Список использованных источников

1. Эрделевский, А.М. Компенсация морального вреда / А.М. Эрделевский. – М. : Юристъ, 1996. – 94 с.
2. Воронович, Т.В. Моральный вред: определение размера возмещения / Т.В. Воронович // Суд. весн. – 2000. – № 3. – С. 49–51.
3. Гацкий, М.А. Правовое регулирование и механизм определения размера компенсации морального вреда в гражданском праве : автореф. дис. ... канд. юрид. наук : 12.00.03 / М.А. Гацкий ; Моск. ун-т МВД России. – М., 2006. – 32 с.
4. Михно, Е.А. Компенсация морального вреда во внедоговорных обязательствах : дис. ... канд. юрид. наук : 12.00.03 / Е.А. Михно. – СПб., 1998. – 162 л.
5. Смиренская, Е.В. Компенсация морального вреда как деликтное обязательство : дис. ... канд. юрид. наук : 12.00.03 / Е.В. Смиренская. – Волгоград, 2000. – 219 л.
6. Эрделевский, А.М. Компенсация морального вреда: анализ и комментарий законодательства и судебной практики / А.М. Эрделевский. – 3-е изд., испр. и доп. – М. : ВолтерсКлувер. – 2004. – 304 с.
7. Компенсация морального вреда [Электронный ресурс]. – Режим доступа: http://pravovsem.by/kompensatsiya-moralnogo-vreda/. – Дата доступа: 15.03.2020.
8. Решение районного суда от 03 окт. 2016 года [Электронный ресурс] // КонсультантПлюс. Беларусь / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. – Минск, 2020.
9. Решение районного суда от 1 сент. 2016 года [Электронный ресурс] // КонсультантПлюс. Беларусь / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. – Минск, 2020.
10. Решение районного суда от 23 марта 2018 года [Электронный ресурс] // КонсультантПлюс. Беларусь / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. – Минск, 2020.
11. Решение районного суда от 30 ноября 2017 [Электронный ресурс] // КонсультантПлюс. Беларусь / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. – Минск, 2020.
12. Толстиков, Н. Компенсация морального вреда / Н. Толстиков // Законность. – 2006. – № 11. – С. 41–43.
13. Южанинова, А.Л. Судебно-психологическая экспертиза по делам о компенсации морального вреда / А.Л. Южанинова. – Саратов : Изд-во Сарат. акад. права, 2000. – 77 с.

Дата поступления в редакцию: 10.04.20

***S.J. Krasovsky**, Postgraduate student of Scientific and Pedagogical Faculty of the MIA of the Republic of Belarus*

COMPENSATION OF MORAL HARM AS A WAY OF CIVIL LEGAL PROTECTION OF INFORMATION ON THE PRIVATE LIFE OF AN INDIVIDUAL

Through a comparative legal analysis of national legislation and law enforcement practice, problems that arise when determining the amount of compensation for moral damage for the illegal collection or dissemination of information about the private lives of individuals are highlighted. Doctrinal approaches to the determination of criteria that allow a reasonable and fair determination of the amount of moral harm inflicted are considered. A methodology for calculating and establishing a basic amount of compensation for non-pecuniary damage for the illegal collection or dissemination of information about the private lives of individuals is proposed.

Keywords: moral harm, compensation for moral harm, civil law protection, private life.

УДК 342

***А.А. Подупейко**, кандидат юридических наук, доцент, профессор кафедры конституционного и международного права Академии МВД Республики Беларусь*
(email: podupeikoalex@mail.ru)

НЕКОТОРЫЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ ПРАВ И СВОБОД ЧЕЛОВЕКА И ГРАЖДАНИНА В СОВРЕМЕННЫХ УСЛОВИЯХ

Рассматриваются нормативные правовые акты, направленные на обеспечение и гарантированность конституционных прав и свобод человека и гражданина. Отмечается, что в современных условиях на эти процессы накладывает развитие IT-технологий, которые часто используются с целью нарушения прав и свобод личности.

Ключевые слова: права и свободы, Конституция Республики Беларусь, Концепция информационной безопасности, информационная сфера, киберпреступления, защита личной информации.

Проблема обеспечения прав и свобод человека и гражданина – одна из значимых в конституционном праве и всегда имеет особое значение для становления и развития демократического, социального и правового государства.

