды. Одни исследователи указывают на то, что за счет совершенствования технологий создаются технические возможности для осуществления в цифровой среде прав, которые человек имеет в офлайновой среде[9]. Так, отечественный юрист М.Ю. Середа отмечает, что с использованием сети Интернет «может быть реализовано практически любое конституционное (основное) право человека»[10]. Вместе с тем осуществление таких основных прав, как право на жизнь, на свободу передвижения, право на благоприятную окружающую среду, и ряда других основных прав человека хотя в настоящее время и может быть сопряжено с выходом в сеть Интернет, но тем не менее происходит не в цифровой среде, а в физическом пространстве и только в этом пространстве обретает смысл.

бюро по правам человека, 2007. 248 с.; Грибанов Д.В. Правовое регулирование кибернетического пространства как совокупности информационных отношений : дис. ... канд. юрид. наук : 12.00.01 / Грибанов Дмитрий Владимировчи. Екатеринбург, 2003. 227 с.; Lessig L. Code: Version 2.0. New York: Basic Books, 2006. 410 p.; Cohen J.E. Cyberspace As/And Space // Columbia Law Review. 2007. V.107. P. 210–256.

[7] Под техническими средствами в настоящем исследовании понимаются оборудование, устройства, программное обеспечение (программы для электронных вычислительных машин и базы данных), предназначенные для обработки информации, представленной в цифровой форме, а также информационно-телекоммуникационные сети, протоколы информационного обмена, шифровальные (криптографические) средства защиты информации.

[8] Под информационными посредниками в настоящем исследовании понимаются лица, которые обеспечивают (опосредуют) для других лиц доступ к информации, ее хранение (размещение информации на технических средствах), обработку, предоставление и распространение в сети Интернет.

[9] Под офлайновой (от англ. off line – «вне связи») средой в данном случае понимается более узкая область пространства, нежели противоположность онлайновой среды. Речь идет не только о сфере взаимодействия в отсутствие подключения к сети Интернет, но и о взаимодействии в целом без использования информации, представленной в цифровой форме.

[10] Середа М.Ю. Механизм ограничения конституционных прав и свобод человека в сети Интернет // Вестник Воронежского государственного университета : Серия «Право». 2013. № 2. С. 84.

Другая точка зрения указывает на возрастающую роль прав человека, осуществление которых происходит в информационной сфере, или информационных прав [11]. В отечественной правовой науке под ними понимаются правомочия «в области поиска, получения, передачи, производства и распространения информации, применения информационных технологий и обеспечения защиты информации»[12].

Некоторые отечественные ученые-юристы полагают, что информационные права отражают эволюционные изменения в институте прав человека и относят их к новому поколению прав [13]. Так, А.Б. Венгеров информационные права относит к четвертому поколению прав наряду с правом на мир, на ядерную безопасность, космос, экологическими правами, которые он в целом называет правами человечества. По его мнению, «четвертое поколение – это правовой ответ вызову XXI века, когда речь пойдет уже о выживании человечества как биологического вида, о сохранении цивилизации, о дальнейшей, космической социализации человечества. Рождается новое, четвертое поколение прав, и, соответственно, возникают международно-правовые процессуальные институты, обеспечивающие эти права» [14].

Вместе с тем основоположник концепции поколений прав человека – чешский ученый-юрист К. Васак исходил не только и не столько из временного, сколько из содержательного их разграничения, в основе которого выдвигались

---

[11] См., напр.: Виноградова, Н. В. Правовой механизм защиты информационных прав и свобод человека и гражданина в Российской Федерации : автореф. дис. ... канд. юрид. наук : 12.00.01 / Виноградова Наталья Владимировна. Саратов, 2011. 26 с.; Чеботарева А.А. Эволюция института прав человека в условиях развития информационного общества // Государственная власть и местное самоуправление. 2012. № 6. С. 27–33; Белевская Ю.А. Теоретико-правовые основы регулирования конституционных прав и свобод человека и гражданина в информационной сфере // Закон и право. М.: ЮНИТИ-ДАНА, 2009, № 3. С. 18–19; Caidi N., Ross A. Information Rights and National Security // Government Information Quarterly. 2005. V. 22. P. 663–684.

[12] См., напр.: Чеботарева А.А. Теоретико-правовые проблемы законодательного обеспечения информационных прав и свобод // Юридический мир. 2015. № 1. С. 50.

[13] См., напр.: Венгеров А.Б. Теория государства и права: Учебник / А.Б. Венгеров. 2-е изд. М.: Омега-Л, 2005. 608 с. С. 584; Права человека : учебник / А.Н. Головистикова, Л.Ю. Грудцына. М.: Эксмо, 2006. 448 с. С. 60; Глушкова С.И. Права человека и гражданина в контексте глобализации // Правовая система России в условиях глобализации. Сборник материалов круглого стола. М.: Ось-89, 2005. С. 46.

[14] Венгеров А.Б. Теория государства и права: Учебник. С. 584

такие идеалы Французской революции, как свобода, равенство и братство[15]. Предложенная им классификация поколений прав является завершенной и не предполагает возможность существования каких-либо иных поколений, кроме определенных им трех поколений прав, отражающих соответствующие идеалы. Согласно данной классификации информационные права, которые на сегодняшний день закреплены в международном и национальном праве, по своему содержанию соответствуют первым двум поколениям прав. Их юридическое закрепление началось задолго до начала постиндустриального периода, появления сети Интернет и иных современных информационных и коммуникационных технологий.

Такое информационное право, как свобода выражения мнений относится к первому поколению прав, признание которого было вызвано буржуазным развитием общества. Данное право выражает так называемую «негативную» свободу и заключается в невмешательстве государства в сферу информационной свободы личности. К первому поколению прав также относится право на неприкосновенность частной жизни, одним из аспектов которого является возможность индивида контролировать использование информации о своей личности. В юридической доктрине индустриального периода данное право справедливо понималось как «право быть оставленным в покое»[16]. Право на доступ к информации[17] по своему содержанию ближе ко второму поколению прав. Его реализация требует развития мер правового регулирования и деятельности государства, обеспечивающих правовое равенство индивидов при осуществлении доступа к информации.

---

[15] См.: Vasak K. Human Rights: A Thirty-Year Struggle: the Sustained Efforts to give Force of law to the Universal Declaration of Human Rights // UNESCO Courier. 1977. Nov. 19. P. 29–30.

[16] См., напр.: Warren S.D., Brandeis L.D. The Right to Privacy // Harvard Law Review. V. 4. № 5. 1890. P. 193–220. URL: https://www.ilrg.com/download/4harvlrev193.txt (дата обращения – 27 марта 2016 г.).

[17] Данное право хотя и закрепляется в конституциях на рубеже XX – XXI веков и в начале XXI века, начало приобретать самостоятельное значение со второй половины прошлого века. См., напр.: Право на доступ к информации. Доступ к открытой информации / Отв. ред. И.Ю Богдановская. М.: ЗАО «Юстицинформ», 2009. 344 с. С. 13.

К правам третьего поколения К. Васак предложил отнести право на коммуникацию, которое связывалось им с концепцией нового международного информационного порядка[18]. Вместе с тем данное информационное право до настоящего времени не получило закрепления в международном праве и его содержание все еще сохраняет дискуссионный характер. Так, в зарубежной юридической литературе отмечается, что содержание данного права является открытым концептом и, по существу, может определяться на национальном уровне в соответствии с национальными потребностями и культурой[19]. Следует согласиться с отечественным ученым-юристом Е.А. Лукашевой, по мнению которой «права третьего поколения – это коллективные права... отдельный человек принимает участие в реализации таких прав, но это участие связано не с его личным статусом, а с его положением как члена какой-либо общности»[20]. Коммуникационные возможности выступают неотъемлемым свойством любого человеческого сообщества и его членов, которое может быть выражено в праве на коммуникацию. Хотя данное право как и другие права третьего поколения остается менее гарантированным, нежели права первого и второго поколения[21], оно соответствует идеалам братства, которые К. Васак вкладывал в понятие прав человека третьего поколения.

Представление о том, что развитие института прав человека в цифровой среде ограничено только информационными правами, преуменьшает влияние, которое на него фактически оказывают новые технологии. Оно не приводит к

---

[18] Данная концепция разрабатывалась специально созданной комиссии при ЮНЕСКО в 70 – 80-х гг. прошлого века в связи с развитием спутниковой связи и доминированием новостных, медийных и иных информационных потоков из развитого мира (прежде всего, США, Великобритании и Франции) в развивающихся государствах. При сопоставлении национального суверенитета с новыми средствами коммуникации развитые государства придерживались свободного потока информации, а страны третьего мира предлагали ограничить подобный поток из других государств. В конечном итоге попытки согласовать на международном уровне данную концепцию оказались безуспешными. См.: Birdsall W.F. A Right to Communicate as an Open Work // Media Development. 2006. V. LIII. P. 41; D'Arcy J. Direct Broadcast Satellites and the Right to Communicate // EBU Review. 1969. V. 118. P. 14–18.

[19] Birdsall W.F. A Right to Communicate as an Open Work. P. 45.

[20] Права человека. Учебник для вузов / Ответственный редактор – член-корр. РАН, доктор юридических наук Е. А. Лукашева. М.: Издательство НОРМА, 2001. 573 с. С. 139–140.

[21] См.: Варламова Н.В. Третье поколение прав человека? // Российский юридический журнал. 2011. № 2. С. 16.

образованию какого-либо нового поколения прав, но в то же время распространяется на права человека, независимо от их видов и поколений.

Происходящие изменения могут быть выражены в понятии «цифровые права». Данные права обусловлены использованием информации, представленной в цифровой форме, которая, по мнению профессора права Джорджтаунского университета Дж. Коен, выступает связующим звеном сетевого и физического (картезианского) пространств, в своем взаимодействии и образующих киберпространство[22]. Из этого также следует и ключевая особенность цифровых прав, заключающаяся в том, что они связаны с возможностями или притязаниями, которые человек реализует в физическом пространстве в целях достижения определенного результата в сетевом пространстве.

В международных документах используется понятие «свобода в Интернете»[23], которое понимается как осуществление в сети Интернет основных прав человека и их защита в соответствии с Конвенцией о защите прав человека и основных свобод 1950 г. (далее – Конвенция 1950 г.)[24]. Речь идет не только о правах человека, которые традиционно связаны с использованием информации, информационных и коммуникационных технологий, но и о других основных правах человека, в том числе о свободе ассоциаций, праве на эффективную правовую защиту. В понятии «свобода в Интернете» подчеркивается ценность свободы, правовая охрана которой обеспечивается в международном и национальном праве путем создания условий для осуществления и защиты соответствующих прав человека.

Вместе с тем понятие «цифровые права» более точно и комплексно отражает суть происходящих изменений в институте прав человека. В цифровых правах выражена ценность не только свободы, но и безопасности. Осуществление цифровых прав связано не только с сетью Интернет, но и шире – с цифровой

---

[22] См.: Cohen J.E. Cyberspace As/And Space. P. 210–256.

[23] См., напр.: Рекомендации Комитета министров Совета Европы № CM/Rec(2016)5 о свободе в Интернете URL: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016806415fa (дата обращения – 20 августа 2016 г.).

[24] Бюллетень международных договоров. № 3. 2001.

средой, в том числе с информацией, представленной в цифровой форме, и с основанными на ней информационными и коммуникационными технологиями. Цифровые права отличает от иных прав человека то, что их осуществление либо происходит в цифровой среде, либо направлено на обеспечение доступа к ней.

Цифровые права также являются более широким понятием, нежели информационные права человека. Они включают в себя правомочия, которые ранее не связывались с информационной сферой, но с развитием информационных и коммуникационных технологий стали проявляться в цифровой среде. То обстоятельство, что данные права обусловлены использованием информации, представленной в цифровой форме, не делает их информационными. Пределы данных прав в условиях развития информационных и коммуникационных технологий не меняются, хотя такие технологии и могут способствовать их осуществлению и защите.

Повышение значимости цифровых прав ставит вопрос об их соотношении с основными (конституционными) правами человека. Так, отечественный ученый М.А. Федотов справедливо отмечает, что «пока Конституция не обретет своего интернет-измерения, всякие попытки правового регулирования деятельности в киберпространстве методами национального законодателя обречены на неудачу» [25]. Следует подчеркнуть, что большая часть цифровых прав уже получила нормативное закрепление в национальном и международном праве.

Формулировки основных прав в международных документах в области прав человека, таких как Всеобщая декларация прав человека 1948 г. [26], Международный пакт об экономических, социальных и культурных правах 1966 г.[27], Международный пакт о гражданских и политических правах 1966 г.[28], а также в Конвенции 1950 г. являются в достаточной степени общими и не зависят от развития технологий. Так, показатели для оценки свободы в сети Интернет, предложенные в рекомендациях Комитета министров Совета Европы,

[25] Федотов М.А. Конституционные ответы на вызовы киберпространства. С. 165.
[26] Российская газета. 10.12.1998.
[27] Бюллетень Верховного Суда Российской Федерации. № 12. 1994.
[28] Там же.

основываются на уже существующих и установленных стандартах прав человека[29] и не предполагают изменения формулировок признанных основных прав или же признания новых прав.

Равным образом не зависят от развития технологий и формулировки прав человека в большинстве современных писаных конституций. В Конституции Российской Федерации права человека сформулированы либо без указания конкретных технологий, с использованием которых они могут осуществляться, либо путем их приведения в форме открытого перечня. Например, согласно части 2 статьи 23 Конституции Российской Федерации каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и *иных* сообщений. Это позволяет без изменения Конституции обеспечить распространение в цифровой среде существующих формулировок основных прав человека в национальном законодательстве и правоприменительной практике.

Необходимость изменения конституции возникает только в случае наличия зависимых от конкретных технологий формулировок основных прав человека. Такие изменения, например, в 1976 г. в Швеции были внесены в статью 2:1 Регерингсформа 1974 г. (один из нормативных правовых актов, составляющих Основной закон Швеции), в соответствии с которыми определение свободы выражения – «права сообщать информацию и выражать идеи, мнения и эмоции, будь то устно, письменно, в графических изображениях» – было дополнено словами «или любым другим способом»[30].

В некоторых государствах при закреплении права на доступ к информации и права на неприкосновенность частной жизни в конституции иногда приводится прямое указание на новые формы представления информации или средства ее обработки. Так, в 2001 г. в рамках конституционной реформы в Конституции Греции 1975 г. было предусмотрено право личности на защиту от сбора, обработки и использования своих персональных данных, в том числе с

---

[29] См.: Рекомендации Комитета министров Совета Европы № CM/Rec(2016)5 о свободе в Интернете.

[30] См.: The Instrument of Government. URL: http://www.riksdagen.se/en/SysSiteAssets/07.-dokument--lagar/the-instrument-of-government-2015.pdf/ (дата обращения – 20 августа 2016 г.).

использованием электронных средств[31]. Хотя подобные поправки и связаны с технологическим развитием современного общества, указание на новые формы представления информации или средства ее обработки не столько дополняют, сколько конкретизируют формулировки прав человека.

В условиях развития информационных и коммуникационных технологий группа цифровых прав расширяется как за счет прав, которые человек имеет в офлайновой среде, так и за счет новых прав человека, характерных именно для цифровой среды. С одной стороны, к ним относятся права человека, имеющие тесную связь с частной жизнью[32] и информацией о личности, например, право на забвение[33], а с другой – права, которые ближе второму поколению прав человека, в том числе право на доступ к сети Интернет и права человека в области взаимодействия с государственными органами[34] в электронном виде.

Право на забвение связано с развитием технологий поиска информации в сети Интернет и возможностью нахождения информации, являющейся

---

[31] Ст. 9A Конституции Греции. URL: http://www.hellenicparliament.gr/UserFiles/f3c70a23-7696-49db-9148-f24dce6a27c8/001-156%20aggliko.pdf (дата обращения – 20 августа 2016 г.).

[32] Как следует из практики Европейского суда по правам человека, определение понятия «частная жизнь» практически не поддается формализации. Можно лишь говорить о различных сферах, элементах, вопросах, которые можно включать в объем понятия «частная жизнь» и которые с развитием общественных отношений также подвержены изменениям. В этой связи Суд включает в объем данного понятия различные составляющие, отмечая, что «такие элементы, как половая принадлежность, имя, сексуальная ориентация и половая жизнь являются важными элементами личной сферы, защищаемой статьей 8 Конвенции 1950 г. Данная статья также защищает право на индивидуальность и личное развитие, равно как и право на установление и развитие отношений с другими людьми и с внешним миром, и может включать в себя деятельность профессионального или делового характера. Таким образом, существует некая зона взаимодействия человека с другими людьми, в том числе и в публичной сфере, которая может включаться в объем понятия «частная жизнь». См., напр.: Велиева Д.С. Право на уважение частной жизни: международные стандарты реализации и защиты // Известия Саратовского университета. Новая серия. Серия Экономика. Управление. Право. 2014. № 2-2. Т. 14. С. 443–448.

[33] К числу данных прав также можно отнести право на защиту от скрытого наблюдения со стороны государства, право на использование шифровальных (криптографических) средств, право на идентичность в цифровой среде, право на анонимность в сети Интернет. См., напр.: Grill L., Redeker D., Gasser U. Towards Digital Constitutionalism? Mapping Attempts to Craft an Internet Bill of Rights. Berkman Center Research Publication № 2015-15. URL: http://ssrn.com/abstract=2687120 (дата обращения – 13 августа 2016 г.); Sullivan C. Digital Citizenship and the Right to Digital Identity Under International Law // Computer Law & Security Review. 2016. V. 32. P. 474–481.

[34] Здесь и далее также имеется в виду взаимодействие с органами местного самоуправления, государственными и муниципальными организациями.

недостоверной или неактуальной, утратившей значение для индивида в силу последующих событий или действий. Оно заключается в возможности лица требовать от оператора поисковой системы в сети Интернет прекращения обработки соответствующей данным критериям информации о нем и корреспондирующей обязанности оператора прекратить выдачу сведений о ссылках, позволяющих получить доступ к такой информации. Его закреплению в национальном законодательстве прежде всего государств-членов Европейского союза и Совета Европы способствовало развитие судебной практики Суда справедливости Европейского союза[35] и Европейского суда по правам человека[36]. В праве на забвение выражается баланс между интересами индивида, сведения о котором распространяются в сети Интернет, и интересами других лиц, между правом на неприкосновенность частной жизни и свободой выражения мнения. В данном случае юридическое закрепление права на забвение приводит к ограничению свободы выражения мнения. В свою очередь преобладающий интерес общества к получению доступа к информации определяет пределы права на забвение. Так, в российском праве такой преобладающий интерес общества обусловлен получением доступа к информации о событиях, содержащих признаки уголовно наказуемых деяний, сроки привлечения к уголовной ответственности по которым не истекли, и к информации о совершении гражданином преступления, по которому не снята или не погашена судимость[37]. В то же время сфера

[35] Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González (C-131/12). Judgment of the Court of Justice (Grand Chamber) of 13 May 2014. URL: http://curia.europa.eu/juris/liste.jsf?num=C-131%2F12 (дата обращения – 20 августа 2016 г.). В данном решении Суд признал, что операторы поисковых машин, такие как Google Spain, являются контролерами данных, то есть на них распространяется действие Data Protection Directive 1996 г., и они должны осуществлять деиндексацию личных данных, если поиск предоставляет сведения, которые могут причинить вред субъекту данных.

[36] Affaire Brunet v. France. URL: http://hudoc.echr.coe.int/eng#{"itemid":["001-146389"]} (дата обращения – 20 августа 2016 г.). Дело касалось человека, чьи данные были размещены в уголовном архиве. После того как спор был решен путем медиации, его данные не были удалены, несмотря на судебный запрос на их удаление. Заявитель жаловался на то, что сохранение данных на срок, составляющий двадцать лет, несмотря на медиацию, является нелегитимным, и требовал их удаления из уголовного архива. Европейский суд по правам человека удовлетворил его требования.

[37] См.: Ст. 10^3 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» в редакции Федерального закона от 13

осуществления права на забвение изначально является узкой, охватывает только результаты запросов, которые обрабатывают операторы поисковых систем, и непосредственно не приводит к блокированию и фильтрации [38] самой информации, доступ к которой в сети Интернет сохраняется. В совокупности с критериями, на основании которых происходит отнесение информации к подлежащей исключению из результатов таких запросов, применение как досудебного, так и специального судебного порядка осуществления данного права позволяет обеспечить баланс интересов различных субъектов правоотношений.

В Европейском союзе происходит дальнейшее развитие данного права, при котором оно становится, с одной стороны, более универсальным, с другой – более сбалансированным. Более универсальным данное право становится, поскольку корреспондирующая ему обязанность возлагается не только на операторов поисковых систем, но и на любых лиц, которые определяют средства и средства обработки персональных данных (контролеров)[39]. Данная обязанность касается удаления не только ссылок на информацию, но и самой информации. В этой связи соответствующее право справедливо получает новое название – право на

июля 2015 г. № 264-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и статьи 29 и 402 Гражданского процессуального кодекса Российской Федерации» // СЗ РФ. 2015. № 29 (часть I). Ст. 4390.

[38] Под блокированием понимаются меры технического характера, в результате применения которых предотвращается доступ к конкретным сайтам в сети Интернет, IP-адресам или доменным именам. Под фильтрацией понимаются меры технического характера, которые используются для предотвращения доступа к отдельным страницам и иным ресурсам сайтов в сети Интернет, содержащим определенную информацию, либо для предотвращения появления ссылок на них при осуществлении поиска информации в сети Интернет. От данных мер следует отличать изъятие информации, под которым понимается ее удаление с сайта в сети Интернет, осуществляемое на основании требования правообладателя, иного заинтересованного лица либо уполномоченного органа государственной власти. См.: Jørgensen R.F., Pedersen A.M. Online Service Providers as Human Rights Arbiters // The Responsibilities of Online Service Providers / ed. by M. Taddeo, L. Floridi. Springer International Publishing, 2017. P. 182.

[39] Универсальный подход к удалению персональных данных по требованию субъекта персональных данных соответствует действующей Директиве о защите данных (Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data. URL: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046 (дата обращения: – 27 апреля 2017 г.), в которой данное требование является составляющей более широкого права доступа (right to access).

удаление (right to erasure)[40]. Контролеры, сделавшие персональные данные доступными, также обязаны с учетом имеющихся технологий и стоимости реализации принять разумные меры, включая технические меры, чтобы проинформировать контролеров, осуществляющих обработку персональных данных, которые субъект персональных данных потребовал стереть, обо всех ссылках на использование, копирование или репликацию этих персональных данных. Более сбалансированным оно становится в силу расширения и детализации перечня исключений, на которые данное право не распространяется. Подобные исключения, обусловленные общественными интересами, в той или иной мере охватывают сферу осуществления права на свободу выражения мнения и свободу информации, обработку персональных данных в соответствии с установленными в наднациональном или национальном праве обязанностями контролера или органа власти, общественные интересы в сфере здравоохранения, архивные, научные, исторические или статистические цели, установление, осуществление или защиту правовых требований.

Подход к новым цифровым правам, связанным с частной жизнью и информацией о личности, который принят в США, развивается под влиянием утвердившегося в американской правовой доктрине и судебной практике принципа свободного потока информации (free flow of information)[41]. Несмотря на то, что данный принцип формировался в условиях холодной войны и имел целью создание нового международного информационного порядка путем расширения сферы влияния западных средств массовой информации на территории

---

[40] См.: Article 17 of 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). Данные Регуляции вступают в силу с 25 мая 2018 г. и в отличие от директив будут иметь прямое действие на территории государств – членов Европейского союза. URL: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679 (дата обращения – 27 апреля 2017 г.).

[41] См.: Houchins v. KQED, Inc., 438 U.S. 1 (1978). URL: http://caselaw.findlaw.com/us-supreme-court/438/1.html (дата обращения – 27 апреля 2017 г.) (в этом деле судья Стивенс отметил, что «сохранение полного и свободного потока информации для широкой общественности уже давно признано основной целью Первой поправки»); Graubart J. What's News: A Progressive Framework for Evaluating the International Debate over the News. California Law Review. V. 77. I. 3. 1989. P. 631.

развивающихся государств, он не только сохраняет силу, но и распространяет свое действие в сети Интернет. В настоящее время в нем выражено ограниченное вмешательство государства в осуществление не только свободы выражения мнения, но и права на неприкосновенность частной жизни в цифровой среде.

Одновременно в развитии соответствующих цифровых прав в европейских государствах, в том числе в России, проявляется информационный патернализм, при котором предпринимаются попытки установить баланс интересов при определении пределов прав человека. Тогда как принцип свободного потока информации допускает исчерпывающий набор исключений, непосредственно предусмотренных Первой Поправкой к Конституции США [42] и связанных с призывами к насилию, реальными угрозами, клеветой и непристойностями[43], в европейском подходе изначально лежит признание допустимости ограничения прав человека для обеспечения правовой охраны более широкого спектра правовых ценностей, в том числе национальной безопасности. Так, Конституционный Суд Российской Федерации в своих решениях [44] признавал соразмерным и, следовательно, допустимым ограничение свободы выражения мнения в сети Интернет для противодействия экстремизму и защиты

[42] В соответствии с Первой Поправкой к Конституции США Конгресс не должен издавать никакого закона относительно установления какой-либо религии, или воспрещающего свободное исповедание всякой религии, или ограничивающего свободу слова и прессы, или право народа – мирно собираться, а также просить правительство о прекращении злоупотреблений.

[43] В 2002 г. в деле American Civil Liberties Union v. Ashcroft Верховный Суд США установил недопустимость ограничения права на свободу выражения мнения в сети Интернет, кроме случаев, указанных в Первой Поправке к Конституции США. См.: URL: http://caselaw.findlaw.com/us-supreme-court/535/564.html (дата обращения – 1 декабря 2016 г.)

[44] См., напр.: Определение Конституционного Суда Российской Федерации от 1 июня 2010 г. № 757-О-О «Об отказе в принятии к рассмотрению жалобы гражданина Леонова Владимира Николаевича на нарушение его конституционных прав положениями подпункта «г» пункта 3.2 статьи 4 и подпункта «ж» пункта 7 статьи 76 Федерального закона «Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации» // Вестник Центризбиркома РФ. 2010. № 7; Постановление Конституционного Суда Российской Федерации от 14 ноября 2005 г. № 10-П «По делу о проверке конституционности положений пункта 5 статьи 48 и статьи 58 Федерального закона «Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации», пункта 7 статьи 63 и статьи 66 Федерального закона «О выборах депутатов Государственной Думы Федерального Собрания Российской Федерации» в связи с жалобой Уполномоченного по правам человека в Российской Федерации» // СЗ РФ. 2005. № 47. Ст. 4968.

политических прав при незаконной предвыборной агитации. Для принципа свободного потока информации такие ограничения являлись бы неприемлемыми.

В связи с различием данных подходов правовая охрана новых цифровых прав, связанных с частной жизнью и информацией о личности, в США и европейских государствах также отличается. Так, в США право на забвение не признается, поскольку его правовая охрана вступала бы в противоречие с принципом свободного потока информации. В свою очередь в прецедентной практике Суда справедливости Европейского союза оно рассматривается в качестве компонента права на неприкосновенность частной жизни. Принципиальное отличие российского подхода к праву на забвение от аналогичного подхода Суда справедливости Европейского союза заключается в том, что в Российской Федерации право на забвение определено как право *sui generis*, тогда как в Европейском союзе оно следует из правового регулирования в области защиты (персональных) данных. Кроме того, в отечественном законодательстве оно сформулировано через обязанность оператора поисковой машины, а не через право человека. В то же время данное различие не отменяет его происхождения как компонента права на неприкосновенность частной жизни. Это следует из того, что суть обязанности оператора поисковой системы – прекращение выдачи сведений об указателе страницы сайта в сети Интернет, позволяющих получить доступ к информации о заявителе, то есть к персональным данным (в смысле определения данного понятия в Федеральном законе от 27 июля 2006 г. № 152-ФЗ «О персональных данных»[45]). Таким образом, право на забвение в тех правовых системах, где обеспечивается его осуществление и защита, логически следует из права на неприкосновенность частной жизни и выступает его компонентом.

В то же время новые цифровые права, соответствующие второму поколению прав, имеют больше предпосылок для признания основными правами человека. Их осуществление в меньшей степени связано с разрешением

[45] СЗ РФ. 2006. № 31 (часть I). Ст. 3451.

конфликта между интересами различных субъектов правоотношений. Хотя данные права и происходят от права на доступ к информации, в настоящее время они уже охватывают не только информацию, но и, например, государственные и иные социально значимые услуги, предоставляемые в электронном виде[46]. На сегодняшний день Греция пока является единственным государством, в конституции которого закреплено право человека, в котором проявляется наибольшее число таких социальных возможностей в цифровой среде, – право на участие в информационном обществе. Оно основано на возможностях доступа как к информационно-телекоммуникационной инфраструктуре, так и к государственным услугам, которые могут быть предоставлены с ее использованием[47]. Данному праву корреспондирует обязанность государства обеспечивать доступ к информации, передаваемой по электронным каналам коммуникации, так же как ее производству, обмену и распространению.

Признание участия в информационном обществе одной из составляющих свободы личности и конституционной ценностью играет важное значение для новых цифровых прав, определяя общее направление их развития. Несмотря на то, что приведенный выше опыт Греции пока является уникальным, отдельные компоненты права на доступ к информационному обществу, прежде всего право на доступ к сети Интернет, получают признание в качестве основных прав человека в практике зарубежных органов конституционной юстиции[48], Европейского суда по правам человека[49] и в документах международных

---

[46] Democracy, Human Rights and the Rule of Law in the Information Society. Contribution by the Council of Europe to the 2nd Preparatory Committee for the World Summit on the Information Society. URL: http://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016805e14ad (дата обращения – 31 июля 2016 г.).

[47] См.: Papakonstantinou A. The Constitutional Right of Participation in the Information Society // Revue of Public and Administrative Law. 2006. № 2. P. 233.

[48] См.: French Constitutional Council: Decision № 2009-580 of June 10th 2009 – Act Furthering the Diffusion and Protection of Creation on the Internet. URL: http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank/download/2009-580DC-2009_580dc.pdf (дата обращения – 31 июля 2016 г.).

[49] См.: Ахмет Йилдырым (Ahmet Yildirim) против Турции. Постановление Европейского суда от 18 декабря 2012 г. (Жалоба № 3111/10) // Прецеденты Европейского суда по правам человека. 2016. № 6(30). В данном решении заявитель жаловался на ограничение доступа к своему сайту, созданному на основе модуля Google, из-за блокировки, установленной в целом в

организаций. В докладе спецпредставителя ООН по вопросу о поощрении и защите права на свободу мнений и свободу выражения от 3 июня 2011 г.[50] предложено рассматривать право на доступ к сети Интернет как естественное право человека, но в то же время указано, что не все государства способны обеспечить его реализацию. В данном предложении по сути отражена двойственность этого права: его естественно-правовое происхождение указывает на его прирожденный и неотчуждаемый характер, а также на необходимость его защиты от произвольных ограничений; в то же время часть расходов на создание инфраструктуры доступа к сети Интернет несут государства. Обязанность государства содействовать всеобщему доступу к сети Интернет подчеркивается в Декларации о свободе выражения мнений в сети Интернет, принятой в 2011 г. совместно ООН, ОБСЕ, Организацией американских государств и Африканской комиссией по правам человека и народов[51]. В этой связи не лишена справедливости точка зрения, высказанная в отечественной юридической доктрине[52], о том, что данное право является не только гарантией ряда личных прав человека, но также и социальным правом. Его осуществление обеспечивается в рамках выполнения государством своей социальной функции. В результате содержание данного права существенно варьируется в зависимости от финансовых и технологических возможностей тех или иных государств.

Таким образом, в условиях цифровой среды происходит развитие института прав человека. Соответствующие изменения связаны с формированием новой группы прав человека – цифровых прав, которые связаны с информацией,

---

отношении данного модуля. В решении суда установлено, что «необходимо признать право на беспрепятственный доступ к сети Интернет».

[50] Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue // URL: http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf (дата обращения – 31 июля 2016 г.).

[51] United Nations, Organization of American States, Organization for Security and Co-operation in Europe, African Commission on Human and Peoples' Rights. «Joint Declaration Concerning the Internet». «Joint Declaration Concerning the Internet». URL: http://www.oas.org/en/iachr/expression/showarticle.asp?artID=848 (дата обращения – 20 августа 2016 г.).

[52] Середа М.Ю. Закрепление права на доступ в сеть Интернет в международно-правовых актах и законодательстве зарубежных стран // Международное публичное и частное право. 2013. № 5. С.44–47.

представленной в цифровой форме. Такие права либо осуществляются в цифровой среде, либо направлены на обеспечение доступа к ней. Группа цифровых прав расширяется как за счет уже закрепленных в международном праве и конституциях прав человека, так и за счет новых прав. К ним относятся права человека, имеющие тесную связь с частной жизнью и личной информацией, например право на забвение, а также права человека, в которых выражается его возможность участия в информационном обществе, в том числе право на доступ к сети Интернет и права человека в области получения государственных услуг в электронном виде. Цифровые права на современном этапе предполагают различные национальные модели их юридического закрепления, соответствующие правовым традициям тех или иных государствах и уровню их социально-экономического развития.

§2. Права человека и цифровая идентичность личности

В цифровой среде личность создает учетные и иные информационные записи, включая аккаунты, блоги, сайты, доменные имена, другими словами – формирует свою цифровую идентичность. Она проявляется в социальных сетях, компьютерных играх, почтовых и иных службах[53] в сети Интернет и охватывает сведения, которые позволяют идентифицировать личность, такие как логин и пароль, а также финансовую, мультимедийную и иную информация о ней. Американские ученые-юристы Д.Р. Джонсон и Д.Г. Пост справедливо отмечают, что «право в Сети должно быть готово к тому, чтобы иметь дело с лицами, которые представляют себя только с помощью идентификационных кодов, пользовательских аккаунтов и доменных имен»[54].

[53] Под службами в данном случае понимается программное обеспечение, которое имеет собственный адрес в сети Интернет и предназначено для оказания услуг с использованием сети Интернет.

[54] Johnson D.R., Post D. Law and Borders – The Rise of Law in Cyberspace // Crypto Anarchy, Cyberstates, and Pirate Utopias / ed. by Peter Ludlaw. Massachusetts Institute of Technology. 2001. P. 173. (Впервые опубликована в Stanford Law Review. 1996. V. 48)

С правовой точки зрения цифровая идентичность указывает на уникальную совокупность информации о личности, представленной в цифровой форме, с использованием которой индивиды вступают в правоотношения, осуществляют права и обязанности. Цифровая идентичность предназначена для того, чтобы физические лица могли через нее действовать от своего имени, под псевдонимом или анонимно в цифровой среде. При этом они не имеют возможности реализовать некоторые свои права, в том числе право на судебную защиту, до тех пор пока не раскроют свою реальную личность. Одно из ключевых отличий цифровой идентичности от создавших ее физических лиц заключается в том, что в правоотношениях цифровая идентичность может выступать в качестве товара. Международным союзом электросвязи указывается, что «цифровая идентичность становится все более ценным товаром, и, как следствие, ее защита и управление ею становится все более актуальным»[55]. Это повышает значение цифровой идентичности не только как нематериального блага, но и как объекта имущественных прав[56].

Создание цифровой идентичности связано с реализацией права на идентичность (личную идентичность или индивидуальность), которое отдельными отечественными и зарубежными исследователями признается одним из основных прав человека[57]. По своему содержанию оно близко к праву на

---

[55] International Telecommunication Union, Digital Life. ITU Internet Report (2006). URL: http://www.itu.int/osg/spu/publications/digitalife/docs/digital-life-web.pdf (дата обращения – 16 июля 2016 г.).

[56] В США с 2015 г. федеральное законодательство о доверительном управлении имуществом было распространено на так называемые цифровые активы, такие как компьютерные файлы, домены, виртуальные валюты. При этом установлен запрет на доступ доверительного управляющего к цифровым коммуникациям обладателя цифровых активнов, включая электронную почту, средства мгновенного обмена сообщениями, аккаунты в социальных сетях до тех пор, пока от него не было получено согласие в письменной форме. В соответствии с федеральным законодательством осуществляется развитие законов штатов. См.: Fiduciary Access to Digital Assets Act, Revised (2015). URL: http://www.uniformlaws.org/Act.aspx ?title=Fiduciary%20Access%20to%20Digital%20Assets%20Act,%20Revised%20(2015) (дата обращения – 16 июля 2016 г.).

[57] См., напр.: Кузнецов Э.В. Право на индивидуальность: к истории вопроса // История государства и права. 2009. № 10. С. 3–5; Андрианова В.В. Личные права в России (право на индивидуальность) // Вестник Российской правовой академии. 2012. № 3. С. 18–21; Marshall J. The Legal Recognition of Personality: Full-Face Veils and Permissible Choice // International Journal of Law in Context. 2014. V.10. P. 64–80. Особое значение данное право принимает при

неприкосновенность частной жизни и заключается в признании и уважении индивида как уникальной личности. Из него, в частности, следуют признание прав на имя, национальность, пол, которые в соответствии с иными характеристиками личности составляют ее индивидуальность. В отличие от права на неприкосновенность частной жизни, которое в цифровой среде предназначено для охраны интересов личности при использовании информации о ее частной жизни, право на идентичность указывает на охрану только информации, необходимой и достаточной для ее идентификации[58].

Способы, условия и в целом возможность осуществления права на идентичность в цифровой среде зависят от информационного посредника, который, с одной стороны, обеспечивает возможность создания цифровой идентичности и управления ею, а с другой – может заблокировать, ликвидировать, внести изменения в связанную с ней информацию.

Создание цифровой идентичности и управление ею осуществляется на основании соглашения между физическим лицом и информационным посредником. Однако период существования цифровой идентичности не ограничен сроком действия такого соглашения. Фактически она существует пока информационный посредник хранит связанную с ней информацию в своих базах данных. В частности, возможности деактивации аккаунта в социальной сети Facebook[59] были предусмотрены только в конце 2009 г. При этом информация, связанная с цифровой идентичностью, сохраняется на серверах Facebook, в результате чего аккаунт может быть вновь активирован по инициативе пользователя[60]. Для удаления аккаунта необходимо заполнение специальной

формировании личности ребенка. В этой связи оно непосредственно закреплено в Конвенции о правах ребенка (одобрена Генеральной Ассамблеей ООН 20.11.1989) (Сборник международных договоров СССР. выпуск XLVI. 1993). См., напр.: Рабец А.М. Право ребенка на индивидуальность и проблемы его реализациив Российской Федерации // Ученые записки Российского государственного социального университета. 2013. Т. 1. № 2 (113). С. 79–87.

[58] См., напр.: Sullivan C. Digital Identity, Privacy and the Right to Identity in the United States of America // Computer Law & Security Review. 2013. V. 29. P. 349, 354, 355.

[59] См.: Деактивация или удаление аккаунта. Справочный центр Facebook. URL: https://www.facebook.com/help/250563911970368/?helpref=hc_fnav (дата обращения – 16 июля 2016 г.).

[60] Там же.

формы. Тем не менее и это не гарантирует полного удаления аккаунта, поскольку направленные с его использованием сообщения другим лицам в социальной сети сохраняются у них[61]. В результате осуществление права на идентичность в цифровой среде зависит не только от условий соглашения с информационным посредником, на основании которого осуществляется создание цифровой идентичности и управление ею, но и от особенностей функционирования технических средств, содержащих связанную с ней информацию.

В цифровой среде возникает проблема защиты права на идентичность личности от неправомерных действий, совершенных другими лицами в отношении ее цифровой идентичности. При этом правомерными следует признать такие действия, на которые получено ее согласие либо которые допускаются в силу закона. Речь, в частности, идет о блокировании учетной записи информационным посредником в соответствии с соглашением с индивидом, например по его требованию либо в случае нарушения им условий соглашения[62]. Такое блокирование, равно как фильтрация информации, передаваемой посредством цифровой идентичности, также применяется для защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства и осуществляется информационным посредником во исполнение решения суда или иного уполномоченного органа государственной власти, принятого в соответствии с национальным законодательством[63]. В ряде государств суды

---

[61] Данная проблема также касается вопросов существования цифровой личности и связанной с ней информации после физической смерти ее обладателя. Их решение способствовало принятию специальных законов во Франции, а также в отдельных штатах США. См., напр: Knowledge Center – Digital Death. URL: http://www.digitaldeath.com/knowledgebase/state-laws-governing-digital-death/ (дата обращения – 16 июля 2016 г.); Mort Numérique ou Éternité Virtuelle : Que Deviennent vos Données Après la Mort? URL: https://www.cnil.fr/fr/mort-numerique-ou-eternite-virtuelle-que-deviennent-vos-donnees-apres-la-mort-0 (дата обращения – 16 июля 2016 г.).

[62] В обратном случае суд может прийти к выводу о нарушении прав таких администраторов, например, если имеет место нарушение законодательства о защите прав потребителей. См., напр.: Апелляционное определение Московского городского суда от 14 июля 2015 г. по делу № 33-24464/2015 // СПС КонсультантПлюс.

