УДК 341.231.14

ОТДЕЛЬНЫЕ АСПЕКТЫ ЗАЩИТЫ ПРАВ ЧЕЛОВЕКА ПРИ ИСПОЛЬЗОВАНИИ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

А.А. Григорьев[1], А.А. Охрименко[2]
[1] Государственная инспекция Республики Беларусь по электросвязи Министерства связи и информатизации Республики Беларусь (республиканское унитарное предприятие по надзору за электросвязью «БелГИЭ»), Минск;
[2] Белорусский государственный университет информатики и радиоэлектроники, Минск

Рассмотрены отдельные проблемные вопросы регламентации использования информационных технологий в контексте международно-правовой защиты прав человека, предложены отдельные меры для совершенствования данных отношений.

Возможность мобильной передачи данных в больших объемах, их ускоренной обработки, простота хранения и быстрота доступа к ним сделали привлекательными использование электронных средств и их интеграцию в систему государственного управления, в том числе при работе с обращениями граждан и юридических лиц, которая является приоритетным направлением развития демократического общества в современных условиях. Проблематика решаемых вопросов в данной сфере довольно обширна и не нашла должной проработки в теории права и не имеет широкой международно-правовой регламентации. Однако государства различных регионов постоянно усиливают внимание к тематике регулирования вопросов защиты прав человека при использовании современных информационных технологий и пытаются обеспечить их надлежащее правовое регулирование.

В этой связи необходимо учитывать, что стремительное развитие информационно-коммуникационных технологий (далее – ИКТ) приводит к постоянному противоборству различных взглядов на права основных субъектов права, использующих ИКТ, в целях обеспечения максимальной полноты их реализации либо обеспечения баланса интересов. При этом большая часть государств давно учитывает использование ИКТ в проведении новых видов военных операций, в том числе информационных войн, включая операции в контексте реализации прав человека и использования ИКТ.

Вместе с тем широкое распространение и активное использование населением, бизнес-структурами и государственными органами, межгосударственными организациями ИКТ и внедрение их в систему управления общественными отношениями, активная реализация программ ”электронного правительства“ в большой части государств, предусматривающая, в ряде случаев, постановку под контроль информационных систем наиболее важных элементов управления обществом, в том числе систем его жизнеобеспечения, заставляет по-новому рассмотреть вопросы правил регламентации системы управления, в том числе в части реализации прав различными субъектами права. Прежде всего, формирование данных систем и особенности их интеграции в общественные отношения влечет возникновение новых угроз для реализации прав, возможность использования прав и ресурсов в антисоциальных целях, а также для традиционных правил поддержания и развития, не только политических, но и экономическим и иным отношениям, обеспечения систем безопасности существования общества, в том числе при внедрении ”компьютерных вирусов“ в системы управления, жизнеобеспечения, обороны, общественной безопасности, энергетики, здравоохранения, транспорта, связи, использование недоработанных систем искусственного интеллекта, формирование планов, созда-

Библиотека БГУИР

ние иных условий и реализация правил ведения ”кибервойны“, в том числе международными террористическими группировками, возможность несанкционированного пользователями изменения данных, их уничтожение, влекут необходимость формирования новых способов защиты прав человека, государства и общества, которые в большинстве стран рассчитаны на традиционные системы управления с минимальным использованием технических и информационных средств.

В данных условиях особую важность приобретают точное и бесперебойное функционирование электронных систем в государственном управлении, в условиях применения оружия массового поражения, иных видов оружия, защита от террористических атак, массовых беспорядков, стихийных бедствий, недопустимость несанкционированного изменения данных. При этом особо значимым в демократическом обществе является исключение возможности причинения вреда гражданам, их здоровью, жизни, имуществу организаций (государства), нарушения прав, свобод и обязанностей граждан, организаций, государства, которые становятся существенно уязвимыми при недостатках защиты применяемых технических систем.

Многие государства, ставшие на путь широчайшего внедрения ИКТ, в систему государственного управления, стали зависимы от данных зачастую технологически несовершенных систем, которые в ряде случаев могут быть поставлены под контроль, в том числе злоумышленниками, что в свою очередь может повлечь не только нарушение прав человека, но также уничтожение и самоуничтожение государств. Не случайно, Сингапур, являющийся одним из лидеров внедрения ИКТ в систему государственного управления, в 2016 году начал принимать меры по ограничению их использования, в том числе путем отключения государственных служб от глобальной компьютерной сети Интернет. Принятие данных мер было вызвано признанием невозможности противостоять хакерским атакам и необходимостью защиты прав граждан, в том числе в части безопасности их персональных данных [1].