Конституция Республики Беларусь (далее – Конституция) одним из основных приоритетов государства определяет обеспечение прав и свобод граждан Республики Беларусь. В ст. 21 Основного Закона закреплено следующее: «Государство гарантирует права и свободы граждан Беларуси, закрепленные в Конституции, законах и предусмотренные международными обязательствами государства». Нормы, направленные на обеспечение прав и свобод личности, содержатся в ряде других статей Конституции Республики Беларусь (2, 7, 10, 59 и др.) и тем самым подчеркивается, что государство берет на себя обязанность обеспечить права человека в полном объеме.

Ряд положений Концепции национальной безопасности Республики Беларусь направлены непосредственно на усиление места и роли личности в обществе и государстве. Например, определяющим фактором на долгосрочную перспективу выступает всестороннее совершенствование механизмов защиты конституционных прав и свобод, законных интересов личности…; важнейшими направлениями выступают сохранение роли государства как гаранта безопасности личности, комплексное совершенствование процессов предупреждения и борьбы с преступностью, в первую очередь с коррупцией, терроризмом и экстремизмом во всех их проявлениях, сепаратизмом, расовой и религиозной нетерпимостью; постоянное повышение эффективности деятельности всех ветвей власти и системы государственного управления нацелено на максимальное удовлетворение общественных интересов и соблюдение прав личности и т. д.

В современных условиях важнейшей проблемой обеспечения конституционных прав и свобод человека и гражданина является, на наш взгляд, стремительное развитие информационно-коммуникационных технологий. Популярность сети Интернет, ее возможности в обмене информацией привели к существенному росту пользователей. В свою очередь, увеличение числа пользователей ведет к зависимости общества от информационных технологий. Повышается роль информационных технологий в реализации прав и свобод граждан, но и возрастает их уязвимость от различного рода информационных посягательств. Кроме того, возрастает потенциальная возможность для самих пользователей стать жертвой преступления с использованием информационных технологий, т. е. их права, свободы и законные интересы могут быть нарушены.

Следует отметить, что по данным МВД Республики Беларусь в 2019 г. зарегистрировано 10 539 (рост в 2,2 раза по сравнению...) преступлений с использованием IT-технологий. При этом свыше двух третьих (76,4 %) составили факты хищения с использование компьютерной техники. Количество таких преступлений увеличивается. Растет число преступлений против информационной безопасности, преобладают факты несанкционированного доступа к личным данным: взламывают аккаунты пользователей в социальных сетях, электронные кошельки и почтовые ящики, системы дистанционного банковского обслуживания. Прогнозируется, что развитие IT-отрасли, игорного бизнеса и финансово-кредитной системы будет способствовать сохранению тенденции увеличения числа преступлений по направлению деятельности в сфере высоких технологий (статистика УРПСВТ – mvd/gov/by). Такое положение чаще всего обусловлено отсутствием необходимых знаний об основах информационной безопасности либо просто пренебрежительным отношением к сохранности своей личной информации. В этих условиях важно и необходимо обеспечить информационную защиту пользователей, выявлять слабые места и блокировать своевременно киберугрозы.

На международном уровне подписан ряд документов, направленных на противодействие преступлениям в информационной сфере. Так, государства – члены Совета Европы подписали Конвенцию о преступности в сфере компьютерной информации (Будапешт, 23 ноября 2001 г.). Участники исходили из понимания глубоких перемен, вызванных внедрением цифровых технологий, объединением и продолжающейся глобализацией компьютерных сетей и необходимостью проведения в приоритетном порядке общей политики в сфере уголовного права, нацеленной на защиту общества от преступности в сфере компьютерной информации, в том числе путем принятия соответствующих законодательных актов и укрепления международного сотрудничества. Одной из важнейших целей подписания данной конвенции являлось обеспечение должного баланса между интересами поддержания правопорядка и уважением основополагающих прав человека.

В рамках СНГ наиболее важным является Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации, заключенное в г. Минске 1 июня 2001 г. В данном документе, в частности, устанавливаются следующие формы сотрудничества: обмен информацией; исполнение запросов; управление в области противодействия компьютерной преступности; сотрудничество в области осуществления кадровой политики; создание информационных систем; взаимная научно-исследовательская кооперация и др.