[63] В Турции на основании решения суда Facebook заблокировал ряд аккаунтов, в которых содержались сведения, оскорбляющие пророка Мухаммеда. См.: Facebook Blocks Pages Insulting

принимали решения о блокировании в целом в отношении социальных сетей или иных служб в сети Интернет, которые в свою очередь приводили к блокированию учетных записей индивидов, созданных с использованием таких служб[64]. Суд справедливости Европейского союза в деле UPC Telekabel Wien GmbH против Constantin Film Verleih GmbH пришел к выводу о том, что в случае нарушения авторских прав подобное блокирование допустимо, если принятые меры не лишают интернет-пользователей возможности законного доступа к информации [65]. В то же время критерии, определенные судом, не позволяют говорить о том, что блокирование отдельных интернет-ресурсов, предоставляющих доступ как к информации, распространяемой с нарушением законодательства, так и к иной информации, будет неправомерным. Национальные и наднациональные суды анализируют легитимность таких мер с точки зрения предотвращения нарушения свободы выражения мнения и права на доступ к информации, а не права на идентичность [66]. Это обусловлено тем, что признание и защита права на

Prophet Mohammed in Turkey. Mashable // URL: http://mashable.com/2015/01/26/facebook-blocks-pages-turkey/#gLHKI9Kmkkq2 (дата обращения – 16 июля 2016 г.).

[64] В Бразилии на основании решения мирового суда был заблокирован интернет-мессенджер WhatsApp на 72 часа в связи с непредставлением его собственником Facebook информации в рамках уголовного расследования. Блокирование сделало невозможным использование аккаунтов около 100 млн пользователей в Бразилии. Однако данное решение было отменено Федеральным Верховным судом Бразилии в связи с несоразмерным характером накладываемых им ограничений. См.: WhatsApp Blocked in Brazil Again. Techcrunch // URL: https://techcrunch.com/2016/07/19/whatsapp-blocked-in-brazil-again/ (дата обращения – 16 июля 2016 г.).

[65] Суд постановил, что праву Европейского союза не противоречат решения национальных судов о блокировании интернет-сайтов, если они соответствуют ряду условий. Так, если решением суда не определяются конкретные меры, которые провайдер доступа к сети Интернет должен предпринять, то такой провайдер может избежать санкций за нарушение этого запрета, показывая, что он принял все разумные меры, при условии что (I) принятые меры не лишают интернет-пользователей возможности законного доступа к информации и (II) что такие меры направлены на предотвращение несанкционированного доступа к объекту охраны или, по крайней мере, делают его труднодоступным и существенно обременяют интернет-пользователей, которые пользуются услугами провайдера, при осуществлении доступа к объекту охраны, доступ к которому был предоставлен им в нарушение прав интеллектуальной собственности, установленных национальными органами исполнительной власти и судами. См.: Telekabel Wien GmbH v Constantin Film Verleih GmbH and Wega Filmproduktionsgesellschaft mbH (C-314/12). Judgment of the Court (Fourth Chamber) of 27 March 2014. URL: http://curia.europa.eu/juris/liste.jsf?num=c-314/12 (дата обращения – 16 июля 2016 г.).

[66] См., напр.: Telekabel Wien GmbH v Constantin Film Verleih GmbH and Wega Filmproduktionsgesellschaft mbH (C-314/12); Определение Конституционного Суда Российской Федерации от 17 июля 2014 г. № 1759-О «Об отказе в принятии к рассмотрению жалобы

идентичность в целом и в цифровой среде в частности пока носит ограниченный характер. Во всяком случае блокирование учетной записи индивида и фильтрация передаваемой с ее использованием информации в отсутствие неправомерного поведения с его стороны, но при наличии правонарушений со стороны информационного посредника, который обеспечивает возможность создания цифровой идентичности и управления ею, признаются отечественными и зарубежными судами допустимыми[67].

Значительную опасность для индивида представляет получение другими лицами информации, с использованием которой обеспечивается доступ к его цифровой идентичности, что делает возможным управление ею без согласия индивида. В отечественной юридической литературе такая информация причисляется к персональным данным, под которыми понимается любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) [68] . В зарубежной юридической литературе в структуре цифровой идентичности выделяется формальная (token) или операционная (transactional) составляющая, использование которой связывается с правом на идентичность[69]. Она охватывает

гражданина Харитонова Владимира Владимировича на нарушение его конституционных прав пунктом 2 части 2 статьи 15^1 Федерального закона «Об информации, информационных технологиях и о защите информации» и пунктом 2 статьи 3 Федерального закона «О внесении изменений в Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» и отдельные законодательные акты Российской Федерации» // СПС КонсультантПлюс.

[67] См., напр.: Определение Московского городского суда от 10 ноября 2016 г. по делу № 33-38783/2016, которым было удовлетворено требование о признании незаконной деятельности интернет-ресурсов (социальная сеть LinkedIn) по сбору, использованию и хранению персональных данных граждан Российской Федерации, обязании принять меры по ограничению доступа к информации в сети Интернет, обрабатываемой с нарушением законодательства Российской Федерации в области персональных данных // СПС КонсультантПлюс.

[68] См., напр.: Жарова А.К., Елин В.М. Источники понятий «персональные данные» и частная жизнь лица в российском праве // Вестник Академии права и управления. 2017. № 46 (1). С. 69–78. Данными авторами, в частности, предложено уточнить законодательное определение «персональные данные» для включения анонимных записей, которые в будущем могут использоваться в сочетании с другой информацией для идентификации отдельных субъектов данных.

[69] См., напр.: Sullivan C. Digital Identity – The Legal Person? // Computer Law & Security Review. 2009. V. 25. P. 227–236; Sullivan C., Stalla-Bourdillon S. Digital Identity and French

только идентификаторы, то есть информацию, которая используется для доступа к цифровой идентичности. Выделение данной составляющей представляется оправданным, поскольку позволяет определить минимальный набор информации, необходимый для идентификации индивида – обладателя цифровой идентичности при вступлении в правоотношения с ним. Установление его личности осуществляется путем предоставления им информационному посреднику идентификаторов, которые последний сопоставляет с имеющимися у него идентификаторами данного индивида и проводит между ними тождество. Подобное установление личности основано на предположении, что только индивид, а также информационный посредник обладают соответствующими идентификаторами. Однако при идентификации информационный посредник проверяет тождество не между индивидом и идентификаторами, а между предоставленными ему и имеющимися у него идентификаторами[70]. В этой связи всегда существует вероятность, что от имени индивида с использованием его цифровой идентичности выступает неуполномоченное лицо, получившее доступ к соответствующим идентификаторам, например, с целью неправомерного использования информации о личности, ее модификации и блокирования, хищения денежных средств индивида, причинения ему вреда в иной форме. Доказать факт правонарушения и установить личность нарушителя не всегда представляется возможным, что в свою очередь влияет на защиту прав личности в цифровой среде.

Так, отечественными судами рассматривались дела о защите чести, достоинства и деловой репутации, защите персональных данных, связанные со взломом аккаунтов в социальных сетях и распространением от имени их

Personality Rights – A Way Forward in Recognising and Protecting an Individual's Rights in His/Her Digital Identity // Computer Law & Security Review. 2015. V. 31. P. 268–279.

[70] В этой связи австралийский ученый-юрист К. Сулливан (Sullivan C. Digital Identity – The Legal Person?) отмечает аналогию между цифровой идентичностью и юридическим лицом. Действительно, как и юридические лица цифровая идентичность образуется не с рождением индивида, а создается им. Ее создателями может являться широкий круг субъектов: отдельные физические лица, группы физических лиц, юридические лица, а также и государственные органы. Как учредители юридического лица могут отличаться от его участников, так и фактические обладатели цифровой идентичности могут не совпадать с их создателями.

обладателей порочащих их сведений. При этом суды признавали за истцами, аккаунты которых взломаны, право на компенсацию морального вреда в случаях, когда факт взлома и личность нарушителя были установлены[71]. При отсутствии соответствующих доказательств суды исходят из того, что размещение информации осуществлялось по воле обладателя аккаунта[72]. В зарубежной правовой науке отмечается, что в финансовой сфере, например, при оказании услуг интернет-банкинга возмещение вреда в связи со взломом учетной записи может осуществляться за счет средств информационного посредника, которым в данном случае выступает финансовое учреждение[73], кроме случаев, когда получатель услуги интернет-банкинга действовал с грубой небрежностью[74].

Анонимность личности в сети Интернет как одно из проявлений ее цифровой идентичности исключает предоставление информационному посреднику информации, на основании которой он или третье лицо может ее идентифицировать. В отличие от права на идентичность право на анонимность в сети Интернет заключается в возможности личности использовать сеть Интернет без указания сведений, позволяющих ее идентифицировать. Данное право призвано оградить личность от предъявления к ней необоснованных требований о предоставлении таких сведений и нарушения процедуры их раскрытия информационными посредниками. Анонимность была названа одной из важнейших гарантий свободы выражения мнения в докладе специального докладчика ООН по вопросу о поощрении и защите права на свободу мысли и свободу выражения мнения Д. Кайе 22 мая 2015 г., который призвал государства не препятствовать анонимности в сети Интернет[75]. Верховный Суд США

---

[71] См., напр.: Апелляционное определение Московского областного суда от 24 июня 2015 г. по делу № 33-14941/2015 // СПС КонсультантПлюс.

[72] См., напр.: Определение Приморского краевого суда от 24 августа 2015 г. по делу № 33-7346/2015 // СПС КонсультантПлюс.

[73] См.: Meulen N.S. van der. You've Been Warned: Consumer Liability in Internet Banking Fraud // Computer Law & Security Review. 2013. V. 29. P. 713–718.

[74] В то же время перечень таких случаев имеет тенденцию к сокращению. См.: Там же.

[75] Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye // Human Rights Council. 29th Session, Agenda item 3 // URL: http://ru.scribd.com/doc/266938105/A-HRC-29-32-AEV (дата обращения – 20 июля 2016 г.). В докладе также содержится призыв к государствам не препятствовать развитию шифровальных

неоднократно[76] признавал право на анонимность в сети Интернет составляющей свободы слова и ассоциаций, распространяя на него Первую Поправку к Конституции США. Для судебной практики в государствах – членах Европейского союза характерно его признание в качестве компонента права на неприкосновенность частной жизни[77]. Точки зрения на право на анонимность в Интернете как на отдельную составляющую права на неприкосновенность частной жизни придерживаются и в отечественной юридической литературе[78]. Отечественный ученый-юрист М.В. Якушев справедливо отмечает совокупность факторов, которые «не позволяют поставить знак равенства между понятием право на анонимность как одним из компонентов права на неприкосновенность частной жизни и понятием основные права и свободы человека»[79].

Вместе с тем анонимные коммуникации представляют проблему для органов государственной власти при обеспечении осуществления и защиты прав других лиц. Решение данной проблемы связано с формированием правовых оснований и преодолением технических ограничений для идентификации личности. Правовые основания обеспечиваются путем возложения на информационных посредников обязанностей по оказанию услуг физическим лицам только при условии указания ими сведений, позволяющих идентифицировать их личность, а также детализации процедуры предоставления информации о личности по запросам государственных органов. Подобная идентификация личности может являться необходимым условием при

(криптографических) средств, которые наряду с анонимностью выступают одной из гарантий свободы выражения мнения.

[76] McIntyre v. Ohio Elections Commission, 514 U.S. 334, 341–342 (1995). URL: http://caselaw.findlaw.com/us-supreme-court/514/334.html (дата обращения – 1 декабря 2016 г.); NAACP v. State of Alabama ex rel. Patterson, 357 U.S. 449, 462 (1958). URL: http://caselaw.findlaw.com/us-supreme-court/357/449.html (дата обращения – 1 декабря 2016 г.).

[77] См.: Устинович Е.С. Зарубежный опыт законодательного регулирования анонимности в Интернете и судебная практика // Вопросы экономики и права. 2016. № 92. С. 7–9.

[78] См., напр.: Якушев М.В. Международно-политические проблемы идентификации в интернете // Индекс безопасности. 2013. Т. 19. № 1 (104). С. 87–102; Андрощук Г. Право на анонимность в интернете: проблемы регулирования // Интеллектуальная собственность. Авторское право и смежные права. 2015. № 12. С. 57–70.

[79] Якушев М.В. Там же. С. 91.

осуществлении доступа к сети Интернет[80], при регистрации доменных имен, при использовании различных служб, получении отдельных услуг и осуществлении платежей в сети Интернет. В России регистрация доменных имен в доменных зонах .RU и .РФ предполагает обязательную идентификацию личности администратора доменного имени, которая в то же время осуществляется в соответствии с правилами, установленными специализированной некоммерческой организацией[81]. Однако правовых оснований может оказаться недостаточно для идентификации личности, если она намеренно скрывает информацию, позволяющую ее идентифицировать, с использованием специализированных технических средств (например, анонимайзеров). Информации, сохраняющейся у информационных посредников, может быть не достаточно для идентификации такой личности. Преодоление данных технических ограничений связано с развитием правового регулирования, в соответствии с которым расширяется сфера обязательной идентификации личности и на информационных посредников возлагаются обязанности по хранению информации о действиях в сети Интернет их пользователей[82]. Право на анонимность призвано разрешить конфликт между необходимостью идентификации личности и сохранением в тайне информации о личности. Оно определяет пределы анонимных коммуникаций и, соответственно, случаи и порядок, при соблюдении которых сведения о личности становятся доступными другим лицам.

Право на анонимность в сети Интернет обеспечивается с использованием специализированных технических средств, которые также позволяют обходить ограничения доступа к информационным ресурсам, установленные в соответствии с законодательством того или иного государства. В результате

---

[80] См.: Постановление Правительства Российской Федерации от 23 января 2006 г. № 32 «Об утверждении Правил оказания услуг связи по передаче данных» // СЗ РФ. 2006. № 5. Ст. 553.

[81] Правила регистрации доменных имен в доменах .RU и .РФ, утвержденные Координационным центром национального домена сети Интернет // URL: https://cctld.ru/files/pdf/docs/rules_ru-rf.pdf?v=30 (дата обращения – 8 октября 2016 г.).

[82] В то же время в Европейском союзе возложение соответствующих обязанностей на информационных посредников было признано не соответствующим Хартии Европейского союза об основных правах (см. §3 главы 2 настоящего исследования).

возникает вопрос о правомерности использования таких технических средств. В правовом государстве на этот вопрос следует ответить утвердительно. В этой связи разработчики проекта федерального закона, направленного на ограничение возможности подобного их использования, отмечают, что «технологии направления трафика российских интернет-пользователей через зарубежные серверы, анонимные прокси-серверы, виртуальные частные сети легальны, существует широкий спектр возможностей их правомерного применения» [83]. Принятый на его основе федеральный закон[84], не вполне справедливо называемый в отдельных средствах массовой информации законом о запрете анонимайзеров[85], в действительности направлен не на их запрет, а на обеспечение соблюдения установленных законодательством ограничений доступа к информационным ресурсам. Данный федеральный закон определяет правовые основы использования специализированных технических средств для анонимных коммуникаций и не препятствует признанию и осуществлению права на анонимность в сети Интернет.

В условиях развития средств цифровых коммуникаций проблема идентификации и анонимности обостряется. Обеспечить защиту прав личности в цифровой среде в полной мере невозможно, если без ее согласия на основе предоставляемой ею информации она может быть идентифицирована. Такая идентификация создает опасность недобросовестного использования информации о личности, нарушения ее прав и причинения ей вреда. Хотя анонимность выступает одной из разновидностей самозащиты прав личности, она не позволяет ей воспользоваться многочисленными службами в сети Интернет и ограничивает возможности коммуникации с другими лицами в цифровой среде. В условиях

---

[83] Пояснительная записка к проекту федерального закона № 195446-7 «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации». URL: http://asozd2.duma.gov.ru/main.nsf/(ViewDoc)?OpenAgent&work/dz.nsf/ByID&07CFD475394B5E984325813A0065B8B8 (дата обращения – 30 июля 2017 г.).

[84] Федеральный закон от 29 июля 2017 г. № 276-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» // СЗ РФ. 2017. № 31. Ст. 4825.

[85] См. напр.: Как запрет анонимайзеров отразится на пользователях Интернета. URL: https://www.kp.ru/daily/26707/3732941/ (дата обращения – 30 июля 2017 г.).

анонимности личности, совершившей противоправное деяние с использованием сети Интернета, существенно ограничиваются возможности защиты прав других лиц. Абсолютная анонимность препятствует вовлечению личности в системы электронного правительства [86] , развитию технологий, ориентированных на интересы и потребности конкретной личности, осуществлению свободы выражения мнения, свободы договора и свободы предпринимательской деятельности в цифровой среде.

Невозможность идентифицировать анонимные личности и привлечь к ответственности за совершенное правонарушение способствовала распространению ответственности за их действия на информационных посредников. Это подтверждается решением Европейского суда по правам человека по делу компании «Делфи АС» (Delfi AS) против Эстонии[87], в котором обжаловалось привлечение компании к ответственности за размещение на принадлежащем ей новостном интернет-портале оскорбительных комментариев третьих лиц. В данном деле суд пришел к выводу о том, что поскольку компания-заявительница сама разрешила оставлять комментарии незарегистрированным индивидам, то тем самым она взяла на себя определенную ответственность за содержание таких комментариев. Характерно, что выработанные Судом справедливости Европейского союза принципы ответственности информационных посредников за действия их пользователей непосредственно связываются с их возможностью контролировать такие действия и своевременно

[86] В сфере публично-правовых отношений цифровая идентичность приобретает качества так называемого электронного гражданина. В отличие от «сетевых граждан» (netizens), под которыми американские ученые-юристы в середине 90-х годов прошлого века понимали виртуальных личностей в киберпространстве (см., напр.: Bennahum D.S. United Nodes of Internet: Are We Forming a Digital Nation? // Crypto Anarchy, Cyberstates, and Pirate Utopias / edited by P. Ludlow. L. : MIT Press, 2001. P. 66.), не связанных суверенитетом конкретного государства, электронный гражданин – это цифровая идентичность, предназначенная для получения ее администратором (физическим лицом) государственных или муниципальных услуг в электронном виде. Соответственно для получения некоторых услуг индивид – обладатель цифровой идентичности должен быть достоверно идентифицирован, в том числе с представлением при ее создании документов, удостоверяющих его личность, и использованием электронной подписи.

[87] Компания «Делфи АС» (Delfi AS) против Эстонии. Постановление Европейского Суда по правам человека от 16 июня 2015 г. (жалоба № 64569/09) // Бюллетень Европейского Суда по правам человека. 2015. № 11(161).

устранять возникшие правонарушения при их обнаружении, в том числе по заявлениям других лиц[88]. При наличии у информационного посредника таких возможностей он отвечает за совершенное правонарушение наряду с пользователем, совершившим соответствующие действия. Данный подход положен в основу, так называемых безопасных гаваней (safe harbor), которые в настоящее время применяются как в США, так и в Европейском союзе и России: если действия информационного посредника имеют технический, автоматический и пассивный характер, указывающий на незнание им содержания хранящейся у него информации и невозможность контролировать ее, то в этом случае он не несет ответственность за действия других лиц, совершенные с использованием такой информации, то есть находится в безопасной гавани. В ином случае информационный посредник отвечает за их действия как за свои собственные.

В международных документах справедливо отмечается, что «подходы к регулированию, разработанные для других средств коммуникации, таких как телефония или телевидение, не могут просто быть перенесены в сеть Интернет, но должны быть специально разработаны для этого»[89]. Правовое регулирование в цифровой среде основано на подходе, при котором допускается отличие цифровой идентичности от реальной. Согласно данному подходу признается право индивида самостоятельно определять свою цифровую идентичность, по своему усмотрению вносить в нее изменения независимо от того, соответствует она его реальной идентичности или нет. В этой связи основным решением проблемы идентификации и анонимности личности в цифровой среде, которое находит воплощение в национальном праве различных государств, становится так называемая деидентификация. Под ней понимаются действия, которые

[88] Google France SARL and Google Inc. v Louis Vuitton Malletier SA (C-236/08), Google France SARL v Viaticum SA and Luteciel SARL (C-237/08) and Google France SARL v Centre National de Recherche en Relations Humaines (CNRRH) SARL and Others (C-238/08). Judgment of the Court of Justice (Grand Chamber) of 23 March 2010. URL: http://curia.europa.eu/juris/liste.jsf?num=C-236/08 (дата обращения – 16 июля 2016 г.); L'Oréal SA and Others v eBay International AG and Others (C-324/09). Judgment of the Court of Justice (Grand Chamber) of 12 July 2011. URL: http://curia.europa.eu/juris/liste.jsf?num=C-324/09 (дата обращения – 16 июля 2016 г.).

[89] United Nations, Organization of American States, Organization for Security and Co-operation in Europe, African Commission on Human and Peoples' Rights. «Joint Declaration Concerning the Internet».

осуществляются с информацией о личности информационным посредником и направлены на ограничение возможности последующей идентификации соответствующей личности с использованием такой информации. В отличие от анонимности, которая в целом исключает данную возможность, при деидентификации установление личности на основе деидентифицированной информации все еще допускается, но при соблюдении определенных условий. Таким образом, деидентификация занимает промежуточное положение между идентификацией и анонимностью. В зарубежной правовой науке справедливо отмечается, что правовая охрана права на неприкосновенность частной жизни не может быть абсолютной по модели «все или ничего» и в настоящее время в большей степени соответствует относительной модели «ограниченного доступа», при которой обеспечивается «некоторая» неприкосновенность и «некоторый» контроль[90]. Подобная правовая охрана в равной степени создает условия для осуществления и защиты прав личности, информация о которой используется, и прав других лиц, то есть права личности охраняются в той мере, в которой это не препятствует осуществлению прав других лиц.

В государствах с различными правовыми традициями подходы к деидентификации при решении проблемы анонимности и идентификации отличаются. Так, в российском праве ранее разрешалось свободное использование персональных данных при условии их обезличивания, а именно совершения действий, в результате которых невозможно определить принадлежность персональных данных конкретному лицу (субъекту персональных данных)[91]. В настоящее время определение понятия «обезличивание» допускает такую возможность при использовании дополнительной информации[92].

Подход к деидентификации в государствах – членах Европейского союза был выработан в рамках реформы правового регулирования в области защиты

---

[90] Mironenko O. Aviation Security and Protection of Individuals: Technologies and Legal Principles. Oslo: University of Oslo, 2016. 532 p. P.36.

[91] См.: Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

[92] См.: Федеральный закон от 25 июля 2011 г. № 261-ФЗ «О внесении изменений в Федеральный закон «О персональных данных» // СЗ РФ. 2011. № 31. Ст. 4701.

данных и основан на их псевдонимизации. При этом данные о личности подвергаются такой обработке, в результате которой они утрачивают связь с конкретным индивидом (субъектом данных) без использования дополнительной информации. В этой связи понятие псевдонимизации данных выступает аналогом понятия обезличивания, которое используется в отечественном законодательстве. Отличие понятия псевдонимизация заключается в том, что соответствующая дополнительная информации должна храниться отдельно и являться объектом технических и организационных мер, гарантирующих, что данные не связаны с определенным или определяемым лицом. Другими словами, конкретные идентификаторы субъекта данных заменяются специальными кодами, при этом информация, позволяющая связать идентификаторы и коды, храниться отдельно. В то же время в зарубежной юридической литературе справедливо указывается на то, что подход, основанный на раздельном хранении данных и дифференциации правовых требований к операторам псевдонимных данных является неполным решением[93]. Псевдонимизация может привести к ослаблению ответственности информационных посредников за использование данных о личности при незначительной модификации существующий мер по обеспечению их защиты. При соблюдении обязанности по осуществлению псевдонимизации информационным посредником гарантии осуществления аналогичных действий его контрагентами, которым он передает информацию о личности, отсутствуют.

Другого подхода придерживается Федеральная торговая комиссия США[94]. Он заключается в том, что приемлемость деидентификации зависит от конкретных обстоятельств рассматриваемого дела, в том числе доступных методов и технологий. При этом деидентификация данных сама по себе не является достаточной мерой для защиты прав человека в цифровой среде, и в этой

[93] Cheung A.S.Y. Re-personalizing Personal Data in the Cloud // Privacy and Legal Issues in Cloud Computing / Ed. by Cheung A.S.Y., Weber R.H. Cheltenham: Edward Elgar Publishing, 2015. P. 90.

[94] Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers (FTC Report March 2012) 21-2. URL: https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf (дата обращения – 16 июля 2016 г.).

связи указывает на вероятность, что индивид будет повторно определен. Комиссия рекомендует организациям проводить деидентификацию как можно более тщательно и брать на себя публичные обязательства не осуществлять попыток реидентификации[95]. Комиссия также рекомендует требовать в рамках договорных отношений таких же публичных обязательств от любого лица, с которыми они делятся информацией об индивиде. Эти требования должны распространяться и на других лиц, которым в последующем может быть передана информация о личности. Таким образом, данный подход не ограничивается техническими мерами по деидентификации данных, но также предусматривает возложение на всех информационных посредников, которыми была получена информация об индивиде, обязанностей не проводить реидентификацию.

Современные системы обработки информации позволяют эффективно оперировать даже деидентифицированной информацией, создавая опасность нарушения права на идентичность и других прав человека[96]. Информационные посредники за счет метаданных, которые сохраняются у них и относятся к цифровой идентичности индивида, могут связать информацию, лишенную идентификаторов, с конкретным человеком и тем самым обеспечить его идентификацию. При этом снижается роль согласия личности на обработку информации о ней, поскольку для получения необходимых результатов

---

[95] Под реидентификацией понимаются действия, обратные деидентификации, то есть направленные на установление связи между конкретной личностью и информацией о нем, которой обладает информационный посредник.

[96] См., напр.: Kshetri N. Big Data's Impact on Privacy, Security and Consumer Welfare // Telecommunications Policy. 2014. V. 38. 1134–1145; Mantelero A., Vaciago G. Data Protection in a Big Data Society. Ideas for a Future Regulation // Digital Investigation. 2015. V. 15. P 104 – 109. Данная проблема обостряется в условиях развития технологий «Больших данных» , в основе определения которого лежит анализ трех компонент: (1) объема данных, (2) разнообразия данных и (3) скорости изменения данных. В последнее время в дополнение к указанным компонентам учитывается изменчивость и сложность данных. См.: Big Data. URL: http://www.gartner.com/it-glossary/big-data/ (дата обращения – 3 апреля 2016 г.); Big Data: What it is and why it matters. URL: https://www.sas.com/en_us/insights/big-data/what-is-big-data.html (дата обращения – 3 апреля 2016 г.). В то же время следует согласиться с подходом, приведенным в отечественной правовой доктрине, согласно которому с правовой точки зрения под «Большими данными» понимаются не столько данные, сколько инструменты и методы их обработки, влияющие на осуществление права на неприкосновенность частной жизни. См.: Савельев А.И. Проблемы применения законодательства о персональных данных в эпоху «Больших данных» (Big Data) // Право. Журнал Высшей школы экономики. 2015. № 1. С. 47.

информационным посредникам не обязательно иметь в наличии сведения об идентификаторах. Большинство индивидов при создании и управлении цифровой идентичностью дает согласие на обработку составляющей ее информации, должным образом не ознакомившись с условиями такого согласия, не понимая его правовых последствий и не предвидя последующее использование информации о своей личности[97]. В результате наличие согласия индивида на обработку информации о нем становится слабым, по существу формальным условием, не обеспечивающим конфиденциальности информации и соблюдения прав личности в цифровой среде. Это способствует дальнейшему развитию методов деидентификации и повышению ответственности информационных посредников и других лиц, участвующих в обработке информации о личности, за раскрытие такой информации и нарушение требований к ее обработке.

Таким образом, в цифровой среде индивиды вступают в правоотношения, осуществляют права и обязанности с использованием уникальной совокупности информации о личности, представленной в цифровой форме или другими словами – цифровой идентичности. Ее создание связано с правом на идентичность, которое признается в правовой доктрине одним из основных прав человека и заключается в признании и уважении индивида как уникальной личности. В соответствии с ним обеспечивается охрана информации, необходимой и достаточной для идентификации личности в цифровой среде. В отличие от права на идентичность право на анонимность в сети Интернет означает возможность личности использовать сеть Интернет без указания сведений, позволяющих ее идентифицировать. Правовое регулирование в цифровой среде основано на подходе, при котором допускается отличие цифровой идентичности от реальной. Согласно данному подходу признается право индивида самостоятельно определять свою цифровую идентичность, по своему усмотрению вносить в нее

---

[97] 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. V. 4:3. P. 560. В данной статье указывается на 244 часа в год, которое надо было бы потратить пользователям, чтобы ознакомиться со всеми политиками конфиденциальности на сайтах, которые они посещают в течении года, – это чуть больше, чем половина времени, проводимого в сети Интернет.

изменения независимо от того, соответствует она его реальной идентичности или нет. В цифровой среде проблема идентификации и анонимности обостряется. Ее решение связано с так называемой деидентификацией, в соответствии с которой на информационных посредников возлагаются обязанности по осуществлению действий с информацией о личности, направленных на ограничение возможности ее идентификации. При этом повышается ответственности информационных посредников и иных лиц, участвующих в обработке информации о личности за раскрытие такой информации и нарушение требований к ее обработке.

§3. Принцип правового равенства в цифровой среде

В условиях развития информационных и коммуникационных технологий обостряется проблема обеспечения социального равенства между различными индивидами, их правами, условиями их осуществления. Как справедливо отмечает В.С. Нерсесянц, «в социальной сфере равенство – это всегда правовое равенство, формально-правовое равенство»[98], «правовое равенство в свободе как равная мера свободы означает и требование соразмерности, эквивалента в отношениях между свободными индивидами, как субъектами права»[99]. Данное требование распространяется и на отношения в цифровой среде. Оно основано на принципе правового равенства, в котором выражается равенство индивидов как формально (юридически) свободных личностей.

Развитие человека в современном обществе, осуществление им своей свободы зависит от наличия у него доступа к информации и знаниям, который в свою очередь определяется доступностью для него информационных и коммуникационных технологий. Возникает проблема неравенства в доступе к таким технологиям между различными социальными группами[100]. Она приводит к

---

[98] Проблемы общей теории права и государства: Учебник для вузов / Под общ. ред. академика РАН, д. ю. н., проф. В.С. Нерсесянца. М.: Норма, 2006. 832 с. С. 163.

[99] Там же. С. 162.

[100] Veit D., Huntgeburth J. Foundations of Digital Government. Springer Berlin Heidelberg, 2014. 158 p. P. 39.

расслоению общества и порождает социальные конфликты, например, между городским и сельским населением, образованной элитой и традиционными общинами. В условиях социального государства ее решение зависит от создания условий для равного доступа к соответствующим технологиям максимально широкому кругу лиц и обеспечения цифрового равенства[101].

С правовой точки зрения цифровое равенство соответствует новому этапу развития принципа правового равенства и заключается в равенстве индивидов в возможностях осуществления их прав с использованием информационных и коммуникационных технологий. С одной стороны, речь идет о физической доступности соответствующих технологий, то есть о физических возможностях индивидов использовать информационные и коммуникационные технологии, включая их территориальную удаленность от индивидов, а с другой – от наличия у индивидов знаний, навыков и умений, необходимых для использования соответствующих технологий. В этой связи обеспечение цифрового равенства обусловлено развитием инфраструктуры доступа к данным технологиям и повышением уровня компьютерной грамотности населения. Социальное и правовое значение доступа к информационным и коммуникационным технологиям подтверждает позиция ООН, согласно которой они представляют собой «инструмент продвижения прав человека; возможность преодолевать бедность в широком смысле слова; обеспечивать лучшие шансы получить качественное образование; поощрять занятость; и в целом «включать» человека в жизнь общества»[102]. Справедливо, что «одна из задач юридической науки состоит в том, чтобы на каждом новом историческим этапе наполнить правовой принцип формального равенства адекватным данному историческому контексту социальным содержанием» [103] . На современном этапе цифровое неравенство

[101] Как отмечается в Окинавской хартии глобального информационного общества, «все люди повсеместно, без исключения должны иметь возможность пользоваться преимуществами глобального информационного общества». См.: URL: http://www.iis.ru/library/okinawa/charter.ru.html (дата обращения – 30 сентября 2016 г.).

[102] Горелик А.С. Императив доступности // Информационное общество. 2010. № 1. С. 6.

[103] Лапаева В.В. Правовой принцип формального равенства // Журнал российского права. 2008. № 2 (134). С. 80.

представляет собой проблему, решение которой возможно на основе принципа правового равенства и способствует его конкретизации и дальнейшему осмыслению.

Поскольку цифровое равенство является одним из проявлений правового равенства, то для его обеспечения в национальном праве осуществляется выработка правовых механизмов разрешения возникающих социальных противоречий. Такие механизмы не имеют своей целью абсолютное преодоление неравенства и обеспечивают только ограниченное социальное равенство, связанное с созданием равных возможностей осуществления только части прав человека и только в тех пределах, которые соответствуют социальной справедливости в данном конкретном государстве. В этой связи обеспечение правового равенства в цифровой среде связано с повышением роли государства при выполнении им своей социальной функции.

В современном обществе преодоление цифрового неравенства начинается с обеспечения юридически равных возможностей для осуществления права на доступ к сети Интернет. В свою очередь данное право создает условия для последующего осуществления других прав в онлайновой среде, включая право на доступ к информации. Для этих целей государство обеспечивает создание инфраструктуры доступа к сети Интернет на базе общедоступных библиотек и иных государственных учреждений, реализует мероприятия, направленные на повышение уровня компьютерной грамотности населения [104] . В данных мероприятиях проявляются основные признаки социального государства – социальное равенство, социальное обеспечение и повышение благосостояния граждан. Как справедливо отмечает В.А. Четвернин, «чрезмерная ориентация государства на принцип социальной государственности в ущерб господству права приводит к перегруженности государства, непомерному разбуханию и

[104] См., напр.: Hilbert M. The End Justifies the Definition: The Manifold Outlooks on the Digital Divide and Their Practical Usefulness for Policy-Making // Telecommunications Policy. 2011. № 35 (8). P. 715–736; Захаров А.Л., Суркова О.Е. Цифровое неравенство России // Евразийский юридический журнал. № 6(85). 2015. С. 301–303; Данилов Н.А. Социальная справедливость в информационном обществе: проблема цифрового равенства // Информационное право. 2012. № 2. С. 5–7.

неэффективности государственного аппарата, снижению производства, оттоку капитала и инфляции»[105]. В этой связи пределы обеспечения правового равенства при осуществлении права на доступ к сети Интернет определяются исходя из стандартов социального обслуживания населения, которые устанавливаются в каждом государстве с учетом его социально-экономического положения.

Данное право как социальное право человека гарантируется государством в соответствии с принципом универсальности публичных услуг. Этот принцип заключается в обеспечении правового равенства в доступе к социально-значимым услугам, он распространяется на создание и обслуживание пунктов открытого доступа, на базе которых организуется открытый доступ к минимальному набору коммуникационных и информационных услуг. На это, в частности, указывают Рекомендации Комитета министров Совета Европы № R(99)14 «О предоставлении публичных услуг, затрагивающих новые информационно-коммуникационные сервисы»[106]. Создание таких пунктов открытого доступа к Интернету, в том числе на базе библиотек или отделений почтовой связи, является минимальным стандартом, который может быть реализован в развивающихся государствах. При этом существует тенденция к снижению роли пунктов коллективного доступа к сети Интернет, в связи с тем что компьютеры, как основные устройства для выхода в сеть Интернет, замещаются различными мобильными устройствами (смартфонами, планшетами и т.д.)[107]. В развитых государствах реализация данного принципа предполагает создание инфраструктуры широкополосного и беспроводного доступа к сети Интернет.

---

[105] Проблемы общей теории права и государства: Учебник для вузов. С. 639.

[106] Recommendation № R(99)14 on Universal Community Service Concerning New Communication and Information Services and its Explanatory Memorandum // URL: http://www.coe.int/t/dghl/standardsetting/media/doc/cm_EN.asp (дата обращения – 31 июля 2016 г.).

[107] Предполагается, что в Российской Федерации до конца 2016 года в населенных пунктах численностью более 50 тыс. жителей пункты коллективного доступа (ПКД) в сеть Интернет завершат свою работу. По данным Россвязи, в 2015 году трафик всех российских ПКД составил 564 Гб – это сопоставимо с ежегодным трафиком, который создает один пользователь сети Интернет в течение года. При этом данный показатель уменьшился на 10% по сравнению с предыдущим годом. См. Пункты коллективного доступа в Интернет могут закрыться в России до конца года. URL: http://www.interfax-russia.ru/Moscow/main.asp?id=775760&p=17 (дата обращения – 28 октября 2016 г.).

Так, в России оказание универсальных услуг связи, к которым в соответствии с отечественным законодательством в области связи[108] относятся, в частности, услуги по передаче данных и предоставлению доступа к сети Интернет, гарантируется с применением не только средств коллективного доступа, но и точек доступа, которые подключаются с использованием волоконно-оптической линии связи и обеспечивают возможность передачи данных на пользовательское оборудование со скоростью не менее чем 10 Мбит/с.

Правовое равенство при осуществлении права на доступ к сети Интернет обеспечивается не только за счет реализации государством своей социальной функции, но и за счет устранения различных форм дискриминации при осуществлении данного права. Такая дискриминация возникает в связи с использованием операторами связи, предоставляющими широкополосный доступ к сети Интернет[109], специальных фильтров для ограничения доступа к определенной информации, изменения ими скорости доступа к ней или условий доступа для отдельных видов технических средств. В данном случае принцип правового равенства конкретизируется в принципе сетевой нейтральности, который впервые был сформулирован в американской правовой науке (Т. Ву)[110]. Он заключается в том, что при оказании услуг доступа к сети Интернет оператор связи должен нейтрально, равным образом относиться ко всем видам передаваемых им данных и не создавать препятствий для получения любых данных его абонентами по своему выбору.

Принцип сетевой нейтральности восходит к тем же идеям, которые заложены в принципе технологической нейтральности. Он определяет, насколько правовое регулирование должно быть нейтральным к использованию тех или иных технологий. В соответствии с данным принципом правовое регулирование,

---

[108] Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи» // СЗ РФ. 2003. № 28. Ст. 2895.

[109] Широкополосным является доступ к сети Интернет, который осуществляется на основе выделенной линии связи и скорость которого превышает скорость доступа к сети Интернет с использованием модема и телефонной сети общего пользования.

[110] Wu T. Network Neutrality, Broadband Discrimination // Journal of Telecommunications and Hight Technology Law. 2003. P. 141–142.

с одной стороны, должно быть одинаковым в онлайновой и офлайновой средах, а с другой – не должно создавать предпочтения или дискриминацию при использовании отдельных технологий[111]. Так же как и сетевая нейтральность, технологическая нейтральность выражается в независимости от технологий. Воплощение данных принципов в правах человека позволяет им сохранять универсальность по отношению к постоянно изменяющимся технологиям. Одновременно технологическая нейтральность и сетевая нейтральность стимулируют конкуренцию и технологическое развитие, исключая необоснованное создание привилегированного режима для одних технологий в ущерб другим. Различие данных принципов заключается не только в том, что технологическая нейтральность связана с более широким спектром технологий, но и в том, что она ориентирована на процессы правотворчества и создание технологически нейтральных правовых норм. Для обеспечения сетевой нейтральности технологической нейтральности правовых норм недостаточно. В данном случае дискриминация возникает из-за использования операторами связи технологически зависимого подхода к оказанию услуг. Поэтому обеспечение сетевой нейтральности связано с возложением на них обязанностей по соблюдению технологически нейтрального подхода в своей деятельности.

При установлении баланса интересов операторов связи, контент- и сервис-провайдеров и интересов личности принцип сетевой нейтральности обусловлен необходимостью создания условий для осуществления и защиты не только права на доступ к сети Интернет, но и других прав человека[112]. Это позволяет

---

[111] Rees C. Taking Sides on Technology Neutrality // SCRIPT-ed. 2007. V. 4. I. 3. P. 266.

[112] Обусловлено это тем, что принцип формального правового равенства конкретизируется в принципе соразмерности (см. §3 главы 2 настоящего исследования). Так, в отношении защиты права на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени Конституционный Суд Российской Федерации указывает, что «право на свободу информации и право на свободное использование своих способностей и имущества для предпринимательской и иной не запрещенной законом экономической деятельности могут быть ограничены федеральным законом… на основе принципа юридического равенства… и вытекающего из него принципа соразмерности, т.е. в той мере, в какой это необходимо в Российской Федерации как демократическом и правовом государстве в целях защиты прав, гарантированных статьями 23, 24 (часть 1) и 25 Конституции Российской Федерации.». См.: Постановление Конституционного Суда Российской Федерации от 31 марта 2011 г. № 3-П «По делу о проверке конституционности части третьей статьи 138 Уголовного кодекса Российской

предотвратить правовую охрану права на доступ к сети Интернет в ущерб другим правам и свободам человека, таким как свобода договора и свобода предпринимательской деятельности. В этой связи в европейской правовой науке справедливо отмечается, что технологическая нейтральность не является панацеей и «законодателю следуют учитывать, что технологически зависимый подход может обеспечить лучшее правовое регулирование»[113]. Технологическая зависимость права, то есть зависимость правового воздействия на субъектов правоотношений от использования ими конкретных технологий, в данном случае направлена на предотвращение нарушений прав человека, которые могут возникнуть в связи с избыточным вмешательством государства в сферу их осуществления при соблюдении принципа сетевой нейтральности.

