Афат ФАРЗУЛЛАЕВА,
диссертант Института права
и прав человека НАНА

АКТУАЛЬНЫЕ ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ ПРАВОГО РЕГУЛИРОВАНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Важнейшим признаком глобального развития выступает информационное общество, фундамент которого составляют новейшие технологии и средства коммуникации (ИКТ). Являясь «специфической формой социальной организации, в которой новые технологии генерирования, обработки и передачи информации стали фундаментальными источниками производительности и власти» (4.с.29), информационное общество подвержено особо сложным угрозам, так как широкий спектр возможностей воздействия ИКТ весьма разнообразен и характеризуется высокой степенью опасности для всех сфер жизнедеятельности социума и функционирования государства. В этом контексте проблема совершенствования системы государственных гарантий конституционных прав человека и гражданина в информационной сфере приобретает особую актуальность.

Можно констатировать, что Интернет стал одним из факторов, активно влияющих на международную и национальную безопасность. Выступая главной и определяющей силой в развитии глобального общества, информационно-телекоммуникативные технологии проникают во все сферы жизнедеятельности национальных государств, способствуя объективно протекающим в мире процессам интеграции, взаимовлияния и взаимозасимости.

В этих условиях информационная безопасность выступает важнейшим направлением деятельности современного государства, требующим отлаженной системы конституционно-правового обеспечения.

Уровень развития информационно-коммуникационных технологий государства является признанным в международном сообществе важным индикатором оценки военно-политического и социально-экономического потенциала государства в целом (11). Азербайджан в данном случае не составляет исключения, так как «создание в стране благоприятных условий для развития информационного общества является одной из политических целей азербайджанского государства»(5).

Правовая основа функционирования единого информационного пространства Азербайджанской Республики способствует развитию информационного общества через: обеспечение конституционных прав человека и гражданина в информационной сфере; гармоничное развитие информационных ресурсов; широкий спектр предоставления информационных услуг; значительный объем средств информационного производства в стране. «В Азербайджанской Республике ведется целенаправленная деятельность в области информационных технологий, которая включена в приоритеты развития страны» (2).

Международное право устанавливает, что обеспечение права на адекватную информацию является условием эффективной реализации всех других прав и свобод граждан (10). На основе соблюдения конституционных норм о неприкосновенности частной жизни и конфиденциальности корреспонденции должна строиться вся система нормативного правового обеспечения безопасности в информационной сфере, поскольку права и свободы человека и гражданина имеют высший приоритет (1).

Закономерно, что концептуальные основы и принципы правового регулирования безопасности в информационной сфере, разработанные на международном уровне, в соответствие с пунктом 49 Резолюции 2200A (XXI) Генеральной Ассамблеи ООН (13) находят

в большей или меньшей степени отражение, как считает комиссия Европейского Союза по кибербезопасности, в национальном законодательстве всех экономически развитых государств (9). Важнейшая стратегическая задача обеспечения информационной безопасности предполагает состояние информационного пространства, в котором исключены возможности нарушения прав личности, общества и государства. Конституционно-правовая база должна создавать основания для реализации политики информационной безопасности всех трех объектов: государства, общества и личности «с учетом специфики требований каждого объекта к защите своих ресурсов» (8, p.126).

Экспоненциальное развитие информационно-коммуникационных технологий становится вызовом для национальной безопасности в контексте защиты триады интересов личности, общества и государства в информационной сфере. Неконтролируемые процессы в глобальных сетях и специфика политической борьбы в виртуальной сфере прямо и опосредованно воздействуют на обеспечение защиты национальных интересов. Этот вызов национальной безопасности крайне актуален в связи «со стихийным созданием открытых информационных сетей общего назначения, их подключением к международным телекоммуникационным сетям» (7. p.67). К примеру, об угрозе национальной безопасности любого государства свидетельствует тот факт, что разработка виртуальной международной сети, обеспечение работоспособности и совершенствование актуальных технологий контролируется Министерством обороны США (9, p.301).