Представляется, что такие меры довольно радикальны. В этой связи полагаем оправданным, чтобы в настоящее время белорусским государственным органам использовать только программное обеспечение, оборудование, каналы связи (иную инфраструктуру), не допускающие хранение и передачу информации в ”облачные“ системы обработки информации за рубежом без согласия Республики Беларусь в лице уполномоченных государственных органов. Не должны использоваться системы, передающие персональные данные иностранным государствам (их государственным и иным организациям) без согласия Республики Беларусь и субъектов персональных данных. Аналогичный комплекс мер (хотя и не без недостатков, в том числе в части противодействия коррупционным схемам) начал применяться с 2015 года в Российской Федерации, которая в обозримом будущем планирует исключить импортную составляющую из системы ИКТ государственного управления, что может создать проблемы взаимодействия государства и граждан, использующих, преимущественно компьютерные программы основных мировых монополистов. Вместе с тем, данные меры не являются достаточными и принимаемые защитные меры правового, идеологического и технико-технологического характера должны носить комплексный характер, исходя из имеющихся угроз.

Их можно условно классифицировать как угрозы, представляющие опасность для международного сообщества, государства, общества в целом, включая негосударственные структуры коммерческого характера, отдельных личностей. Исходя из уровней данных угроз, необходимо предпринимать меры защиты на межгосударственном и национальном уровнях правовой регламентации общественных

Библиотека БГУИР

отношений, а также формировать единую общественную позицию, отвергающую противоправные деяния.

Однако формирование новых правовых норм в области регламентации общественных отношений затруднено в условиях конфликта интересов различных структур, в том числе государства, доминирования ряда бизнес структур в интенсивном формировании новых технологий и их внедрения в жизнь, и необходимости защиты прав личности в демократическом обществе.

Основные послевоенные права человека в условиях существования в демократическом обществе в концентрированном виде изложены во Всеобщей декларации прав человека (принята и провозглашена резолюцией 217 А (III) Генеральной Ассамблеи от 10 декабря 1948 г.) [2]. Они также отражены в различной степени и в ряде современных конституций, в том числе Российской Федерации и Республики Беларусь. Всеобщая декларация прав человека, хотя и относится к числу обычных норм международного права, не установила единых общеобязательных норм права и не содержат прямого указания на использование ИКТ в реализации норм права. Однако ее нормы национальные законодательства вправе конкретизировать и уточнять в зависимости от конкретных местных условий, что влечет дифференциацию подходов в реализации ее предписаний в условиях использования современных ИКТ, что в ряде случаев влечет несовпадение подходов к стандартным проблемным вопросов в ряде государств.

В связи с незаконным использованием ИКТ также был издан Указ Президента Республики Беларусь от 15 марта 2016 г. № 98 ”О совершенствовании порядка передачи сообщений электросвязи“, который призван создать систему противодействия нарушениям порядка пропуска трафика на сетях электросвязи, представляющую собой совокупность программно-технических средств, информационных ресурсов и информационных технологий, а также мер правового, организационно-технического и экономического характера, направленных на предупреждение, выявление и пресечение нарушений порядка пропуска голосовых и иных сообщений электросвязи [2]. В этой связи Указ запрещает пользователям услуг электросвязи общего пользования применять программные и технические средства, в совокупности используемые для преобразования протокола обмена данными, по которому передаются голосовые и иные сообщения электросвязи от вызывающего абонента, и передачи этих сообщений вызываемому абоненту с использованием абонентских номеров, не принадлежащих вызывающему абоненту. Данная мера позволяет устранить ряд правонарушений, в том числе в сфере незаконной конкуренции в сфере электросвязи и ограничить безлицензионное оказание услуг электросвязи. При этом впоследствии предполагается установить меры ответственности за несоблюдение данных предписаний. Ввиду ряда новаций названый Указ стал основой для правовой регламентации данных отношений, установив ряд норм, которые не встречались ранее в праве стран СНГ.

Следует обратить внимание на то, что установление специализированных мер ответственности, связанных с использованием ИКТ и регламентация отношений не ново. Например, в рамках Совета Европы еще 28 января 1981 г. подписана Конвенция о защите физических лиц при автоматизированной обработке персональных данных (ETS № 108) [3]. При этом до сих пор сохраняется актуальность норм данной Конвенции, закрепленных в статье 7, о защите персональных данных, хранящихся в автоматизированных файлах, данных, направленных на предотвращение их случайного или несанкционированного уничтожения или случайной потери, а также на предотвращение несанкционированного доступа, их изменения или распространения таких данных. Однако не все Члены Совета Европы реализуют в необходимой степени нормы данной Конвенции.

Библиотека БГУИР

Здесь важно отметить, что опасности могут подвергаться даже данные руководителей государств. Например, показательна утечка персональных данных лидеров некоторых государств мира, которые стали известны одному из ведомств Австралии в ходе осуществления его деятельности [4].