Существуют различные подходы к соблюдению данного принципа – от полной сетевой нейтральности до компромиссной, допускающей определенные исключения для действий операторов связи, предоставляющих широкополосный доступ к сети Интернет. Компромисс основан на обеспечении баланса различных интересов с учетом структуры телекоммуникационного рынка, состояния телекоммуникационной инфраструктуры и интересов различных субъектов правоотношений в сети Интернет.

Наиболее значимым в этой связи являются модели регулирования сетевой нейтральности в США, а также Европейском союзе и составляющих его государств, поскольку они оказывает влияние на содержание данного принципа в национальном праве других государств.

Модель регулирования сетевой нейтральности в США [114] основана на подходе, сформулированном Т.Ву и воспроизведенном Федеральной комиссией

Федерации в связи с жалобами граждан С.В. Капорина, И.В. Коршуна и других» // СЗ РФ. 2011. № 15. Ст. 2191.

[113] Rees C. Taking Sides on Technology Neutrality. P. 283.

[114] В своем становлении данная модель прошла несколько этапов, обусловленных развитием административной практики комиссии и проверкой ее легитимности судами США. См., напр.: Federal Communications Commission: Protecting and Promoting the Open Internet, Report and Order on Remand, Declaratory Ruling, and Order, FCC 15-24. URL: https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-24A1.pdf (дата обращения – 15 мая 2017 г.).

по связи в четырех принципах[115]. В соответствии с ними признавались права потребителей на доступ к любым законным ресурсам в Интернете по своему выбору, запуск приложений по своему выбору, подключение любых устройств, не нарушающих работу сети, а также наличие конкуренции между операторами связи, контент- и сервис-провайдерами. Данные принципы были конкретизированы в приказах комиссии, в которых устанавливались требования открытости основных характеристик доступа к Интернету и запреты блокирования информации и необоснованной дискриминации[116], предусматривался дифференцированный подход для быстрых и медленных каналов связи. В последующем совершенствование регулирования сетевой нейтральности происходило в условиях открытого обсуждения и политических дебатов. В результате был закреплен отказ от дифференцированного подхода к сетевой нейтральности в пользу его меньшей технологической зависимости[117]. Она была распространена как на проводное, так и на беспроводное подключение к сети Интернет и выразилась в принципах запрета блокирования, регулирования потока информации (трафика) и платной приоритизации (запрет получения платы за дополнительную скорость)[118]. В настоящее время модель регулирования сетевой нейтральности в США предусматривает возможность установления исключений из общих правил, которые рассматриваются комиссией в индивидуальном порядке. Анализ модели регулирования сетевой нейтральности в

---

[115] New Principles Preserve and Promote the Open and Interconnected Nature of Public Internet. FCC Adopts Policy Statement. 2005. URL: https://apps.fcc.gov/edocs_public/attachmatch/DOC-260435A1.pdf (дата обращения – 15 мая 2017 г.).

[116] Federal Communications Commission. Preserving the Open Internet 2010. URL: https://www.gpo.gov/fdsys/pkg/FR-2011-09-23/pdf/2011-24259.pdf (дата обращения – 15 мая 2017 г.).

[117] Разработка данного приказа была направлена на исполнение решения Окружного суда Округа Колумбия в деле Verizon Communications Inc. v. Federal Communications Commission, который в январе 2014 г. установил, что Комиссия не имеет полномочий по осуществлению правового регулирования в области обеспечения сетевой нейтральности, до тех пор пока операторы связи, оказывающие услуги по доступу к Интернету, не классифицированы как организации, предоставляющие публичные услуги (common carriers) в соответствии с разделом 2 Закона о коммуникациях 1934 г. См.: URL: https://www.cadc.uscourts.gov/internet/opinions.nsf/5DFE38F28E7CAC9185257C610074579E/$file/11-1355-1475317.pdf (дата обращения – 15 мая 2017 г.).

[118] Federal Communications Commission. The Open Internet. 2015. URL: https://www.fcc.gov/general/open-internet (дата обращения – 15 мая 2017 г.).

США показывает, что содержание данного принципа меняется в пользу все большей нейтральности к различным технологиям при оказании услуг доступа к сети Интернет. В то же время его признание как правового принципа зависит от социальной функции государства, которая во многом обусловлена социально-политическим контекстом [119], и при изменении социальной политики его содержание также подвержено изменениями.

В основе модели регулирования сетевой нейтральности, который вырабатывается на уровне Европейского союза и во внутреннем праве его государств-членов, лежит комбинация наднационального и национального права. Этот подход пришел на смену сочетанию национального регулирования и саморегулировани[120]. Подобное регулирование было направлено на поддержку конкуренции, которая рассматривалась как оптимальный способ обеспечения доступных цен и высокого качества предоставляемых провайдерами доступа к сети Интернет услуг [121]. Как показало исследование, проведенное Органом европейских регуляторов в сфере электронных коммуникаций (Body of European Regulators for Electronic Communications – BEREC), несмотря на то, что в целом провайдеры доступа к сети Интернет соблюдали сетевую нейтральность, в ряде стран имели место случаи дискриминации по отношению к IP-телефонии и

[119] С приходом администрации Д.Трампа новый руководитель комиссии заявил о планах по отмене ранее установленных правил сетевой нейтральности и намерении позволить операторам связи применять их в добровольном порядке. См.: F.C.C. Invokes Internet Freedom While Trying to Kill It. The New York Time. URL: https://www.nytimes.com/2017/04/29/opinion/sunday/fcc-invokes-internet-freedom-while-trying-to-kill-it.html (дата обращения – 15 мая 2017 г.).

[120] Данный подход к регулированию сетевой нейтральности был предусмотрен в рамках Директивы по универсальному обслуживанию. См.: Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on Universal Service and Users' Rights Relating to Electronic Communications Networks and Services, Directive 2002/58/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector and Regulation (EC) № 2006/2004 on Cooperation Between National Authorities Responsible for the Enforcement of Consumer Protection Laws. URL: http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32009L0136 (дата обращения – 8 октября 2016 г.).

[121] См., напр.: Frieden R. Network Neutrality in the EU, Canada and the U.S. // Intereconomics. V.50. I.6. P. 363–364; Shin D.-H. A Comparative Analysis of Net Neutrality: Insights Gained by Juxtaposing the U.S. and Korea // Telecommunications Policy. 2014. V. 38. I. 11. P.1117–1133; Leal M.C. The EU Approach to Net Neutrality: Network Operators and Over-the-Top Players, Friends or Foes? // Computer Law & Security Review. 2014. V. 30. 506–520.

передаче данных в пиринговых сетях[122]. В настоящее время, так же как и в модели регулирования сетевой нейтральности в США, на наднациональном уровне Европейского союза установлен запрет дискриминации и регулирования потока информации (трафика) [123]. Модель регулирования сетевой нейтральности в Европейском союзе предусматривает, что конечные пользователи (end-users) должны иметь право на доступ и распространение информации и контента, использование и предоставление приложений и сервисов, а также использование оконечного оборудования по своему выбору, независимо от своего местоположения или местоположения провайдера, происхождения или назначения информации, контента, приложения или услуги, которые предоставляются с использованием услуг по обеспечению доступа к сети Интернет. Модель регулирования сетевой нейтральности в Европейском союзе более ограничена, нежели аналогичная модель в США, и допускает регулирование провайдерами цен, объемов данных и скорости их передачи. Данная модель не охватывает запрет ценового регулирования и предусматривает ряд исключений, таких как возможность управления информационными потоками и оказание провайдерами дополнительных услуг, отличных от услуг доступа к сети Интернет.

Тенденция совершенствования технологий передачи данных и связанной с ними инфраструктуры и, следовательно, удешевления стоимости передачи данных в сети Интернет снижает остроту проблемы сетевой нейтральности для операторов связи. Тем самым техническое обеспечение права на доступ к сети Интернет, выраженное в развитии соответствующей инфраструктуры,

---

[122] Пиринговые сети основаны на равноправии их участников, каждый из которых может выступать как сервером, так и клиентом. См.: Savirimuthu J. Response to the Consultation by the Body of European Regulators in Electronic Communications BEREC on Net Neutrality Policy. European Journal for Law and Technology. V. 3. №. 1. 2012. URL: http://ejlt.org/article/view/134/214 (дата обращения – 8 октября 2016 г.).

[123] Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 Laying Down Measures Concerning Open Internet Access and Amending Directive 2002/22/EC on Universal Service and Users' Rights Relating to Electronic Communications Networks and Services and Regulation (EU) № 531/2012 on Roaming on Public Mobile Communications Networks within the Union. URL: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32015R2120&rid=2 (дата обращения – 8 октября 2016 г.).

способствует обеспечению цифрового равенства. В то же время, как показывает правовое регулирование соответствующих отношений в США и Европейском союзе, принцип сетевой нейтральности допускает компромиссы, позволяющие исключить установление избыточных ограничений на свободу предпринимательской деятельности и свободную конкуренцию.

Особое значение для обеспечения цифрового равенства приобретает устранение различных форм дискриминации по отношению к лицам с ограниченными возможностями здоровья при осуществлении права на доступ к Интернету и права на доступ к информации в сети Интернет. Для целей обеспечения полного и эффективного участия в постиндустриальном обществе инвалидов наряду с другими лицами в международном праве предусмотрен принцип доступности[124]. Данный принцип является конкретизацией принципа правового равенства, в частности, он заключается в развитии надлежащих форм оказания инвалидам помощи и поддержки, обеспечивающих им доступ к информации, поощрении доступа инвалидов к новым информационным и коммуникационным технологиям и системам, включая сеть Интернет, поощрении проектирования, разработки, производства и распространения изначально доступных информационных и коммуникационных технологий и систем, причем доступность этих технологий и систем должна достигаться при минимальных затратах[125]. Данный принцип положен в основу мер, которые принимаются государством для обеспечения инвалидам доступа наравне с другими к информационно-коммуникационным технологиям и системам, включая сеть Интернет.

Соблюдение принципа доступности выражается в возложении обязанностей на организации, осуществляющие предоставление и распространение информации и оказание услуг, в том числе с использованием сети Интернет, предназначенных для широкого круга лиц, и государственные органы по

---

[124] См.: Конвенция о правах инвалидов (заключена в г. Нью-Йорке 13.12.2006) // СЗ РФ. 2013. № 6. Ст. 468.

[125] Данный принцип не ограничен информационной сферой и в целом направлен на развитие доступной для инвалидов инфраструктуры. См. Там же.

внедрению доступных для инвалидов форматов и использованию технологий, учитывающих различные формы инвалидности. Данные меры позволяют обеспечить права инвалидов на свободу выражения мнения и убеждений, включая свободу искать, получать и распространять информацию и идеи наравне с другими, пользуясь по своему выбору всеми формами общения.

Воплощение данного принципа в национальном праве осуществляется под влиянием предложенного консорциумом W3C Руководства по обеспечению общедоступности веб-контента [126]. Однако в каждой стране имеются свои особенности его соблюдения. В правовой науке выделяют ригористский (строгий), технологический и особый подходы[127].

В соответствии с ригористским подходом соблюдение принципа доступности обеспечивается в рамках национального законодательства в области создания условий для осуществления и защиты прав инвалидов и телекоммуникаций. Например, законодательством США на производителей оборудования и провайдеров телекоммуникационных услуг возлагается обязанность по обеспечению доступности соответствующих оборудования и услуг для инвалидов[128], установлен запрет на разработку, поддержку, закупки и применение оборудования и услуг, создающих неравенство при осуществлении доступа к ним лиц с ограниченными возможностями [129]. В Законе США об американцах с ограниченными возможностями [130] установлен запрет на дискриминацию в области телекоммуникаций. В практике американских судов

[126] В настоящее время действует вторая редакция данного руководства. См.: Web Content Accessibility Guidelines (WCAG) 2.0. W3C Recommendation 11 December 2008 // URL: http://www.w3.org/TR/WCAG20/ (дата обращения – 8 октября 2016 г.).

[127] Исследование обеспечения доступности интернет-ресурсов Рунета для людей с ограниченными возможностями здоровья (ОВЗ) // URL: https://perspektiva-inva.ru/userfiles/download/Accessibility_of_Runet_2013.pdf (дата обращения – 8 октября 2016 г.).

[128] Telecommunications Act of 1996. URL: https://www.fcc.gov/general/telecommunications-act-1996 (дата обращения – 8 октября 2016 г.).

[129] Section 508 Amendment to the Rehabilitation Act of 1973 (29 U.S.C. § 794d). URL: https://www.law.cornell.edu/uscode/text/29/794d (дата обращения – 8 октября 2016 г.).

[130] Americans with Disabilities Act. (42 U.S.C. 12101 et seq.). URL: https://www.ada.gov/pubs/adastatute08.htm (дата обращения – 15 мая 2017 г.).

данный запрет был частично распространен на доступность сайтов в сети Интернет[131].

Технологический подход реализуется в отсутствие специального правового регулирования исключительно за счет технологических и организационных мер, в его основу может быть положена деятельность специализированного органа. Например на Филиппинах соблюдение принципа доступности обеспечивается Филиппинской Группой по вопросам доступности веб-ресурсов (PWAG)[132] при Правительстве Филиппин путем аудита сайтов в сети Интернет и разработки рекомендаций для их владельцев и разработчиков. В рамках данного подхода также распространено принятие специализированных стандартов или руководств по доступности сайтов в сети Интернет с учетом рекомендаций W3C, как, например в Японии[133] и в Тайланде[134]. Данному подходу также отвечает и соблюдение принципа доступности в Российской Федерации, в основе которого лежит принятие специализированного национального стандарта, применение которого осуществляется в добровольном порядке[135]. Вместе с тем в связи с ратификацией Российской Федерацией Конвенции о правах инвалидов наблюдается тенденция возложения в отечественном законодательстве обязанностей на государственные органы по обеспечению доступности официальных сайтов для инвалидов по зрению[136].

---

[131] См., напр.: National Federation of the Blind (NFB), et al. v. Target Corporation. Disability Rights Advocates. URL: http://dralegal.org/case/national-federation-of-the-blind-nfb-et-al-v-target-corporation/ (дата обращения – 15 мая 2017 г.).

[132] Philippine Web Accessibility Group. URL: http://www.pwag.org/ (дата обращения – 8 октября 2016 г.).

[133] JIS Web Content Accessibility Guideline. URL: http://www.comm.twcu.ac.jp/~nabe/data/JIS-WAI/ (дата обращения – 8 октября 2016 г.).

[134] Thai Web Content Accessibility Guidelines. URL: http://thwcag.com/ (дата последнего обращения – 8 октября 2016 г.); Maisak R. Accessibility of Thai University Websites: Awareness, Barriers and Drivers for Accessible Practice. 2015. URL: http://ro.ecu.edu.au/theses/1715 (дата обращения – 8 октября 2016 г.).

[135] ГОСТ Р 52872-2012 «Национальный стандарт Российской Федерации. Интернет-ресурсы. Требования доступности для инвалидов по зрению» // М.: Стандартинформ, 2014; См.: Исследование обеспечения доступности интернет-ресурсов Рунета для людей с ограниченными возможностями здоровья (ОВЗ).

[136] Федеральный закон от 1 декабря 2014 г. № 419-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам социальной защиты инвалидов в связи с ратификацией Конвенции о правах инвалидов» // СЗ РФ. 2014. № 49 (часть VI).

Особый подход характерен для Великобритании, в которой принцип доступности находит воплощение в статуте, направленном на обеспечение равенства[137], и принятого в развитие данного статута об устранении различных форм дискриминации при оказании услуг[138]. В совокупности положения данных правовых актов указывают на обязанность организаций и государственных органов, оказывающих услуги с использованием сайтов в сети Интернет, обеспечить их доступность для инвалидов путем учета их физических возможностей.

В отличие от принципа сетевой нейтральности соблюдение принципа доступности является технологически зависимым. Его практическое воплощение в деятельности организаций и государственных органов обусловлено созданием и использованием специализированного программного обеспечения и других технических средств для обеспечения прав инвалидов на доступ к сети Интернет и права на доступ к информации в сети Интернет. Однако, как показывает опыт Российской Федерации, наличия технических норм для создания таких технических средств недостаточно для устранения дискриминации при осуществлении инвалидами данных прав. В связи с этим технические нормы дополняют правовые нормы, которыми устанавливаются обязанности организаций и государственных органов по внедрению соответствующих технических средств в своей деятельности.

Обеспечение правового равенства при осуществлении права на доступ к информации в сети Интернет не ограничено устранением дискриминации лиц с ограниченными возможностями здоровья и является общей тенденцией развития данного права. Расширение аналитических возможностей для обработки данных,

---

Ст. 6928; приказ Минкомсвязи России от 30 ноября 2015 г. № 483 «Об установлении Порядка обеспечения условий доступности для инвалидов по зрению официальных сайтов федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и органов местного самоуправления в сети «Интернет» // Российская газета. № 27. 10.02.2016.

[137] Equality Act 2010. URL: http://www.legislation.gov.uk/ukpga/2010/15 (дата обращения – 8 октября 2016 г.).

[138] Equality Act 2010. Banning Age Discrimination In Services. An Overview for Service Providers and Customers. URL: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/85004/age-discrimination-ban.pdf (дата обращения – 8 октября 2016 г.).

хранящихся в различных базах данных, одновременно с существенным увеличением объемов обработки информации приводит к постановке вопроса о расширении доступности информации о деятельности органов государственной власти. В настоящее время развитие права на доступ к такой информации осуществляется под влиянием концепции открытых данных. Под открытыми понимаются данные, доступ к которым предоставляется без каких-либо ограничений или условий использования[139]. Открытые данные направлены на обеспечение доступа к информации для наиболее широкого круга лиц и для наиболее широкого круга задач. И хотя данная концепция может быть взята за основу при обеспечении осуществления и защиты права на доступ к любой общедоступной информации, как правило, ее особая роль проявляется в отношении информации о деятельности органов государственной власти. Она отражает происходящие изменения права на доступ к такой информации, при которых наряду с ценностью доступности информации повышается значение возможностей поиска, обработки и последующего использования информации. Важное значение в данной концепции уделяется открытому формату представления данных, то есть платформенно-независимому, машиночитаемому и доступному для общества без ограничений, которые бы препятствовали повторному использованию соответствующей информации[140]. В национальном законодательстве государств, готовых к повышению стандартов социального обслуживания при обеспечении доступа к информации, устанавливаются обязанности органов государственной власти по внедрению в своей деятельности открытых данных [141]. На развитие национального законодательства в данной

[139] См.: M. Janssen, J. van den Hoven. Big and Open Linked Data (BOLD) in Government: A Challenge to Transparency and Privacy? // Government Information Quarterly. 2015. V. 32. P. 363–368.

[140] См., напр.: Open Government Directive. URL: https://obamawhitehouse.archives.gov/open/documents/open-government-directive (дата обращения – 15 мая 2017 г.).

[141] В государствах-членах Европейского Союза данные процессы происходят в рамках реализации Директивы ЕС об информации в публичном секторе. В США Президентом Б. Обамой утверждена Директива открытых данных 2009 г. В России внедрение технологии открытых данных при обеспечении права на доступ к официальной информации связано с принятием Федерального закона от 7 июня 2013 г. № 112-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации»

области оказывает влияние Декларация открытых государств [142], принятие которой является условием для присоединения к Партнерству открытых государств, созданному в 2011 г.[143], и Хартия открытых данных Г8[144]. Концепция открытых данных реализуется в соответствии с национальными планами (государственными программами), связанными с созданием и совершенствованием государственных информационных систем и баз данных, в том числе с повышением эффективности государственных услуг, предоставляемых посредством сети Интернет, повышением доступности информации о деятельности органов государственной власти в сети Интернет, рассекречиванием информации, повышением открытости средств и методов обеспечения безопасности, бюджетной транспарентности, открытости в области устойчивого развития и охраны окружающей среды, открытости судебной системы, доступности участия граждан в управлении государством. Хотя в концепции открытые данные и отдается предпочтение технологической нейтральности в отношении технических средств, которые используются лицами, обладающими правом доступа к информации, в целом она является технологически зависимой. В данном случае на органы государственной власти возлагается обязанность по внедрению в своей деятельности таких информационных и коммуникационных технологий, которые позволяют создать условия для осуществления и защиты прав человека, соответствующие современному техническому уровню. Развитие права на доступ к информации о деятельности органов государственной власти, также как устранение дискриминации инвалидов при осуществлении доступа к информации в сети

и Федеральный закон «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления». См., напр.: Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the Re-use of Public Sector Information. URL: http://ec.europa.eu/digital-agenda/en/european-legislation-reuse-public-sector-information (дата обращения 2 апреля 2016 г.); Open Government Directive; СЗ РФ. 2013. № 23. Ст. 2870.

[142] Open Government Declaration. URL: http://www.opengovpartnership.org/about/open-government-declaration (дата обращения – 2 апреля 2016 г.).

[143] На сегодняшний день к данному партнерству присоединилось 75 государств. Россия не является членом данного партнерства.

[144] URL: https://www.gov.uk/government/publications/open-data-charter (дата обращения – 2 апреля 2016 г.).

Интернет, свидетельствует о повышении значения технологически зависимого подхода при обеспечении осуществления и защиты прав человека.

При обеспечении цифрового равенства возникает необходимость установить баланс между различными правами, включая право на доступ к сети Интернет, право на доступ к информации, на свободу выражения мнения, право на неприкосновенность частной жизни, права на результаты интеллектуальной деятельности. В отечественной литературе высказывается точка зрения о том, что принцип правового равенства может быть применим только к одним и тем же правам. Как отмечает отечественный ученый-юрист В.В. Лапаева, принцип правового равенства позволяет «соизмерять правоспособность различных субъектов одного и того же права и находить такую меру вторжения закона в сферу его реализации, которая обеспечивает принцип формального равенства»[145]. С этой точки зрения проводить равенство между правом на доступ к информации и, например, правом на неприкосновенность частной жизни некорректно, баланс между ними невозможен по определению и его поиск может привести исключительно к произвольному решению. Другими словами, данный принцип предназначен для исключения привилегий и дискриминации в сфере осуществления конкретного права человека. Вместе с тем такая точка зрения вступает в противоречие с требованием соразмерности и эквивалента в отношениях между свободными индивидами, которое лежит в основе данного принципа, когда определяется сбалансированность правовой охраны одних прав при вмешательстве в сферу осуществления других прав. Поскольку требование соразмерности и эквивалента лежит в основе принципа правового равенства, то обеспечение равенства различных прав также является и его составляющей.

Равенство различных прав обеспечивается, если они в равной степени обеспечиваются правовой охраной, если охрана одних прав человека путем ограничения других прав не приводит к вторжению в сферу, составляющую

[145] Лапаева В.В. Критерии ограничения прав человека с позиций либертарной концепции правопонимания // Журнал российского права. № 4 (112). 2006. С. 106.

сущность и содержание права человека, то есть не приводит к их умалению[146]. В соответствии с рядом международных деклараций, включая Венскую декларацию и программу действий 1993 г.[147], отмечается эквивалентность различных прав человека. Согласно пункту 5 данной декларации, «все права человека универсальны, неделимы, взаимозависимы и взаимосвязаны. Международное сообщество должно относиться к правам человека глобально, на справедливой и равной основе, с одинаковым подходом и вниманием». Правовая наука также говорит о равенстве различных прав человека[148]. В этой связи не лишена справедливости точка зрения Р. Дворкина о том, что из всех прав наиболее фундаментальным является право на равенство, которое он назвал «право на равную заботу и уважение»[149]. В данном случае это означает, что уважение и защита прав различных субъектов правоотношений должна осуществляться в равной степени, без дискриминации. В этом заключается их правовое равенство.

Вместе с тем при наличии правового равенства различных прав человека в онлайновой среде усиливается их фактическое неравенство, если данные права осуществляются другими лицами. Обусловлено оно различием правового статуса их обладателей, а именно тем, что права человека занимают более высокую иерархию среди прав иных субъектов. В правовом государстве при разрешении конфликта прав человека, осуществляемых с использованием сети Интернет, и прав других субъектов правоотношений – пусть даже речь идет об одних и тех же правах по содержанию – различие статуса их обладателей приведет к тому, что

---

[146] См., напр.: Постановление Конституционного Суда Российской Федерации от 7 июня 2012 г. № 14-П «По делу о проверке конституционности положений подпункта 1 статьи 15 Федерального закона «О порядке выезда из Российской Федерации и въезда в Российскую Федерацию» и статьи 24 Закона Российской Федерации «О государственной тайне» в связи с жалобой гражданина А.Н. Ильченко» // СЗ РФ. 2012. № 28. Ст. 3977; Пчелинцев С.В. Соотношение понятий «умаление прав и свобод» и «ограничение прав и свобод»: теоретические аспекты // Современное право. 2006. № 4. С. 47–50.

[147] Международное публичное право. Сборник документов. Т. 1. М.: БЕК, 1996. С. 521–540.

[148] См., напр.: Ducoulombier P. Conflicts between Fundamental Rights and the European Court of Human Rights: An Overview // Conflicts between Fundamental Rights / Ed. By Eva Brems. Intersentia, 2008. XVIII + 690 p. P. 217, 234.

[149] Дворкин Р. О правах всерьез / Пер. с англ.; Ред. Л. Б. Макеева. М.: «Российская политическая энциклопедия» (РОССПЭН), 2004. 392 с. С.12.

права человека будут защищены в большей степени. Это определяет неравенство различных прав.

Таким образом, в современном обществе решение проблемы цифрового равенства связано с развитием принципа правового равенства, его конкретизацией и наполнением новым содержанием. В основе обеспечения цифрового равенства лежит создание юридически равных возможностей для осуществления права на доступ к сети Интернет. Данное право развивается как социальное в соответствии с принципом универсальности публичных услуг, который заключается в обеспечении правового равенства в доступе к социально значимым услугам. Принцип правового равенства конкретизируется в принципе сетевой нейтральности и принципе доступности. В условиях различных национальных моделей регулирования сетевой нейтральности соблюдение данного принципа основано на технологически нейтральном подходе. Принцип доступности связан с устранением различных форм дискриминации по отношению к лицам с ограниченными возможностями здоровья на основе технологически зависимого подхода путем внедрения доступных для инвалидов форматов и иных технических средств, учитывающих различные формы инвалидности. Технологическая зависимость также свойственна концепции открытых данных, которая лежит в основе новых подходов к обеспечению права на доступ к информации о деятельности органов государственной власти. Наряду с проблемой цифрового неравенства обостряется проблема неравенства различных прав. В правовом государстве при разрешении конфликта прав человека, осуществляемых с использованием сети Интернет, и прав других субъектов правоотношений, пусть даже речь идет об одних и тех же правах по содержанию, различие статуса их обладателей приведет к тому, что права человека будут защищены в большей степени.

ГЛАВА 2. ТЕОРЕТИКО-ПРАВОВЫЕ АСПЕКТЫ СООТНОШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ПРАВ ЧЕЛОВЕКА

§1. Информационная свобода и информационная безопасность как правовые ценности

В изменяющемся обществе происходит трансформация человеческих ценностей, в основе которой лежит преодоление экономической, материальной мотивации, характерной для предшествующих периодов, формирование соответственно «постэкономической»[150] и «постматериалистической»[151] системы ценностей. Информационные и коммуникационные технологии увеличивают возможности человека для развития и самовыражения и тем самым расширяют его свободу. Люди получают разнообразные инструменты для постоянной дистанционной коммуникации друг с другом, доступа ко все большей информации и к знаниям об окружающем мире. Одновременно с развитием использования данных технологий в различных сферах жизни общества повышается значение обеспечения безопасности. Такие проблемы, как сочетание свободы и безопасности [152], все чаще выходят на первый план. Происходящие процессы оказывают на правовые ценности влияние, выражающееся прежде всего в их переоценке, изменении их системы и иерархии, смене ориентиров в развитии права, а также условий, при которых обеспечивается его стабильность. Под правовыми ценностями понимаются правовые явления, воплощающие в себе общественные идеалы и выступающие благодаря этому как эталон должного.

---

[150] Toffler A. The Adaptive Corporation. New York: McGraw-Hill, 1985. 217 p. P. 100.

[151] Inglehart R. Culture Shift in Advanced Industrial Society. Princeton: Princeton University Press, 1990. P. 151.

[152] См.: Hicks. J. Wealth and Welfare, Collected Essays on Economic Theory. V. 1. Oxford: Basil Blackwell. 1981. 320 p. P. 138 – 139. Согласно Инглхарт-Вельцельской культурной карте мира, основанной на результатах международного научно-исследовательского проекта World Values Survey (Обзор мировых ценностей), существует высокая зависимость уровня развития постиндустриального общества от отношения его членов к ценностям выживания (физической и экономической безопасности) и ценностям самовыражения (свободы и развития). См.: WVS Database. URL: http://www.worldvaluessurvey.org/WVSContents.jsp (дата обращения – 31 июля 2016 г.).

Правовые ценности берут начало в субъективной оценке человеком и социумом правовой действительности, определении в ней идеалов и облечении их в правовую форму.

В постиндустриальный период повышается правовая ценность информационной свободы и информационной безопасности, которые соотносятся со свободой и безопасностью как часть и целое. Традиционно свобода понимается как свободное волеизъявление человека, его возможность осуществлять выбор собственного поведения, тогда как безопасность выражается в отсутствии опасности для человека, состоянии его защищенности. В настоящем исследовании суть информационной свободы заключается в возможности человека осуществлять выбор собственного поведения при использовании [153] информации, а также информационных и коммуникационных технологий. Информационная безопасность в качестве правовой ценности указывает на отсутствие опасности для человека, состояние его защищенности в информационной сфере.

Информационная свобода соответствует свободе личности как нравственному идеалу, облеченному в правовую форму, не ограниченному свободами других людей или же правовым принуждением. Хотя в отечественной правовой науке признается, что «по своей юридической природе и системе гарантий права и свободы идентичны»[154] и «различие в терминологии является скорее традиционным» [155] , информационная свобода как правовая ценность отличается от информационных прав человека. Информационные права гарантируются государством, которое обеспечивает их осуществление и защиту с использованием правового принуждения. Такие права имеют установленные в результате сопоставления с правами и свободами других лиц границы. В отличие от информационных прав в информационной свободе выражено не столько

[153] Под использованием в данном случае понимается широкий круг действий, которые могут быть осуществлены в отношении информации, информационных и коммуникационных технологий, в том числе создание, поиск, хранение, обработка, предоставление и распространение, обеспечение доступа к ним, применение и защита.

[154] Права человека. Учебник для вузов. С. 133.

[155] Там же.

правопритязание, сколько автономия личности, ее независимость, в том числе от государства. Информационная свобода выступает ценностной основой для широкого круга прав человека – не только таких, как право на свободу выражения мнения и свободу информации, но и, например, право на неприкосновенность частной жизни при использовании личной информации.

В зарубежной правовой доктрине используется близкое по содержанию к информационной свободе понятие «интеллектуальная свобода» (intellectual freedom), под которым понимается информационная автономия, заключающаяся в независимости принятия решений в отношении выбора информации, мыслей и выражения [156] или, другими словами, «функция автономии, которую индивиды выбирают в отношении информации, поступающей к ним, исходящей от них, или же связанной с ними» [157] . В основе условий интеллектуальной свободы в отношении информации, поступающей к индивиду, лежит информированность индивида о ее существовании и возможностях доступа к ней, наличие у индивида хотя бы минимальных способностей по ее предварительной обработке и критическому анализу, а также непрерывный и постоянный рост количества различной информации. Информация, исходящая от индивида, представляет собой результат творческих процессов. Условиями интеллектуальной свободы в данном случае наряду с доступом к информации и критическим мышлением является независимость от манипуляций, свобода использования определенных видов информации, являющихся общественным достоянием, а также результатами свободы выражения иных лиц, в том числе для критики и комментариев. Интеллектуальная свобода в отношении информации, связанной с индивидом, обусловлена наличием информационной неприкосновенности частной жизни, которая в свою очередь влияет на критическое мышление и самостоятельность в принятии решений по поводу получения и создания информации. При соблюдении указанных выше условий обеспечивается

[156] Cohen J.E. Information Rights and Intellectual Freedom // Ethics and the Internet / Ed. by A.Vedder. Antwerp: Intersentia, 2001. P. 2.

[157] Ibid. P.21.

информационная автономия индивида и предотвращение избыточного информационного патернализма.

В отличие от интеллектуальной свободы информационная свобода связана не только с информацией, но также с отношениями в сфере информационных и коммуникационных технологий, с помощью которых обеспечивается доступ к информации или ее использование. Свобода в выборе таких технологий непосредственно влияет на возможности выбора информации, которая поступает к индивиду, создается им, на ее количество и содержание, а также на выбор технических средств, с использованием которых обеспечивается информационная неприкосновенность частной жизни. Доступ к информационным и коммуникационным технологиям, включая сеть Интернет, в настоящее время является одной из важнейших составляющих информационной автономии личности и определяет доступ индивида не только к информации, но и к многочисленным услугам, которые оказываются с их использованием. Подавление данной свободы, монополизация в сфере информационных и коммуникационных технологий не только создает условия для манипуляции информацией и ограничения ее разнообразия, но и подавляет самостоятельность личности при выборе соответствующих услуг. Определение данной свободы как информационной является более точным, нежели ее определение как интеллектуальной. Несмотря на то, что интеллектуальная, критическая оценка информации в данном случае играет бóльшее значение, чем для других свобод, особый характер информационной свободе придает именно информация, а также информационные и коммуникационные технологии, с использованием которых связана такая свобода выбора индивида.

Информационная безопасность служит ценностным критерием при определении пределов прав человека путем сопоставления с правами других лиц. Необходимость обеспечения национальной и государственной безопасности, а следовательно, и информационной безопасности как их составляющей определена в качестве основания для ограничения свободы выражения мнения в статье 10 Конвенции о защите прав человека и основных свобод 1950 г. (далее – Конвенция

1950 г.)[158] и статье 19 Международного пакта о гражданских и политических правах 1966 г.[159] В то же время без признания, соблюдения и защиты прав человека его информационная безопасность в полной мере обеспечена быть не может. Исходя из этого в Доктрине информационной безопасности Российской Федерации обеспечение реализации конституционных прав и свобод человека и гражданина выступает одной из составляющих информационной безопасности Российской Федерации. В Стратегии кибербезопасности Европейского союза[160] защита фундаментальных прав, свободы выражения, персональных данных и неприкосновенности частной жизни названа одним из ключевых ее принципов.

Информационная свобода и информационная безопасность выступают правовыми ценностями независимо от того, обозначены они явно в тексте нормативных правовых актов или нет. Справедливо, что «подход, при котором предпринимается попытка вычленить из правового текста понятия, которыми, как правило, обозначаются социальные ценности, назвав их на этом основании «правовыми ценностями», во многом поверхностен»[161]. Ценность

---

[158] Бюллетень международных договоров, № 3, 2001.

[159] Бюллетень Верховного Суда Российской Федерации, № 12, 1994.

[160] См.: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. URL: https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf (дата обращения – 6 марта 2016 г.). Единообразного понимания термина «кибербезопасность» в зарубежных стратегических документах и правовой науке на сегодняшний день не выработано (см. напр.: Luiijf H., Besseling K., Spoelstra M., de Graaf P. Ten National Cyber Security Strategies: a comparison // Critical Information Infrastructure Security. 6th International Workshop, CRITIS 2011, Lucerne, Switzerland, September 8-9, 2011, Revised Selected Papers. Berlin: Springer Berlin Heidelberg, 2011. P. 1 – 17). В настоящее время преобладают два подхода. В первом подходе, который следует из Стратегии кибербезопасности Европейского союза, кибербезопасность определяется через конфиденциальность, целостность и доступность, аналогично информационной безопасности, и соотносится с ней как часть и целое. Во втором подходе информационная безопасность, кибербезопасность и безопасность в сфере информационных и коммуникационных технологий определяются как пересекающиеся множества. (См.: Solms R. von, Niekerk J. van. From Information Security to Cyber Security // Computers & Security. 2013. V. 38. P. 101). При этом предполагается наличие областей, в которых правовое обеспечение информационной безопасности и кибербезопасности не пересекаются. Речь идет о случаях, при которых отсутствует информационная цель, основа и сфера посягательства на личность. К таким случаям, в частности, относятся так называемая «кибертравля», неавторизованное проникновение во внутридомовые автоматизированные системы, кибертерроризм, имеющий своей целью поражение жизненно важной инфраструктуры.

[161] Мурашко Л.О. Аксиологическое измерение процесса правообразования: история и современность: дис. ... д-ра юрид. наук : 12.00.01 / Мурашко Людмила Олеговна. Москва, 2015. 378 с. С. 67.

информационной свободы и информационной безопасности является правовой, поскольку в условиях расширения сфер цифровых коммуникаций данные ценности определяют развитие связанных с ними правовых явлений и находят в них свое особое выражение. В результате информационная свобода и информационная безопасность становятся одним из ориентиров в развитии как информационных прав, так и иных прав человека, осуществление которых в настоящее время связано с информацией, представленной в цифровой форме.

В постиндустриальном обществе информационная свобода и информационная безопасность приобретают характер не только личной, но также публичной правовой ценности. Правовая охрана информационной свободы всех членов такого общества, являясь индикатором его развития, становится одним из государственных приоритетов, тогда как обеспечение информационной безопасности государства – гарантией устойчивого функционирования его институтов. Тогда как личные правовые ценности могут обеспечиваться правовой охраной в условиях минимального государства и максимальной автономии индивида, для правовой охраны публичных правовых ценностей роль правового государства повышается – оно осуществляет позитивные действия, выраженные прежде всего в развитии правового регулирования и направленные на создание условий для осуществления и защиты прав человека. В конечном итоге правовая охрана информационной свободы и информационной безопасности способствует уважению не только прав человека, но и таких правовых ценностей, как правовое государство и автономия личности. Это обусловлено тем, что правовая охрана информационной свободы и информационной безопасности возможна только при условии уважения и защиты соответствующих правовых ценностей.

Между информационной свободой и информационной безопасностью существует конфликт, который берет начало из общего конфликта свободы и безопасности, подобного противопоставлению личности и государства. Причина данного конфликта заключается в том, что национальное право, даже если оно направлено на создание условий для осуществления и защиты прав человека и обеспечение его безопасности, связано с правовым принуждением, которое само

по себе вступает в противоречие со свободой и автономией личности (еще И. Бентам говорил, что «всякий закон есть нарушение свободы» [162] и «без законов не может существовать безопасности» [163]). В связи с этим встает вопрос о разрешении данного конфликта [164] . Он может быть решен исходя из их соотношения в системе правовых ценностей и достижения баланса их правовой охраны.

Правовые ценности обеспечиваются такой правовой охраной, которая соответствует их позиции в системе правовых ценностей. В отечественной юридической литературе справедливо опровергается точка зрения о том, что правовые ценности равнозначны и между ними невозможно выстроить иерархию [165] . Несмотря на то, что правовые ценности лежат в основе прав человека, они не являются равнозначными и между ними всегда существуют иерархические связи. Подход к правовой охране ценностей, расположенных на одном иерархическом уровне, соответствует ценностной иерархии, которую отечественный юрист А.Н. Бабенко называет равновесной, справедливо отмечая, что при таком подходе правовые ценности гармонично взаимодействуют, выступая в своем формально-правовом выражении[166]. Равновесная иерархия не тождественна равнозначной и обусловлена тем, что даже при различном значении правовых ценностей в конкретной правовой системе и в конкретные исторические периоды баланс между ними достигается при условии предоставления им такой правовой охраны, которая в равной степени обеспечит их уважение и защиту.

---

[162] «Исключение из этого составляют законы, дозволяющие то, что запрещалось другими законами, т.е. такие, которыми отменяются другие законы, ограничивающие свободу». См. Бентам И. Избранные сочинения. Т. 1. СПб, 1867. LXII, 678 с. С. 319–470.

[163] Там же.

[164] Р. Дворкин справедливо указывает на то, что в связи с любым законом «встает вопрос не о том, ущемляет ли он свободу, ибо он действительно ее ущемляет, а о том, оправдано ли это ущемление какими-либо конкурирующими ценностями, например, равенством, безопасностью или общественным удобством». См.: Дворкин Р. О правах всерьез. С. 354.

[165] См., напр.: Лановая Г.М. Базовые ценности современного права // История государства и права. 2014. № 20. С. 23–27. Обратная точка зрения представлена в работе Сидоровой Е.В. См.: Сидорова Е.В. Миф о правовых ценностях // История государства и права. 2012. № 11. С. 24–25.