В целях обеспечения конституционных прав и свобод граждан в информационной сфере и информационной безопасности в целом в Республике Беларусь разработана и утверждена Концепция

информационной безопасности Республики Беларусь (далее – Концепция), принятая постановлением Совета Безопасности Республики Беларусь от 18 марта 2019 г. № 1. В ст. 9 отмечено, что основополагающим национальным интересом Республики Беларусь в информационной сфере с точки зрения гуманитарного аспекта является реализация конституционных прав граждан на получение, хранение и распространение полной, достоверной и своевременной информации, свободу мнений, убеждений и их свободного выражения, а также права на тайну личной жизни.

В содержание права на защиту от незаконного вмешательства в личную жизнь, в том числе от посягательств на тайну корреспонденции, телефонных и иных сообщений, на честь и достоинство (ст. 28 Конституции) включается представленная человеку и гарантированная государством возможность контролировать информацию о самом себе, препятствовать разглашению сведений личного, интимного характера.

Право на личную жизнь выражается в свободе общения между людьми на неформальной основе в семье, родственных и дружеских связей, интимных и других личных отношений, привязанностей, симпатий и антипатий. Образ мыслей, мировоззрение, увлечения и творчество также относится к проявлениям личной жизни. К личной жизни относятся тайна исповеди, медицинская тайна, тайна судебной защиты, предварительного следствия, усыновления, нотариальных действий.

В содержание свободы мнений и убеждений входит свобода мысли, слова и свобода печати, как одно из средств выражения свободы слова. Свобода слова представляет собой право каждого свободно выражать свои мысли перед другими как индивидуально, так и коллективно.

Конституционно-правовой гарантией свободы мнений и убеждений являются положения Конституции о том, что никто не может быть принужден к выражению своих убеждений или отказу от них, а также недопустимость цензуры (ст. 33).

Право на свободу, неприкосновенность и достоинство личности (ст. 25 Конституции) предусматривает возможность конкретного человека совершать действия по своему усмотрению, не подвергаясь при этом незаконному ограничению в своих правах от кого бы то ни было. Индивидуальная свобода тесно связана с личной неприкосновенностью. Неприкосновенность личности включает защиту от каких-либо противоправных препятствий располагать самим собой, своими поступками.

Согласно ст. 151 Гражданского кодекса Республики Беларусь «жизнь и здоровье, достоинство личности, личная неприкосновенность, честь и доброе имя, деловая репутация, неприкосновенность частной жизни, личная и семейная тайна, право свободного передвижения, выбора места пребывания и жительства, право на имя, право авторства, иные личные неимущественные права и другие нематериальные блага, принадлежащие гражданину от рождения или в силу акта законодательства, неотчуждаемы и непередаваемы иным способом. ... Нематериальные блага защищаются в соответствии с гражданским законодательством…».

Система обеспечения безопасности информационных ресурсов основана на стратегическом принципе соблюдения баланса свободы информации и права на тайну, гарантиях государства на распространение или предоставление общедоступной информации. Государство обеспечивает расширение безопасного доступа к информационным ресурсам добросовестных пользователей, развитие сервисов качественного и удобного предоставления информации, совершенствование систем ее данных (ст. 81 Концепции). Множественные угрозы и риски незаконного и необоснованного вмешательства в личную жизнь граждан, похищение персональных данных, компрометация реквизитов доступа и т. д. сужают личное пространство человека и нарушают его право на частную жизнь. Раскрытие личной информации стало неотъемлемым атрибутом корыстных преступлений и преступлений против личности.

Правонарушения, непосредственно связанные с использованием компьютерных технологий и сети Интернет, включающие в себя распространение вирусов, нелегальную загрузку файлов, кражу персональной информации (например, информации по банковским счетам) определяются как киберпреступления.

В соответствии с Концепцией преступлениями в информационной сфере являются предусмотренными Уголовным кодексом Республики Беларусь преступления против информационной безопасности (киберпреступления) и иные преступления, предметом или средством совершения которых являются информация, информационные системы и сети.