Следует подчеркнуть, что Конвенция носит региональный характер (Австралия в ней не участвует). При этом даже не все государства нашего региона, включая те страны, которые имеют тесные интеграционные связи, в том числе при электронном обмене персональными данными, например, при регламентации визовых вопросов в Союзном государстве, участвуют в ней (например, Беларусь не участвует в данной Конвенции, действующей для всех сопредельных с ней государств: Латвии – с 1 сентября 2001 г., Литвы – с 1 октября 2001 г., Польши – с 1 сентября 2002 г., России – с 1 сентября 2013 г., Украины – с 1 января 2011 г.). Представляется, что в целях усиления международно-правовой защиты в данной сфере целесообразны присоединение Беларуси к данной Конвенции, разработка и принятие универсального международного договора в рамках ООН, а для стран постсоветского пространства – также договоров в рамках СНГ, Евразийского экономического союза, Союзного государства с учетом специфики соответствующих интеграционных структур. Указанные структуры не могут быть в стороне от процессов, связанных с защитой персональных данных граждан соответствующих государств, при продолжении взаимного обмена информацией, требующегося в современном обществе.

При этом в связи с угрозами терроризма и иных правонарушений государства широко вмешиваются в сферу частной жизни граждан и ограничения их коммуникационных прав, что вызвало большой скандал в средствах массовой информации в связи с разоблачительными сообщениями бывшего агента АНБ Э.Сноудена, но не устранило соответствующих правил. Так же стало уже практически нормой информирование населения о том, что спецслужбы продолжают свою деятельность по получению предаваемых с помощью ИКТ сведений, не только рядовых граждан, но и глав государств. Боле того, несмотря на выигранные гражданами суды по защите своих персональных данных заключаются новые соглашения, направленные на сбор и обмен информации в данной сфере [5]. Однако все названные меры, включая ранее признанное Европейским судом недействительным соглашение ”Безопасная гавань“, по тотальному контролю ИКТ не позволили избежать наиболее крупных актов терроризма в современной Европе, и не привели к пресечению распространения в сети Интернет информации запрещенных террористических организаций, что вызывает обоснованные вопросы граждан об истинных целях принимаемых властями мер и их эффективности, которые по ряду причин, не попадают в поле зрения прессы и крупных международных правозащитных организаций.

Вместе с тем следует учитывать, что несмотря на опыт государственных структур и хакеров, частные коммерческие структуры, в том числе, занимающие значительную часть рынка также продолжают сбор сведений о деятельности граждан в области ИКТ и их персональных данных [6]. При этом взаимоотношения граждан и данных структур имеет различный результат, что не позволяет пока выработать универсальные применимые на практике правила в этой сфере. Известны случаи побед граждан и общественных структур в борьбе за свои права, например, выразившиеся в наложении штрафов на Facebook решениями судов Германии в 2012 и 2016 гг. в связи с тем, что компания не предоставляла достаточно четкие разъяснения о пределах распоряжаться данными, размещенными на страницах пользователей и Бельгии (2015 год) в связи с использованием компанией специального программного обеспечения, позволяющего отслеживать всех интернет-пользователей страны [7]. Также известны случаи призна-

Библиотека БГУИР

ния действий по сбору информации не противоречащими законодательству [8]. При этом также известны случаи побед компаний, например, по признанию судом Гамбурга права Facebook требовать от пользователей представления настоящими именами, в том числе без применения разрешенных гражданским правом ряда стран, в том числе Германии и Беларуси, псевдонимами (вымышленными именами) [9]. При этом в связи с растущим числом террористических актов в европейской прессе усиливается обсуждение предложений специализированных государственных служб о расширении сотрудничества с ними соответствующих коммерческих структур в части расширения возможностей государства по сбору и обработке полученной негосударственными структурами информации о жизни граждан.

Следует отметить, что отдельные государства начали всерьез регламентировать, отношения, возникающие в сети Интернет, в том числе для защиты прав граждан, предусмотренных ранее принятыми правовыми актами. Например, в мае 2011 года во Французский Уголовный кодекс была включена статья 226-4-1, которая устанавливает ответственность в форме лишения свободы на срок в один год и штрафа в 15 000 евро за использование в общественных интернет-отношениях имени третьего лица или отдельных идентификационных данных, чтобы нарушить спокойствие других или нанести ущерб чести [10]. Представляется, что такая мера была бы полезна и для права иных государств, в том числе в связи с набирающим распространение практики формирования ”виртуальных личностей“, не имеющих реального существования, но приобретающих права и обязанности вследствие использования вымышленных или чужих персональных данных, в том числе для совершения имущественных правонарушений.