[166] См.: Бабенко А.Н. Правовые ценности и освоение их личностью : автореф. дис. ... д-ра юр. наук : 12.00.01 / Бабенко Андрей Николаевич. М., 2002. 46 с. С. 12.

Если же правовые ценности расположены на различных уровнях в иерархии правовых ценностей, то между ними существует отношение соподчиненности, и конфликт между ними будет разрешаться путем признания приоритета и доминирования ценности, которая имеет более высокий уровень.

Соотношение между информационной свободой и информационной безопасностью следует из общего соотношения свободы и безопасности в системе ценностей. Традиционные подходы к разрешению конфликта между свободой и безопасностью основаны на доминировании той или иной ценности. Данные подходы были разработаны в ранней европейской правовой доктрине. Приоритет безопасности был сформулирован еще в «Левиафане» Т. Гоббса[167]. По мнению Т. Гоббса люди, объединяясь в государства, ограничивают свою свободу в целях самосохранения, то есть безопасности[168]. При таком подходе цель достижения баланса между свободой и безопасностью отсутствует – безопасность в любом случае носит первоочередной характер [169] . Напротив, приоритет свободы отстаивался в трудах Дж. Локка [170] , который указывал на то, что люди «отказываются от равенства, свободы и исполнительной власти, которой они обладают в естественном состоянии, … лишь с намерением как можно лучше сохранить себя, свою свободу и собственность»[171]. Обеспечение безопасности не может произвольно служить основанием для ограничения естественных прав человека и выступает в таком качестве, только если подчинено главной цели объединения людей в государства, а именно сохранению их жизни, свободы и собственности.

В современной правовой доктрине подходы, предложенные Т. Гоббсом и Дж. Локком, к разрешению противоречий между свободой и безопасностью

---

[167] См., напр.: Гоббс Т. Левиафан. М. : Мысль, 2001. 478 с.

[168] См.: Гоббс Т. Левиафан. С. 116.

[169] Данный подход также нашел отражение в теории коммунитаризма американского социолога А.Этциони, который рассматривает право на безопасность приоритетным в кругу иных прав. См.: Etzioni A. Security First. For a Muscular, Moral Foreign Policy. New Haven (Ct.): Yale University Press, 2008. 336 p.

[170] См., напр.: Локк Дж. Сочинения в трех томах: Т. 3. М.: Мысль, 1988. 668 с.

[171] Локк Дж. Сочинения в трех томах: Т. 3. С. 336.

сохраняют актуальность и при определении соотношения информационной свободы и информационной безопасности.

В условиях развития цифровых коммуникаций для сторонников позиции Дж.Локка приоритет информационной свободы по отношению к информационной безопасности выражается в недопустимости ограничения свободы выражения мнения и свободы информации в сети Интернет[172]. Хотя государство может быть заинтересовано в том, чтобы ограничить доступ к определенной информации в сети Интернет, существует преобладающий интерес «сетевых граждан» к обеспечению глобального и свободного от ограничений потока информации (Д.Р. Джонсон, Д.Г. Пост)[173]. Приоритет информационной свободы выражается в самоопределении и самостоятельности индивида в решении вопросов защиты не только собственно информационной свободы, но и информационной безопасности. При таком подходе отрицается ключевая роль принуждения в праве, а утверждается принцип ненасилия (non-aggression principle)[174]. Исходя из него провозглашаются практически неограниченные свобода выражения мнения и свобода информации, а также определяются пределы принуждения в праве, как правило сводящиеся к ограничению роли правовых предписаний в сети Интернет.

В то же время неограниченная свобода вступает в противоречие с правовой ценностью правового государства, которое предусматривает не только уважение и защиту со стороны государства признаваемых в обществе правовых ценностей,

---

[172] К сторонникам данного подхода относятся американские ученые-юристы Дж.П. Барлоу (Гарвардская школа права), Д.Г. Пост (Школа права университета Джорджтауна), Д.Р. Джонсон (Институт права киберпространства) и др. См., напр.: Barlow J.P. The Economy of Ideas: A Framework for Patents and Copyright in the Digital Age. Wired. 2.03.1994; Johnson D.R., Post D. Law and Borders – The Rise of Law in Cyberspace. P. 146–195.

[173] Johnson D.R., Post D. Law and Borders – The Rise of Law in Cyberspace. P. 168.

[174] Данный принцип следует из естественно-правовой доктрины Дж. Локка, согласно которой «все люди равны и независимы… ни один из них не должен наносить ущерб жизни, здоровью, свободе или собственности другого» (Локк Дж. Сочинения в трех томах: Т. 3. С. 265.). Принцип ненасилия был определен как основополагающий в либертарианской теории М.Н. Ротбарда и Р. Нозика, в основе которой лежат идеи полной личной, политической и экономической свобод. См. Nozick R. Anarchy, State, and Utopia // Basic Books, 2013. 592 p. (первое издание 1974 г.); Rothbard M.N. Egalitarianism as a Revolt Against Nature and Other Essays / 2nd ed. Auburn: The Ludwig von Mises Institute. 2000. 324 p. P. 116. (первое издание 1973 г.)

но и принятие практических действий для их правовой охраны [175] . Его неотъемлемыми составляющими являются правовое регулирование и правовое принуждение, которые определяют пределы свободы. Поэтому развитие правовой охраны информационной свободы и информационной безопасности и связанного с ней правового принуждения следует признать одним из направлений деятельности современного правового государства.

Противоположный подход признает приоритет информационной безопасности. В условиях цифровых коммуникаций из этого следует приоритет внутреннего права государства над информационной свободой индивида в сети Интернет. Без правовых норм, установленных государством, возникает анархия[176]. Только государство в условиях законно избранной власти в сочетании с правовыми нормами обладает необходимой демократической легитимностью и должно обеспечить правовую охрану как информационной свободы, так и информационной безопасности, а также осуществление и защиту основанных на них прав человека. Развитие данного подхода связано с зарубежной правовой мыслью. Так, по мнению профессора права Школы права университета Техаса Н.У. Натанеля, «либеральное государство является более эффективным гарантом либеральных прав» [177]. Вместе с тем полное отрицание возможностей человека самостоятельно обеспечивать защиту ценностей информационной свободы и информационной безопасности вступает в противоречие с такой правовой ценностью, как автономия личности. Ее важной составляющей является самозащита, для осуществления которой на сегодняшний день разработаны различные технические средства, предоставляющие личности возможности самостоятельно обеспечивать информационную безопасность.

---

[175] Государственное право Германии. Сокр. пер. с нем. Т. 1 // Отв. ред.: Топорнин Б.Н. М.: ИГиП РАН, 1994. 312 с. С. 55.

[176] См., напр.: Goldsmith J.L. Against Cyberanarchy // University of Chicago Law Review. V. 65. 1998. P. 1199–1250; Wu T.S. Cyberspace Sovereignty? – The Internet and the International System // Harvard Journal of Law & Technology. V. 10. 1997. P. 647–666; Наумов В.Б. Нормативизм против цифрового либертарианства (Комментарий к трактату Дж. П. Барлоу «Экономика идей») // Русский журнал. 1999. URL: http://old.russ.ru/netcult/99-05-13/naumov.htm (дата обращения – 9 мая 2016 г.).

[177] Netanel N.W. Cyberspace Self-Governance: A Skeptical View from Liberal Democratic Theory // California Law Review. 2000. V.88. P. 488.

При неограниченном приоритете информационной безопасности как публичной правовой ценности происходит девальвация личных правовых ценностей и умаление прав человека, в основу которых они положены. Подобное соотношение информационной безопасности и прав человека не соответствует принципам правового государства, в котором права человека признаются высшей ценностью. Однако доминанта информационной безопасности как публичной правовой ценности возможна и в правовых государствах, например в случае введения чрезвычайного положения [178] . В отличие от государств, которые отвергают высшую ценность прав человека, в правовых государствах такая доминанта является временной[179]. Восстановление приоритета информационной свободы и информационной безопасности личности и ее прав возможно при условии обеспечения необходимого и достаточного контроля над угрозами информационной безопасности как публичной правовой ценности.

---

[178] Так, согласно статье 2 Федерального конституционного закона от 30 мая 2001 г. № 3-ФКЗ «О чрезвычайном положении» целями введения чрезвычайного положения являются устранение обстоятельств, послуживших основанием для его введения, обеспечение защиты прав и свобод человека и гражданина, защиты конституционного строя Российской Федерации // СЗ РФ. 2001. № 23. Ст. 2277.

[179] См., напр.: Согласно части 2 статьи 1 Федерального конституционного закона от 30 мая 2001 г. № 3-ФКЗ «О чрезвычайном положении» введение чрезвычайного положения является временной мерой, применяемой исключительно для обеспечения безопасности граждан и защиты конституционного строя Российской Федерации // Там же; Примером временного введения ограничений прав человека также может служить принятие Акта об объединении и укреплении Америки путем предоставления надлежащих средств, необходимых для предотвращения и пресечения терроризма (USA PATRIOT Act) 2001 г. (URL: https://epic.org/privacy/terrorism/hr3162.pdf (дата обращения – 2 апреля 2016 г.), в котором права граждан подверглись широким ограничениям в целях обеспечения национальной безопасности и противодействия терроризму. Данный акт предоставил органам исполнительной власти США полномочия для доступа к разнообразной информации о частной жизни без определенных оснований, равно как полномочия проникать в жилище и проводить тайные обыски, без предупреждений в течение нескольких недель, месяцев и даже в течение неопределенного срока. Часть положений USA PATRIOT Act 2001 г., предоставляющих таким органам ограничения права на неприкосновенность частной жизни, с 1 июня 2015 г. утратила силу. Вместо них был принят новый Акт о свободе (USA Freedom Act) 2015 г. (URL: http://legislink.org/us/pl-114-23 Pub.L. 114–23 (дата обращения – 2 апреля 2016 г.), в котором полномочия органов исполнительной власти были ограничены. В частности, прослушивание переговоров резидентов и граждан США, которых подозревают в причастности к террористической деятельности, и которые не являются участниками организованных групп, с принятием данного акта возможно только на основании судебного ордера.

Таким образом, неограниченный приоритет как информационной безопасности, так и информационной свободы вступает в противоречие с правовыми ценностями и принципами правового государства и автономией личности. Несмотря на то, что между ними существует конфликт, они взаимосвязаны – свобода может быть выражена через безопасность, которая определяет ее пределы. Каждая из этих правовых ценностей выступает опорой для другой и выражается через нее. Это означает, что в системе правовых ценностей они находятся на одном уровне и соотношение между ними является равновесным. Данное соотношение нашло прямое отражение в Доктрине информационной безопасности Российской Федерации, согласно которой деятельность государственных органов по обеспечению информационной безопасности основывается на принципе соблюдения баланса между потребностью граждан в свободном обмене информацией и ограничениями, связанными с необходимостью обеспечения национальной безопасности, в том числе в информационной сфере.

Соотношение ценности информационной свободы и информационной безопасности в обществе не всегда соответствует балансу их правовой охраны. Например, в России, согласно опросам «Левада-Центра» в октябре 2016 г. по сравнению с октябрем 2012 г. повысилась ценность информационной свободы по отношению к ценности информационной безопасности[180]. Это выразилось в том, что в 2016 г. более 60% опрошенных выступили за ограничение свободы выражения мнения в сети Интернет, тогда как в 2012 г. их было 68%. Категоричность вывода о необходимости таких ограничений также снизилась более чем на 30%[181]. В этот же период в России был принят ряд федеральных законов, в которых, наоборот, был выражен приоритет информационной безопасности по отношению к информационной свободе путем определения

[180] См.: Доверие СМИ и цензура. URL: http://www.levada.ru/2016/11/18/doverie-smi-i-tsenzura/ (дата обращения – 13 августа 2016 г.).

[181] На вопрос «Как вы считаете, необходима ли цензура (запрещение доступа к отдельным сайтам и материалам) в Интернете?» в октябре 2012 г. «Определенно да» ответило 38% и «Скорее да» 30% опрошенных, тогда как в октябре 2016 г. соответственно 24% и 36%. См.: Там же.

порядка распространения и ограничения доступа к определенной информации в сети Интернет[182]. Тогда как в период становления сети Интернет баланс правовой охраны данных правовых ценностей был смещен в сторону информационной свободы, в связи с чем американский ученый-юрист Т. Ву справедливо отмечал, что такая свобода существует только благодаря инерции и «государства только приступили к определению своих приоритетов» [183], в настоящее время все большее значение приобретает информационная безопасность и ее правовая охрана. Вместе с тем смещение баланса правовой охраны в сторону информационной безопасности способствует повышению ценности информационной свободы.

Располагаясь в системе правовых ценностей, как информационная свобода, так и информационная безопасность связаны не только между собой, но и с другими правовыми ценностями. Такие связи и формируют систему правовых ценностей, основная цель которой – обеспечение уважения и защиты правовых ценностей, находящихся на вершине в их иерархии. В правовом государстве права человека признаются высшей правовой ценностью. При этом баланс информационной свободы и информационной безопасности выражается в правах человека, особенностях их осуществления и защиты. Права человека выступают одним из результатов разрешения конфликта между данными ценностями. Иными словами, правовая охрана информационной свободы и информационной безопасности является сбалансированной, если она направлена на обеспечение осуществления и защиты прав человека как высшей ценности. Только в этом

[182] См., напр.: Федеральный закон от 5 мая 2014 г. № 97-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и отдельные законодательные акты Российской Федерации по вопросам упорядочения обмена информацией с использованием информационно-телекоммуникационных сетей» (СЗ РФ. 2014. № 19. Ст. 2302); Федеральный закон от 28 июля 2012 г. № 139-ФЗ «О внесении изменений в Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» и отдельные законодательные акты Российской Федерации» (СЗ РФ. 2012. № 31. Ст. 4328); Федеральный закон от 24 ноября 2014 г. № 364-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и Гражданский процессуальный кодекс Российской Федерации» (СЗ РФ. 2014. № 48. Ст. 6645).

[183] Wu T.S. Cyberspace Sovereignty? – The Internet and the International System. P.665.

случае такой баланс является осмысленным и гармонично встроенным в общую систему и иерархию правовых ценностей.

Постиндустриальное развитие общества осуществляется в условиях, когда ценность прав человека становится менее значимой по отношению к публичным ценностям, в том числе информационной безопасности. Как отмечает Н.С. Бондарь, «на смену интернационализации на основе демократических ценностей приходит тенденция глобализации на основе критериев (принципов) безопасности личности, общества, государства» [184]. В этой связи в отечественной правовой науке отмечается «тенденция некоторого отхода от индивидуалистической концепции, когда права человека являются приоритетными, и все большего рассмотрения их с точки зрения общечеловеческих ценностей и публичных (общественных) интересов» [185]. В конечном итоге данный подход приводит к сопоставлению прав человека и интересов общества (и государства), при котором признается верховенство общественных интересов [186] или же их несоразмерность [187], а также ставится вопрос «о достижении оптимального компромисса прав человека и публичных интересов»[188]. С правовой точки зрения такой компромисс выражается в достижении баланса правовых ценностей, лежащих в основе таких интересов. Как справедливо отмечает Е.А. Лукашева, «право и права человека – индикатор национальной безопасности… Состояние прав человека, их обеспеченность дают наиболее убедительное представление о положении в любой сфере…» [189]. В правовом государстве другие ценности, в том числе лежащие в основе публичных

---

[184] Бондарь Н.С. Конституционное правосудие как фактор модернизации российской государственности // Журнал российского права. 2005. № 11 (107). С. 16.

[185] Пчелинцев С.В. Права человека и интересы безопасности: выбор приоритетов правовой политики // Социология власти. 2006. № 2. С. 107.

[186] См.: Воеводин Л.Д. Юридический статус личности в России. Учеб. пособие. М.: Изд-во Моск. ун-та, 1997. 298 с. С. 248.

[187] См.: Коробова А.П. Приоритеты правовой политики // Российская правовая политика. М.: Норма, 2003. 528 с. С. 103.

[188] Пчелинцев С.В. Права человека и интересы безопасности: выбор приоритетов правовой политики. С. 108.

[189] Лукашева Е.А. Права человека – индикатор национальной безопасности // Труды Института государства и права Российской академии наук. 2013. № 1. С. 13.

интересов, подлежат правовой охране и являются легитимными, только если они основаны на осуществлении и защите прав человека.

Несмотря на то, что в правовом государстве права человека занимают наивысшее положение в иерархии ценностей, соотношение прав человека с информационной свободой и информационной безопасностью не всегда основано на доминировании. Как справедливо отмечает итальянский ученый-юрист У. Пагало, разрешение конфликта между правами человека и безопасностью может быть связано с отсутствием баланса, если речь идет о приоритете прав человека над безопасностью, либо с таким балансом, который позволяет надлежащим образом обеспечить правовую охрану и безопасности, и прав личности[190]. В правовом государстве абсолютный приоритет безопасности в целом и информационной безопасности в частности над правами человека недопустим. Данный подход также распространяется и на соотношение информационной свободы и прав человека. Приоритет прав человека возникает, если между ними и другими ценностями существует отношение соподчиненности. Такое их соотношение характерно для случаев, когда другие ценности не находят выражения в правах человека. Другими словами, если такие ценности прямо или косвенно не связаны с созданием условий для осуществления и защитой прав человека, более того, если они связаны с их нарушениями, то данные ценности не являются правовыми и баланс между такими ценностями и правами человека невозможен, права человека в данном случае доминируют. И наоборот, о балансе правовой охраны речь идет в случае, когда одни права человека соизмеряются с ценностями, в основе которых лежит создание условий для осуществления и защита других прав человека, независимо от того являются такие ценности личными или публичными. Это обусловлено тем, что в данном случае речь идет о балансе правовой охраны различных прав человека, который определяет и пределы прав человека, что выражается в максиме: «права одного человека заканчиваются там, где начинаются права других людей».

---

[190] Pagalo U. Online Security and the Protection of Civil Rights: A Legal Overview // Philosophy & Technology. V. 26. I. 4. P. 394.

Таким образом, в условиях постиндустриального развития происходит трансформация правовых ценностей, в ходе которой повышается значение информационной свободы и информационной безопасности. Между данными правовыми ценностями существует конфликт, который следует из общего конфликта свободы и безопасности. Он может быть решен исходя из их соотношения в системе правовых ценностей и достижения баланса их правовой охраны. Традиционные подходы к соотношению информационной свободы и информационной безопасности основаны на доминировании одной либо другой ценности. Вместе с тем в правовом государстве данные правовые ценности находятся на одном уровне в системе правовых ценностей. Соотношение между ними исключает доминирование одной правовой ценности над другой, при этом баланс между ними выражается в обеспечении осуществления и защиты прав человека как высшей правовой ценности.

§2. Информационная безопасность как правовая категория

В постиндустриальный период информационная безопасность приобретает характер социального явления, которое оказывает все бóльшее влияние на тенденции развития современного общества. Его теоретическое осмысление происходит в различных областях научного знания. Как отмечается в отечественной технической литературе, «работы в области технических и технологических аспектов обеспечения информационной безопасности, как всякая инженерная деятельность, самодостаточны и традиционно ориентируются прежде всего на защиту информационных активов, процессов, коммуникаций»[191]. Для характеристики информационной безопасности в социальных науках определяющее значение имеет защищенность информационной сферы

[191] Юсупов Р.М., Шишкин В.М. Информационная безопасность, кибербезопасность и смежные понятия: Cyber Security vs Информационной безопасности // Информационное противодействие угрозам терроризма. 2013. № 21 (21). С. 29.

взаимодействия личности, общества и государства и их интересов [192] . Многоаспектность информационной безопасности также находит отражение в праве.

В отечественной правовой науке и российских нормативных правовых актах преобладает подход, при котором понятия «безопасность», «информационная безопасность» и «национальная безопасность» раскрываются через «жизненно важные интересы личности, общества и государства» [193] или «национальные интересы» [194] . В результате информационная безопасность понимается как состояние защищенности национальных интересов в информационной сфере от внутренних и внешних угроз. Вместе с тем в отечественной юридической литературе встречаются и альтернативные определения информационной безопасности как состояния защищенности совокупности различных элементов (информации, информационных систем и инфраструктуры), которые образуют информационную сферу[195]. В данном случае понятие «информационная безопасность» является более общим понятием по отношению к защите информации, представляющей собой комплекс мероприятий

[192] См., напр.: Шемякин В.П. Информационная безопасность Российской Федерации в современных российских условиях : социолого-управленческие аспекты: автореф. дис. … канд. социол. наук : 22.00.08 / Шемякин Владимир Петрович. М., 2004. 29 с.; Чеботарева А.А. Научные подходы к определению понятия «информационная безопасность» // Информационное право. М.: Юрист, 2011, № 1 (24). С. 3–5.

[193] См.: Полякова Т.А. Правовое обеспечение информационной безопасности при построении информационного общества в России : дисс… д-ра юрид. наук : 12.00.14 / Полякова Татьяна Анатольевна. М., 2008. 438 с. С. 112; Лопатин, В. Н. Информационная безопасность России: дисс… д-ра юрид. наук : 12.00.01 / Лопатин Владимир Николаевич. М., 2003. 433 с. С. 91; Указ Президента Российской Федерации от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»; Указ Президента Российской Федерации от 31 декабря 2015 г. № 683 «О Стратегии национальной безопасности Российской Федерации» // СЗ РФ. 2016. № 1. Ст. 212.

[194] См., напр.: Зорькин В.Д. Национальные интересы, современный миропорядок и конституционная законность // Актуальные проблемы развития судебной системы и системы добровольного и принудительного исполнения решений Конституционного Суда РФ, судов общей юрисдикции, арбитражных, третейских судов и Европейского суда по правам человека. Сборник научных статей. СПб., Краснодар: Юрид. центр Пресс, 2008. С. 21–58; Указ Президента Российской Федерации от 31 декабря 2015 г. № 683 «О Стратегии национальной безопасности Российской Федерации».

[195] Схожий подход к определению информационной безопасности содержался в утратившем в 2006 г. силу Федеральном законе от 4 июля 1996 г. № 85-ФЗ «Об участии в международном информационном обмене» (СЗ РФ. 1996. № 28. Ст. 3347), в котором использовался термин «информационная среда общества».

и действий, направленных на обеспечение безопасности информации[196]. При этом понятие «защита информации» отечественным законодателем используется в федеральных законах чаще[197], нежели понятие «информационная безопасность», что указывает на преобладание в правовом регулировании технического подхода к данному социальному явлению.

В правовой науке зарубежных государств бóльшее распространение получил подход к информационной безопасности, при котором она рассматривается как совокупность свойств информационных систем, таких как конфиденциальность, целостность и доступность[198].

Конфиденциальность связана с возможностью информационных систем предотвратить неавторизованный доступ к содержащейся в них информации. Ее обеспечение осуществляется на основе классификации информации в зависимости от прав доступа к ней, в том числе путем определения, так называемой, чувствительной информации, которой предоставляется максимальная защита – шифрование информации, проведение организационных и технических мероприятий, направленных на подтверждение прав лиц, которые получают доступ к информации.

---

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

[197] На 1 сентября 2017 г. термин «защита информации» использовался в 158 федеральных законах (в том числе 64 федеральных законах о внесении изменений в другие федеральные законы), тогда как термин «информационная безопасность» только в 24 федеральных законах (в том числе 10 федеральных законах о внесении изменений в другие федеральные законы) // По данным СПС Консультант Плюс.

[198] См., напр.: Grama J. Legal Issues in Information Security. Jones & Bartlett Publishers, 2010. 526 p. P. 4.; Nelson S.D., Isom D.K., Simek J.W. Information Security for Lawyers and Law Firms // Chicago, IL: American Bar Association, 2006. 424 p. P. 9–12. Данный подход соответствует дефинициям, предусмотренным международными стандартами. См.: ISO/IEC 27002: Code of Practice for Information Security management 2005 (Preview // URL: https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-2:v1:en (дата обращения – 1 декабря 2016 г.). В соответствии с данным стандартом, кроме конфиденциальности, целостности и доступности, также учитываются и такие свойства информации и средств ее обработки, как аутентичность, подотчетность, неотрекаемость и надежность. Этот подход также предусмотрен в ГОСТ Р ИСО/МЭК 13335-1-2006 «Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий» (М.: Стандартинформ, 2007).

Целостность характеризует возможность информационных систем обеспечивать предотвращение несанкционированных модификаций информации. Речь идет о модификации как в результате действий различных лиц, так и в силу случайных событий. Ее обеспечение связано с проверками информации на отсутствие изменений и, также как и в случае с конфиденциальностью, с защитой от неавторизованного доступа к ней.

Доступность в данном случае – это возможность информационных систем противостоять случайному или намеренному раскрытию данных или получению доступа к ним, а также способность восстанавливаться после таких событий. Она также связана с обеспечением работоспособности информационной системы, то есть с возможностью ее использования в соответствии с ее функциональным назначением.

Информационная безопасность достигается за счет нахождения надлежащего баланса между конфиденциальностью, целостностью и доступностью, который становится краеугольным камнем любых законодательных мер в данной области [199]. Данный подход выражается в установлении обязанностей различных субъектов правоотношений по обеспечению конфиденциальности, целостности или же доступности, а также ответственности за их нарушение.

В основе перехода от технического и социального подходов к определению понятия «информационная безопасность» к рассмотрению ее как правовой категории лежит соотношение данного социального явления с правами человека. В этой связи профессор права Лапландского университета А. Сааренпаа справедливо отмечает, что при определении «информационной безопасности» законодатель часто забывает про ее правовое измерение, концентрируясь на «административных и технических мерах, которые принимаются для того, чтобы гарантировать, что данные доступны для тех, кто уполномочен на их использование, данные могут быть изменены теми, кто уполномочен на это, и

[199] Information Security and Privacy: a Practical Guide for Global Executives, Lawyers, and Technologists / Thomas J. Shaw, editor. 395 p. P. 17–18.

информационные системы могут быть использованы теми, кто уполномочен на это»[200]. Права человека определяют ценностную ориентацию информационной безопасности. Признание прав человека высшей ценностью способствует исключению произвольного и избыточного вмешательства в сферу их осуществления при обеспечении информационной безопасности личности, общества и государства. В результате с общетеоретической позиции правовая категория информационной безопасности может быть определена как состояние защищенности прав человека в информационной сфере.

Целями правового регулирования в области обеспечения информационной безопасности является достижение конфиденциальности, целостности и доступности в информационной сфере. Данные цели отличают информационную безопасность от иных видов безопасности и определяют направленность соответствующего правового регулирования. Основные идеи и руководящие положения, на которые оно ориентируется, могут быть выражены в правовых принципах конфиденциальности, целостности и доступности.

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. В связи с этим принцип конфиденциальности обусловливает различные ограничения данного права. Равным образом, исходя из данного принципа следуют ограничения свободы выражения мнения и свободы информации, поскольку на его основе определяются случаи и условия раскрытия конфиденциальной 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

[200] См.: Saarenpää A. The Importance of Information Security in Safeguarding Human and Fundamental Rights // URL: http://www.juridicum.su.se/iri/e08/ documentation/ahti_saarenpaa-information_security_and_human_rights-paper.pdf (дата обращения – 27 февраля 2016 г.); Act on the Protection of Privacy in Electronic Communications 516/2004 // URL: http://www.finlex.fi/en/laki/kaannokset/2004/ en20040516.pdf (дата обращения – 27 февраля 2016 г.).

безопасности личности, общества или государства. Данному принципу соответствует своего рода право «таить» информацию, т.е. сохранять ее в тайне, ограничивать право доступа к ней третьих лиц, контролировать ее целевое использование.

В отличие от конфиденциальности обеспечение целостности информации стало актуальным в процессе развития компьютерной техники 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 и достоверности информации, что 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. Поэтому нарушением данного принципа не будет являться уничтожение или модификация информации и ее носителя, которые произведены уполномоченным лицом.

Принцип доступности играет важную роль для обеспечения осуществления и защиты права на доступ к информации. Данный принцип направлен на предотвращение ограничения и создание условий для доступа к социально значимой информации прежде всего при взаимодействии человека с государственными органами, а также к иной информации, предоставления которой он вправе требовать. В соответствии с данным принципом определяются условия доступа к информации, в том числе платность или бесплатность ее предоставления, форма представления, доступность для лиц с ограниченными возможностями здоровья, доступность во времени и пространстве. Этот принцип лежит в основе реализации мер по обеспечению доступа к информации о деятельности государственных органов, экологической информации, в том числе

путем размещения информации на официальных сайтах органов и организаций, а также использования иных форм раскрытия и распространения информации.

В отечественной юридической литературе под конфиденциальностью и доступностью, как правило, понимаются специфические правовые режимы информации[201]. Как справедливо отмечает Л.К. Терещенко, «конфиденциальность – это установленный режим информации; как любой режим, он может быть введен либо его действие может быть прекращено» [202]. Вместе с тем конфиденциальность и доступность как правовые режимы информации отличаются от конфиденциальности и доступности как правовых принципов. Соответствующие режимы не являются неотъемлемым свойством информации и устанавливаются в правовом регулировании в целях обеспечения «информационной безопасности субъектов, в качестве которых могут выступать личность, государство, общество в целом» [203]. В то же время соблюдение правовых принципов конфиденциальности и доступности является непреложным условием обеспечения информационной безопасности независимо от правового режима информации. Правовой режим информации определяется совокупностью правовых средств, которые для конфиденциальности и доступности могут быть выражены в запретах и обязанностях, разрешениях и ограничениях определенных действий. При этом правовые принципы конфиденциальности и доступности определяют условия, при которых использование таких правовых средств является правомерным.

Воплощение правовых принципов конфиденциальности, целостности и доступности при обеспечении информационной безопасности в правовом регулировании предполагает комплексность, при которой оно соизмеряется с каждым из них. Это означает, что каждый из указанных принципов определяет направленность правового регулирования при обеспечении информационной

---

[201] См., напр.: Терещенко Л.К. К вопросу о правовом режиме информации // Информационное право. 2008. № 1. С. 20–27; Соловяненко Н.И. Теоретическое осмысление правового режима информации // Право. Журнал Высшей школы экономики. 2008. № 1. С. 121–124.

[202] Право на доступ к информации. Доступ к открытой информации. С. 56.

[203] Терещенко Л.К. Правовой режим информации. М.: ИД «Юриспруденция», 2007. 192 с.

безопасности независимо от правового режима информации и предпринимаемых организационно-технических мер. Так, если правовое регулирование связано с необходимостью сохранить в тайне определенный вид информации, то в нем выражается не только принцип конфиденциальности, но и иные принципы. Тайна не может быть абсолютной – наряду с запретом и ограничением доступа к информации, отдельным категориям лиц всегда предоставляется право доступа к ней. При этом запрет, ограничение или же право доступа к информации не имеют практического смысла, если не обеспечивается ее целостность.

С развитием информационных и коммуникационных технологий возникает необходимость соблюдения принципов конфиденциальности, целостности и доступности не только в отношении информации, но и в отношении ее носителя, формы и форматов ее представления, средств обеспечения доступа к ней. Происходит распространение данных принципов также на информационные системы и инфраструктуру, в том числе на информационно-телекоммуникационные сети. Их конфиденциальность, целостность и доступность предопределяют соблюдение соответствующих правовых принципов и в отношении информации, которая с их помощью обрабатывается, хранится, передается и иным образом используется. При этом обеспечение информационной безопасности и, следовательно, соблюдение правовых принципов конфиденциальности, целостности и доступности в цифровой среде становится необходимым условием осуществления и защиты любых цифровых прав человека.

Появление новых вызовов и угроз в информационной сфере приводит к постановке вопроса о признании права человека на информационную безопасность. Для его решение могут быть использованы традиционные подходы к праву на безопасность как более общей правовой категории. При этом данное право либо признается самостоятельным правом человека, либо выводится из других прав, в том числе рассматривается как интегративное право,

охватывающее другие права человека[204]. Так, в отечественной и зарубежной юридической литературе высказывается точка зрения о наличии самостоятельного права на информационную безопасность [205], которое основывается на необходимости охраны интересов личности в информационной сфере от произвольного вмешательства других лиц и предполагает активную защиту со стороны государства.

Вместе с тем указанная точка зрения не в полной мере раскрывает особенности правомочий личности в области обеспечения информационной безопасности. Как в российском, так и зарубежном законодательстве право на информационную безопасность нормативно не закреплено. Национальные суды рассматривают юридические конфликты, связанные с нарушением информационной безопасности личности, при осуществлении защиты достоинства личности, чести и доброго имени, деловой репутации, неприкосновенности частной жизни, личной и семейной тайны, права на свободу выражения мнения, свободу информации. В этой связи более убедительной является точка зрения, высказанная в зарубежной литературе, которая заключается в том, что обеспечение информационной безопасности самостоятельного права не образует [206]. Равным образом право на информационную безопасность не является интегративным правом и не охватывает указанные выше права человека, поскольку их содержание значительно шире вопросов обеспечения информационной безопасности.

Информационная безопасность проявляется не в одном правомочии, а в совокупности прав. В них выражаются возможности и притязания индивида,

---

[204] См., напр.: Ардашев А.И. Конституционно-правовое обеспечение права человека на безопасность в Российской Федерации // Современное право. 2008. № 1. С. 39 – 44; Калина Е.С. Понятие безопасности и право на безопасность как одно из личных прав // Безопасность бизнеса. М.: Юрист, 2004, № 4. С. 9–10; Колоткина О.А. Право личности на безопасность: понятие, место в системе прав человека и особенности изучения в курсе конституционного права РФ // Право и образование. 2007, № 11. С. 109–114.

[205] См., напр.: Чеботарева А.А. Человек и электронное государство: право на информационную безопасность. Чита: ЧИТГУ, 2011. 160 с.; Saarenpää A. The Importance of Information Security in Safeguarding Human and Fundamental Rights.

[206] См., напр.: Mitrakas A. Information Security Regulation: Tomorrow Never Dies? // Highlights of the Information Security Solutions Europe 2006 Conference. 2006. P. 433–434.

связанные с соблюдением принципов конфиденциальности, целостности или же доступности информации и технических средств, предназначенных для ее хранения, обработки, передачи и иного использования. Однако из признания данных прав в национальном законодательстве и судебной практике не следует признание права человека на информационную безопасность, поскольку вопросы информационной безопасности составляют только часть их содержания.

Некоторые права в сфере обеспечения информационной безопасности получили юридическое закрепление в национальном праве в качестве основных прав, другие выступают отдельными компонентами уже признанных прав человека.

В первом случае такими правами, например, являются права на целостность и конфиденциальность информационных систем, признанные основными правами в решении Федерального Конституционного суда Германии 2008 г.[207] на основе результатов анализа основного права на информационное самоопределение, провозглашенного судом еще в 80-х годах прошлого века[208]. В соответствии с решением суда негласное проникновение в информационную систему для ее использования, а также извлечения содержащейся в ней информации конституционно допустимы, только если существует фактическая опасность для ценностей, имеющих более важное правовое значение[209]. Тенденцию признания в качестве основных прав также имеют право на доступ к информации о

---

[207] Headnotes to the Judgment of the First Senate of 27 February 2008. 1 BvR 370/07. URL: http://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2008/02/rs20080227_ 1bvr037007en.html (дата обращения – 20 мая 2017 г.).

[208] В решении Федерального конституционного суда Германии 1983 г., которое было связано с принятием закона о государственной переписи населения, официально признано фундаментальное (основное) право на информационное самоопределение. В своем решении суд указал, что в условиях современных способов обработки данных защита личности от неограниченного сбора, хранения, использования и раскрытие ее личных данных гарантируется фундаментальным (основным) правом личности, закрепленным в Конституции. Данное фундаментальное (основное) право гарантирует возможность личности контролировать раскрытие и использование её личных данных. Ограничения данного права на информационное самоопределение допускаются только при наличии преобладающего общественного интереса. См., напр.: Волчинская Е.К. Защита персональных данных: Опыт правового регулирования. М.: Галерия, 2001. 236 с.

[209] К таким ценностям Суд, в частности, отнес жизнь, здоровье, свободу личности, основы конституционного строя государства.

деятельности органов государственной власти и право на доступ к сети Интернет, которые равным образом могут рассматриваться как права человека в области обеспечения информационной безопасности, поскольку в них выражается требование соблюдения доступности определенной информации, информационных систем и инфраструктуры.

Во втором случае к таким правам, в частности, можно отнести отдельные компоненты права на неприкосновенность частной жизни. Следует согласиться с утверждением, что «без информационной безопасности не может быть неприкосновенности частной жизни» [210] . Обеспечение информационной безопасности личности составляет основу ее правовой защиты. К правам, связанным с соблюдением конфиденциальности, целостности и доступности информации о частной жизни относятся отдельные права субъектов персональных данных, а также такие относительно новые цифровые права, как право на анонимность в сети Интернет и право на забвение.

В национальном, наднациональном и международном праве в целях обеспечения соблюдения и защиты данных прав осуществляется конкретизация принципов конфиденциальности, целостности и доступности. Так, международными организациями были выработаны специальные принципы защиты права на неприкосновенность частной жизни [211] и права доступа к информации о деятельности органов государственной власти [212] . Данные

---

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

[211] Специальные правовые принципы в области защиты права на неприкосновенность частной жизни были сформированы на базе так называемых Справедливых информационных принципов, разработанных ОЭСР в 1980 г. В 2013 г. они получили обновление. 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 апреля 2015 г.).

[212] См., напр.: Рекомендации Совета Европы 1037 (1986) «О защите данных и свободе информации». URL: http://assembly.coe.int/Main.asp?link=/Documents/AdoptedText/ta86/EREC1037.htm (дата обращения – 25 января 2016 г.); Рекомендация Совета Европы № R(81)19 о праве на доступ к информации, находящейся в ведении государственных организаций, принята Комитетом министров 25 ноября 1981 г. URL: http://www.media-advocat.ru/european/?p=press&pid=19 (дата обращения – 25 января 2016 г.); Рекомендации Совета Европы № Rec(2002)2 по доступу к официальным документам // URL: http://ppt.ru/news/4357 (дата обращения – 25 января 2016 г.).

принципы получили юридическое закрепление в международном праве[213], которое в свою очередь оказывает влияние на их признание в национальном праве[214]. Так, аналогичные принципы, предусмотренные Конвенцией Совета Европы о защите физических лиц при автоматизированной обработке персональных данных от 28 января 1981 г., легли в основу законодательства о персональных данных государств – членов Совета Европы, в том числе в основу Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных». Данные принципы конкретизируют принципы конфиденциальности, целостности и доступности и определяют содержание соответствующих прав в области обеспечения информационной безопасности личности.

В отличие от информации о личности (персональных данных), которая, по общему правилу[215], является конфиденциальной, информация о деятельности органов государственной власти в правовом государстве выступает общедоступной, если иное не определено законом. В связи с принципом конфиденциальности специальные правовые принципы защиты права на неприкосновенность частной жизни определяют возможность сбора информации о личности только законными и добросовестными средствами и для конкретно определенных целей при условии предварительного уведомления или согласия

---

[213] 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; Конвенция Совета Европы о доступе к официальным документам – данная конвенция открыта к подписанию 18 июня 2009 г. и вступит в силу после ее ратификации 10 государств – членов Совета Европы.

[214] Напр., принципы обеспечения права на неприкосновенность частной жизни содержатся в Акте Канады о защите личной информации и электронных документов 2000 г. (Personal Information Protection and Electronic Documents Act (PIPEDA). URL: http://laws-lois.justice.gc.ca/PDF/P-8.6.pdf (дата обращения – 25 января 2016 г.) 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); принципы обеспечения права доступа к информации о деятельности органов государственной власти содержатся в Федеральном законе от 9 февраля 2009 г. № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» (СЗ РФ. 2009 г. № 7. Ст. 776).

[215] См., напр.: Часть 9 статьи 9 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», статья 7 (Конфиденциальность персональных данных) Федерального закона от 27 июня 2006 г. № 152-ФЗ «О персональных данных».

индивида, обеспечения их защиты от таких рисков, как потеря или несанкционированный доступ, уничтожение, использование, изменение или раскрытие данных. В свою очередь конфиденциальность информации о деятельности органов государственной власти обеспечивается путем выработки дополнительных принципов, при соблюдении которых могут быть установлены ограничения права на доступ к такой информации[216]. Речь идет о том, что при предоставлении и распространении информации о деятельности государственных органов, должны соблюдаться не только государственная или служебная тайны, но также права на неприкосновенность частной жизни, личную и семейную тайну, права индивида на защиту чести и деловой репутации, права организаций на защиту их деловой репутации.

Наряду с принципом целостности при обеспечении осуществления и защиты права на неприкосновенность частной жизни ОЭСР [217] предлагается принцип, при соблюдении которого информация о личности должна соответствовать целям ее использования и в соответствии с такими целями должна быть точной, полной и актуальной. В российском праве данный принцип выражается в том, что при обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных [218] . Принцип достоверности информации о деятельности государственных органов является одним из ключевых принципов, который, в частности, получил закрепление в отечественном законодательстве[219].