Киберпреступлениями считаются только те преступления, в которых ведущую роль играют компьютер и информационная сеть. Объектом посягательства выступает информация, обрабатываемая в виртуальном пространстве. Компьютер или мобильное средство связи с соответствующим программным обеспечением и выходом в сеть Интернет служат средствами или орудиями посягательства. Преступное завладение и использование правонарушителями компьютеров и мобильных

средств связи, их программных компонентов, имеющих доступ в сеть Интернет и сферу мобильных коммуникаций, проявляется как способ совершения преступлений.

По механизму и способам совершения преступления в сфере информационно-коммуникационных технологий имеют свою специфику и характеризуются высокой латентностью. По различным данным она составляет 85–90 %. Киберпреступность имеет социальную, политическую, финансово-экономическую, террористическую, сексуальную и др. направленность. Можно выделить следующие виды киберпреступлений: кибервымогательство, вишинг (или фишинг), кража персональных данных, шпионаж, спам, кража произведений, на которые распространяется авторское право, преступления на почве ненависти, домогательства, терроризм, кибербуллинг, груминг, распространение фотографий порнографического характера, наркотических средств, оружия и др. Необходимо отметить, что киберпреступность совершенствуется, и количество таких деяний постоянно растет. Объектами таких преступных посягательств становятся не только отдельные физические лица, но и крупные компании.

Более того, сегодня стало обыденным, когда человек сам сознательно размещает информацию о себе, личной жизни и другие персональные данные, выкладывает фото и т. д. в различные информационные сети. Это служит не только средством общения, но и часто способствует причинению вреда самой личности, например, передача сведений личного характера посторонним лицам, организациям, маркировка местонахождения и т. д., что приводит к совершению преступлений и нарушению прав и свобод самой личности.

В настоящее время к проблемным вопросам обеспечения прав и законных интересов личности можно и необходимо отнести следующие.

1. Развитие и использование информационных технологий осуществлялось значительно более быстрыми темпами, чем возможные механизмы контроля, защиты от киберпосягательств и, соответственно, обеспечения прав и свобод человека.

2. К основным угрозам, связанным с развитием информационных технологий, необходимо отнести и «облачную» обработку данных. Такая обработка данных включает систему обработки данных, при которых доступ к файлам, программному обеспечению и вычислительным сервисам производится через сеть Интернет, а не с локального персонального компьютера. С точки зрения выявления киберпреступлений «облачные» вычисления создают проблемы при их раскрытии и расследовании, поскольку в ряде случаев невозможно определить, на каком сервере и в какой стране находятся данные. Следовательно, возникают проблемы со своевременным установлением лиц, совершивших преступные деяния, получением доказательств, подтверждающих совершение правонарушения, и т. д.

3. Уязвимость персональной информации в социальных сетях.

4. Анонимность сети Интернет, уязвимость беспроводного доступа значительно затрудняют обнаружение преступников: для совершения преступления может использоваться цепочка серверов, преступления могут быть совершены путем выхода в сеть Интернет через точки общего доступа (например, интернет-кафе). Информационные технологии позволяют также взломать доступ в чужую беспроводную сеть Wi-Fi.

5. Раскрытие и расследование преступлений в глобальной компьютерной сети Интернет обычно требует быстрого анализа и сохранения электронных данных, которые очень уязвимы по своей природе и могут быть быстро уничтожены. При этом следует учитывать, что киберпреступность не знает границ, а деятельность правоохранителей по расследованию транснациональных преступлений в этом случае требует множества согласований и временных затрат.

6. Необходимо ускоренное совершенствование правового регулирования противодействия преступлениям в информационной сфере, а также выработка механизмов более тесного международного сотрудничества.

7. С учетом низкого уровня профилактики преступлений в информационной сфере, своевременное информирование граждан о различных видах преступлений в информационной сфере будет способствовать их сокращению.

8. Необходимость подготовки специалистов правоохранительных органов, владеющих в совершенстве информационно-коммуникационными технологиями, и постоянное повышение их квалификации и др.

В настоящее время растет количество электронных, информационных, коммуникационных систем, которые предоставляют различные возможности для вмешательства в личную жизнь человека и тем самым позволяют определенным структурам контролировать информацию о личности. К таковым можно отнести различные учеты в органах внутренних дел, Следственного комитета, налоговых органах, жилищно-коммунальном хозяйстве; сеть мобильных операторов и интернет-провайдеров; системы осуществления банковских транзакций, кредитные истории, учеты в поликлинике, исполнительно-распорядительных органах и др. При этом личность спокойно существует

во множестве этих электронных базах данных, не задумываясь о том, что практически утрачивает право на личную жизнь. В этом случае для государственных органов и организаций важно обеспечить сохранность и защиту информации о гражданах, а также гарантировать использование только в служебных целях.