Динамика и характер развития информационных технологий интенсифицируют новейшие вызовы и угрозы, направленные на личность как уязвимый субъект информационных отношений, поскольку достигает потенциально глобальной аудитории посредством пиринговых сетей и подключения к сети Интернет (9, p.73). Окинавская хартия глобального информационного общества декларирует: «информационно-коммуникационные технологии являются одним из наиболее важных факторов, влияющих на формирование обще-

ства XXI века. Их революционное воздействие касается образа жизни людей, их образования и работы, а также взаимодействия правительства и гражданского общества. Информационно-коммуникационные технологии быстро становятся жизненно важным стимулом развития мировой экономики. Перед всем миром открываются огромные возможности» (6).

Информационная безопасность как понятие отличается сложностью толкования, так как может характеризовать как любой вид информации как таковой, недопустимой в параметрах законодательства страны, например, пропаганда расовой дискриминации или атеизма, так и ее носителей, средств и способов передачи и т.п. Обеспечение информационной безопасности должно сопровождаться совершенствованием системы государственных гарантий конституционных прав человека и гражданина в информационной сфере. Недостаточная разработанность правового содержания информационной безопасности позволяет предложить рассматривать информационную безопасность в широком и узком толковании.

В узком смысле информационную безопасность, на наш взгляд, следует рассматривать как защищенность информации и поддерживающей ее инфраструктуры. В доктринальных документах международного права и теоретических исследованиях под широким понятием информационной безопасности постулируется защищенность и\или состояние защищенности жизненно важных интересов субъектов от внутренних и внешних угроз. В частности, в Законе Азербайджанской Республики о национальной безопасности (29 июня 2004) под национальными интересами в информационной безопасности понимается обеспечение таких конституционных прав граждан, как получение законным путем, передача, подготовка и распространение информации; защита и развитие информационных ресурсов; формирование информационного пространства и обеспечение его защищенности; интеграция в мировую систему связи и информации (3). Состояние защищенности национальных интересов Азербайджанской Республики в информационной безопасности определяется совокуп-

ностью сбалансированных интересов личности, общества и государства в информационной сфере. Обеспечение информационной безопасности предполагает защиту от информационной опасности независимости, суверенитета, территориальной целостности, конституционного строя азербайджанского государства, национальных интересов народа и страны, прав и интересов личности и общества и государства от внутренних и внешних угроз.

Само определение информационной безопасности указывает на многоаспектный характер проблемы, которая характеризуется различными категориями субъектов, вступающих в информационные отношения. С развитием процессов информатизации и возникновением в этой связи новых общественных отношений особую актуальность представляет адекватность правового регулирования с позиций конституционного обеспечения прав человека в информационных отношений. Сложность заключается в том, что в правовые отношения вступают различные категории субъектов, защиту информационной безопасности которых государство обязуется исполнять. Динамика и характер развития глобального информационного общества создают широкие возможности для интенсификации новейших вызовов и угроз, направленных именно наличность как уязвимый субъект информационных отношений.

Многогранность и сложность проблемы конституционно-правового обеспечения безопасности определяется такими видами угроз для информационной безопасности, как киберпреступления и кибертерроризм. Серьезную угрозу несет нелегальное приобретение платных информационных услуг, предоставляемых распределительной системой, обеспечивающей доступ к связанным между собой документам, расположенным на различных компьютерах, подключённых к Интернету рядом серверов(12),а также несанкционированное изменение маршрутов сообщений с целью их раскрытия или получения копий (14). Возможно также изменение сообщений, сознательное искажение информации, находящейся в Сети (15), что может способствовать совершению финансовых преступлений или раскрытию государственных тайн.

На стадии формирования находится новая область правового регулирования, предметом которой выступает интенсивно растущий электронный обмен данными, оказывающий в условиях глобализационной взаимозависимости исключительное влияние на экономику, особенно в ее инвестиционном и кредитном сегменте, борьбу с коррупцией, а также защиту прав человека и научно-техническое сотрудничество. Постоянно находящаяся в процессе модернизации мировая система информационных технологий выступает для национальных государств своеобразным триггером не только в интенсивным экономическом и военно-стратегическом развитии, но и в обеспечении защиты от возрастающих новых угроз для международной и национальной безопасности, связанных с противоправным использованием информационных сетей и систем.