---

[216] См., напр.: Global Principles on National Security and the Right to Information (“THE TSHWANE PRINCIPLES”) Finalized in Tshwane, South Africa Issued on 12 June 2013. URL: http://fas.org/sgp/library/tshwane.pdf (дата обращения – 25 января 2016 г.).

[217] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

[218] Часть 6 статьи 5 Федерального закона от 27 июня 2006 г. № 152-ФЗ «О персональных данных».

[219] Пункт 4 статьи 4 Федерального закона от 9 февраля 2009 г. № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления».

Доступность[220], наоборот, в меньшей степени свойственна правовому режиму информации о личности, тогда как для информации о деятельности органов государственной власти она является ключевой. О доступности информации о личности можно говорить только в отношении возможности самого индивида получать доступ к информации о его частной жизни, если эта информация находится у других лиц, или же получения доступа к такой информации другими лицами с согласия индивида или в соответствии с законом. В данном случае принцип доступности дополняется правовыми принципами, которые создают условия для доступа индивида к информации о наличии у других лиц и характере обрабатываемой ими информации о его частной жизни, основных целях использования такой информации, о личности и месте нахождения таких лиц, а также наделяют индивида дополнительными правами, включая возможность уничтожения, исправления, дополнения или изменения личной информации.

Для права на доступ к информации о деятельности органов государственной власти данный принцип в национальном праве может дополняться такими принципами, как транспарентность, открытость, гласность, публичность, прозрачность. Как справедливо отмечается в отечественной юридической литературе, «все эти термины в той или иной степени связаны с доступностью информации, однако различаются в средствах и объемах ее обеспечения»[221]. Каждый из указанных терминов отражает определенный аспект доступности информации о деятельности государственных органов в публично-правовых отношениях, но может также охватывать и вопросы физического доступа на определенные мероприятия, территорию или помещения органов государственной власти.

---

[220] Так, законодательством Российской Федерации в области персональных данных предусмотрено специальное регулирование в случаях, если персональные данные сделаны общедоступными субъектом персональных данных или получены из общедоступного источника.

[221] Право на доступ к информации. Доступ к открытой информации. С. 199.

Развитие права на доступ к информации о деятельности органов государственной власти на основе концепции открытых данных способствует дальнейшей конкретизации принципов целостности и доступности. На сегодняшний день международными экспертами предложено восемь ключевых принципов открытых данных [222]. В число данных принципов, которые дополняют принцип целостности, входят принципы первичной информации (данные собираются из источника с максимально возможным уровнем детализации без агрегации и модификации), возможности автоматизированной обработки (открытые данные должны быть в достаточной степени структурированы для автоматизированной обработки). В дополнении к принципу доступности они охватывают принципы полноты (ко всем открытым данным предоставляется доступ; на открытые данные не распространяются ограничения, связанные с конфиденциальностью, безопасностью и иными изъятиями), своевременности (к данным предоставляется доступ так быстро, как это необходимо для сохранения их ценности), недискриминации (открытые данные должны быть доступны всем пользователям без прохождения регистрации), свободного формата (данные должны быть представлены в формате, в отношении которого никто не имеет исключительных прав), отсутствия объектов исключительного права (открытые данные не должны являться объектом авторского, патентного права, средств индивидуализации, охраняемых правом, ноу-хау). Развитие данной группы принципов продолжается[223], определяя новые условия и способы осуществления права на доступ к информации о деятельности государственных органов государственной власти.

Правовые принципы конфиденциальности, целостности и доступности представляют собой универсальную модель, которая не зависит от развития

---

[222] См.: 8 Principles of Open Government Data. URL: https://public.resource.org/8_principles.html (дата обращения – 17 января 2016 г.).

[223] В частности, концепция открытых данных постепенно переходит в концепцию открытых связанных данных, для которой характерно наличие внутренних ссылок в документах в одних базах данных на связанные с ними данные и документы в других базах данных. См., напр.: Attard J. et al. A Systematic Review of Open Government Data Initiatives / Government Information Quarterly. 2015. V. 32. P. 399–418.

информационных и коммуникационных технологий и может применяться в разных странах и правовых системах. Однако конкретизация данных принципов при определении содержания прав в области обеспечения информационной безопасности в той или иной степени зависит от правовых традиций государства. Так, в различных государствах состав и содержание правовых принципов защиты права на неприкосновенность частной жизни может отличаться.

В национальном праве европейских государств, включая Россию, право на неприкосновенность частной жизни рассматривается как основное право[224] и его защита, как правило, гарантируется конституциями. Так, в государствах – членах Европейского союза приоритет полного контроля личности над информацией о его частной жизни перед традиционными свободами, такими как свобода предпринимательской деятельности и свобода выражения мнения, лежит в основе нескольких поколений национальных законов в сфере защиты неприкосновенности частной жизни, нормативных правовых актах Европейского союза и решениях Суда справедливости Европейского союза.

В отличие от европейских государств в США специальное правовое регулирование в области обработки информации о частной жизни установлены только в наиболее чувствительных сферах[225], а также в сфере деятельности федеральных государственных учреждений[226]. Право на неприкосновенность частной жизни прямо не предусмотрено в Конституции США однако выводится Верховным Судом США исходя из содержания отдельных поправок к

---

[224] См., напр.: 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 – 13 сентября 2015 г.).

[225] Например, в США такими сферами являются сбор данных с помощью онлайн-сервисов о детях младше 13 лет, финансовых институтах о своих клиентах, бюро кредитных историй о клиентах и медицинскими работниками о пациентах, а также некоторые другие области, по которым приняты специальные законы // Children's Online Privacy Protection Act of 1998, Gramm-Leach-Bliley Act of 1999, Fair Credit Report Act of 1992, Health Insurance Portability and Accountability Act (HIPAA) of 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).

[226] Privacy Act of 1974. URL: https://www.gpo.gov/fdsys/pkg/STATUTE-88/pdf/STATUTE-88-Pg1896.pdf (дата обращения – 2 апреля 2016 г.).

Конституции США. В то же время Конституция США предоставляет защиту только от вмешательства государства в сферу осуществления данного права. В остальных сферах государство отдает приоритет саморегулированию, в основе которого лежит свобода предпринимательской деятельности, свобода договора, свобода выражения мнения [227] . При этом органы исполнительной власти федерального уровня во главе с Президентом США воздействуют на общественные отношения путем издания различного рода рекомендаций и политических заявлений. Защита права на неприкосновенность частной жизни также может осуществляться в соответствии с законодательством о защите прав потребителей с учетом решений Федеральной торговой комиссии США и законодательства штатов в сфере деликтов. В основу таких решений положены принципы добросовестной информационной практики, разработанные комиссией, которые отличаются от признанных экспертами ОЭСР и в европейских государствах[228]. В правовой науке США их также называют упрощенными (lite) – не только из-за того, что состав данных принципов уже, чем предусмотрено рекомендациями ОЭСР, но и в силу значения, которое придается в практике административных органов и организаций уведомлениям об использовании информации о личности вместо получения ее предварительного согласия на такое использование[229]. В результате создаются более благоприятные условия, нежели в европейских государствах, для развития интернет-коммерции, индустрии

---

[227] 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.

[228] В частности, речь идет о принципах уведомления/информированности (потребитель должен быть проинформирован об использовании информации о нем), выбора/согласия (потребителю должна быть предоставлена возможность дать предварительное согласие на предоставлении информации о нем (opt-in) либо последующий отказ от предоставления такой информации (opt-out)), доступа/участия (потребителю должны быть предоставлены доступные инструменты для того, чтобы он мог получить доступ к информации о нем для проверки ее точности и достоверности), целостности/безопасности (должна быть обеспечена целостность и защищенность информации о личности) и правоприменения/возмещения (данный принцип предусматривает гарантии от правонарушений, в первую очередь – механизмы саморегулирования, во вторую – возмещение вреда, в третью – возложение санкций органами государственной власти)

[229] См.: Bamberger K.A., Mulligan D.K. Privacy on the Books and on the Ground // Stanford Law Review. 2011. V. 63. P. 254.

информационных брокеров, а также использования современных технологий обработки информации о личности в деятельности государственных органов.

Таким образом, информационная безопасность как правовая категория выражается в состоянии защищенности прав человека в информационной сфере. Основные идеи и руководящие положения, на которые ориентируется правовое регулирование в области обеспечения информационной безопасности, заключаются в правовых принципах конфиденциальности, целостности и доступности. Информационная безопасность лежит в основе совокупности прав, в которых представлены возможности и притязания индивида, связанные с соблюдением данных правовых принципов. Некоторые из них получили юридическое закрепление в национальном праве в качестве основных прав, другие выступают отдельными компонентами уже признанных прав человека. В национальном, наднациональном и международном праве могут предусматриваться особенности их осуществления и защиты на основе конкретизации правовых принципов конфиденциальности, целостности и доступности.

§3. Правовые и технические гарантии прав человека при обеспечении информационной безопасности

С развитием информационных и коммуникационных технологий обостряются проблемы обеспечения информационной безопасности прежде всего в цифровой среде. Речь идет о таких проблемах, как преступления в сфере компьютерной информации, пропаганда терроризма и экстремизма, разжигание ненависти и распространение детской порнографии. Нарушение информационной безопасности может представлять собой опасность в информационной сфере и создавать не только опасность для отдельных индивидов, но и экзистенциальные риски для государства и общества[230].

[230] В первом случае речь идет о рисках, которые могут привести к потере жизни или повреждению имущества отдельных частных лиц без создания угрозы для существования

В отечественной правовой литературе обеспечение информационной безопасности традиционно рассматривается как один из видов деятельности и как средство деятельности, направленной на «создание условий, при которых нанесение вреда зависящим от информации свойствам или составляющим объекта безопасности невозможно» [231] . Такую деятельность осуществляют индивиды, институты гражданского общества и государственные органы, обеспечивая состояние защищенности сбалансированных интересов личности, общества и государства в информационной сфере. В правовом государстве она направлена на создание условий, при которых обеспечивается состояние защищенности прав человека в информационной сфере, как основная цель и ценность информационной безопасности. В результате ее обеспечение становится одной из гарантий прав человека в информационной сфере. Под гарантиями прав человека традиционно понимается система условий, средств и способов, с помощью которых обеспечиваются равные возможности для осуществления, обеспечения охраны и защиты прав человека[232].

Обеспечение информационной безопасности как гарантия прав человека неразрывно связана с другими видами гарантий и в них находит свое выражение. Цифровая среда не умаляет значимости общечеловеческих ценностей и социальных норм, которые выражаются в правах человека. В этой связи в резолюции 2014 г. Совета по правам человека при ООН отмечается, что «права, которые человек имеет в офлайновой среде, должны защищаться и в онлайновой

государства. Во втором (экзистенциальные риски) – о рисках, которые могут привести к разрушению государственности или к многочисленным человеческим жертвам и(или) причинить значительный ущерб стратегическим активам и национальной инфраструктуре. См.: Columbic M.C. Fighting Terror Online: The Convergence of Security, Technology, and the Law. New York: Springer New York, 2008. XIV, 178 p. P. 16.

[231] Организационно-правовое обеспечение информационной безопасности : монография / А.В. Морозов, Т.А. Полякова; РПА Минюста России. М.: РПА Минюста России, 2013. 276 с. С. 16–18.

[232] См., напр.: Мордовец А.С. Гарантии прав личности: понятие и классификация // Теория государства и права: Курс лекций / Под ред. Н.И. Матузова, А.В. Малько. М.: Юристъ, 2000. С. 311–319.

среде…»[233]. Весь комплекс гарантий, которыми обеспечивается осуществление и защита прав человека в офлайновой среде, равным образом распространяется и на права человека в киберпространстве и цифровой среде в целом. В то же время условия осуществления и защиты прав человека в цифровой и офлайновой средах различаются. В цифровой среде права человека сталкиваются с вызовами информационной безопасности, которые способствуют развитию гарантий прав человека. Так, для цифровой среды характерны технические гарантии прав человека, которые представлены в форме технических средств и технических норм[234]. С одной стороны, такие технические средства используются индивидами для самозащиты, например программное обеспечение, предназначенное для конфиденциальных или анонимных коммуникаций. С другой – применяются в деятельности информационных посредников и органов государственной власти для обеспечения осуществления и защиты прав человека в информационной сфере. К ним также относятся информационно-телекоммуникационные сети, технические средства, которые обеспечивают право на доступ к сети Интернет и позволяют осуществлять права человека с ее использованием. Технические нормы, включая технико-юридические нормы как их разновидность [235] ,

[233] Поощрение, защита и осуществление прав человека в Интернете: Резолюция, принятая Советом по правам человека от 14 июля 2014 г. № A/HRC/RES/26/13. См.: URL: http://www.refworld.org.ru/docid/5583e0004.html (дата обращения – 20 августа 2016 г.).

[234] Технические гарантии прав человека отличаются от традиционно выделяемых в отечественной литературе организационных и организационно-технических гарантий (см., напр.: Мордовец А.С. Гарантии прав личности: понятие и классификация. С. 311–319) тем, что в отличие от таких гарантий представляет собой не деятельность, связанную с использованием технических средств, а непосредственно сами технические средства и технические нормы, в соответствии с которыми они создаются и используются.

[235] Наряду с техническим нормами, предусмотренными стандартами и техническими регламентами, увеличивается количество технических норм, представленных в правовых формах, которые отечественный ученый-юрист В.Б. Исаков справедливо называет технико-юридическими. См.: Исаков В.Б. Преемственность правовых норм в сфере технического регулирования. Юридическая техника. 2011. № 5. С.188. Подобные технико-юридические нормы устанавливаются нормативными правовыми актами и предписывают, например, создание технических условий для блокирования и фильтрации информации, размещенной в сети Интернет, определяют требования к шифровальным (криптографическим) средствам при осуществлении лицензирования деятельности в области их разработки, производства, распространения и использования, требования к средствам защиты информации.

предваряют разработку таких технических средств и определяют требования к ним, способам и методам их использования[236].

При обеспечении информационной безопасности в цифровой среде возрастает роль таких технических гарантий прав человека, которые выражены в технических способах их защиты. В частности, в их число входят технические средства, которые функционируют без передачи конфиденциальной информации другим техническим средствам. Например, к ним относятся Система глобального позиционировании (GPS), позволяющая без использования конфиденциальной информации передавать информацию о географическом расположении, протокол DHCP [237] , который без передачи информации о личности обеспечивает подключение к сети Интернет. Таким техническим гарантиям прав человека соответствуют разработанные в зарубежной юридической литературе концепции «неприкосновенность частной жизни за счет проектных решений» (privacy by design)[238] и «безопасность за счет проектных решений» (security by design[239])[240].

---

[236] Такие нормы устанавливаются не только государством и наднациональными союзами посредством технического регулирования, но и негосударственными организациями. Например, в сфере деятельности кредитных и других организаций – субъектов национальной платежной системы Российской Федерации – широко распространены стандарты Ассоциации пользователей стандартов по информационной безопасности АБИСС. Данные стандарты становятся обязательными для организаций, если они добровольно принимают решение об их введении. Их соблюдение становится, в частности, гарантией прав субъектов персональных данных, права на неприкосновенность частной жизни и других прав человека, осуществление и защита которых зависит от обеспечения информационной безопасности. См.: Библиотека Документов АБИСС. URL: http://www.abiss.ru/standards/document_library/ (дата обращения – 27 апреля 2017 г.).

[237] DHCP (англ. Dynamic Host Configuration Protocol – протокол динамической настройки узла) – протокол, который используется для автоматического предоставления цифровым устройствам сетевого адреса и конфигурационных параметров, необходимых для подключения к сети Интернет.

[238] См., напр.: Cavoukian A. Privacy by Design. The 7 Foundational Principles. URL: https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf (дата обращения – 27 апреля 2017 г.); Resolution on Privacy by Design. 32nd International Conference of Data Protection and Privacy Commissioners (October 2010). URL: https://edps.europa.eu/sites/ edp/files/publication/10-10-27_jerusalem_resolutionon_ (дата обращения – 27 апреля 2017 г.privacybydesign_en.pdf (дата обращения – 27 апреля 2017 г.); Klitou D. Privacy-Invading Technologies and Privacy by Design: Safeguarding Privacy, Liberty and Security in the 21st. T.M.C. Asser Press, 2014. XIX, 338 p.

[239] В контексте данной концепции обеспечение безопасности направлено на разработку программного обеспечения и технических устройств, исключающую наличие уязвимостей или

Неприкосновенность частной жизни за счет проектных решений предполагает встроенную в технические средства защиту информации о личности, при которой исключается ее передача другим лицам. В свою очередь безопасность за счет проектных решений не только не ограничена защитой права на неприкосновенность частной жизни, но и указывает на необходимость защиты прав всех участников информационного взаимодействия. В этой связи она допускает передачу конфиденциальной информации, если это необходимо для защиты прав других лиц. Как следствие, подходы к реализации данных концепций отличаются. В зарубежной юридической литературе они определяются через совокупность принципов, при соблюдении которых использование технических средств обеспечивает защиту прав человека в цифровой среде.

Принципы неприкосновенности частной жизни за счет проектных решений сформулированы канадским ученым-юристом А. Кавоукян[241]. В их число входят проактивность (защита от нарушения (предотвращение нарушения) прав вместо защиты нарушенных прав), защита по умолчанию (защита прав обеспечивается в качестве базовых настроек технических средств, которые не требуют от человека их изменения), защита как структурный компонент (защита прав лежит в основе структуры технических средств и не требует их модификации), бескомпромиссность (защита прав не требует компромиссов между информационной свободой и информационной безопасность или же между информационной безопасностью личности и национальной безопасностью – их правовая охрана обеспечивается в равной степени), защита на протяжении жизненного цикла (защита прав обеспечивается от момента начала работы технических средств до момента их утилизации), доступность и открытость

ошибок, из-за которых может быть причинен вред как лицу, непосредственно использующему такие технические средства, так и иным лицам.

[240] Принципиальные положения данной концепции были включены в Дискуссионный документ Национального агентства по информационным технологиям и телекоммуникациям при Министерстве науки и информационных технологий Дании. Новые модели обеспечения цифровой безопасности. См.: New Digital Security Models. Discussion Paper. URL: http://blog.privacytrust.eu/public/Reports/NewDigitalSecurityModels.pdf (дата обращения – 27 апреля 2017 г.).

[241] Cavoukian A. Privacy by Design. The 7 Foundational Principles.

(информация о всех компонентах технического средства, обеспечивающих защиту прав, и принципах их работы является доступной и открытой), ориентированность на человека (при разработке технических средств права личности, которая будет их использовать, обеспечиваются в первую очередь).

Принципы безопасности за счет проектных решений, сформулированные голландским ученым С. Енгбергом, основаны на обеспечении безопасности для всех участников информационного взаимодействия (субъектов правоотношений), отделении информации, которой обладает человек, от его реальной личности, использовании косвенных (атрибутивных) учетных данных (идентификаторов)[242] и изоляции транзакций[243], переход от идентификации к проверке (валидации) личности. Их отличие от принципов неприкосновенности частной жизни за счет проектных решений заключается в том, что они не связаны с бескомпромиссностью. Наоборот, они основаны на компромиссе, который позволяет обеспечить баланс интересов всех субъектов правоотношений. Данная концепция не ориентирована на защиту исключительно или преимущественно прав личности, использующей технические средства.

Возложение на разработчиков технических средств обязанностей определяет отличие вышеуказанных концепций от традиционного подхода к обеспечению осуществления и защиты прав человека, при котором обязанности возлагаются на информационных посредников и иных обладателей конфиденциальной информации[244]. Такие производители технических средств,

---

[242] Такие учетные данные являются эквивалентными атрибутам учетных данных в физическом мире, таких как автобусные билеты, монеты, бюллетени и т.д. Они имеют встроенные механизмы безопасности, предотвращающие мошенничество, но позволяют их владельцу сохранить конфиденциальность своей личности при их использовании. См.: New Digital Security Models. Discussion Paper.

[243] Речь идет, в частности, об использовании для каждого информационного посредника различных идентификаторов «цифровой личности», с тем чтобы информация о личности, которой обладают различные информационные посредники, не могла быть связана между собой.

[244] Возложение обязанностей на разработчиков технических средств и повышение их ответственности становится все более актуальным с развитием технологии Интернета вещей (The Internet of Things), под которой понимается сеть физических объектов, содержащих встроенные технологии для связи, восприятия и взаимодействия друг с другом или внешней средой. (См.: Gartner IT Glossary. URL: http://www.gartner.com/it-glossary/internet-of-things/ (дата

как «Microsoft», «Hewlett-Packard», «Sun Microsystems» и «IBM» добровольно внедрили в своей деятельности принципы неприкосновенности частной жизни за счет проектных решений [245] . Однако добровольный характер концепции неприкосновенности частной жизни за счет проектных решений подвергается справедливой критике в зарубежной правовой литературе [246] в силу того, что лежащие в ее основе принципы слабо структурированы и не позволяют однозначно определить, соблюдаются ли разработчиками соответствующие обязанности. Так, несмотря на то что «Google» и «Facebook» заявили о том, что неприкосновенность частной жизни будет обеспечиваться изначально при разработке программного обеспечения, с их стороны неоднократно имели место факты разработки служб в сети Интернет, нарушающих право на неприкосновенность частной жизни, что было подтверждено Федеральной торговой комиссией США, регуляторами в Канаде, государствах – членах Европейского союза[247].

обращения – 27 апреля 2017 г.). Физическими объектами в данном случае являются разнообразные технические средства с возможностью подключения к сети Интернет. Поскольку разработчики таких устройств допускают ошибки в разработке их системы защиты, они становятся средством для нарушения права человека на неприкосновенность частной жизни. Нарушения могут быть выражены как в получении доступа к таким объектам и обрабатываемой ими информации о личности без согласия собственника устройства, так и в их неправомерном использовании для совершения DDOS-атак (выражается в направлении запросов к сайтам в сети Интернет с большого количества технических средств, подключенных к сети Интернет, в целях доведения таких сайтов до отказа в обслуживании). На сегодняшний день в отечественной и зарубежной правовой науке предлагаются различные подходы к решению данных проблем, которые, как правило, предполагают, наряду с обеспечением технических гарантий прав человека при создании и использовании соответствующих устройств, правовые гарантии, в том числе связанные с открытостью в части состава информации о личности, которая используется с помощью технических средств, наличием согласия обладателя устройства на участие в обработке информации о нем, и минимизации используемых данных о личности. См., напр.: Weber R.H. Internet of Things: Privacy Issues Revisited // Computer Law & Security Review. 2015. V. 31. P. 618–627; Архипов В.В., Наумов В.Б., Пчелинцев Г.А., Чирко Я.А. Открытая концепция регулирования Интернета вещей // Информационное право. 2016. № 2. С. 18–25.

[245] См.: The Role of Privacy by Design in Protecting Consumer Privacy. CTR. URL: https://www.cdt.org/policy/role-privacy-design-protecting-consumer-privacy (дата обращения – 27 апреля 2017 г.).

[246] Rubinstein I.S., Nathaniel G. Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents // Berkeley Technology Law Journal. 2013. V. 28. P. 1338–1340.

[247] Ibid.

Технические гарантии прав человека становятся необходимой составляющей обеспечения информационной безопасности в цифровой среде. Одновременно возрастает значение правовых гарантий прав человека. Так, существует тенденция признания принципов неприкосновенность частной жизни на основе проектных решений в национальном и наднациональном праве в качестве правовых. Федеральная торговая комиссия США указывает на обеспечение неприкосновенности частной жизни за счет проектных решений в качестве одной из рекомендуемых мер для защиты прав человека в онлайновой среде[248]. В свою очередь защите данных за счет проектных решений и по умолчанию (by default) посвящен отдельный раздел в Общих регуляциях по защите данных Европейского союза[249]. Для их подтверждения предполагается использовать механизм добровольной сертификации.

Как следует из предложений Европейской рабочей группы по вопросам персональных данных, хотя в условиях развития информационных и коммуникационных технологий необходимость совершенствования правовых принципов защиты неприкосновенности частной жизни действительно имеет место, существующие принципы продолжают сохранять свою актуальность[250]. Это означает, что данные принципы равным образом применяются и в новых технологических условиях, но требуют конкретизации, например в принципах «неприкосновенности частной жизни за счет проектных решений». В свою очередь Федеральная торговая комиссия США указывает на то, что наряду с созданием технических средств, соответствующих концепции

[248] FTC Report (March 2012). Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Business and Policy-makers. URL: https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf (дата обращения – 27 апреля 2017 г.).

[249] 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).

[250] Statement on Statement of the WP29 on the Impact of the Development of Big Data on the Protection of Individuals with Regard to the Processing of Their Personal Data in the EU. Article 29 Data Protection Working Party, WP221. September 16, 2014. URL: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp221_en.pdf (дата обращения – 2 апреля 2016 г.).

«неприкосновенности частной жизни за счет проектных решений», не менее важным является соблюдение принципов защиты права на неприкосновенность частной жизни, выработанных ОЭСР[251]. Без признания и соблюдения базовых правовых принципов обеспечение информационной безопасности на основе принципов «неприкосновенности частной жизни за счет проектных решений» не сможет выступать гарантией соответствующего права человека.

Правовые гарантии направлены на определение порядка применения соответствующих технических средств их обладателями, обеспечение контроля его соблюдения, а также ответственности за его нарушение. В правовом государстве создание и введение в действие технических норм, на основании которых осуществляется разработка соответствующих технических средств, не заменяет, но дополняет правовое регулирование. Технические средства могут выступать гарантией прав человека только при наличии правовых гарантий, предоставляющих механизмы правовой защиты от их произвольного использования. Такие правовые гарантии обеспечиваются государством в рамках осуществления им функции по обеспечению безопасности общества в целом. Следует согласиться с позицией В.С. Нерсесянца, который функцию государства по «обеспечению свободы, безопасности и собственности» [252] определяет как правовую функцию. Именно правовое начало составляет существо обеспечения информационной безопасности государством и выражено в форме его законодательной, исполнительной и судебной деятельности.

В то же время обеспечение информационной безопасности выступает одной из целей, для достижения которой устанавливаются ограничения прав человека. В этой связи в зарубежной правовой доктрине отмечается, что «принцип правового государства не сводится к защите человека от государственных притязаний, а преследует двойную цель: в равной степени ограничивать и обеспечивать

[251] Указывается прежде всего на принципы защиты информации, рациональных ограничений сбора данных, рациональных методов хранения и точности данных.

[252] Проблемы общей теории права и государства: Учебник для вузов. С. 632.

деятельность государства»[253]. В свою очередь в решении Конституционного Суда Российской Федерации указывается, что публичные интересы «оправдывают правовые ограничения прав и свобод, только если такие ограничения адекватны социально необходимому результату и, не будучи чрезмерными, необходимы и строго обусловлены этими публичными интересами; цели же одной только рациональной организации деятельности органов власти не могут служить основанием для ограничения прав и свобод»[254]. Такие ограничения определяют меру и границу свободы личности в постиндустриальном обществе – прежде всего информационной свободы[255]. Они также затрагиваются информационную безопасность, поскольку свобода и безопасность в совокупности находят выражение в правах человека.

Ограничения прав человека в целях обеспечения информационной безопасности призваны установить баланс между интересами личности и публичными интересами в информационной сфере. С одной стороны, публичные интересы заключаются в соблюдении запретов и ограничений на предоставление и распространение определенных видов информации, а с другой – в получении доступа к информации о частной жизни индивида, включая информацию о переписке, телефонных переговорах, почтовых, телеграфных и иных сообщениях, передаваемых по сетям электрической и почтовой связи. В первом случае ограничения устанавливаются в отношении свободы выражения мнения, свободы информации, права на доступ к информации и права на доступ к сети Интернет. Так, голландский ученый-юрист П. Хустинкс справедливо указывает на то, что

---

[253] Это позволяет «гарантировать достоинство человека, свободу, справедливость и правовую защищенность его как в отношениях с государственной властью, так и между индивидами». См.: Государственное право Германии. Сокращенный перевод немецкого семитомного издания. Т. 1 С. 54

[254] Постановление Конституционного Суда Российской Федерации от 7 июня 2012 г. № 14-П.

[255] В отечественной юридической литературе отмечается, что права человека «реализуются на основе их взаимного признания участниками социального общения, а значит, и ограничения свободы каждого свободой другого». Варламова Н.В. Интересы национальной безопасности как основание ограничений прав человека (по материалам практики Европейского суда по правам человека) / Труды Института государства и права Российской академии наук. № 1/2013. С. 164–165.

ограничение права на доступ к сети Интернет касается миллионов законопослушных пользователей сети Интернет, в том числе детей и подростков, последствия лишения доступа к сети Интернет, отключения человека от работы, культуры, электронного правительства и т.д. могут быть значительными[256]. Это утверждение верно и в отношении права на доступ к информации в сети Интернет. Во втором случае ограничения устанавливаются в отношение права на неприкосновенность частной жизни, включая такие его компоненты, как право на тайну корреспонденции, права субъектов персональных данных. Ограничение данных прав в свою очередь приводит к ограничению информационной безопасности их обладателей.

В правовом государстве создаются гарантии прав человека от избыточных и чрезмерных их ограничений, установленных в целях обеспечения информационной безопасности. В романо-германской правовой семье основной такой правовой гарантией служит правовой принцип соразмерности (пропорциональности[257]). Данный принцип развивается Европейским судом по правам человека, который способствует выработке единообразного подхода к его применению в практике национальных судов и таких международных судов, как например, Суд справедливости Европейского союза. Им сформулированы критерии, определяющие пределы ограничений прав человека. В соответствии с ними ограничения должны (1) быть установлены для достижения легитимной цели, (2) действительно способствовать ее достижению, (3) быть минимально необходимыми, (4) быть соразмерными (пропорциональными) в строгом смысле

[256] См.: Opinion of the European Data Protection Supervisor on the Current Negotiations by the European Union of an Anti-Counterfeiting Trade Agreement (ACTA) (2010/C 147/01). URL: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2010/10-02-22_ACTA_EN.pdf (дата обращения – 31 июля 2016 г.). Развитию мер правового регулирования, связанных с ограничением права человека на доступ к Интернету в связи с нарушением им прав интеллектуальной собственности, особое внимание уделено в докладе спецпредставителя ООН по вопросу о поощрении и защите права на свободу мнений и свободу выражения от 3 июня 2011 г. См.: Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue.

[257] От англ. proportionality.

(*stricto sencu*) [258]. В зарубежной правовой науке справедливо указывается на то, что в основе принципа соразмерности всегда лежит поиск баланса интересов, в противном случае он будет приводить к принятию формальных и нереалистичных решений[259]. В правовых системах общего права баланс при ограничении прав человека устанавливается путем взвешивания интересов с учетом принципов разумности (reasonableness), надлежащей правовой процедуры (due process) и других принципов, вырабатываемых высшими национальными судами [260]. Влияние принципа соразмерности в таких правовых системах проявляется в меньшей степени. Так, в юридической доктрине США преобладает точка зрения, согласно которой для признания принципа соразмерности в том же объеме, что и в европейской судебной практике, потребуется пересмотр как перечня конституционных прав, так и обоснований правомерности их ограничений[261]. Тем не менее в зарубежной юридической литературе также отмечается дальнейшее развитие подходов к обеспечению баланса интересов при ограничении прав человека в различных правовых семьях, при котором происходит их сближение[262].

Роль принципа соразмерности заключается в сопоставлении мер, которые предпринимаются органами государственной власти для обеспечения информационной безопасности, с правами человека. Например, Федеральный Конституционный суд Германии в деле о секретных магнитофонных записях[263]

---

[258] См., напр.: Barak A. Proportionality. Constitutional Rights and their Limitations. N.Y.: Cambridge University Press, 2012. xxvi, 611 p. P. 243–370.

[259] Cristoffersen J. Human Rights and Balancing: The Principle of Proportionality. P. 34.

[260] См., напр.: Associated Provincial Picture Houses Ltd. v. Wednesbury Corporation // URL: http://www.bailii.org/ew/cases/EWCA/Civ/1947/1.html (дата обращения – 1 декабря 2016 г.); Council of Civil Service Unions v. the United Kingdom // http://www.bailii.org/cgi-bin/format.cgi?doc=/eu/cases/ECHR/1987/34.html&query=(11603/85) (дата обращения – 1 декабря 2016 г.).

[261] См., напр.: Jackson V.C. Ambivalent Resistanceand Comparative Constitutionalism: Opening Up the Conversation on ‘Proportionality’, Rights and Federalism. University of Pennsylvania Journal of Constitutional Law. 1999. V. 1. P. 583, 616; Jackson V.C. Being Proportional about Proportionality. Constitutional Commentary. 2004. V. 21. P. 803, 842.

[262] См., напр.: Коэн-Элия М., Порат И. Американский метод взвешивания интересов и немецкий тест на пропорциональность: исторические корни // Сравнительное конституционное обозрение. 2011. № 3(82). С. 74–75.

[263] В данном деле Конституционный суд Германии рассмотрел вопрос о допустимости использования в качестве доказательства в суде записи, сделанной без ведома и согласия лица. Суд указал, что использование такой записи ограничивает право на «свободное развитие

отметил следующее: «Не вся сфера личной жизни подпадает под абсолютную защиту основных прав... Индивид как часть общества должен принимать такое государственное вмешательство, которое основано на преобладающих интересах общества при условии строгого соблюдения принципа соразмерности, пока оно не влияет на неприкосновенность частной жизни»[264]. Данный принцип положен в основу решений Конституционного Суда Российской Федерации, в которых дана оценка правомерности установления ограничений прав человека в целях защиты сведений, составляющих государственную тайну, как одного из направлений обеспечения информационной безопасности государства[265]. Так, по мнению суда, «любая информация должна быть доступна гражданину, если собранные документы и материалы затрагивают его права и свободы, а федеральный законодатель не предусматривает в качестве исключения из общего дозволения специальный правовой статус такой информации, не подлежащей распространению в соответствии с конституционными принципами, обосновывающими необходимость ограничений прав и свобод в сфере получения информации и их соразмерность целям защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства»[266]. В этой связи правовой принцип соразмерности является универсальным в том смысле, что он применим для проверки легитимности любых ограничений прав человека, установленных в целях обеспечения информационной безопасности.

Обеспечение информационной безопасности выступает легитимной целью установления ограничений прав человека, поскольку она может быть соотнесена с

личности», которое защищается статьей 2(1) Основного закона. BVerfGE 34, 238 // URL: http://www.servat.unibe.ch/dfr/bv034238.html#Rn002 (дата обращения – 1 декабря 2016 г.).

[264] Michalowski S., Woods L. German Constitutional Law: The Protection of Civil Liberties. Sudbury, MA: Dartmouth Publishing Co Ltd. 1999. 373 p. P. 127.

[265] См., напр.: Постановление Конституционного Суда Российской Федерации от 6 ноября 2014 г. № 27-П «По делу о проверке конституционности статьи 21 и статьи 21.1 Закона Российской Федерации «О государственной тайне» в связи с жалобой гражданина О.А. Лаптева» // СЗ РФ. 2014. № 46. Ст. 6425; Постановление Конституционного Суда Российской Федерации от 7 июня 2012 г. № 14-П.

[266] Постановление Конституционного Суда Российской Федерации от 6 ноября 2014 № 27-П.

нормами международного права. В соответствии с ними установление ограничений прав человека допускается для достижения таких целей, как, например, обеспечение национальной и государственной безопасности, охрана общественного порядка, здоровья, нравственности населения, прав и свобод отдельных индивидов в информационной сфере[267]. Легитимность данной цели определяется не столько буквальным ее соответствием целям, предусмотренным международными договорами, сколько их толкованием в конкретной национальной юрисдикции [268] . В России обеспечение информационной безопасности как цель ограничения прав человека рассматривается в контексте положений Конституции Российской Федерации, прежде всего части 3 статьи 55, согласно которой такие ограничения допускаются в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

Минимальная необходимость ограничений прав человека, установленных с целью обеспечения информационной безопасности, основана на достижении данной цели путем наименьшего из доступных ограничений прав [269] . Несоответствующим данному критерию Европейским судом по правам человека было, в частности, признано ограничение права на неприкосновенность частной жизни в форме бессрочного хранения органами исполнительной власти в электронной базе данных отпечатков пальцев и образцов ДНК лиц, обвиненных в совершении преступления, но в последующем оправданных, либо лиц, с которых

---

[267] См., напр.: статья 29 Всеобщей декларацией прав человека 1948 г. (Российская газета, 10.12.1998.), статья 19 Международного пакта о гражданских и политических правах 1966 г., статьи 8 и 10 Конвенции 1950 г.

[268] Так, ограничение права на распространение в сети Интернет информации, содержащей нацистскую символику, которое признается легитимным в Германии и Франции, будет являться нелегитимным в Великобритании или США (если не сопряжено с запугиванием и намеренным причинением вреда).

[269] См., напр., позицию Европейского суда по правам человека в делах Вебер и Саравия (Weber and Saravia) против Германии. Решение Европейского суда по правам человека от 29 июня 2006 г. (Жалоба № 54934/00) // Бюллетень Европейского суда по правам человека. 2007. № 2.; Либерти и другие (Liberty and Others) против Соединенного Королевства. Постановление Европейского суда по правам человека от 1 июля 2008 г. (Жалоба № 58234/00) // Бюллетень Европейского суда по правам человека. 2008. № 12.

такие обвинения были сняты[270]. Для соблюдения данного критерия ограничение прав человека по срокам его установления и объему налагаемых обременений не должно выходить за пределы, при которых оно становится избыточным и чрезмерным, то есть неоптимальным по сравнению с иными доступными способами достижения той же цели. Минимальная необходимость ограничения может быть обеспечена если существуют альтернативные способы релевантного достижения одной и той же цели, при этом выбирается способ, налагающий наименьшие ограничения. В этой связи ограничения прав человека судом в рамках состязательного процесса в большей степени соответствуют данному критерию, нежели их ограничение в рамках административного процесса.

Так, Конституционный совет Франции признал неконституционным основную часть Закона HADOPI[271], который позволял уполномоченному органу исполнительной власти без решения суда ограничивать право на доступ к сети Интернет пользователей – физических лиц, уличенных в нарушении авторских прав в сети Интернет. По мнению совета, подобные положения приводят к нарушению презумпции невиновности, принципа разделения властей и свободы выражения[272]. С учетом того, что в своем решении Конституционный совет Франции отнес право на доступ к сети Интернет к числу основных прав, его ограничение в административном порядке в отсутствии состязательного судебного процесса свидетельствовало о его нелегитимном характере. В то же время совет признал соответствующей Конституции Французской Республики измененную версию данного закона, предусматривающую судебную процедуру принятия решения об ограничении права на доступ к сети Интернет[273].

---

[270] S. и Марпер (S. and Marper) против Соединенного Королевства. Постановление Европейского Суда по правам человека от 4 декабря 2008 г. (Жалобы № 30562/04, 30566/04) // Бюллетень Европейского Суда по правам человека. 2009. № 4.

[271] Название закона совпадает с названием французского агентства по защите авторских прав HADOPI (Haute Autorité Pour la Diffusion des Œuvres et la Protection des Droits sur Internet). См.: URL: http://www.hadopi.fr/ (дата обращения – 31 июля 2016 г.).

[272] См.: French Constitutional Council: Decision № 2009-580 of June 10th 2009 – Act Furthering the Diffusion and Protection of Creation on the Internet.

[273] См.: French Constitutional Council: Décision № 2009-590 DC of October 22 2009 – Loi Relative à la Protection Pénale de la Propriété Littéraire et Artistique sur Internet URL:

Судебная проверка соразмерности ограничений прав человека также позволяет выявить так называемые нерелевантные (или нерациональные) ограничения при оценке их соответствия той цели, для достижения которой они были установлены. Так, вывод о нерелевантности ограничения прав человека, заключающихся в сплошной фильтрации и блокировании обмена сообщениями в файлообменных сетях, содержится в различных решениях Суда справедливости Европейского союза[274]. Такого рода ограничения, установленные в целях защиты авторских прав, признавались судом нарушающими свободу выражения мнения и права на неприкосновенность частной жизни, поскольку затрагивали обмен сообщениями, не связанными с использованием объектов авторских прав. Это означает, что для обеспечения релевантности недостаточно частичного соответствия ограничения прав человека цели его установления. Ограничение является нерелевантным, если между каждым случаем его реализации и целью его установления отсутствует рациональная связь, при которой ограничение с неизбежностью ведет к результату, соответствующему достижению заданной цели. На это, в частности, указывается в решении Европейского суда по правам человека по делу «Ахмет Йилдырым против Турции», в котором было признано, что ограничение свободы выражения мнения в форме блокирования доступа к сайту в сети Интернет на основании превентивных мер в рамках уголовного дела, которое не имеет никакого отношения к такому сайту, вступает в противоречие с соответствующим положением Конвенции 1950 г. [275] Нерелевантность ограничения в данном случае обусловлена техническими особенностями способа его реализации. Блокирование сайта в сети Интернет информационным посредником по решению суда или органа исполнительной власти на основе

---

http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank_mm/decisions/2009590dc/2009590dc.pdf (дата обращения – 31 июля 2016 г.).