В ряде случаев законодательство предусматривает обязательное предоставление персональных данных, не гарантируя при этом необходимую защиту. Например, в соответствии со ст. 68 Избирательного кодекса Республики Беларусь лицо, выдвинутое кандидатом в Президенты Республики Беларусь, депутаты, обязано при регистрации предоставить декларацию о доходах и имуществе, а также их супруги (супруга) и совершеннолетние близкие родственники, совместно с ним проживающие и ведущие общее хозяйство. Центральная комиссия, окружная, территориальная избирательная комиссия после регистрации кандидатов в Президенты Республики Беларусь, в депутаты направляют в печать для опубликования сообщение о регистрации кандидатов, а также сведений о доходах и имуществе или другим способом информируют об этом избирателей.

В процессе избирательной компании граждане часто указывают свои персональные данные: при сборе подписей в поддержку того или иного кандидата, при формировании инициативных групп по сбору подписей и др. В этом случае можно говорить, что граждане добровольно указывают необходимые данные, но механизм защиты не предусматривается в законодательстве. Необходимо также учитывать, что Закон «Об информации, информатизации и защите информации» устанавливает, что «сбор, обработка, хранение информации о частной жизни физического лица и персональных данных, а также пользование ими осуществляются с письменного согласия данного физического лица, если иное не установлено законодательными актами Республики Беларусь».

Несмотря на то что вопросам защиты и сохранности личной информации на уровне государства уделяется большое внимание и планируется принятие ряда нормативных правовых актов в этой сфере, самим пользователям также следует проявлять осторожность при общении в социальных сетях и проявлять бдительность, когда кто-либо требует указать личные сведения под любым предлогом.

Например, по рекомендациям Национального банка Республики Беларусь владельцы банковских платежных карточек должны сами для сохранности своих денежных средств соблюдать следующие правила: не хранить PIN-код рядом с карточкой или в легкодоступном месте, никому его не говорить; установить лимиты на снятие наличности и на безналичные расчеты; при возможности подключить услуги «SMS-оповещение» и 3D-secure; ограничить круг стран, в которых возможно совершение операций; при расчетах держать свою банковскую платежную карточку всегда на виду, а вне проведения расчетов не показывать ее номер и защитный код.

Законодательство по защите персональных данных личности должно совершенствоваться. При принятии закона о персональных данных, на наш взгляд, необходимо четко определить перечень персональных данных, предусмотреть механизмы их сохранности (защиты) и ответственности, прежде всего должностных лиц в случае несанкционированного распространения. Меры по защите персональных данных от разглашения должны быть приняты с момента, когда персональные данные были предоставлены физическим лицом.

Таким образом, эффективность противодействия преступлениям в информационной сфере и, соответственно, обеспечение прав и свобод личности требуют скоординированной деятельности правоохранительных органов, средств массовой информации, сетевых сообществ, самих граждан. В первую очередь видится необходимым своевременно информировать население о видах преступлений в информационной сфере, проводить воспитательно-профилактические мероприятия и просветительские кампании. На государственном уровне должна быть создана система противодействия компьютерным атакам и гибкая система ее применения, а также обеспечена сохранность сведений о гражданах и предусмотрены необходимые меры ответственности должностных лиц в случае нарушения законодательства об информационной безопасности.

Дата поступления в редакцию: 06.05.20

***A.A. Podupeyko**, Candidate of Juridical Sciences, Associate Professor, Professor of the Department of Constitutional and International Law of the Academy of the MIA of the Republic of Belarus*

SOME ASPECTS OF ENSURING HUMAN AND CIVIL RIGHTS AND FREEDOMS IN THE MODERN WORLD

The article discusses regulatory legal acts aimed at ensuring and guaranteeing the constitutional human and civil rights and freedoms. It is noted that in the modern world these processes are superimposed by the development of the IT and they are often used to violate the rights and freedoms of the individual.

Keywords: rights and freedoms, the Constitution of the Republic of Belarus, the Concept of information security, information sphere, cybercrime, protection of personal information.