В целом существующие правовые нормы в большей мере распространяются на правоотношения по поводу государственной тайны, в значительно меньшей степени на перечисленные выше угрозы. В результате нормативная правовая база в регулировании информационной безопасности характеризуется фрагментарностью, параллелизмом, ощутимыми пробелами, что во многом объясняется отсутствием юридических традиций в регулировании данной сферы, что вполне естественно, учитывая незначительный по историческим масштабам период функционирования ИКТ. Необходимо использовать как предшествующий опыт классической цивилистики, так и аналоги закрепления новых правовых отношений в информационной сфере национальных законодательствах.

Подводя определенные итоги, можно отметить, что конституционно-правовая ситуация в Азербайджанской Республики, характерной чертой которой является четко выраженная тенденция инкорпорации в современные тренды пространства международной юстиции, обусловливает потребность приведения норм национальной нормативно-правовой базы в соответствие с международными концепциями в сфере обеспечения информационной безопасности.В условиях глобального развития информационного общества

одна из главных задач конституционно-правового обеспечения информационной безопасности заключается в правовом регулировании информационного пространства, в котором будут исключены возможности нарушения прав личности, общества и государства.

Конституционно-правовому обеспечению информационной безопасности в сфере государственного управления отводится важнейшая роль в конструировании эффективной системы взаимоотношений между органами законодательной и исполнительной власти и органами местного самоуправления, хозяйствующими субъектами, общественными объединениями. С этих позиций конституционно-правовое обеспечения информационной безопасности должно отвечать возросшим общественным потребностям этих субъектов в информационной сфере и уже действующим международно-правовыми стандартам.

Сложный характер взаимосвязи нарастания информационных угроз и вызовов информационной безопасности в условиях *экспоненциального* развития ИКТ, с одной стороны, и конституционно-правовых возможностей противодействия данным угрозам, с другой, настоятельно требует не только соблюдения принципов сбалансированности, но и создания организационно-правовых основ системы социально-психологического и государственно-правового содействия позитивным и противодействия негативным тенденциям в обеспечении информационной безопасности.

ИСПОЛЬЗОВАННАЯ ЛИТЕРАТУРА

1. Всеобщая декларация прав человека http://www.un.org/ru/universal-declaration-human-rights/index
2. Государственная Программа Электронный Азербайджан. http://ict.az/ru/content/86.
3. Закон Азербайджанской Республики О национальной безопасности (29 июня 2004). http://republic.preslib.az/ru_d4-74.html

4. Кастельс*М.* Информационная эпоха: экономика, общество и культура. М.: ГУ ВШЭ, 2000.
5. Национальная стратегия по информационным и коммуникационным технологиям во имя развития Азербайджанской Республики. http://mincom.gov.az/upload/files/
6. Окинавская Хартия глобального информационного общества.года. www.unesco.org/new/fileadmin/MULTIMEDIA/FIEL
7. Castells, M. The Rise of the Network Society. Information Age, vol. 1; 2nd Edition with a New Preface edition. Wiley-Blackwell, 2009.
8. Chuck Easttom,Jeff Taylor. Computer Crime, Investigation, and the Law.International Cannel Center.Boston.2018.
9. Cybersecurity Strategy of the European Union:An Open, Safe and Secure Cyberspace. https://eeas.europa.eu/archives/docs/policies/ /eu-cyber-security/
10. Freedom of Information. https://www.un.org/ruleoflaw/thematic-areas/ /governance/freedom-of-information/
11. Information Security Indicators. /www.etsi.org/technologiesclusters/
12. Global Threat Intelligence Report 2017 - NTT DATA Services https://us.nttdata.com/en/-/media/nttdataamerica/files/americasd
13. International Covenant on Civil and Political Rights. Adopted and opened for signature, ratification and accession by General Assembly resolution 2200A (XXI)of 16 December 1966, entry into force 23 March 1976. http://www.un.org/en/development/desa/population
14. Takaaki Koyama, Bo Hu, Security Orchestration with a Global Threat Intelligence Platfor/www.ntt-review.jp/archive/ntttechnical.
15. Takaaki Koyama,Daiki Chiba. Cyberattack Countermeasure Technology to Support NTT's Security Business. www.ntt-review.jp/archive/ /ntttechnical.