[274] Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) (C-70/10). Judgment of the Court of Justice (Grand Chamber) of 24 November 2011. URL: http://curia.europa.eu/juris/liste.jsf?num=c-70/10 (дата обращения – 31 июля 2016 г.); Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV (C-360/10). Judgment of the Court of Justice (Third Chamber) of 16 February 2012. URL: http://curia.europa.eu/juris/liste.jsf?num=C-360%2F10 (дата обращения – 31 июля 2016 г.).

[275] Ахмет Йилдырым против Турции. Постановление Европейского суда от 18 декабря 2012 г.

сведений об IP-адресе[276] такого сайта может приводить к одновременному блокированию и других сайтов, которые привязаны к этому же IP-адресу[277]. Таким образом, соответствие ограничения прав человека при обеспечении информационной безопасности в сети Интернет цели его установления во многом зависит от особенностей его реализации, из-за которых даже при условии легитимности такой цели ограничение может стать нелегитимным.

При обеспечении информационной безопасности правовое регулирование дополняется саморегулированием. Оно создает условия для разрешения возникающих социальных конфликтов с минимальным участием органов государственной власти, вмешательство которых в основном ограничивается вопросами привлечения к ответственности за совершенные правонарушения. В этой связи саморегулирование при обеспечении информационной безопасности осуществляется в соответствии с принципом субсидиарности[278], который заключается в том, что регулирующее воздействие саморегулирования носит дополнительный характер по отношению к правовому регулированию. В условиях цифровой среды значение саморегулирования при обеспечении информационной безопасности повышается. Примером являются различные горячие линии, создаваемые провайдерами доступа к сети Интернет, в том числе в рамках соглашений между органами государственной власти и такими провайдерами, кодексы поведения отраслевых ассоциаций и иные формы партнерства между государством и негосударственными организациями, на основе которых информационные посредники осуществляют блокирование и фильтрацию информации[279], тем самым ограничивая свободу выражения мнения и право на доступ к информации.

---

[276] IP-адрес (адрес интернет-протокола, от англ. Internet Protocol Address) - уникальный адрес узла в вычислительной сети, основанной на протоколе IP.

[277] В результате происходит, так называемая, «сверхблокировка» («overblocking»).

[278] См., напр.: Петров Д.А. Принципы саморегулирования: критерии систематизации и виды // Академический юридический журнал. 2012. № 2 (48). С. 44–48.

[279] См., напр.: Tropina T., Callanan C. Self- and Co-regulation in Cybercrime, Cybersecurity and National Security // Springer International Publishing. 2015. 100 p.

Так, в отдельных государствах в случае выявления нарушений физическими лицами авторских прав в файлообменных сетях применяются ограничения их права на доступ к сети Интернет, основанные на договорных обязательствах между индивидами и провайдерами доступа к сети Интернет, а также такими провайдерами и правообладателями (их ассоциациями). На развитие данной практики направлено законодательство таких государств, как, например, США и Тайвань. В данных государствах провайдеры доступа к сети Интернет освобождаются от ответственности за нарушение авторских прав, в случае если ими принимаются меры по отключению от сети Интернет физических лиц, которые совершили многократные правонарушения. В США это способствовало заключению между ведущими провайдерами доступа к сети Интернет и медиахолдингами соглашения[280], в соответствии с которым была установлена шестиэтапная процедура отключения от сети Интернет, а на Тайване, напротив, подобные меры к развитию саморегулирования так и не привели[281]. Это подтверждает, что саморегулирование не является универсальным механизмом для обеспечения информационной безопасности, его реализация зависит от правовой культуры и условий, в которых развивается институт саморегулирования в тех или иных странах.

В случае если права человека ограничиваются в рамках саморегулирования возникает вопрос о легитимности таких ограничений[282] в части их соразмерности в строгом смысле. При проверке ограничения прав человека на соответствие данному критерию определяется наличие баланса между общественной пользой, достигаемой за счет установления тех или иных ограничений прав человека, и вредом, который причиняется обладателям соответствующих прав. Тогда как в

---

[280] См.: Center for Copyright Information. Resources & FAQ. URL: http://www.copyrightinformation.org/wp-content/uploads/2014/05/Phase-One-And_Beyond.pdf (дата обращения – 31 июля 2016 г.). Действие данной программы было завершено в январе 2017 г.

[281] В то же время установление данных мер стало основанием для исключения Тайвани из специального наблюдательного перечня, издаваемого Торговым представительством США. См.: USTR Announces Conclusion of the Special 301 Out-of-Cycle Review for Taiwan. URL: https://ustr.gov/about-us/policy-offices/press-office/press-releases/2009/january/ustr-announces-conclusion-special-301-out-cycle-re (дата обращения – 31 июля 2016 г.).

[282] См., напр.: Jørgensen R.F., Pedersen A.M. Online Service Providers as Human Rights Arbiters. P. 187.

других критериях соразмерности анализируется цель ограничения и способы ее достижения, в данном случае предметом анализа является отношение между правами человека и соответствующей целью. Оно выводится из соотношения ценностей и принципов, которые лежат в основе прав человека и целей их ограничения. Правила балансировки таких ценностей и принципов имеют прежде всего нормативный характер, то есть следуют из норм права (например, из требований о том, что ограничения признаются допустимыми, если они предусмотрены законом). Лишь в случае отсутствия таких норм исследуется социальное значение соответствующих ценностей и принципов.

Например, в 2008 г. в сети Интернет был опубликован перечень сайтов, заблокированных провайдерами доступа к сети Интернет по предписанию полиции Дании, которая совместно с некоммерческой организацией «Спаси ребенка» выявляла сайты с детской порнографией[283]. Из содержания данного перечня следовало, что ряд сайтов не имел никакого отношения к детской порнографии, что свидетельствовало об избыточных ограничениях свободы выражения мнения и права на доступ к информации. В этой связи следует согласиться с позицией профессора факультета права университета Бильги (Стамбул) Я. Акдениза, согласно которой «система блокирования доступа, основанная исключительно на саморегулировании или «соглашениях добровольного блокирования», представляет риск нелегитимного вмешательства в осуществление фундаментальных прав»[284]. Ограничение прав человека информационным посредником будет легитимным только при наличии закона, создающего для этого правовые основания и обеспечивающего правовые гарантии от избыточных и чрезмерных ограничений.

---

[283] См.: Talk:Denmark: 3863 Sites on Censorship List, Feb 2008. URL: https://wikileaks.org/wiki/Talk:Denmark:_3863_sites_on_censorship_list%2C_Feb_2008 (дата обращения – 31 июля 2016 г.).

[284] Акдениз Я. Отчет. Свобода выражения мнения в Интернете. Исследование правовых норм и практик, связанных со свободой выражения мнения, свободным потоком информации и плюрализмом СМИ в Интернете в государствах – участниках ОБСЕ. URL: http://www.osce.org/ru/fom/89063?download=true (дата обращения – 31 июля 2016 г.).

Правовые ограничения прав человека в цифровой среде, то есть формально определенные и закрепленные в нормативных правовых актах, дополняются фактическими (материальными) ограничениями. Они выражаются в обязанностях по осуществлению действий технического характера, которые возлагаются на разработчиков технических средств и информационных посредников. Такие обязанности устанавливаются либо техническими нормами, либо правоприменительными актами. Технический характер таких ограничений прав человека обусловлен тем, что сфера осуществления прав человека с использованием сети Интернет изначально ограничена функциональными возможностями технических средств[285], с помощью которых человек получает доступ к киберпространству или пользуется в нем теми или иными социальными благами. Изменение или использование данных функциональных возможностей приводит к расширению сферы осуществления или ограничению прав человека.

Возлагая на разработчиков технических средств и информационных посредников такие обязанности, органы государственной власти фактически (материально) ограничивают права индивидов, которые используют соответствующие технические средства или получают услуги информационных посредников. На основе таких обязанностей осуществляется принудительное исполнение решений органов государственной власти даже в случаях, когда индивид, права которого ограничиваются, находится за пределами национальной юрисдикции. Для описания данной разновидности ограничений прав человека американский ученый-юрист Дж. Бойл [286] использует термин «материальное

[285] Как отмечает американский ученый-юрист Л. Лессиг, в киберпространстве одной из форм регулирования общественных отношений становятся программный код и технологическая инфраструктура сети Интернета (См.: Lessig L. Code: Version 2.0.). Программное обеспечение и другие технические средства ограничивают возможные способы осуществления прав человека, тем самым определяя пределы соответствующих прав в цифровой среде.

[286] См.: Boyle J. Foucault In Cyberspace: Surveillance, Sovereignty, and Hard-Wired Censors. 1998. URL: https://law.duke.edu/boylesite/foucault.htm (дата обращения – 20 апреля 2016 г.). Данный термин он заимствовал из доктрины французского философа М. Фуко; Фуко М. Безопасность, территория, население. Курс лекций, прочитанных в Колледж де Франс в 1977–1978 уч. году / пер. с фр. Ю.Ю. Быстрова, Н.В. Суслова, А.В. Шестакова. СПб.: Наука, 2011. 544 с.

принуждение». Материальное принуждение индивида к определенному поведению достигается за счет создания условий, при которых иное его поведение становится невозможным.

В правовом государстве допустимо только такое материальное принуждение, которое одновременно является правовым, то есть имеющим правовые основания и процедурные формы осуществления, регламентированные правом. Это, в частности, означает, что связанные с материальным принуждением ограничения прав человека должны быть сформулированы в национальном законодательстве таким образом, чтобы в ясной и недвусмысленной форме определять, какое право человека и в каком объеме ограничено. При соблюдении данных условий материальное принуждение не создает избыточных ограничений прав человека по отношению к тем, которые предусмотрены законом, в противном случае оно представляет собой акт государственного насилия. К подобным актам, в частности, относится, так называемый, шатдаун [287] или временный разрыв соединения с сетью Интернет на определенной территории или для определенной социальной группы, осуществляемый операторами связи по требованию органов исполнительной власти. В результате шатдауна осуществление прав человека с использованием сети Интернет в целом становится временно невозможным, то есть происходит умаление прав человека, искажение самого их существа, что позволяет сделать вывод об избыточном характере таких ограничений.

Материальное принуждение становится одним из способов обеспечения доступа государственных органов к информации о личности и, тем самым, выступает в качестве ограничения права на неприкосновенность частной жизни в цифровой среде. Так, компания «Google» указывает на то, что количество поступивших к ней запросов данных об индивидах, которым она оказывает

[287] В 2015–2016 гг. шатдаун использовался в таких государствах, как Демократическая Республика Конго, Нигер, Йемен, Алжир, Ирак, Турция, Бразилия, Индия, Эквадор, Сирия, Пакистан, Вьетнам, и в некоторых других государствах, в том числе в целях предотвращения массовых протестов. При этом в 2016 г. было зафиксировано более 50 шатдаунов, что в 3 раза превышает показатель 2015 г. См.: #KeepItOn – Access Now. URL: https://www.accessnow.org/keepiton/ (дата обращения – 1 декабря 2016 г.).

услуги, от органов исполнительной власти и судебных инстанций разных стран увеличилось с 26 тыс. в 2009 г. до 76 тыс. в 2015 г.[288] Не все информационные посредники предоставляют государственным органам соответствующую информацию по запросам, особенно информационное взаимодействие затруднено с информационными посредниками, которые расположены в других национальных юрисдикциях. Получая доступ к такой информации, государственные органы не всегда имеют возможность установить ее содержание из-за применяемых индивидами средств шифрования. Следствием этого является выработка мер материального принуждения, в результате применения которых обеспечивается доступ государственных органов к соответствующей информации независимо от воли информационных посредников или же индивида и подведение под такое принуждение правовых оснований.

Так, во Франции с принятием закона Loppsi-2[289] были созданы правовые основания для ограничения права на неприкосновенность частной жизни путем предоставления полиции полномочий по согласованию с прокуратурой при расследовании тяжких преступлений внедрять в компьютеры физических лиц троянские программы, так называемые, кейлоггеры. Для реализации данного ограничения на практике должны существовать определенные условия, включая непосредственно доступ к компьютерам. В этой связи также получает развитие[290] форма материального принуждения, связанная с возложением обязанностей на разработчиков технических средств по обеспечению на уровне операционных систем и программных продуктов доступа органов исполнительной власти к информации, которая хранится на технических средствах, принадлежащих физическим лицам, или обрабатывается с их помощью.

---

[288] Отчет Google о доступности сервисов и данных. URL: https://www.google.com/transparencyreport/userdatarequests/ (дата обращения – 31 июля 2016 г.).

[289] LOI n° 2011-267 du 14 mars 2011 d'Orientation et de Programmation pour la Performance de la Sécurité Intérieur.

[290] По сообщению агентства Рейтер компания Yahoo в 2015 году внедрила в свои почтовые сервисы программу, которая по требованию Агентства национальной безопасности США осуществляла сканирование электронных писем своих пользователей. См.: Yahoo Scanning Order Unlikely to be Made Public: Sources. Reuters. URL: http://www.reuters.com/article/us-yahoo-nsa-congress-idUSKCN12P2FL (дата обращения – 31 июля 2016 г.).

Правомерность возложения подобных обязанностей на разработчиков технических средств неоднократно становилась предметом судебной проверки в спорах между ФБР и компанией «Apple». Так, в 2015 г. в Окружном суде Восточного округа Нью-Йорка рассматривалась правомерность запроса ФБР о разблокировке «Apple» телефона iPhone с операционной системой iOS7 в целях поиска сообщников обвиняемого, который признал свою вину[291]. Свое требование ФБР основывало на Законе США обо всех исковых заявлениях и постановлениях судов 1789 г.[292], устанавливающем, что суды США имеют право выпускать любые приказы, способствующие установлению правосудия, если эти приказы согласуются с законом и правоприменительной практикой. Разумность подобных требований в данном случае проверялась исходя из трех факторов: связь компании «Apple» с преступным поведением и государственным расследованием; обременение, возлагаемое на компанию «Apple» в результате издания судебного приказа; и необходимости возложения такого обременения на компанию «Apple». Суд, изучив обстоятельства дела и доводы сторон, пришел к выводу, что ни один из этих факторов не оправдывал наложение на компанию «Apple» обязательства оказывать помощь в расследовании против его воли. В данном случае компания «Apple» никак не препятствовала проведению расследования и, например, самостоятельному обходу блокировки телефона ФБР.

Еще один спор между ФБР и компанией «Apple» должен был стать предметом рассмотрения в Окружном суде США по Центральному судебному округу штата Калифорния. В данном случае ФБР потребовало в мировом суде от «Apple» создать специальную версию iOS, установка которой на заблокированный iPhone позволила бы получить доступ к зашифрованной на нем информации[293]. Свое требование ФБР также основывало на Законе США обо всех

---

[291] In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by the Court. 1:15-mc-1902 (JO). URL: https://www.documentcloud.org/documents/2728314-Orenstein-Order.html (дата обращения – 1 декабря 2016 г.).

[292] All Writs Act 1789. 28 U.S.C. §1651. URL: https://www.law.cornell.edu/uscode/text/28/1651 (дата обращения – 1 декабря 2016 г.).

[293] Данный запрос был обусловлен необходимостью доступа к информации, содержащейся на iPhone, который принадлежал одному из террористов, совершивших

исковых заявлениях и постановлениях судов. Мировой суд удовлетворил требование ФБР и выпустил судебный приказ, который компания «Apple» обжаловала в окружном суде, полагая, что ФБР использовал расширительное толкование данного закона и для обоснования предъявляемых им требований необходимо принятие отдельного закона в Конгрессе [294]. За один день до судебного заседания ФБР отозвало свое требование, заявив, что смогло разблокировать iPhone с помощью третьих лиц. Похожий случай произошел в Бруклине, когда мировой суд установил, что Закон США обо всех исковых заявлениях и постановлениях судов не может быть использован для возложения на «Apple» обязанности по разблокировке iPhone. ФБР обжаловало это решение в окружном суде, но в последующем прекратило участие в данном деле, поскольку нашло правильный пароль к iPhone.

Подобные обязанности, возлагаемые на разработчиков технических средств органами исполнительной власти или по их требованию судами, фактически создают условия для ограничения права на неприкосновенность частной жизни неопределенного круга лиц, то есть их последствия простираются далеко за рамки расследования конкретного уголовного дела. Несмотря на это, рассмотрение возникающих при этом юридических споров в США происходит не столько с точки зрения исключения избыточных и чрезмерных ограничений права на неприкосновенность частной жизни, сколько с точки зрения правомерности возложения обязанностей на юридических лиц – разработчиков технических средств. В результате происходит подмена прав человека, которые в действительности подвергаются ограничениям, обязанностями юридических лиц.

Европейский суд по правам человека и Суд справедливости Европейского союза подходят к вопросам легитимности материального принуждения на основе правового принципа соразмерности, то есть анализируют легитимность не только

террористический акт в Сан-Бернардино в декабре 2015 г. Телефон оказался заблокирован четырехзначным паролем и после 10 неудачных попыток должен был ликвидировать содержавшуюся на нем информацию.

[294] В этот же период в Конгрессе рассматривался законопроект, в соответствии с которым допускалось возложение таких обязанностей на разработчиков, но который так и не был принят.

и не столько возложения обязанностей на информационных посредников и разработчиков технических средств, сколько легитимность связанных с ними ограничений прав человека в онлайновой среде. Так, по мнению Европейского суда по правам человека, высказанному в деле «Класс и другие против Германии», «право ведения тайного наблюдения за гражданами, которое характерно для полицейского государства, терпимо в соответствии с Конвенцией только тогда, когда оно строго необходимо для сохранения демократических институтов» [295]. Государства «не могут во имя борьбы против шпионажа и терроризма предпринимать любые действия, которые они считают подходящими»[296].

Различие в подходах, принятых в Европейском союзе и США, повлияло на принятие Судом справедливости Европейского союза решения о признании недействительным соглашения между США и Европейским союзом о «безопасной гавани» в области обмена персональными данными из-за опасений того, что американская разведка может получить доступ к соответствующим данным [297]. Действующая в Европейском союзе Директива о защите данных 95/46/ЕС, также как вступающие в силу в 2018 г. Общие регуляции по защите данных, запрещают передачу персональных граждан государств – членов Европейского союза, независимо от того, являются они или нет чувствительными, в государства, не входящие в Европейское экономическое сообщество. Исключением является «передача персональных данных в третьи страны, которые обеспечивают адекватный уровень защиты». До недавнего времени признавалось, что операторами персональных данных из США такая защита обеспечивается, если они соответствуют определенным принципам и требованиям, которые

[295] Класс и другие против Федеративной Республики Германии. Решение Европейского Суда по правам человека от 6 сентября 1978 г. (Жалоба № 5029/71) Европейский суд по правам человека. Избранные решения. Т. 1. М.: Норма, 2000. С. 168–186.

[296] Там же.

[297] Maximillian Schrems v. Data Protection Commissioner, C-362/14 (CJEU October 6, 2015), http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf (дата обращения – 1 апреля 2016 г.). На принятие данного решения повлияло раскрытие Э.Сноуденом информации о программе слежения PRISM в США, которая с точки зрения Суда справедливости Европейского союза привела к несоразмерным ограничениям права на неприкосновенность частной жизни граждан государств – членов Европейского союза.

получили название «схема безопасной гавани»[298]. Соответствующее соглашение между США и Европейским союзом регулировало стандарты трансатлантического обмена данными таких компаний, как «Google», «Microsoft» и «Facebook». Однако в связи с раскрытием информации о том, что государственные органы США имели общий доступ к персональным данным граждан государств-членов Европейского союза, 6 октября 2015 г. Суд справедливости Европейского союза признал недействительным решение Европейской комиссии о безопасной гавани. По мнению суда, «закон, позволяющий государственным органам иметь общий доступ к содержимому электронных сообщений должен рассматриваться как нарушение фундаментального права на уважение частной и семейной жизни»[299]. В настоящее время вместо схемы безопасной гавани выработано совместное соглашение Европейского союза и США о «Щите неприкосновенности частной жизни»[300], которым повышаются требования к операторам персональных данных. Новое соглашение включает в себя обязательства США, заключающиеся в том, что государственные органы США будут иметь доступ к персональным данным, переданным в соответствии с новой схемой, только если законодательством США будут предусмотрены четкие условия, ограничения и контроль, предотвращающие общий доступ к любым электронным коммуникациям. В этой связи новое соглашение не запрещает передачу персональных данных граждан государств – членов Европейского союза операторам из США, но признает ее допустимой при соблюдении определенных условий.

Подход к вопросам легитимности материального принуждения в Российской Федерации занимает промежуточное положение между

---

[298] U.S.-EU Safe Harbor Framework Documents URL: http://webarchive.loc.gov/all/20150405033356/http%3A//export%2Egov/safeharbor/eu/eg_main_018493%2Easp (дата обращения – 1 июня 2016 г.).

[299] Case C-362/14 Maximillian Schrems v Data Protection Commissioner: The Court of Justice Declares that the Commission's US Safe Harbour Decision is Invalid.

[300] Article 29 Working Party Statement on the Decision of the European Commission on the EU-U.S. Privacy Shield. URL: http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/20160726_wp29_wp_statement_eu_us_privacy_shield_en.pdf (дата обращения – 1 июня 2016 г.).

приведенными выше подходами США и Европейского союза. Этот подход, в частности, выражается в обязанности оператора персональных данных, осуществляющего сбор персональных данных, в том числе посредством сети Интернет, обеспечивать запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации[301]. Законодатель определяет требования к местонахождению баз данных, в которых содержатся персональные данные, независимо от воли субъектов персональных данных. Нахождение соответствующих баз данных на территории Российской Федерации, с одной стороны, упрощает контроль и надзор за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных и одновременно доступ к содержащимся в базах данных информации для органов исполнительной власти, но с другой – приводит к ограничению прав субъектов персональных данных, которые при определении способа их обработки уже лишены возможности самостоятельно определять территорию его реализации. Данные требования развиваются в так называемом пакете Яровой – Озерова[302], которым устанавливаются новые обязанности информационных посредников – организаторов распространения информации в сети Интернет по хранению электронных сообщений пользователей сети Интернет и, в случае использования дополнительного кодирования электронных сообщений или предоставления такой возможности пользователям,

[301] Федеральный закон от 21 июля 2014 г. № 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях» // СЗ РФ. 2014. № 30. Ст. 4243.

[302] Федеральный закон от 6 июля 2016 г. № 374-ФЗ «О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» // СЗ РФ. 2016. № 28. Ст. 4558. Федеральный закон от 6 июля 2016 г. № 375-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» // СЗ РФ. 2016. № 28. Ст. 4559.

представлению в ФСБ России [303] информации, необходимой для их декодирования. Хранение таких сообщений, так же как предоставление информации, необходимой для их декодирования, осуществляется независимо от наличия признаков совершения противоправного деяния, что отличается от подходов, принятых в США и Европейском союзе.

Так, решением Суда справедливости Европейского союза Директива 2006/24/ЕС о хранении метаданных о пользователях (была принята после террористических актов в Мадриде и Лондоне в 2006 г.) была признана несоответствующей Хартии Европейского союза об основных правах и в этой связи недействительной. Суд в своем решении отметил: «Тот факт, что данные были сохранены и в дальнейшем использовались без сообщения об этом абоненту или зарегистрированному пользователю, мог породить в сознании заинтересованных лиц ощущение, что их частная жизнь была предметом постоянного наблюдения… Требуя осуществлять сбор и хранение этих данных, а также предоставляя соответствующим органам власти доступ к ним, Директива крайне серьезным образом вмешивается в сферу фундаментальных прав человека и нарушает право на уважение личной жизни и защиту персональных данных»[304]. Возложение на информационных посредников соответствующих обязанностей обеспечивает дополнительные условия для предотвращения, пресечения и расследования преступлений, но в то же время создает риски для необоснованного вмешательства в частную жизнь.

---

[303] См.: Приказ ФСБ России от 19 июля 2016 г. № 432 «Об утверждении Порядка представления организаторами распространения информации в информационно-телекоммуникационной сети «Интернет» в Федеральную службу безопасности Российской Федерации информации, необходимой для декодирования принимаемых, передаваемых, доставляемых и (или) обрабатываемых электронных сообщений пользователей информационно-телекоммуникационной сети «Интернет» // Бюллетень нормативных актов федеральных органов исполнительной власти. № 36. 2016.

[304] The Court of Justice Declares the Data Retention Directive to be Invalid. URL: https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf (дата последнего обращения – 1 июня 2016 г.).

Ранее[305] отечественным законодателем на организаторов распространения информации в сети Интернет была возложена обязанность по реализации требований к оборудованию и программно-техническим средствам, используемым указанным организатором в эксплуатируемых им информационных системах, для проведения этими органами в случаях, установленных федеральными законами, мероприятий в целях реализации возложенных на них задач, а также обязанность принимать меры по недопущению раскрытия организационных и тактических приемов проведения данных мероприятий[306]. Вместе с тем отечественным законодателем также были уточнены условия проведения оперативно-розыскных мероприятий [307] , в соответствии с которыми получение компьютерной информации, как одно из оперативно-розыскных мероприятий в случае ограничения конституционных прав человека и гражданина, допускается только на основании судебного решения. В результате, хотя на информационных посредников и возлагаются различные обязанности, исполнение которых упрощает органам исполнительной власти доступ к персональным данным и приводит к ограничению права на неприкосновенность частной жизни, необходимым условием для проведения оперативно-розыскных мероприятий и осуществления доступа к такой информации остается наличие судебного решения.

Легитимность обеспечения информационной безопасности как цели осуществления материального принуждения у наднациональных судов в целом не вызывает сомнения. Однако для признания легитимности самого материального принуждения недостаточно подвести правовые основания под соответствующие

---

[305] Федеральный закон от 5 мая 2014 г. № 97-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и отдельные законодательные акты Российской Федерации по вопросам упорядочения обмена информацией с использованием информационно-телекоммуникационных сетей».

[306] Требований к соответствующему оборудованию и программно-техническим средствам до настоящего времени не установлено. Установление данных требований возложено на Минкомсвязи России по согласованию с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации.

[307] Федеральный закон от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» // СЗ РФ.1995. № 33. Ст. 3349.

обязанности разработчиков технических средств и информационных посредников. Условием его легитимности также является создание правовых гарантий прав человека, на которые накладываются ограничения в результате исполнения таких обязанностей.

Например, Европейский суд по правам человека в деле «Роман Захаров против Российской Федерации»[308], в котором была рассмотрена легитимность ограничений прав человека в связи с использованием в России системы технических средств для обеспечения функций оперативно-розыскных мероприятий в сетях электросвязи (так называемый СОРМ-2), отметил, что ограничение права на неприкосновенность частной жизни (в данном случае прослушивание мобильных телефонов) преследует законные цели, такие как предотвращение преступлений и защита национальной безопасности, общественного порядка и экономического благосостояния страны. В то же время для установления соответствующих ограничений необходимы адекватные и эффективные правовые гарантии данного права в национальном законодательстве, в числе которых четкое определение ситуаций, когда органы исполнительной власти имеют право использовать негласные оперативно-розыскные мероприятия, и ситуации, когда данные мероприятия должны быть прекращены, а собранные данные уничтожены, а также детальная процедура выдачи разрешения на прослушивание, обеспечение надзора за законностью прослушки и эффективные средства обжалования. Отсутствие данных гарантий в отечественном законодательстве при использовании системы СОРМ-2 послужило признанию судом нарушения статьи 8 Конвенции 1950 г. Реализация данных гарантий в полном объеме является сложной и высокозатратной, при этом снижает скорость принятия решения об установления скрытого наблюдения. В то же время – «из нарушения права не рождается право». Развитие правовых гарантий прав человека, выраженных в детализации материальных и

[308] Постановление Европейского суда по правам человека от 4 декабря 2015 г. Дело «Роман Захаров (Roman Zakharov) против Российской Федерации» (Жалоба № 47143/06) (Большая Палата Европейского Суда) // Бюллетень Европейского суда по правам человека. 2016. № 6(168).

процессуальных правовых норм, на основании которых осуществляются ограничения прав человека, является неизбежной тенденцией в правовых государствах.

Таким образом, обеспечение информационной безопасности является одной из гарантий прав человека в информационной сфере, которая неразрывно связана с другими видами гарантий и в них находит свое выражение. В цифровой среде возрастает роль технических гарантий, выраженных в технических средствах и технических нормах. В правовом государстве создание и введение в действие технических норм, на основании которых осуществляется разработка соответствующих технических средств, не заменяет, но дополняет правовое регулирование. Технические средства могут выступать гарантией прав человека только при наличии правовых гарантий, предоставляющих механизмы правовой защиты от их произвольного использования. В то же время обеспечение информационной безопасности выступает основанием для ограничения прав человека. В правовом государстве создаются правовые гарантии прав человека от избыточных и чрезмерных их ограничений в целях обеспечения информационной безопасности, которые выражаются в правовых принципах, таких как принцип соразмерности. Наряду с правовыми ограничениями прав человека при обеспечении информационной безопасности происходит развитие фактических (материальных) их ограничений, которые выражены в материальном принуждении. Оно заключается в возложении на информационных посредников и разработчиков технических средств обязанностей, исполнение которых влияет на пределы прав человека. Для легитимности материального принуждения не достаточно юридического закрепления обязанностей разработчиков технических средств и информационных посредников. Его легитимность обусловлена такой детализацией правового регулирование, выступающего основанием для материального принуждения, которая бы позволила создать правовые гарантии от избыточных и чрезмерных ограничений прав человека.

ЗАКЛЮЧЕНИЕ

Развитие информационных и коммуникационных технологий способствует изменениям в общественных отношениях, которые в свою очередь оказывают влияние на институт прав человека. В условиях цифровой среды происходит формирование новой группы прав человека – цифровых прав, которые обусловлены использованием информации, представленной в цифровой форме. Осуществление данных прав либо происходит в цифровой среде, либо направлено на обеспечение доступа к ней. Большая часть цифровых прав относится к основным правам, осуществление которых возможно с использованием современных информационных и коммуникационных технологий. Формулировки таких прав человека на международном и конституционном уровнях являются в достаточной степени общими и не зависят от развития технологий. Для признания возможности их осуществления с использованием современных информационных и коммуникационных технологий внесения изменений в такие формулировки, как правило, не требуется.

В число цифровых прав включаются не только права, которые человек имеет в офлайновой среде, но и новые права, характерные именно для цифровой среды. Так, новые цифровые права человека, связанные с информацией о частной жизни, являются компонентами уже признанных основных прав, таких как свобода выражения мнения и право на неприкосновенность частной жизни. В то же время цифровые права, соответствующие второму поколению прав человека, получают юридическое закрепление в качестве основных прав. Развитие цифровых прав на современном этапе обусловлено различными национальными моделями их юридического закрепления, соответствующих правовым традициям тех или иных государствах и уровню их социально-экономического развития.

В цифровой среде личность для осуществления своих прав создает учетные и иные информационные записи или другими словами, формирует свою цифровую идентичность. С правовой точки зрения цифровая идентичность указывает на уникальную совокупность информации о личности, представленной

в цифровой форме, с использованием которой индивиды вступают в правоотношения, осуществляют права и обязанности. Ее создание связано с реализацией права на идентичность, которое признается в правовой доктрине одним из основных прав человека. По своему содержанию оно близко к праву на неприкосновенность частной жизни и заключается в признании и уважении индивида как уникальной личности. В отличие от права на неприкосновенность частной жизни, которое в цифровой среде предназначено для охраны интересов личности при использовании информации о ее частной жизни, право на идентичность указывает на охрану только информации, необходимой и достаточной для ее идентификации. В цифровой среде обеспечение защищенности права на идентичность приобретает особое значение. Оно выражается в предотвращении неправомерного доступа к составляющей цифровую идентичность информации о личности, исключении возможности ее использования без согласия ее создателя либо его идентификации, установления связи между ним и имеющейся у другого лица информацией.

Анонимность личности в сети Интернет является проявлением ее цифровой идентичности и исключает предоставление информационному посреднику информации, на основании которой он или другое лицо может ее идентифицировать. В отличие от права на идентичность право на анонимность в сети Интернет означает возможность личности использовать сеть Интернет без указания сведений, позволяющих ее идентифицировать. В цифровой среде происходит развитие правового регулирования, в соответствии с которым на личность возлагаются обязанности по предоставлению таких сведений, как при доступе к сети Интернет, так и при получении различных услуг в сети Интернет. Право на анонимность в сети Интернет обеспечивается с использованием специализированных технических средств. Поскольку они также позволяют обходить ограничения доступа к информационным ресурсам в сети Интернет, установленные в соответствии с законодательством того или иного государства, то возникает вопрос об их легитимности. В правовом государстве использование

таких технических способов защиты права на анонимность в сети Интернет является допустимым.

Правовое регулирование в цифровой среде основано на подходе, при котором допускается отличие цифровой идентичности от реальной. Согласно данному подходу признается право индивида самостоятельно определять свою цифровую идентичность, по своему усмотрению вносить в нее изменения независимо от того, соответствует она его реальной идентичности или нет. В цифровой среде проблема идентификации и анонимности обостряется. Ее решение связано с так называемой деидентификацией, в соответствии с которой на информационных посредников возлагаются обязанности по осуществлению действий с информацией о личности, направленных на ограничение возможности ее идентификации. При этом повышается ответственности информационных посредников и иных лиц, участвующих в обработке информации о личности за раскрытие такой информации и нарушение требований к ее обработке.

В настоящее время возникает проблема неравенства в доступе к информационным и коммуникационным технологиям между различными социальными группами. Ее решение связано с обеспечением цифрового равенства, которое соответствует новому этапу в развитии принципа правового равенства. В его основе лежит обеспечение юридически равных возможностей для осуществления права на доступ к сети Интернет. В свою очередь данное право создает условия для последующего осуществления других прав в цифровой среде, включая право на доступ к информации. Пределы обеспечения правового равенства при осуществлении права на доступ к сети Интернет определяются исходя из стандартов социального обслуживания населения и устранения различных форм дискриминации. Принцип правового равенства конкретизируется в принципе сетевой нейтральности и принципе доступности.

Принцип сетевой нейтральности заключается в том, что при оказании услуг доступа к сети Интернет информационные посредники обеспечивают всем получателям их услуг доступ ко всем информационным ресурсам в сети Интернет в равной степени. Принцип сетевой нейтральности отличается от принципа

технологической нейтральности, который определяет насколько правовое регулирование должно быть нейтральным к использованию тех или иных технологий. Для обеспечения сетевой нейтральности технологической нейтральности правовых норм недостаточно. В данном случае дискриминация возникает из-за использования информационными посредниками технологически зависимого подхода к оказанию услуг. Поэтому обеспечение сетевой нейтральности связано с возложением на них обязанностей по соблюдению технологически нейтрального подхода в своей деятельности.

Принцип доступности является международно-правовым и лежит в основе устранения различных форм дискриминации по отношению к лицам с ограниченными возможностями здоровья при осуществлении не только права на доступ к сети Интернет, но и права на доступ к информации в сети Интернет. Принцип доступности также проявляется в концепции открытых данных, которая находит воплощение в праве на доступ к информации о деятельности органов государственной власти и определяет тенденции его развития. Важное значение в данной концепции уделяется открытому формату представления данных, то есть независимому от используемых технических средств, машиночитаемому и доступному для общества без ограничений, которые бы препятствовали повторному использованию соответствующей информации.

В отличие от принципа сетевой нейтральности создание условий для осуществления и защита права на доступ к информации о деятельности органов государственной власти в соответствии с концепцией открытые данные, также как устранение дискриминации инвалидов при осуществлении доступа к информации в сети Интернет, основаны на технологически зависимом подходе, значение которого при обеспечении правового равенства повышается. Данный подход предполагает внедрение в деятельности организаций и государственных органов таких информационных и коммуникационных технологий, которые соответствуют современному уровню их развития. При этом технические нормы дополняют правовые нормы, которыми устанавливаются обязанности

организаций и государственных органов по внедрению соответствующих технических средств в своей деятельности.

Наряду с проблемой цифрового неравенства обостряется проблема неравенства различных прав, которая возникает при необходимости установить баланс между различными правами, такими как право на доступ к сети Интернет, право на доступ к информации в сети Интернет, свобода выражения мнения, право на неприкосновенность частной жизни. В результате при разрешении конфликта прав человека, осуществляемых с использованием сети Интернет, и прав других субъектов правоотношений, пусть даже речь идет об одних и тех же правах по содержанию, различие статуса их обладателей приведет к тому, что права человека будут защищены в большей степени.

В постиндустриальном обществе повышается значение правовых ценностей, среди которых особую роль играют информационная свобода и информационная безопасность. Они становятся одним из ориентиров в развитии различных прав человека, в том числе прав, осуществление которых ранее не связывалось с информацией, информационными и коммуникационными технологиями. Информационная свобода и информационная безопасность приобретают характер не только личной, но также публичной правовой ценности. Правовая охрана информационной свободы становится одним из государственных приоритетов, тогда как обеспечение информационной безопасности государства – гарантией устойчивого функционирования его институтов.

Между информационной свободой и информационной безопасностью как правовыми ценностями существует конфликт, который берет начало из общего конфликта ценностей свободы и безопасности и может быть решен исходя из их соотношения в системе правовых ценностей и достижения баланса их правовой охраны. Традиционные подходы к разрешению данного конфликта основаны на доминировании той или иной ценности. Приоритет информационной свободы по отношению к информационной безопасности выражается в недопустимости ограничения свободы выражения мнения и свободы информации. Однако

неограниченная свобода вступает в противоречие с правовой ценностью правового государства, которое предполагает правовое регулирование с опорой на правовое принуждение. Противоположный подход признает приоритет информационной безопасности. Вместе с тем ее доминирование над информационной свободой вступает в противоречие с такой правовой ценностью, как автономия личности. Доминанта информационной безопасности как публичной ценности может возникнуть и в правовых государствах. В отличие от государств, которые отвергают высшую ценность прав человека, в правовых государствах такая доминанта носит временный характер – до установления необходимого и достаточного контроля над угрозами информационной безопасности как публичной правовой ценности.

Хотя между информационной свободой и информационной безопасностью существует конфликт, они взаимосвязаны. В иерархии правовых ценностей они находятся на одном уровне и соотношение между ними является равновесным. При этом они связаны не только между собой, но и с другими правовыми ценностями, прежде всего с правами человека, которые в правовом государстве признаются высшей ценностью. Права человека выступают одним из результатов разрешения конфликта между данными ценностями. Несмотря на то, что постиндустриальное развитие общества осуществляется в условиях, когда ценность прав человека становится менее значимой по отношению к публичным ценностям, в правовых государствах такие ценности подлежат правовой охране, только если они основаны на создании условий для осуществления и защите прав человека. Соотношение прав человека с информационной свободой и информационной безопасностью не всегда основано на доминировании прав человека, при котором отсутствует баланс данных ценностей. Баланс правовой охраны возможен в случае, когда одни права человека соизмеряются с ценностями, в основе которых лежит создание условий для осуществления и защита других прав человека, независимо от того, являются такие ценности личными или публичными. В данном случае он соответствует балансу правовой охраны различных прав.

В настоящее время доминируют два подхода к определению понятия информационной безопасности, один из которых указывает на состояние защищенности национальных интересов в информационной сфере, а другой – на конфиденциальность, целостность, доступность информации и информационных систем. Права человека определяют ценностную ориентацию обеспечения информационной безопасности. Признание прав человека высшей ценностью способствует исключению произвольного и избыточного вмешательства в сферу их осуществления при обеспечении информационной безопасности личности, общества и государства. В результате информационная безопасность как правовая категория может быть Основные идеи и руководящие положения, на которые ориентируется правовое регулирование в области обеспечения информационной безопасности, заключаются в правовых принципах конфиденциальности, целостности и доступности.

Конфиденциальность и доступность как правовые режимы информации отличаются от конфиденциальности и доступности как правовых принципов. Правовой режим информации определяется совокупностью правовых средств, которые для конфиденциальности и доступности могут быть выражены в запретах и обязанностях, разрешениях и ограничениях определенных действий. В то же время правовые принципы конфиденциальности и доступности определяют условия, при которых использование таких правовых средств является правомерным. С развитием информационных и коммуникационных технологий правовые принципы конфиденциальности, целостности и доступности также распространяются на различные средства хранения, обработки, передачи и иного использования информации.

Информационная безопасность проявляется в совокупности прав человека, в которых выражаются возможности и притязания индивида, связанные с соблюдением принципов конфиденциальности, целостности или же доступности информации и технических средств, предназначенных для ее хранения, обработки, передачи и иного использования. Из признания данных прав в национальном законодательстве и судебной практике не следует признание права

человека на информационную безопасность, поскольку вопросы информационной безопасности составляют только часть содержания каждого из них.