В связи с глобализацией отношений, усилением миграции требует универсального правового решения вопрос рассмотрения электронных обращений граждан и организаций, осуществления в отношении них административных процедур, которые не во всех случаях могут быть идентифицированы при помощи электронной цифровой подписи (при этом данный вид идентификации также не является абсолютно надежным при появлении копий таких ключей). Данный вопрос может быть урегулирован нормами международных договоров. При этом в них следует особо оговорить правила, исключающие ответственность чиновников и иных лиц, рассматривающих обращения, при рассмотрении сообщений, сформированных виртуальными машинами, в том числе с использованием вымышленных или похищенных персональных данных, учитывая, что соответствующие права, свободы и обязанности при создании электронных обращений могут существовать только у реальных граждан и организаций, а не у виртуальных или иных механизмов и структур.

Вместе с тем представляется, что в настоящее время необходимо формирование универсальных правил поведения в сети Интернет с закреплением их на национальном и межгосударственных уровнях, основанных, в том числе на нормах морали и нравственности, которые бы одинаково применялись, как гражданам, так и к компаниям, в том числе транснациональным, так и в отношении государств, устанавливающих единые подходы к деятельности названных субъектов права. При формировании таких норм права следует помнить, что согласно пункту 2 статьи 29 Всеобщей декларации прав человека при осуществлении своих прав и свобод каждый человек должен подвергаться только таким ограничениям, какие установлены законом исключительно с целью обеспечения должного признания и уважения прав и свобод других и удовлетворения справедливых требований морали, общественного порядка и общего благосостояния в демократическом обществе. При этом согласно статье 30 названной Декларации ничто в ней не может быть истолковано, как предоставление какому-либо государству, группе лиц или отдельным лицам права заниматься какой-либо деятельностью или совершать

Библиотека БГУИР

действия, направленные к уничтожению прав и свобод, изложенных в данной Декларации [2].

Таким образом, представляется оправданным более активное сотрудничество государств, в том числе должностных лиц и научных работников, в различных областях знания, в целях уменьшения угроз обществу и государствам, международному сообществу в целом при использовании средств электронных коммуникаций. При этом учитывая актуальность рассматриваемых вопросов, передовой опыт Республики Беларусь в сфере регулирования ИКТ, представляется, что она может в инициировать предложения о заключении международных договоров, направленных на регламентацию защиты прав человека при использовании современных информационных технологий. Представляется, что это позволит занять Беларуси лидирующее положение в данной сфере (в условиях практически полного отсутствия специализированных договоров данной направленности) и будет способствовать формированию положительного образа нашей страны.

Список литературы

1. Лось, П. Сингапур капитулировал перед компьютерными мошенниками? / Лось Павел // [Электронный ресурс]. – 2016. – Режим доступа: http://dw.com/p/1J8Ox. Дата доступа:128.08.2016.

2. ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2016.

3. Конвенция о защите частных лиц в отношении автоматизированной обработки данных личного характера (ETS N 108). Заключена в г. Страсбурге 28.01.1981 г., (с изм. от 08.11.2001) // [Электронный ресурс]. – 2016. – Режим доступа: http://conventions.coe.int/Treaty/RUS/Treaties/html/108.htm. - Дата доступа: 08.08.2016.

4. Personal details of world leaders accidentally revealed by G20 organisers. URL: http://www.theguardian.com/world/2015/mar/30/personal-details-of-world-leaders-accidentally-revealed-by-g20-organisers. – Date of access: 21.01.2016.

5. Сотников, И. ЕС и США заключили новое соглашение об обмене данными // [Электронный ресурс]. – 2016. – Режим доступа: http://dw.com/p/1HoGH – Дата доступа: 08.08.2016.

6. Алимов, Т. Facebook уличили в слежке за всеми пользователями интернета // [Электронный ресурс]. – 2016. – Режим доступа: http://digital.rg.ru. – Дата доступа: 08.08.2016.

7. Ordnungsgeld: Facebook muss 100.000 Euro zahlen // [Электронный ресурс]. – 2016. – Режим доступа: http://www.vzbv.de/pressemitteilung/ordnungsgeld-facebook-muss-100000-euro-zahlen – Date of access: 08.08.2016.

8. Роскомнадзор не нашел в Windows 10 несоответствия закону об информации // [Электронный ресурс]. – 2016. – Режим доступа: http://ria.ru/technology/20150918/1259748462.html – Дата доступа: 08.08.2016.

9. Ромашенко, С. Facebook отбился от требований защитников частных данных // [Электронный ресурс]. – 2016. – Режим доступа: http://dw.com/p/1I6y9 – Дата доступа: 21.03.2016.

10. Code pénal // [Электронный ресурс]. – 2016. – Mode of access: https://www.legifrance.gouv.fr. – Date of access: 08.08.2016.

Библиотека БГУИР