Некоторые права человека в сфере обеспечения информационной безопасности получили юридическое закрепление в национальном праве в качестве основных прав человека, другие выступают отдельными компонентами уже признанных основных прав. В первом случае такими правами, например, являются права на целостность и конфиденциальность информационных систем, признанные основными Федеральным Конституционным судом Германии. Во втором случае к ним также можно отнести отдельные компоненты права на неприкосновенность частной жизни, в том числе отдельные права субъектов персональных данных, а также относительно новые право на анонимность в сети Интернет и право на забвение. В международном, наднациональном и национальном праве в целях обеспечения осуществления и защиты данных прав происходит конкретизация правовых принципов конфиденциальности, целостности и доступности. Хотя данные правовые принципы представляют собой универсальную модель и могут применяться в разных странах и правовых системах, их конкретизация зависит от правовых традиций государства.

Обеспечение информационной безопасности выступает одной из гарантией прав человека в информационной сфере. Весь комплекс правовых гарантий, с помощью которых обеспечивается осуществление и защита прав человека в офлайновой среде, равным образом распространяется и на права человека, которые осуществляются в цифровой среде. В то же время в цифровой среде права человека сталкиваются с вызовами, которые способствуют развитию гарантий прав человека, повышается значение технических гарантий прав человека, выраженных в технических средства и технических нормах, в соответствии с которыми они создаются и используются. Развитие технических гарантий прав человека осуществляется в соответствии с принципами неприкосновенности частной жизни за счет проектных решений и безопасности за счет проектных решений. При этом принципы неприкосновенности частной жизни за счет проектных решений становятся правовыми и находят воплощение в

различных правовых системах. В правовом государстве создание правовых гарантий предшествует введению в действие технических норм, на основании которых осуществляется разработка соответствующих технических средств.

В то же время обеспечение информационной безопасности выступает одной из целей, для достижения которой устанавливаются ограничения прав человека. В правовом государстве создаются гарантии прав человека от избыточных и чрезмерных их ограничений в целях обеспечения информационной безопасности, которые выражаются в правовых принципах, таких как принцип соразмерности. Данный принцип является основной такой гарантией в государствах романо-германской правовой семьи и практике европейских наднациональных судов. В соответствии с ним ограничения прав человека, должны быть установлены для достижения определенной легитимной цели, действительно способствовать ее достижению, быть минимально необходимыми, быть соразмерными (пропорциональными) в строгом смысле (stricto sencu). В правовых системах общего права влияние принципа соразмерности незначительно – в данном случае баланс при ограничении прав человека устанавливается путем взвешивания интересов с учетом принципов, вырабатываемых высшими национальными судами. При этом наблюдается сближение подходов к обеспечению баланса интересов при ограничении прав человека в различных правовых системах. Правовой принцип соразмерности становится универсальным, поскольку он применим для проверки легитимности любых ограничений прав человека, установленных с целью обеспечения информационной безопасности.

Правовые ограничения прав человека в цифровой среде дополняются фактическими (материальными) ограничениями, выраженными в материальном принуждении индивида к определенному поведению. Оно заключается в возложении обязанностей на разработчиков технических средств и информационных посредников, которые влияют на пределы прав человека. Возлагая на них такие обязанности, органы государственной власти фактически (материально) ограничивают права индивидов, которые используют соответствующие технические средства или получают услуги информационных

посредников. Для легитимности материального принуждения не достаточно юридического закрепления обязанностей разработчиков технических средств и информационных посредников. Ограничения прав человека признаются легитимными, только если они сформулированы в национальном законодательстве таким образом, чтобы в ясной и недвусмысленной форме определять, какое право человека и в каком объеме ограничено. Вследствие этого легитимность материального принуждения обусловлена такой детализацией материальных и процессуальных правовых норм, выступающих основанием для его применения, которая бы позволила исключить избыточные и чрезмерные ограничения прав человека.

Несмотря на то, что при обеспечении информационной безопасности в цифровой среде повышается значение технических способов защиты прав человека и фактических (материальных) их ограничений, в правовом государстве регулирующее воздействие на общественные отношения основано на преобладающей роли права как социального регулятора. Именно в праве обеспечивается баланс между информационной свободой и информационной безопасностью как правовыми ценностями постиндустриального периода на основе правовых принципов, таких как принципы правового равенства и соразмерности. В изменяющемся обществе происходит дальнейшее развитие гарантий прав человека при обеспечении информационной безопасности и конкретизация соответствующих правовых принципов, с тем чтобы они соответствовали особенностям осуществления и защиты прав человека в условиях развития информационных и коммуникационных технологий.

СПИСОК ЛИТЕРАТУРЫ

Нормативные правовые акты

Международные нормативные правовые акты и иные документы

1. Всеобщая декларация прав человека 1948 г. // Российская газета, 10.12.1998.
2. Венская декларация и программа действий 1993 г. // Международное публичное право. Сборник документов. Т. 1. – М. : БЕК, 1996. С. 521 – 540.
3. Договор о Евразийском экономическом союзе 2014 г. // URL: http://www.eurasiancommission.org/
4. Конвенции о защите прав человека и основных свобод 1950 г. // Бюллетень международных договоров. – 2001. – № 3.
5. Конвенция о правах инвалидов (заключена в г. Нью-Йорке 13.12.2006) // СЗ РФ. 2013. № 6. Ст. 468.
6. Конвенции о правах ребенка (одобрена Генеральной Ассамблеей ООН 20.11.1989) // Сборник международных договоров СССР. выпуск XLVI. 1993.
7. 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.
8. Конвенция Совета Европы о преступлениях в сфере компьютерной информации // URL: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm
9. Конвенция Совета Европы о доступе к официальным документам // URL: http://www.coe.int/ru/web/conventions/full-list/-/conventions/treaty/205.
10. Конвенция об обеспечении международной информационной безопасности (концепция). // URL: http://www.scrf.gov.ru/documents/6/112.html
11. Международный пакт об экономических, социальных и культурных правах 1966 г. // Бюллетень Верховного Суда Российской Федерации, № 12, 1994.

12. Международный пакт о гражданских и политических правах 1966 г. // Бюллетень Верховного Суда Российской Федерации. – 1994. – № 12.
13. Устав Организации Объединенных Наций (Сан-Франциско, 26 июня 1945 г.). // Сборник действующих договоров, соглашений и конвенций, заключенных СССР с иностранными государствами, Вып. XII, – М., 1956, с. 14 – 47.
14. Алексей Овчинников (Aleksey Ovchinnikov) против России. Постановление Европейского суда по правам человека от 16 декабря 2010 г. (Жалоба № 24061/04) // Бюллетень Европейского суда по правам человека. – 2011. – № 10.
15. Ахмет Йилдырым (Ahmet Yildirim) против Турции. Постановление Европейского суда от 18 декабря 2012 г. (Жалоба № 3111/10) // Прецеденты Европейского суда по правам человека. – 2016. – № 6(30).
16. Класс и другие против Федеративной Республики Германии. Решение Европейского суда по правам человека от 6 сентября 1978 г. (Жалоба № 5029/71) // Европейский суд по правам человека. Избранные решения. Т. 1. – М. : Норма, 2000. С. 168 – 186.
17. Вебер и Саравия (Weber and Saravia) против Германии. Решение Европейского суда по правам человека от 29 июня 2006 г. (Жалоба № 54934/00) // Бюллетень Европейского суда по правам человека. – 2007. – № 2.
18. Либерти и другие (Liberty and Others) против Соединенного Королевства. Постановление Европейского суда по правам человека от 1 июля 2008 г. (Жалоба № 58234/00) // Бюллетень Европейского суда по правам человека. – 2008. – № 12.
19. Лю и Лю (Liu and Liu) против Российской Федерации. Постановление Европейского суда по правам человека от 6 декабря 2007 г. (Жалоба № 42086/05) // Бюллетень Европейского суда по правам человека. – 2012. – № 8.

20. Роман Захаров (Roman Zakharov) против Российской Федерации. Постановление Европейского суда по правам человека от 4 декабря 2015 г. Дело (Жалоба № 47143/06) (Большая Палата Европейского суда) // Бюллетень Европейского суда по правам человека. – 2016. – № 6(168).
21. Шимоволос (Shimovolos) против Российской Федерации. Постановление Европейского суда по правам человека от 21 июня 2011 года. (Жалоба № 30194/09) // Бюллетень Европейского суда по правам человека. – 2012. – № 1.
22. Компания «Делфи АС» (Delfi AS) против Эстонии. Постановление Европейского Суда по правам человека от 16 июня 2015 г. (жалоба № 64569/09) // Бюллетень Европейского Суда по правам человека. – 2015. – № 11(161).
23. S. и Марпер (S. and Marper) против Соединенного Королевства. Постановление Европейского Суда по правам человека от 4 декабря 2008 г. (Жалобы № 30562/04, 30566/04) // Бюллетень Европейского Суда по правам человека. – 2009. – № 4.
24. Окинавская хартия глобального информационного общества. URL: http://www.iis.ru/library/okinawa/charter.ru.html
25. Поощрение, защита и осуществление прав человека в Интернете: Резолюция, принятая Советом по правам человека от 14 июля 2014 г. № A/HRC/RES/26/13 // URL: http://www.refworld.org.ru/docid/5583e0004.html
26. Правила поведения в области обеспечения международной информационной безопасности: письмо постоянных представителей Китая, Российской Федерации, Таджикистана и Узбекистана при Организации Объединенных Наций от 12 сентября 2011 г. на имя Генерального секретаря. A/66/359 // URL: http://rus.rusemb.org.uk/data/doc/internationalcoderus.pdf
27. Резолюция Генеральной Ассамблеи ООН A/RES/54/49 Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности // URL: http://www.ifap.ru/ofdocs/un/5449.pdf

28. Рекомендации Комитета министров Совета Европы № CM/Rec(2016)5 о свободе в Интернете. URL: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016806415fa
29. Рекомендации Совета Европы 1037 (1986) «О защите данных и свободе информации» // URL: http://assembly.coe.int/Main.asp?link=/Documents/AdoptedText/ta86/EREC1037.htm
30. Рекомендация Совета Европы № R(81)19 о праве на доступ к информации, находящейся в ведении государственных организаций, принята Комитетом министров 25 ноября 1981 г. // URL: http://www.media-advocat.ru/european/?p=press&pid=19
31. Рекомендации Совета Европы № Rec(2002)2 по доступу к официальным документам // URL: http://ppt.ru/news/4357
32. Сиракузские принципы толкования ограничений и отступлений от положений международного пакта (Документ ООН E/CN.4/1985/4) // URL: http://medialaw.asia/posts/10-05-2012/61617.html

Нормативные правовые и иные акты Российской Федерации

33. Федеральный конституционный закон от 30 мая 2001 г. № 3-ФКЗ «О чрезвычайном положении» // СЗ РФ. 2001. № 23. ст. 2277.
34. Гражданский кодекс Российской Федерации (часть четвертая) // СЗ РФ. 2006. № 52 (1 ч.). ст. 5496.
35. Федеральный закон от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» // СЗ РФ, 1995, № 33, ст. 3349.
36. Федеральный закон от 4 июля 1996 г. № 85-ФЗ «Об участии в международном информационном обмене» (утратил силу) // СЗ РФ. 1996. № 28. ст. 3347.
37. Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи» // СЗ РФ. 2003. № 28. ст. 2895.

38. Федеральном законе от 27 июля 2006 г. № 152-ФЗ «О персональных данных» // СЗ РФ. 2006 г. № 31 (часть I). Ст. 3451.
39. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СЗ РФ. 2006. № 31 (1 ч.). ст. 3448.
40. Федеральном законе от 9 февраля 2009 г. № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» // СЗ РФ. 2009 г. № 7. Ст. 776.
41. Федеральный закон от 25 июля 2011 г. № 261-ФЗ «О внесении изменений в Федеральный закон «О персональных данных». СЗ РФ. 2011. № 31. ст. 4701.
42. Федеральный закон от 28 июля 2012 г. № 139-ФЗ «О внесении изменений в Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» и отдельные законодательные акты Российской Федерации» // СЗ РФ. 2012. № 31. ст. 4328.
43. Федерального закона от 7 июня 2013 г. № 112-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и Федеральный закон «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» // СЗ РФ. 2013. № 23. ст. 2870.
44. Федеральный закон от 2 июля 2013 г. № 187-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам защиты интеллектуальных прав в информационно-телекоммуникационных сетях» // СЗ РФ, 2013, № 27, ст. 3479.
45. Федеральный закон от 5 мая 2014 г. № 97-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и отдельные законодательные акты Российской Федерации по вопросам упорядочения обмена информацией с использованием информационно-телекоммуникационных сетей» // СЗ РФ. 2014. № 19. ст. 2302.

46. Федеральный закон от 21 июля 2014 г. № 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях» // СЗ РФ. 2014. № 30. ст. 4243.
47. Федеральный закон от 24 ноября 2014 г. № 364-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и Гражданский процессуальный кодекс Российской Федерации» // СЗ РФ. 2014. № 48, ст. 6645.
48. Федеральный закон от 1 декабря 2014 г. № 419-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам социальной защиты инвалидов в связи с ратификацией Конвенции о правах инвалидов» // СЗ РФ. 2014. № 49 (часть VI), ст. 6928.
49. Федеральный закон от 13 июля 2015 г. № 264-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и статьи 29 и 402 Гражданского процессуального кодекса Российской Федерации» // СЗ РФ. 2015. № 29. Ст. 4390.
50. Федеральный закон от 6 июля 2016 г. № 374-ФЗ «О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» // СЗ РФ, 11.07.2016, № 28, ст. 4558.
51. Федеральном законе от 6 июля 2016 г. № 375-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» // СЗ РФ. 2016. № 28. ст. 4558.
52. Федеральный закон от 29 июля 2017 г. № 276-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» // СЗ РФ. 2017. № 31. ст. 4825.

53. Стратегия национальной безопасности Российской Федерации до 2020 года, утвержденная Указом Президента Российской Федерации от 12 мая 2009 г. № 537 (утратила силу) // СЗ РФ. 2009. № 20. Ст. 2444.
54. Указ Президента Российской Федерации от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СЗ РФ. 2016. № 50. ст. 7074
55. Указ Президента Российской Федерации от 31 декабря 2015 г. № 683 «О Стратегии национальной безопасности Российской Федерации» // СЗ РФ. 2016. № 1. ст. 212.
56. Доктрина информационной безопасности Российской Федерации, утвержденной Президентом Российской Федерации от 9 сентября 2000 г. № Пр-1895 (утратила силу) // Российская газета, 28 сентября 2000 г.
57. Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года, утвержденные Президентом Российской Федерации 24.07.2013 № Пр-1753 // URL: http://www.scrf.gov.ru/
58. Постановление Правительства Российской Федерации от 23 января 2006 г. № 32 «Об утверждении Правил оказания услуг связи по передаче данных» // СЗ РФ. 2006. № 5. ст. 553.
59. Приказ ФСБ России от 19 июля 2016 г. № 432 «Об утверждении Порядка представления организаторами распространения информации в информационно-телекоммуникационной сети «Интернет» в Федеральную службу безопасности Российской Федерации информации, необходимой для декодирования принимаемых, передаваемых, доставляемых и (или) обрабатываемых электронных сообщений пользователей информационно-телекоммуникационной сети «Интернет» // Бюллетень нормативных актов федеральных органов исполнительной власти. № 36. 2016.
60. Приказ Минкомсвязи России от 30 ноября 2015 г. № 483 «Об установлении Порядка обеспечения условий доступности для инвалидов по зрению официальных сайтов федеральных органов государственной власти,

органов государственной власти субъектов Российской Федерации и органов местного самоуправления в сети «Интернет» // Российская газета, № 27, 10.02.2016.

61. Постановление Конституционного Суда Российской Федерации от 14 ноября 2005 г. № 10-П «По делу о проверке конституционности положений пункта 5 статьи 48 и статьи 58 Федерального закона «Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации», пункта 7 статьи 63 и статьи 66 Федерального закона «О выборах депутатов Государственной Думы Федерального Собрания Российской Федерации» в связи с жалобой Уполномоченного по правам человека в Российской Федерации» // СЗ РФ. 2005. № 47. ст. 4968.
62. Постановление Конституционного Суда Российской Федерации от 07.06.2012 № 14-П «По делу о проверке конституционности положений подпункта 1 статьи 15 Федерального закона «О порядке выезда из Российской Федерации и въезда в Российскую Федерацию» и статьи 24 Закона Российской Федерации «О государственной тайне» в связи с жалобой гражданина А.Н. Ильченко» // СЗ РФ. 2012. № 28. ст. 3977.
63. Постановление Конституционного Суда Российской Федерации от 06.11.2014 № 27-П «По делу о проверке конституционности статьи 21 и статьи 21.1 Закона Российской Федерации «О государственной тайне» в связи с жалобой гражданина О.А. Лаптева» // СЗ РФ. 2014. № 46. ст. 6425.
64. Постановление Конституционного Суда Российской Федерации от 07.06.2012 № 14-П «По делу о проверке конституционности положений подпункта 1 статьи 15 Федерального закона «О порядке выезда из Российской Федерации и въезда в Российскую Федерацию» и статьи 24 Закона Российской Федерации «О государственной тайне» в связи с жалобой гражданина А.Н. Ильченко» // СЗ РФ. 2012. № 28. ст. 3977.
65. Постановление Конституционного Суда Российской Федерации от 31.03.2011 № 3-П «По делу о проверке конституционности части третьей статьи 138 Уголовного кодекса Российской Федерации в связи с жалобами

граждан С.В. Капорина, И.В. Коршуна и других» // СЗ РФ. 2011. № 15. ст. 2191.

66. Определении Конституционного Суда Российской Федерации от 1 июня 2010 г. № 757-О-О «Об отказе в принятии к рассмотрению жалобы гражданина Леонова Владимира Николаевича на нарушение его конституционных прав положениями подпункта «г» пункта 3.2 статьи 4 и подпункта «ж» пункта 7 статьи 76 Федерального закона «Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации» // Вестник Центризбиркома РФ. № 7. 2010.
67. Определение Конституционного Суда Российской Федерации от 17 июля 2014 г. № 1759-О «Об отказе в принятии к рассмотрению жалобы гражданина Харитонова Владимира Владимировича на нарушение его конституционных прав пунктом 2 части 2 статьи 15.1 Федерального закона «Об информации, информационных технологиях и о защите информации» и пунктом 2 статьи 3 Федерального закона «О внесении изменений в Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» и отдельные законодательные акты Российской Федерации» // СПС КонсультантПлюс.
68. Апелляционное определение Московского городского суда от 14.07.2015 по делу № 33-24464/2015 // СПС КонсультантПлюс.
69. Апелляционное определение Московского областного суда от 24.06.2015 по делу № 33-14941/2015 // СПС КонсультантПлюс.
70. Определение Приморского краевого суда от 24.08.2015 по делу № 33-7346/2015 // СПС КонсультантПлюс
71. Определение Московского городского суда от 10.11.2016 по делу № 33-38783/2016 // СПС КонсультантПлюс.
72. Пояснительная записка к проекту федерального закона № 195446-7 «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» // URL:

http://asozd2.duma.gov.ru/main.nsf/(ViewDoc)?OpenAgent&work/dz.nsf/ByID&07CFD475394B5E984325813A0065B8B8

73. ГОСТ Р 52292-2004 «Информационная технология. Электронный обмен информацией. Термины и определения» // М. : ИПК Издательство стандартов, 2005.
74. ГОСТ Р ИСО/МЭК 13335-1-2006 «Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий» // М. : Стандартинформ, 2007.
75. ГОСТ Р 52872-2012 «Национальный стандарт Российской Федерации. Интернет-ресурсы. Требования доступности для инвалидов по зрению» // М. : Стандартинформ, 2014.

Монографии

76. Алексеев, С. С. Социальная ценность права в советском обществе. – М. : Юрид. лит., 1971. – 222 с.
77. Бачило, И. Л. Информационное право: учебник для вузов / И. Л. Бачило. – М.: Высшее образование, Юрайт-Издат, 2009. – 454 с.
78. Белл, Д. Грядущее постиндустриальное общество Опыт социального прогнозирования / Пер. с англ. Изд. 2-е, испр. и доп. – М. : Academia, 2004. – CLXX, 788 с.
79. Бентам, И. Избранные сочинения / Пер. по англ. изд. Боуринга и фр. Дюмона, А. Н. Пыпина и А. Н. Неведомского. Т. 1. – СПб., 1867. – LXII, 678 с.
80. Белевская, Ю. А. Право и информационная безопасность. Учебное пособие / Белевская Ю. А., Глоба Ю. А., Касилов А. Н., Савин В. И., и др.; Под ред.: Белевская Ю. А., Фисун А. П. – М.: Приор-издат, 2005. – 272 с.
81. Бержель, Ж.-Л. Общая теория права / под ред. В.И. Даниленко. – М. : NOTA BENE, 2000. – 576 с.

82. Бернам, У. Правовая система США. 3-й выпуск. – М. : «Новая юстиция», 2006. – 1216 с.
83. Венгеров, А. Б. Теория государства и права : Учебник. 2-е изд. – М. : Омега-Л, 2005. – 608 с.
84. Воеводин, Л. Д. Юридический статус личности в России. Учеб. пособие. – М. : Изд-во Моск. ун-та, 1997. – 298 с.
85. Волчинская, Е. К. Защита персональных данных : Опыт правового регулирования. – М. : Галерия, 2001. – 223 с.
86. Глобальная безопасность в цифровую эпоху: стратагемы для России. Под общ. ред. Смирнова А. И. – М. : ВНИИгеосистем, 2014. – 394 с.
87. Гоббс, Т. Левиафан. – М. : Мысль, 2001. – 478 с.
88. Государственное право Германии. Сокращенный перевод немецкого семитомного издания. Т. 1 // Отв. ред.: Топорнин Б. Н. – М. : Изд-во ИГиП РАН, 1994. – 312 с.
89. Головистикова, А. Н. Права человека : учебник / А. Н. Головистикова, Л. Ю. Грудцына. – М. : Эксмо, 2006. – 448 с.
90. Городов, О. А. Информационное право: учебник. М.: Проспект, 2008. – 256 с.
91. Давид, Р. Основные правовые системы современности / Р. Давид, К. Жоффре-Спинози; пер. с фр. В. А. Туманова. – М. : Междунар. отношения, 1996. – 399 с.
92. Дворкин, Р. О правах всерьез / Пер. с англ.; Ред. Л. Б. Макеева. М. : «Российская политическая энциклопедия» (РОССПЭН), 2004. – 392 с.
93. Интеллектуальные права. Понятие. Система. Задачи кодификации: Сборник статей / Дозорцев В. А. – М. : Статут, 2003. – 416 с.
94. Кириленко, В.П. Международное право и информационная безопасность государства / В.П. Кириленко, Г.В. Алексеев : монография. – СПб. : СПбГИКиТ, 2016. – 396 с.
95. Лессиг, Л. Код и другие законы киберпространства. – М. : Мысль. 1999. – 225 с.

96. Локк, Дж. Сочинения в трех томах: Т. 3. – М. : Мысль, 1988. – 668 с.
97. Лукашева, Е. А. Человек, право, цивилизация: нормативно-ценностное измерение. – М. : Издательство «Норма», 2009. – 384 с.
98. Малько, А. В. Стимулы и ограничения в праве: Теоретико–информационный аспект. 3–е изд., перераб. и доп. – М. : Юристъ, 2012. – 363 с.
99. Махлуп, Ф. Производство и распространение знаний в США. – М. : Прогресс, 1966. – 462 с.
100. Морозов, А. В. Организационно-правовое обеспечение информационной безопасности : монография / А. В. Морозов, Т. А. Полякова; РПА Минюста России. – М. : РПА Минюста России, 2013. – 276 с.
101. Неновски, Н. Право и ценности. Пер. с болг. – М. : Прогресс. 1987. – 245 с.
102. Ниесов, В. А. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для бакалавриата и магистратуры / В. А. Ниесов, Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова ; под ред. Т. А. Поляковой, А. А. Стрельцова. – М. : Издательство Юрайт, 2016. –325 с.
103. Общая теория национальной безопасности: учебник / Под общ. ред. А.А. Прохожева. – М. : Изд-во РАГС, 2005. – 344 с.
104. Права человека. Учебник для вузов / Ответственный редактор – член-корр. РАН, доктор юридических наук Е. А. Лукашева. – М. : Издательство НОРМА, 2001. – 573 с.
105. Право на доступ к информации. Доступ к открытой информации / Отв. ред. И. Ю Богдановская. – М. : ЗАО «Юстицинформ», 2009. – 344 с.
106. Проблемы общей теории права и государства: Учебник для вузов / Под общ. ред. академика РАН, д. ю. н., проф. В. С. Нерсесянца. – М. : Норма, 2006. – 832 с.
107. Рассолов, И. М. Информационное право: учебник. – М. : Издательство Юрайт, 2011. – 440 с.

108. Рассолов, И. М. Право и киберпространство. – М. : Московское бюро по правам человека, 2007. – 248 с.

109. Рассолов, И. М. Право и Интернет. Теоретические проблемы / Рассолов И. М. 2-е изд. –М. : Норма, 2009. – 384 с.

110. Терещенко, Л.К. Правовой режим информации. М.: ИД «Юриспруденция», 2007. 192 с.

111. Хайек, Ф. Право, законодательство и свобода: современное понимание либеральных принципов справедливости и политики. – Серия: Политич. наука. – Изд-во: ИРИСЭН, 2006. – 644 с.

112. Чеботарева, А. А. Человек и электронное государство: право на информационную безопасность. – Чита: ЧИТГУ, 2011. – 160 с.

113. Чистое учение о праве Ганса Кельзена: сб. пер.: [в 2 вып.] / Ин-т науч. информ. по обществ. наукам Акад. наук СССР; отв. ред.: В. Н. Кудрявцев, Н. Н. Разумович. – М. : ИНИОН АН СССР, 1987–1988. – 2 вып. – 213 с.

114. Фатьянов, А. А. Правовое обеспечение информационной безопасности в Российской Федерации. – М.: Юрист, 2001. – 412 с.

115. Философия права. Учебник для вузов / Нерсесянц В. С. – М.: Норма, 1997. – 652 с.

116. Фуко, М. Безопасность, территория, население. Курс лекций, прочитанных в Колледж де Франс в 1977—1978 уч. году / пер. с фр. Ю. Ю. Быстрова, Н. В. Суслова, А. В. Шестакова. – СПб. : Наука, 2011. – 544 с.

Статьи

117. Андрианова В. В. Личные права в России (право на индивидуальность) // Вестник Российской правовой академии. – 2012. – № 3. – С. 18-21

118. Андрощук, Г. Право на анонимность в интернете: проблемы регулирования // Интеллектуальная собственность. Авторское право и смежные права. – 2015. – № 12. – С. 57 – 70.

119. Амирова, Р. Р. Содержание и виды гарантий прав человека в теории конституционного права // Ученые записки Казанского университета. Серия: Гуманитарные науки. – 2007. – Т. 149. – № 6. – С. 58 – 66.

120. Ардашев, А. И. Конституционно-правовое обеспечение права человека на безопасность в Российской Федерации // Современное право. – 2008. – № 1. – С. 39 – 44.

121. Архипов, В. В. Открытая концепция регулирования Интернета вещей / Архипов В. В., Наумов В. Б., Пчелинцев Г. А., Чирко Я. А. // Информационное право. – 2016. – № 2. – С. 18 – 25.

122. Белевская, Ю. А. Теоретико-правовые основы регулирования конституционных прав и свобод человека и гражданина в информационной сфере // Закон и право. – 2009. – № 3. – С. 18 – 19.

123. Блинов, А. А. Интернет в арабском мире // Восточная аналитика. – 2011. – № 2. – С. 188-196.

124. Бондарь, Н. С. Конституционное правосудие как фактор модернизации российской государственности // Журнал российского права. – 2005. – № 11 (107). – С. 15 – 30.

125. Буадана, И. Электронное управление административно-территориальных образований и защита персональных данных во французской системе // Право цифровой администрации в России и во Франции. Сборник научных материалов Российско-французской международной конференции. 27–28 февраля 2013 года. – М.: ООО «ПОЛИГРАФ-ПЛЮС», 2013. – 178 с. – С. 69-78.

126. Варламова, Н. В. Интересы национальной безопасности как основание ограничений прав человека (по материалам практики Европейского суда по правам человека) / Труды Института государства и права Российской академии наук. – 2013. – № 1. – С. 164 – 165.

127. Велиева, Д. С. Право на уважение частной жизни: международные стандарты реализации и защиты // Известия Саратовского университета.

Новая серия. Серия Экономика. Управление. Право. – 2014. – № 2-2. – Т. 14. – С. 443 – 448.

128. Ветютнев, Ю. Ю. Аксиологический статус правового равенства // Философия права. – 2012. – № 1 (50). – С. 90 – 95.

129. Ветютнев, Ю. Ю. Ценностные аспекты конституционных прав // В сборнике: Конституция России: глобальное, национальное, региональное Материалы Международной научно-практической конференции. – 2013. – С. 19 – 21.

130. Ветютнев, Ю. Ю. Аксиология права в постсоветской России // В сборнике: Проблемы постсоветской теории и философии права Сборник статей. Московская высшая школа социальных и экономических наук. – М., 2016. – С. 280 – 288.

131. Волков, Ю. В. Защищенность субъекта при автоматизированной обработке его персональных данных // Вестник УрФО. Безопасность в информационной сфере. – 2012. – № 3 – 4. – С. 49 – 53.

132. Глушкова, С. И. Права человека и гражданина в контексте глобализации // Правовая система России в условиях глобализации. Сборник материалов круглого стола. – М.: Ось-89, 2005. – С. 45 – 46.

133. Горелик, А. С. Императив доступности. Информационное общество. – 2010. – № 1. – С. 6 – 8.

134. Данилов, Н. А. Социальная справедливость в информационном обществе: проблема цифрового равенства // Информационное право. – 2012. – № 4 (31). – С. 5 – 7.

135. Демидов, О. Обеспечение международной информационной безопасности и российские национальные интересы // Индекс безопасности. – № 1(104). – Т. 19. – С. 129 – 168.

136. Дракер, П. Посткапиталистическое общество // Новая постиндустриальная волна на Западе. Антология / Под ред. В.Л.Иноземцева. – М. : Academia, 1999. – С. 70 – 100.

137. Жарова, А. К. Источники понятий «персональные данные» и частная жизнь лица в российском праве / Жаров А. К., Елин В. М. // Вестник Академии права и управления. – 2017. – № 46 (1). – С. 69 – 78.

138. Захаров, А. Л. Цифровое неравенство России / Захаров А. Л., Суркова О. Е. // Евразийский юридический журнал. – 2015. – № 6(85). – С.301 – 303.

139. Зорькин, В. Д. Аксиологические аспекты Конституции России // Конституционные ценности в теории и судебной практике: сборник докладов. – М., 2009. – С. 7 – 20.

140. Зорькин, В. Д. Национальные интересы, современный миропорядок и конституционная законность // Актуальные проблемы развития судебной системы и системы добровольного и принудительного исполнения решений Конституционного Суда РФ, судов общей юрисдикции, арбитражных, третейских судов и Европейского суда по правам человека. Сборник научных статей. – СПб. : Краснодар: Юрид. центр Пресс, 2008. – С. 21 – 58.

141. Исаков, В. Б. Преемственность правовых норм в сфере технического регулирования. Юридическая техника. – 2011. – № 5. – С.188.

142. Калина, Е. С. Понятие безопасности и право на безопасность как одно из личных прав // Безопасность бизнеса. – 2004. – № 4. – С. 9 – 10.

143. Калятин, В. О. О некоторых тенденциях развития законодательства об ответственности интернет-провайдеров // Закон. – 2012. – № 7. – С. 27 – 34.

144. Карташкин, В. А. Права человека и международная безопасность // Труды Института государства и права Российской академии наук. – 2013. – № 1. – С. 33 – 59.

145. Карташкин, В. А. Принцип уважения прав человека и государственный суверенитет // Международная защита прав человека и государственный суверенитет : мат. Международной научно-практической конференции / отв. ред. Т. А. Сошникова. – М. : Изд-во Моск. гуманит. ун-та, 2015. – С. 11 – 17.

146. Карташкин, В. А. Универсализация прав человека и традиционные ценности человечества // Современное право. – № 8. – 2012. – С.3 – 9.

147. Ковалева, Н. Н. Система правового регулирования применения информационных технологий в избирательном процессе // Информационное общество: проблемы развития законодательства. Сборник научных работ. – М. : ИГП РАН, юридическое издательство «ЮРКОМПАНИ», 2012. – С. 57 – 65.

148. Коробова, А. П. Приоритеты правовой политики // Российская правовая политика. Курс лекций / Афанасьев С.Ф., Беляев В.П., Вавилин Е.В., Демидов А.И., и др.; Под ред.: Малько А.В., Матузов Н.И. – М.: Норма, 2003. – 528 с. – С. 97 – 111.

149. Колмаков, С. Ю. Сравнительно-правовое исследование свободы слова в России и Китае. Влияние российской правовой системы на китайскую // Сравнительная политика. – 2013. – 2(12). – С. 87 – 91.

150. Колоткина, О. А. Право личности на безопасность: понятие, место в системе прав человека и особенности изучения в курсе конституционного права РФ // Право и образование. – 2007. – № 11. – С. 109 – 114.

151. Коротков, А. В. Безопасность критических информационных инфраструктур в международном гуманитарном праве / Коротков А. В., Зиновьева Е. С. // Вестник МГИМО Университета. – 2011. – № 4. – С. 154 – 162.

152. Кривошеев, А. В. Имплементация норм договора ВОИС об авторском праве и договора ВОИС по исполнениями и фонограммам в части технических средств защиты объектов авторского права и смежных прав // Вестник Российского университета дружбы народов. – 2009. – № 4. – С. 48 – 56.

153. Крутских, А. В. Война и мир: международные аспекты информационной безопасности // Научные и методологические проблемы информационной безопасности: сб. ст. / под ред. В. П. Шерстюка. – М.: МЦНМО, 2004. – С. 85 – 96.

154. Кузнецов, П. У. Конституционные ценности в информационной сфере // Новые вызовы и угрозы информационной безопасности: правовые

проблемы / Отв. ред. Т. А. Полякова, И. Л. Бачило, В. Б. Наумов. Сб. науч. работ. – Москва: ИГП РАН – Издательство «Канон+» РООИ «Реабилитация», 2016. – 320 с. – С. 35 – 52.

155. Кузнецов, Э. В. Право на индивидуальность: к истории вопроса // История государства и права. – 2009. – № 10. – С. 3 – 5.

156. Лановая, Г. М. Базовые ценности современного права // История государства и права. – 2014. – № 20. – С. 23 – 27.

157. Лапаева, В. В. Критерии ограничений прав человека с позиций либертарной концепции правопонимания // Журнал российского права. – 2006. – № 4. – С. 103 – 115.

158. Лапаева, В. В. Конституция РФ об основаниях и пределах ограничения прав и свобод человека и гражданина // Законодательство и экономика. – 2005. – № 1. – С.11 – 17.

159. Лапаева, В. В. Правовой принцип формального равенства // Журнал российского права. – 2008. – № 2 (134). – С.67 – 80.

160. Лаптева, Л. Е. Политико-правовые ценности: история и современность (симпозиум) // Государство и право. – 1997. – № 7. – С. 84 – 86.

161. Лукашева, Е. А. Права человека – индикатор национальной безопасности // Труды Института государства и права Российской академии наук. – 2013. – № 1. – С. 7 – 33.

162. Луман, Н. Решения в «информационном обществе» // Проблемы теоретической социологии. Вып 3. / Отв. ред. А.О. Бороноев. – СПб. : Издательство СПбГУ, 2000. – С. 36 – 45.

163. Мартышин, О. В. Проблема ценностей в теории государства и права // Государство и право. – 2004. – № 10. – С. 5 – 14.

164. Монахов, В. Основные информационные права и свободы: проблемы правопонимания и правоприменения // Труды по интеллектуальной собственности. – 2003. – Т. 6. – № 1. – С. 58 – 68.

165. Мозолин, В. П. Информация и право / Мозолин В. П., Петровичева Ю. В. // Журнал российского права. – 2004. – № 8. – С. 54 – 64.

166. Мордовец, А. С. Гарантии прав личности: понятие и классификация // Теория государства и права: Курс лекций / Под ред. Н. И. Матузова, А. В. Малько. – М.: Юристъ, 2000. – С. 311 – 319.

167. Муромцев, Г. И. Права человека: культурно-исторический аспект // Права человека в современном мире: новые вызовы и трудные решения : материалы международной научной конференции / отв. ред. Т. А. Сошникова – М. : Изд-во Моск. гуманит. ун-та, 2014. – 382 с. – С. 24 – 28.

168. Петров, Д. А. Принципы саморегулирования: критерии систематизации и виды // Академический юридический журнал. – 2012. – № 2 (48). – С. 44-48.

169. Пряхина, Т. М. Европейская Конвенция о защите прав человека и основных свобод в правовой системе России // Международная защита прав человека и государственный суверенитет : мат. международной научно-практической конференции / отв. ред. Т. А. Сошникова. – М. : Изд-во Моск. гуманит. ун-та, 2015. – 330 с. – С. 64 – 68.

170. Пчелинцев, С. В. Права человека и интересы безопасности: выбор приоритетов правовой политики // Социология власти. – 2006. – № 2. – С. 104 – 109.

171. Пчелинцев, С. В. Соотношение понятий «умаление прав и свобод» и «ограничение прав и свобод»: теоретические аспекты // Современное право. – 2006. – № 4. – С. 47 – 50.

172. Рабец, А. М. Право ребенка на индивидуальность и проблемы его реализации в Российской Федерации // Ученые записки Российского государственного социального университета. – 2013. – Т. 1. – № 2 (113). – С. 79 – 87.

173. Савельев, А. И. Проблемы применения законодательства о персональных данных в эпоху «Больших данных» (Big Data) // Право. Журнал Высшей школы экономики. – 2015. – № 1. – С. 43 – 66.

174. Середа, М. Ю. Механизм ограничения конституционных прав и свобод человека в сети Интернет // Вестник Воронежского государственного университета : Серия «Право». – 2013. – № 2. – С.83 – 93.

175. Середа, М. Ю. Закрепление права на доступ в сеть Интернет в международно-правовых актах и законодательстве зарубежных стран // Международное публичное и частное право. – 2013. – № 5. – С. 44 – 47.

176. Сидорова, Е. В. Миф о правовых ценностях // История государства и права. – 2012. – № 11. – С.24 – 25.

177. Соколов, М. С. Информационная безопасность. К вопросу о содержании понятия «информационная безопасность» // Закон и право. – 2011. – № 5. – С. 9 – 14.

178. Соловяненко, Н. И. Теоретическое осмысление правового режима информации // Право. Журнал Высшей школы экономики. – 2008. – № 1. – С. 121 – 124.

179. Терещенко, Л. К. К вопросу о правовом режиме информации // Информационное право. – 2008. – № 1. – С. 20 – 27.

180. Устинович, Е. С. Зарубежный опыт законодательного регулирования анонимности в Интернете и судебная практика // Вопросы экономики и права. – 2016. – № 92. – С. 7 – 9.

181. Федотов, М. А. Конституционные ответы на вызовы киберпространства // Lex Russica. – 2016. – № 3. – С. 164 – 182.

182. Чеботарева, А. А. Научные подходы к определению понятия «информационная безопасность» // Информационное право. – 2011. – № 1 (24). – С. 3 – 5.

183. Чеботарева, А. А. Теоретико-правовые проблемы законодательного обеспечения информационных прав и свобод // Юридический мир. – 2015. – № 1. – С. 49 – 53.

184. Чеботарева, А. А. Эволюция института прав человека в условиях развития информационного общества // Государственная власть и местное самоуправление. – 2012. – № 6. – С. 27 – 33.

185. Чиркин, В. Е. К вопросу о ценности российской Конституции 1993 г. // Актуальные проблемы российского права. – 2013. – № 12. – С. 1517 – 1522.

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

187. Юсупов, Р. М. Информационная безопасность, кибербезопасность и смежные понятия: Cyber Security vs Информационной безопасности / Юсупов Р. М., Шишкин В. М. // Информационное противодействие угрозам терроризма. –2013. – № 21 (21). – С. 27 – 35.

188. Якушев, М. В. Международно-политические проблемы идентификации в интернете // Индекс безопасности. – 2013. – Т. 19. – № 1 (104). – С. 87 – 102.

Диссертации, авторефераты диссертаций

189. Анохин, П. В. Государственные интересы и права человека: соотношение и приоритеты : автореф. дисс. … канд. юрид. наук : 12.00.01 / Анохин Павел Викторович. – СПб., 2001. – 24 с.

190. Бабенко, А. Н. Правовые ценности и освоение их личностью : автореф. дис. ... д-ра юр. наук : 12.00.01 / Бабенко Андрей Николаевич. – М., 2002. – 46 с.

191. Буданов, С. А. Правовое обеспечение информационной безопасности несовершеннолетних: автореф. дис. ... канд. юрид. наук : 05.13.19 / Буданов Сергей Александрович. – Воронеж, 2006. – 24 с.

192. Виноградова, Н. В. Правовой механизм защиты информационных прав и свобод человека и гражданина в Российской Федерации : автореф. дис. ... канд. юрид. наук : 12.00.01 / Виноградова Наталья Владимировна. – Саратов, 2011. – 26 с.

193. Головин, С. Н. Правовое регулирование электронных форм организации социального государства и обеспечения информационной безопасности в

Российской Федерации : автореф. дис. ... д-ра юрид. наук : 05.26.02, 12.00.14 / Головин Сергей Николаевич. – М., 2006. – 54 с.

194. Грибанов, Д. В. Правовое регулирование кибернетического пространства как совокупности информационных отношений : дис. ... канд. юрид. наук : 12.00.01 / Грибанов Дмитрий Владимирович. – Екатеринбург, 2003. – 227 с.

195. Жаров, А. С. Конституционно-правовое регулирование информационной безопасности личности в Российской Федерации : автореф. дис. ... канд. юрид. наук : 12.00.01 / Жаров Анатолий Сергеевич. – М., 2006. – 24 с.

196. Журавлев, Ю. А. Правовые основы обеспечения информационной безопасности юридических лиц : автореф. дис. ... канд. юрид. наук : 12.00.14 / Журавлев Юрий Александрович. – М., 2009. – 28 с.

197. Калмыков, Д. А. Информационная безопасность: понятие, место в системе уголовного законодательства РФ, проблемы правовой охраны : автореф. дис. ... канд. юрид. наук : 12.00.08 / Калмыков Дмитрий Александрович. – Казань, 2005. – 24 с.

198. Коврижных, Л. А. Обеспечение информационной безопасности подготовки и проведения выборов (референдума) в условиях применения ГАС «Выборы» : дис. … канд. юрид. наук : 12.00.14 / Коврижных Любовь Александровна. – М., 2004. – 179 с.

199. Коровяковский, Д. Г. Правовое обеспечение информационной безопасности в налоговых органах Российской Федерации : дис. … канд. юрид. наук: 12.00.14 / Коровяковский Денис Геннадьевич. – М., 2004. – 191 с.

200. Кубышкин, А. В. Международно-правовые проблемы обеспечения информационной безопасности государства : автореф. дис. ... канд. юрид. наук : 12.00.10 / Кубышкин Алексей Викторович. – М., 2002. – 32 с.

201. Лопатин, В. Н. Информационная безопасность России: дисс… д-ра юрид. наук : 12.00.01 / Лопатин Владимир Николаевич. – М., 2003. – 433 с.

202. Михайлов, С. В. Правовые ценности: теоретико-правовой аспект : автореф. дис. ... канд. юр. наук : 12.00.01 / Михайлов Станислав Владимирович. – Волгоград, 2011. – 27 с.

203. Мурашко, Л. О. Аксиологическое измерение процесса правообразования: история и современность : дис. ... докт. юрид. наук : 12.00.01 / Мурашко Людмила Олеговна. – Москва, 2015. – 378 с.

204. Полякова, Т. А. Теоретико-правовой анализ законодательства в области обеспечения информационной безопасности Российской Федерации. Автореф. дис. ... канд. юрид. наук : 12.00.01 / Полякова Татьяна Анатольевна. – М., 2002. – 24 с.

205. Полякова, Т. А. Правовое обеспечение информационной безопасности при построении информационного общества в России : дисс… д-ра юрид. наук : 12.00.14 / Полякова Татьяна Анатольевна. – М., 2008. – 438 с.

206. Полянская, Н. А. Правовое регулирование информационной безопасности в чрезвычайных ситуациях : дис. ... канд. юрид. наук : 05.26.02 / Полянская Наталья Анатольевна – СПб., 2006. – 169 с.

207. Степанов, О. А. Теоретико-правовые основы безопасного функционирования и развития информационно-электронных систем: дис. … докт. юрид. наук : 12.00.01 / Степанов Олег Анатольевич. – М., 2005. – 365 с.

208. Стрельцов, А. А. Теоретические и методологические основы правового обеспечения информационной безопасности России: дис. … докт. юрид. наук : 05.13.19 / Стрельцов Анатолий Александрович. – М., 2004. – 371 с.

209. Тамодлин, А. А. Государственно-правовой механизм обеспечения информационной безопасности личности : автореф. дис. ... канд. юрид. наук : 12.00.01 / Тамодлин Александр Анатольевич. – Саратов, 2006. – 23 с.

210. Тедеев, А. А. Теоретические основы правового регулирования информационных отношений, формирующихся в процессе использования глобальных компьютерных сетей : автореферат дис. ...докт. юрид. наук : 12.00.14 / Тедеев Астамур Анатольевич. – М., 2007. – 58 с.

211. Федотова, О.А. Административная ответственность за правонарушения в сфере обеспечения информационной безопасности : дис. … канд. юрид. наук : 12.00.14 / Федотова Ольга Анатольевна. – М., 2003. – 195 с.

212. Шемякин, В. П. Информационная безопасность Российской Федерации в современных российских условиях : социолого-управленческие аспекты: автореф. дис. … канд. социол. наук : 22.00.08 / Шемякин Владимир Петрович. – М., 2004. – 29 с.

213. Янина, Е. В. Гражданско-правовое регулирование информационной безопасности : дис. … канд. юрид. наук : 12.00.14 / Янина Елена Владимировна. – М., 2004. – 166 с.

Электронные ресурсы

214. Акдениз, Я. Отчет. Свобода выражения мнения в Интернете. Исследование правовых норм и практик, связанных со свободой выражения мнения, свободным потоком информации и плюрализмом СМИ в Интернете в государствах-участниках ОБСЕ. – URL: http://www.osce.org/ru/fom/89063? download=true

215. Асфандиаров Б.М. Правовое регулирование использования Интернета в КНР и Вьетнаме // Современное право. – № 8. – 2005. – URL: https://www.sovremennoepravo.ru

216. Библиотека Документов АБИСС. – URL: http://www.abiss.ru/standards/ document_library/

217. Деактивация или удаление аккаунта. Справочный центр Facebook. – URL: https://www.facebook.com/help/250563911970368/?helpref=hc_fnav

218. Доверие СМИ и цензура. Левада-Центр. – URL: http://www.levada.ru/2016/11/18/doverie-smi-i-tsenzura/

219. Исследование обеспечения доступности интернет-ресурсов Рунета для людей с ограниченными возможностями здоровья (ОВЗ. – URL: https://perspektiva-inva.ru/userfiles/download/Accessibility_of_Runet_2013.pdf

220. Йоханнесбургские принципы «Национальная безопасность, свобода выражения мнения и доступ к информации». – URL: http://www.unesco.kz/ip/ countries/johannesburg_principles_rus.htm

221. Как запрет анонимайзеров отразится на пользователях интернета. – URL: https://www.kp.ru/daily/26707/3732941/

222. Наумов, В. Б. Нормативизм против цифрового либертарианства (Комментарий к трактату Дж. П. Барлоу «Экономика идей») // Русский журнал. – 1999. – URL: http://old.russ.ru/netcult/99-05-13/naumov.htm

223. Отчет Google о доступности сервисов и данных. – URL: https://www.google.com/transparencyreport/userdatarequests/

224. Правила регистрации доменных имен в доменах .RU и .РФ, утвержденные Координационныим центром национального домена сети Интернет. – URL: https://cctld.ru/files/pdf/docs/rules_ru-rf.pdf?v=30

225. Пункты коллективного доступа в интернет могут закрыться в России до конца года. Интерфакс. – URL: http://www.interfax-russia.ru/Moscow/main.asp?id=775760&p=17

Литература на иностранных языках

Международные и зарубежные правовые акты и иные документы

226. Act on the Protection of Privacy in Electronic Communications 516/2004. – URL: http://www.finlex.fi/en/laki/kaannokset/2004/en20040516.pdf

227. Affaire Brunet v. France. (Requête № 21010/10). – URL: http://hudoc.echr.coe.int/eng#{"itemid":["001-146389"]}

228. All Writs Act 1789. 28 U.S.C. §1651. – URL: https://www.law.cornell.edu/uscode/text/28/1651

229. American Civil Liberties Union v. Ashcroft. – URL: http://caselaw.findlaw.com/us-supreme-court/535/564.html

230. Americans with Disabilities Act. (42 U.S.C. 12101 et seq.). – URL: https://www.ada.gov/pubs/adastatute08.htm

231. Article 29 Working Party Statement on the Decision of the European Commission on the EU-U.S. Privacy Shield. – URL: http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/20160726_ wp29_wp_statement_eu_us_ privacy_shield_en.pdf

232. Associated Provincial Picture Houses Ltd. v. Wednesbury Corporation. [1948] 1 KB 223, [1947] EWCA Civ 1. – URL: http://www.bailii.org/ew/ cases/EWCA/Civ/1947/1.html

233. Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV (C-360/10). Judgment of the Court of Justice (Third Chamber) of 16 February 2012. – URL: http://curia.europa.eu/juris /liste.jsf?num=C-360%2F10

234. BVerfGE 34, 238. – URL: http://www.servat.unibe.ch/dfr/ bv034238. html#Rn002

235. 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

236. Council of Civil Service Unions v. the United Kingdom // URL: http://www.bailii.org/cgi-bin/format.cgi?doc=/eu/cases/ECHR/1987/34.html& query = (11603/85)

237. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. – URL: https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf

238. Democracy, Human Rights and the Rule of Law in the Information Society. Contribution by the Council of Europe to the 2nd Preparatory Committee for the World Summit on the Information Society. – URL:

http://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016805e14ad

239. Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information. – URL: http://ec.europa.eu/digital-agenda/en/european-legislation-reuse-public-sector-information

240. Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on Universal Service and Users' Rights Relating to Electronic Communications Networks and Services, Directive 2002/58/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector and Regulation (EC) № 2006/2004 on Cooperation Between National Authorities Responsible for the Enforcement of Consumer Protection Laws. – URL: http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32009L0136

241. Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data. – URL: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046

242. Equality Act 2010. – URL: http://www.legislation.gov.uk/ukpga/2010/15

243. European Security Strategy, December 2003. – URL: http://www.consilium.europa.eu/uedocs/cmsUpload/78367.pdf

244. Federal Communications Commission: Protecting and Promoting the Open Internet, Report and Order on Remand, Declaratory Ruling, and Order, FCC 15-24. – URL: https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-24A1.pdf

245. Federal Constitutional Court, Decision of Feb 27, 2008, 1 BvR 370/07, DuD 2008. – URL: http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html

246. Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers (FTC Report March 2012) 21-2. – URL: https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-

commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf

247. French Constitutional Council: Decision № 2009-580 of June 10th 2009 – Act Furthering the Diffusion and Protection of Creation on the Internet. – URL: http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank/download/2009-580DC-2009_580dc.pdf

248. French Constitutional Council: Décision № 2009-590 DC of October 22 2009 – Loi Relative à la Protection Pénale de la Propriété Littéraire et Artistique sur Internet. – URL: http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank_mm/decisions/ 2009590dc/2009590dc.pdf

249. Global Principles on National Security and the Right to Information ("THE TSHWANE PRINCIPLES") Finalized in Tshwane, South Africa Issued on 12 June 2013. – URL: http://fas.org/sgp/library/tshwane.pdf

250. Google France SARL and Google Inc. v Louis Vuitton Malletier SA (C-236/08), Google France SARL v Viaticum SA and Luteciel SARL (C-237/08) and Google France SARL v Centre National de Recherche en Relations Humaines (CNRRH) SARL and Others (C-238/08). Judgment of the Court of Justice (Grand Chamber) of 23 March 2010. – URL: http://curia.europa.eu/juris/liste.jsf?num=C-236/08

251. Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González (C-131/12). Judgment of the Court of Justice (Grand Chamber) of 13 May 2014. – URL: http://curia. europa.eu/juris/liste.jsf?num=C-131%2F12

252. Handyside v. United Kingdom (Application № 5493/72). – URL: http://hudoc.echr.coe.int/eng#{"dmdocnumber":["695376"],"itemid":["001-57499"]}

253. Headnotes to the Judgment of the First Senate of 27 February 2008. 1 BvR 370/07. – URL: http://www.bundesverfassungsgericht.de/SharedDocs/ Entscheidungen/EN/2008/02/rs20080227_1bvr037007en.html

254. Houchins v. KQED, Inc., 438 U.S. 1 (1978). – URL: http://caselaw.findlaw.com/us-supreme-court/438/1.html

255. In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by the Court. 1:15-mc-1902 (JO). – URL: https://www.documentcloud.org/documents/2728314-Orenstein-Order.html

256. International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World / SEAL of the President of the United States. Washington D.C., 2011. May. 26 p. – URL: https://info.publicintelligence.net/WH-InternationalCyberspace.pdf

257. Internet: case-law of the European Court of Human Rights. Updated: June 2015. – URL: http://www.echr.coe.int/Documents/Research_report_internet_ENG.pdf

258. ISO/IEC 27002: Code of Practice for Information Security Management 2005. Preview. – URL: https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-2:v1:en

259. L'Oréal SA and Others v eBay International AG and Others (C-324/09). Judgment of the Court of Justice (Grand Chamber) of 12 July 2011. – URL: http://curia.europa.eu/juris/liste.jsf?num=C-324/09

260. LOI n° 2011-267 du 14 mars 2011 d'Orientation et de Programmation pour la Performance de la Sécurité Intérieur. – URL: http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000023707312&fastPos=1&fastReqId=1447818568&categorieLien=id& oldAction=rechTexte

261. Maximillian Schrems v. Data Protection Commissioner, C-362/14 (CJEU October 6, 2015). – URL: http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf

262. McIntyre v. Ohio Elections Commission, 514 U.S. 334, 341-342 (1995). – URL: http://caselaw.findlaw.com/us-supreme-court/514/334.html

263. NAACP v. State of Alabama ex rel. Patterson, 357 U.S. 449, 462 (1958). – URL: http://caselaw.findlaw.com/us-supreme-court/357/449.html

264. Nation Security Strategy, February 2015. – URL: https://www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy.pdf

265. National Federation of the Blind (NFB), et al. v. Target Corporation. Disability Rights Advocates. – URL: http://dralegal.org/case/national-federation-of-the-blind-nfb-et-al-v-target-corporation/

266. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. – URL: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

267. Open Data Charter. – URL: https://www.gov.uk/government/publications/open-data-charter

268. Open Government Declaration. – URL: http://www.opengovpartnership.org/open-government-declaration

269. Open Government Directive. – URL: https://obamawhitehouse.archives.gov/open/documents/open-government-directive

270. Opinion of the European Data Protection Supervisor on the Current Negotiations by the European Union of an Anti-Counterfeiting Trade Agreement (ACTA) (2010/C 147/01). – URL: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2010/10-02-22_ACTA_EN.pdf

271. Other Requirements Relating to Uses and Disclosures of Protected Health Information. 45 CFR (n 50) s. 164.514(2)(i). – URL: https://www.gpo.gov/fdsys/pkg/CFR-2002-title45-vol1/pdf/CFR-2002-title45-vol1-sec164-514.pdf

272. Personal Information Protection Act 2011 (South Korea); unofficial English translation by Whon-il Park. – URL: http://koreanlii.or.kr/w/images/b/b9/PIPAct1601en.pdf

273. Personal Information Protection and Electronic Documents Act (PIPEDA). – URL: http://laws-lois.justice.gc.ca/PDF/P-8.6.pdf

274. Privacy Act of 1974. – URL: https://www.gpo.gov/fdsys/pkg/STATUTE-88/pdf/STATUTE-88-Pg1896.pdf

275. Recommendation № R(99)14 on Universal Community Service Concerning New Communication and Information Services and its Explanatory Memorandum. – URL: http://www.coe.int/t/dghl/standardsetting/media/doc/cm_EN.asp

276. 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). – URL: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

277. Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 Laying Down Measures Concerning Open Internet Access and Amending Directive 2002/22/EC on Universal Service and Users' Rights Relating to Electronic Communications Networks and Services and Regulation (EU) № 531/2012 on Roaming on Public Mobile Communications Networks within the Union. – URL: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32015R2120 &rid=2

278. Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye // Human Rights Council. 29th Session, Agenda item 3. – URL: http://ru.scribd.com/doc/266938105/A-HRC-29-32-AEV

279. Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue. – URL: http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

280. Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) (C-70/10). Judgment of the Court of Justice (Grand Chamber) of 24 November 2011. – URL: http://curia.europa.eu/juris/liste.jsf?num=c-70/10

281. Section 508 Amendment to the Rehabilitation Act of 1973 (29 U.S.C. § 794d). – URL: https://www.law.cornell.edu/uscode/text/29/794d

282. Statement on Statement of the WP29 on the Impact of the Development of Big Data on the Protection of Individuals with Regard to the Processing of Their Personal Data in the EU. Article 29 Data Protection Working Party, WP221. September 16, 2014. – URL: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp221_en.pdf

283. Telecommunications Act of 1996. – URL: https://www.fcc.gov/general /telecommunications-act-1996

284. Telekabel Wien GmbH v Constantin Film Verleih GmbH and Wega Filmproduktionsgesellschaft mbH (C-314/12). Judgment of the Court (Fourth Chamber) of 27 March 2014. – URL: http://curia.europa.eu/juris/liste.jsf?num=c-314/12

285. The Constitution of Greece. – URL: http://www.hellenicparliament.gr /UserFiles/f3c70a23-7696-49db-9148-f24dce6a27c8/001-156%20aggliko.pdf

286. The Instrument of Government. – URL: http://www.riksdagen.se/en/SysSite Assets/07.-dokument--lagar/the-instrument-of-government-2015.pdf/

287. The International Principles on the Application of Human Rights to Communications Surveillance. – URL: https://www.necessaryandproportionate.net

288. The ITU National Cybersecurity Strategy Guide. – URL: http://www.itu.int /ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurity StrategyGuide.pdf

289. Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community. – URL: http://www.consilium. europa.eu/uedocs/ cmsUpload/cg00014.en07.pdf

290. U.S.-EU Safe Harbor Framework Documents. – URL: http://webarchive. loc.gov/all/20150405033356/http%3A//export%2Egov/safeharbor/eu/eg_main_018493%2Easp

291. United Nations, Organization of American States, Organization for Security and Co-operation in Europe, African Commission on Human and Peoples' Rights. «Joint Declaration Concerning the Internet». – URL: http://www.oas.org/en/iachr/expression/showarticle.asp?artID=848

292. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001. – URL: https://epic.org/privacy/terrorism/hr3162.pdf

293. Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-collection and Online Monitoring Act (USA FREEDOM Act) 2015 г. – URL: http://legislink.org/us/pl-114-23 Pub.L. 114–23

294. UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH and Wega Filmproduktionsgesellschaft mbH (C-314/12). Judgment of the Court of Justice (Fourth Chamber), 27 March 2014. – URL: http://curia.europa.eu /juris/liste.jsf?num=c-314/12

295. Verizon Communications Inc. v. Federal Communications Commission. – URL: https://www.cadc.uscourts.gov/internet/opinions.nsf/ 5DFE38F28E7CAC9 185257C610074579E/$file/11-1355-1475317.pdf

Монографии

296. Barak, A. Proportionality. Constitutional Rights and their Limitations. – N.Y., 2012. – xxvi, 611 p.

297. Banakar, R. Normativity in Legal Sociology: Methodological Reflections on Law and Regulation in Late Modernity. – Springer International Publishing, 2015. – 292 p.

298. Castells, M. The Rise of the Network Society: The Information Age: Economy, Society and Culture. – Wiley, 2000. – 624 p.

299. Columbic, M. C. Fighting Terror Online: The Convergence of Security, Technology, and the Law. – New York: Springer New York, 2008. – XIV, 178 p.

300. Christou, G. Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy. – L: Palgrave Macmillan UK, 2016. – 222 p.

301. 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.

302. Etzioni, A. Security First. For a Muscular, Moral Foreign Policy. – New Haven (Ct.): Yale University Press, 2008. – 336 p.

303. Ferrarotti, F. The Myth of Inevitable Progress. Westport (Conn.) / F. Ferrarotti – L., 1985. – 208 p.

304. Grama, J. Legal Issues in Information Security. – Jones & Bartlett Publishers, 2010. – 526 p.

305. Gutwirth, S. Privacy and the Information Age. – Lanham, MD: Rowman & Littlefield Publishers, 2002. – 144 p.

306. Hicks, J. Wealth and Welfare, Collected Essays on Economic Theory. V. 1. – Oxford: Basil Blackwell. 1981. – 320 p.

307. Information Security and Privacy: a Practical Guide for Global Executives, Lawyers, and Technologists / Thomas J. Shaw, editor. – Chicago: American Bar Association, 2011. – 395 p.

308. Inglehart, R. Culture Shift in Advanced Industrial Society. – Princeton: Princeton University Press, 1990. – P. 151.

309. Klitou, D. Privacy-Invading Technologies and Privacy by Design: Safeguarding Privacy, Liberty and Security in the 21st. T.M.C. – Asser Press, 2014. – XIX, 338 p.

310. Lessig, L. Code: Version 2.0. – New York: Basic Books, 2006. – 410 p.

311. Mahoney, J. The Challenge of Human Rights: Origin, Development, and Significance. – Malden: Blackwell Publ., 2007. – 215 p.

312. Masuda, Y. The Information Society as Postindustrial Society. – Wash., 1983. – 171 p.

313. McLuhan, M., Powers, B. R. The Global Village: Transformations in Word Life of Media in 21st Century. – N.Y., Oxford, 1989. – XV. 220 p.

314. Michalowski S. German Constitutional Law: The Protection of Civil Liberties / Michalowski S., Woods L. – Sudbury, MA: Dartmouth Publishing Co Ltd. 1999. – 127 p.

315. Mironenko, O. Aviation Security and Protection of Individuals: Technologies and Legal Principles. – Oslo: University of Oslo, 2016. – 532 p.

316. Nelson, S. D. Information Security for Lawyers and Law Firms / Nelson S. D., Isom D. K., Simek J. W. – Chicago, IL: American Bar Association, 2006. – 424 p.

317. Nickel, J. W. Making Sense of Human Rights. – Oxford: Blackwell Publ., 2007. – 267 p.

318. Nozick, R. Anarchy, State, and Utopia. – Basic Books, 2013. – 592 p. (первое издание 1974 г.)

319. Price, M. E. Self-Regulation and the Internet / Price M. E., Verhulst S. G. – The Hague: Kluwer Law International, 2005. – 208 p.

320. Rothbard, M. N. Egalitarianism as a Revolt Against Nature and Other Essays / 2nd ed. – Auburn: The Ludwig von Mises Institute, 2000. – 324 p. (первое издание 1973 г.)

321. Steiner, H. J. International Human Rights in Context: Law, Politics, Morals / H. J. Steiner, Ph. Alston, R. Goodman. – New York: Oxford Univ. Press, 2008. – 149 p.

322. Toffler, A. The Adaptive Corporation. – New York: McGraw-Hill, 1985. – 217 p.

323. Tropina, T., Callanan, C. Self- and Co-regulation in Cybercrime, Cybersecurity and National Security. – Springer International Publishing, 2015. – 100 p.

324. Veit, D. Foundations of Digital Government / Veit D., Huntgeburth J. Springer Berlin Heidelberg, 2014. – 158 p.

325. Ziccardy, G. Resistance, Liberation Technology and Human Rights in the Digital. – Springer Netherlands Age. 2013. – 328 p.

Статьи

326. Attard, J. et al. A Systematic Review of Open Government Data Initiatives // Government Information Quarterly. – 2015. – V. 32. – P. 399–418.

327. Barlow, J. P. The Economy of Ideas: A Framework for Patents and Copyright in the Digital Age // Wired. – 2.03.1994.

328. Bamberger, K. A. Privacy on the Books and on the Ground / Bamberger K. A., Mulligan D. K. // Stanford Law Review. – 2011. – V. 63. – P. 247 – 315.

329. Bell, D. The Social Framework of Information Society // The Computer Age: A Twenty Year View / Ed. M. L. Dertonzos, L. Moses. – MA: MIT Press, 1980. – P. 163-212.

330. Bennahum, D. S. United Nodes of Internet: Are We Forming a Digital Nation? // Crypto Anarchy, Cyberstates, and Pirate Utopias / edited by P. Ludlow. – L. : MIT Press, 2001. – 485 p. – P. 39 – 45.

331. Birdsall, W. F. A Right to Communicate as an Open Work // Media Development. – 2006. – V. LIII. – P.41 – 47.

332. Boyle, J. Foucault In Cyberspace: Surveillance, Sovereignty, and Hard-Wired Censors. 1998. – URL: https://law.duke.edu/boylesite/foucault.htm

333. Caidi, N., Ross, A. Information Rights and National Security // Government Information Quarterly. – 2005. – V.22. – P. 663 – 684.

334. Cheung, A. S. Y. Re-personalizing Personal Data in the Cloud // Privasy and Legal Issues in Cloud Computing / Ed. by Cheung A. S. Y., Weber R. H. – Cheltenham: Edward Elgar Publishing, 2015. – P. 69 – 05.

335. Cohen, J. E. Cyberspace As/And Space // Columbia Law Review. – 2007. – V. 107. – P. 210 – 256.

336. Cohen, J. E. Information Rights and Intellectual Freedom // Ethics and the Internet / Ed. by A.Vedder. – Antwerp: Intersentia, 2001. – P. 11 – 32.

337. Cristoffersen, J. Human Rights and Balancing: The Principle of Proportionality // Research Handbook On Human Rights and Intellectual

Property / Ed. by Geiger C. Cheltenham. – UK: Edward Elgar Publishing, 2015. – 727 p.

338. D'Arcy, J. Direct Broadcast Satellites and the Right to Communicate // EBU Review. – 1969. – V. 118. – P. 14 – 18.

339. Ducoulombier, P. Conflicts between Fundamental Rights and the European Court of Human Rights: An Overview // Conflicts between Fundamental Rights / Ed. By Eva Brems. Intersentia, 2008. – XVIII + 690 p. – P. 217 – 247.

340. Frieden R. Network Neutrality in the EU, Canada and the U.S. // Intereconomics. – 2015. – V.50. – I.6. – P. 363 – 364.

341. Giblin, R. Evaluating Graduated Response // Columbia Journal of Law & the Arts. 2014. V. 37. P. 147-209.

342. Goldsmith, J. L. Against Cyberanarchy // University of Chicago Law Review. – 1998. – V. 65. – P. 1199 – 1250.

343. Graubart, J. What's News: A Progressive Framework for Evaluating the International Debate over the News // California Law Review. – 1989. – V. 77. – I. 3. – P. 629 – 663.

344. Greenleaf G. South Korea's Innovations in Data Privacy Principles: Asian Comparisons / Greenleaf G., Park W // Computer Law & Security Review. – 2014. – V. 30. – P. 492 – 505.

345. Hardy, I. T. The Proper Legal Regime for 'Cyberspace' // University of Pittsburgh Law Review. – 1994. – V. 55. – P. 993 – 1055.

346. Hilbert, M. The End Justifies the Definition: The Manifold Outlooks on the Digital Divide and Their Practical Usefulness for Policy-Making // Telecommunications Policy. – 2011. – № 35 (8). – P. 715 – 736.

347. Hughes, J. The Internet and the Persistence of Law // Boston College Law Review. – 2003. – V. 44. – P. 359 – 396.

348. Jansen, M. Big and Open Linked Data (BOLD) in Government: A Challenge to Transparency and Privacy? / Janssen M., van den Hoven J. // Government Information Quarterly. – 2015. – V. 32. – P. 363 – 368.

349. Jørgensen, R. F. Online Service Providers as Human Rights Arbiters / Jørgensen R. F., Pedersen A. M. // The Responsibilities of Online Service Providers / ed. by M. Taddeo, L. Floridi. – Springer International Publishing, 2017. – P.179 – 199.

350. Jackson, V. C. Ambivalent Resistanceand Comparative Constitutionalism: Opening Up the Conversation on 'Proportionality', Rights and Federalism // University of Pennsylvania Journal of Constitutional Law. – 1999. – V. 1. – P. 583 – 639.

351. Jackson, V. C. Being Proportional about Proportionality // Constitutional Commentary. – 2004. – V. 21. – № 3. – P. 803 – 860.

352. Johnson, D. R. Law and Borders – The Rise of Law in Cyberspace / Johnson D. R., Post D. // Crypto Anarchy, Cyberstates, and Pirate Utopias / ed. by Peter Ludlaw. Massachusetts Institute of Technology. – 2001. – P. 146 – 195. (Впервые опубликована в Stanford Law Review. – 1996. – V.48)

353. Kshetri, N. Big Data's Impact on Privacy, Security and Consumer Welfare / Telecommunications Policy. – 2014. – V. 38. – P. 1134 – 1145.

354. Leal, M. C. The EU Approach to Net Neutrality: Network Operators and Over-the-Top Players, Friends or Foes? // Computer Law & Security Review. – 2014. – V. 30. – 506 – 520.

355. Luiijf, H. Ten National Cyber Security Strategies: a Comparison / Luiijf H., Besseling K., Spoelstra M., de Graaf P. // Critical Information Infrastructure Security. 6th International Workshop, CRITIS 2011, Lucerne, Switzerland, September 8-9, 2011, Revised Selected Papers. – Berlin: Springer Berlin Heidelberg, 2011. – P. 1 – 17.

356. Mantelero, A. Data Protection in a Big Data Society. Ideas for a Future Regulation / Mantelero A., Vaciago G. // Digital Investigation. – 2015. – V. 15. – P 104 – 109.

357. Marshall, J. The Legal Recognition of Personality: Full-Face Veils and Permissible Choice // International Journal of Law in Context. – 2014. – V. 10. – P. 64 – 80.

358. McDonald, A.M. The Cost of Reading Privacy Policies / McDonald A. M., Cranor L. F. // I/S: A Journal of Law and Policy for the Information Society. – 2008. – V. 4:3. – P. 560.

359. Meulen, N.S. van der. You've Been Warned: Consumer Liability in Internet Banking Fraud // Computer Law & Security Review. – 2013. – V. 29. – P. 713 – 718.

360. Mitrakas, A. Information Security Regulation: Tomorrow Never Dies? // Securing Electronic Business Processes / S. Paulus, N. Pohlmann, H. Reimer (Editors). Vieweg. – 2006. – P. 433 – 438.

361. Netanel, N. W. Cyberspace Self-Governance: A Skeptical View from Liberal Democratic Theory // California Law Review. – 2000. – V.88. – P.488.

362. Odlyzko, A. Network Neutrality, Search Neutrality, and the Never-Ending Conflict between Efficiency and Fairness in Markets // Review of Network Economics. – 2009. – V. 8. – № 1. – P. 40 – 60.

363. Pagalo, U. Online Security and the Protection of Civil Rights: A Legal Overview // Philosophy & Technology. – 2013. – V. 26. – I. 4. – P. 381 – 395.

364. Papakonstantinou, A. The Constitutional Right of Participation in the Information Society // Revue of Public and Administrative Law. – 2006. – № 2. – P.233.

365. Perritt, H. H. Cyberspace Self-Government: Town Hall Democracy or Rediscovered Royalist? // Berkeley Technology Law Journal. – 1997. – V. 12. – P. 413 – 482.

366. Rees, C. Who Owns Our Data? / Computer Law & Security Review. – 2014. – V. 30. – P. 75 – 79.

367. Rees, C. Taking Sides on Technology Neutrality // SCRIPT-ed. – 2007. – V. 4. – I. 3. – P.263 – 284.

368. Reidenberg, J. R. Governing Networks and Rule-Making in Cyberspace // Emory Law Journal. – 1996. – V. 45. – P. 911 – 930.

369. Rubinstein, I. S. Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents / Rubinstein I. S., Nathaniel G. // Berkeley Technology Law Journal. – 2013. – V. 28. – P. 1333 – 1413.

370. Savirimuthu, J. Response to the Consultation by the Body of European Regulators in Electronic Communications BEREC on Net Neutrality Policy // European Journal for Law and Technology. – 2012. – V. 3. – №. 1. – URL: http://ejlt.org/article/view/134/214

371. Shin, D.-H. A Comparative Analysis of Net Neutrality: Insights Gained by Juxtaposing the U.S. and Korea // Telecommunications Policy. – 2014. – V. 38. – I. 11. – P.1117 – 1133.

372. Solms, R. From Information Security to Cyber Security / Solms R., Niekerk J. // Computers & Security. – 2013. – V. 38. – P. 97 – 102.

373. Sullivan, C. Digital Citizenship and the Right to Digital Identity under International Law // Computer Law & Security Review. – 2016. – V. 32. – P. 474 – 481.

374. Sullivan, C. Digital Identity, Privacy and the Right to Identity in the United States of America // Computer Law & Security Review. – 2013. – V. 29. – P. 348 – 358.

375. Sullivan, C. Digital Identity – The Legal Person? // Computer Law & Security Review. – 2009. – V. 25. – P. 227 – 236.

376. Sullivan, C. Digital Identity and French Personality Rights – A Way Forward in Recognising and Protecting an Individual's Rights in His/Her Digital Identity / Sullivan C., Stalla-Bourdillon S. // Computer Law & Security Review. – 2015. – V. 31. – P.268 – 279.

377. Trachtman, J. P. Cyberspace, Sovereignty, Jurisdiction and Modernism // Indiana Journal of Global Legal Studies. – 1998. – V. 5. – P.561 – 581.

378. Umesao, T. Information Industry Theory: Dawn of the Coming Era of the Ectodermal Industry / T. Umesao // Hoso Asahi. – 1963. – Jan. – P. 4 – 17.

379. Wiebe A. The New Fundamental Right to IT Security – First evaluation and comparative view at the U.S. // Datenschutz und Datensicherheit. – 2008. – V. 11. – P. 713 – 716.

380. Weber, R. H. Internet of Things: Privacy Issues Revisited // Computer Law & Security Review. – 2015. – V. 31. – P. 618 – 627.

381. Wu, T.S. Cyberspace Sovereignty? – The Internet and the International System. Harvard Journal of Law & Technology. – 1997. – V. 10. – P.647 – 666.

382. Wu, T. Network Neutrality, Broadband Discrimination // Journal of Telecommunications and Hight Technology Law. – 2003. – V. 2. – P. 141 – 142.

Электронные ресурсы

383. 8 Principles of Open Government Data. – URL: https://public.resource.org/8_principles.html

384. Barlow, J. P. A Declaration of the Independence of Cyberspace. – 1997. – URL: https://projects.eff.org/~barlow/Declaration-Final.html

385. Big data. – URL: http://www.gartner.com/it-glossary/big-data/

386. Big Data: What it is and why it matters. – URL: https://www.sas.com/en_us/insights/big-data/what-is-big-data.html

387. Castro, D. A Declaration of the Interdependence of Cyberspace. Computer World, February 8, 2013. – URL: http://www.computerworld.com/article/2494710/internet/a-declaration-of-the-interdependence-of-cyberspace.html

388. Cavoukian, A. Privacy by Design. The 7 Foundational Principles. – URL: https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf

389. Center for Copyright Information. Resources & FAQ. – URL: http://www.copyrightinformation.org/resources-faq/

390. Equality Act 2010. Banning Age Discrimination In Services. An Overview for Service Providers and Customers. – URL: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/ 85004/age-discrimination-ban.pdf

391. European Legislation on Reuse of Public Sector Information. – URL: http://ec.europa.eu/digital-agenda/en/european-legislation-reuse-public-sector-information

392. F.C.C. Invokes Internet Freedom While Trying to Kill It. The New York Time. – URL: https://www.nytimes.com/2017/04/29/opinion/sunday/fcc-invokes-internet-freedom-while-trying-to-kill-it.html

393. Facebook Blocks Pages Insulting Prophet Mohammed in Turkey. Mashable. – URL: http://mashable.com/2015/01/26/facebook-blocks-pages-turkey/#gLHKI9Kmkkq2

394. Federal Communications Commission. Preserving the Open Internet 2010. – URL: https://www.gpo.gov/fdsys/pkg/FR-2011-09-23/pdf/2011-24259.pdf

395. Federal Communications Commission. The Open Internet. 2015. – URL: https://www.fcc.gov/general/open-internet

396. Fiduciary Access to Digital Assets Act, Revised (2015). URL: http://www.uniformlaws.org/Act.aspx?title=Fiduciary%20Access%20to%20Digital%20Assets%20Act,%20Revised%20(2015)

397. FTC Report (March 2012). Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Business and Policy-makers. – URL: https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf

398. Grill L. Towards Digital Constitutionalism? Mapping Attempts to Craft an Internet Bill of Rights. Berkman Center Research Publication № 2015-15 / Grill L., Redeker D., Gasser U. – URL: http://ssrn.com/abstract=2687120

399. Gartner IT Glossary. – URL: http://www.gartner.com/it-glossary/internet-of-things/

400. HADOPI (Haute Autorité Pour la Diffusion des Œuvres et la Protection des Droits sur Internet). – URL: http://www.hadopi.fr/

401. JIS Web Content Accessibility Guideline. – URL: http://www.comm.twcu.ac.jp/~nabe/data/JIS-WAI/

402. How Companies Learn Your Secrets, The New York Times, Charles Duhigg, 16 February 2012. – URL: http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html

403. International Telecommunication Union, Digital Life. ITU Internet Report (2006). – URL: http://www.itu.int/osg/spu/publications/digitalife/docs/ digital-life-web.pdf

404. Knowledge Center – Digital Death // URL: http://www.digitaldeath.com/knowledgebase/state-laws-governing-digital-death/

405. Kosinski, M. Private Traits and Attributes are Predictable from Digital Records of Human Behavior / Kosinski M., Stillwell D., Graepel Th. – URL: http://www.pnas.org/content/early/2013/03/06/1218772110.full.pdf+html?with-ds=yes

406. Maisak, R. Accessibility of Thai University Websites: Awareness, Barriers and Drivers for Accessible Practice. 2015. – URL: http://ro.ecu.edu.au/theses/1715

407. Mell, P. The NIST Definition of Cloud Computing (Draft): Recommendations of the National Institute of Standards and Technology / Mell P., Grance T. – URL: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/ nistspecialpublication800-145.pdf

408. Moglen, E. Why Political Liberty Depends on Software Freedom More Than Ever. URL: https://www.softwarefreedom.org/events/2011/fosdem/moglen-fosdem-keynote.html

409. Mort Numérique ou Éternité Virtuelle : Que Deviennent vos Données Après la Mort ? // URL: https://www.cnil.fr/fr/mort-numerique-ou-eternite-virtuelle-que-deviennent-vos-donnees-apres-la-mort-0

410. New Digital Security Models. Discussion Paper. – URL: http://blog.privacytrust.eu/public/Reports/ NewDigitalSecurityModels.pdf

411. New Principles Preserve and Promote the Open and Interconnected Nature of Public Internet. FCC Adopts Policy Statement. 2005. – URL: https://apps.fcc.gov/edocs_public/attachmatch/DOC-260435A1.pdf

412. Resolution on Privacy by Design. 32nd International Conference of Data Protection and Privacy Commissioners (October 2010). – URL: https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_

413. Philippine Web Accessibility Group. – URL: http://www.pwag.org/

414. Saarenpää, A. The Importance of Information Security in Safeguarding Human and Fundamental Rights. – URL: http://www.juridicum.su.se/iri/e08/documentation/ahti_saarenpaa-information_security_and_human_rights-paper.pdf

415. Talk:Denmark: 3863 Sites on Censorship List, Feb 2008. – URL: https://wikileaks.org/wiki/Talk:Denmark:_3863_sites_on_censorship_list%2C_Feb_2008

416. Thai Web Content Accessibility Guidelines. – URL: http://thwcag.com/

417. The Role of Privacy by Design in Protecting Consumer Privacy. CTR. – URL:https://www.cdt.org/policy/role-privacy-design-protecting-consumer-privacy

418. The Court of Justice Declares the Data Retention Directive to be Invalid. – URL:https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf

419. The Internet of Things: Building Trust to Maximize Consumer (2014). – URL:Benefitshttps://www.ftc.gov/system/files/documents/public_statements/203011/140226cpetspeech.pdf

420. Warren, S.D. The Right to Privacy / Warren S. D., Brandeis L. D. // Harvard Law Review. – 1890. – V. 4. – № 5. – P. 193 – 220. – URL: https://www.ilrg.com/download/4harvlrev193.txt

421. Web Content Accessibility Guidelines (WCAG) 2.0. W3C Recommendation 11 December 2008. – URL: http://www.w3.org/TR/WCAG20/

422. WhatsApp Blocked in Brazil Again. Techcrunch. – URL: https://techcrunch.com/2016/07/19/whatsapp-blocked-in-brazil-again/

423. WVS Database. – URL:http://www.worldvaluessurvey.org/WVSContents.jsp

424. USTR Announces Conclusion of the Special 301 Out-of-Cycle Review for Taiwan. – URL: https://ustr.gov/about-us/policy-offices/press-office/press-releases/2009/january/ustr-announces-conclusion-special-301-out-cycle-re

425. Yahoo Scanning Order Unlikely to be Made Public: Sources. Reuters. – URL: http://www.reuters.com/article/us-yahoo-nsa-congress-idUSKCN12P2FL