ЧАСТЬ III. ИНСТИТУТ ЗАЩИТЫ И БЕСПРЕПЯТСТВЕННОЙ ТРАНСГРАНИЧНОЙ ПЕРЕДАЧИ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Защита персональных данных и их беспрепятственной трансграничной передачи как институт международного информационного права.

Ключевые слова: персональные данные – трансграничная передача – принципы защиты данных.

Закрепление права человека на приватность в универсальных и региональных международных договорах послужило основой для развития системы специальных норм и принципов, составляющих современный международно-правовой институт защиты персональных данных. Стимулом для становления и дальнейшего развития этого института международного права служат не только интересы международного сообщества в защите права человека на приватность, но в значительной степени также интересы государств в обеспечении ускорения темпов трансграничной передачи персонифицированной информации.

Последнее связано с тем фактом, что персонифицированная информация используется в различных сферах общественной жизни. Учитывая расширение международных информационных обменов, свободная передача информации, несмотря на границы, становится фактором, обусловливающим успех международного сотрудничества.

В то же время, создание национальными правительствами искусственных препятствий для свободного трансграничного оборота персонифицированной информацией негативно отражается на международном сотрудничестве во многих сферах. Понимание этой проблемы побудило международное сообщество к развитию сотрудничества с целью обеспечения ускорения темпов информационного обмена, которое привело к созданию совокупности международных норм и принципов, которые охватываются международно-правовым институтом защиты персональных данных и их беспрепятственной трансграничной передачи.

Международно-правовой институт защиты персональных данных и их беспрепятственной трансграничной передачи

содержит соответствующие нормы и принципы, направленные на обеспечение ускорения темпов передачи информации через границы. Однако, эта цель неразрывно связана с международно-правовой защитой права человека на приватность, что составляет стержневой элемент всего международно-правового механизма регулирования трансграничной передачи персонифицированной информации.

Закрепленные в различных международных документах и национальных законах принципы справедливого обращения с информацией персонального характера по содержанию практически совпадают, но в значительной степени отличаются по механизму их обеспечения. Информация, касающаяся индивидов (т.н. «субъектов данных»), должна:

— собираться с согласия субъектов данных или на других справедливых и законных основаниях;

— использоваться только для заранее определенных законных целей;

— быть адекватной, соответствующей и не чрезмерной по объему относительно целей ее обработки (под обработкой понимаются такие операции, как сбор, хранение, использование, распространение);

— быть достоверной и обновленной (актуализированной);

— доступной субъектам данных для ознакомления, исправления или возражения обработке;

— охраняться от несанкционированного доступа или повреждения;

— не сохраняться дольше, чем это необходимо для достижения целей сбора.

Законодательное урегулирование вопросов сбора, использования, хранения, распространения персональных данных призвано предоставить субъекту данных возможность контроля над этими операциями. Теряя контроль над своими данными, человек становится уязвимым для ряда рисков неправомерного вмешательства в частную жизнь, сферу своего окружения. Негативные социальные последствия такого явления были использованы для аргументации Федеральным Конституционным Судом Германии решения о признании неконституционным федерального закона о переписи населения в 1983 году:

«Если человек не в состоянии быть достаточно уверен в том, какая информация, касающаяся его в определенных аспектах социального окружения является известной, и если человек не в состоянии представить какую информацию о нем имеют потенциальные собеседники, его свобода планировать и выбирать свои собственные поступки в значительной мере ограничивается ...»

Среди проблем регулирования защиты персональных данных наиболее актуальным остается вопрос ограничения сбора данных. Активист правозащитной организации «Прайвеси Интернэшнл» Саймон Дэвис считает, что это является основным недостатком современного поколения нормативных актов в этой области, поскольку они оставляют вне поля зрения законодателя вопрос ограничения сбора персонифицированной информации, а сосредоточивается в основном на регулировании процедуры их сбора, хранения, использования и доступа[1]. Бывший Федеральный уполномоченный Канады по вопросам приватности и свободы информации, Дэвид Флехерти, также отмечает на примере Британской Колумбии, что на законодательном уровне интересы лица в защите от неограниченного сбора персонифицированной информации определены неадекватно, хотя этот вопрос является основным для защиты права человека на приватность[2].

Принципы защиты персональных данных закреплены в таких международно-правовых актах: Конвенции Совета Европы о защите лиц относительно автоматизированной обработки персональных данных 1981 года, «Руководящих принципах, регулирующих защиту приватности и трансграничные потоки персональных данных» Организации Экономического Сотрудничества и Развития 1980 г., «Руководящих принципах в отношении компьютеризированных баз персональных данных», принятых Генеральной Ассамблеей ООН в 1990 г.

1. Davies S. G. Re−Engineering the Right to Privacy : How Privacy Has Been Transformed from a Right to a Commodity // Technology and Privacy : The New Landscape; Ed. Philip E. Agre, Marc Rotenberg. − Cambridge : The MIT Press, 1997. − P. 150 − 152.

2. Flaherty D. H. Controlling Surveillance : Can Privacy Protection Be Made Effective? // Technology and Privacy : The New Landscape; Ed. Philip E. Agre, Marc Rotenberg. − Cambridge : The MIT Press, 1997. − P. 171.

Ранее упоминалось, что в указанных международно-правовых актах, нормативно воплощенная концепция компьютерной приватности, направлена на обеспечение беспрепятственной передачи данных и имеет основу в экономических и политических интересах государств. В Рекомендациях Совета ОЭСР о руководящих принципах, регулирующих защиту приватности и трансграничные потоки персональных данных, в частности, отмечается, что «...автоматизированная обработка и трансграничные потоки персональных данных порождают новые формы отношений между странами и требуют выработки соответствующих правил и практики; трансграничные потоки персональных данных способствуют экономическому и социальному развитию; внутреннее законодательство по защите приватности в отношении трансграничных потоков персональных данных может препятствовать таким трансграничным потокам...»[1].

Именно необходимость обеспечения интересов общего рынка является ключевой причиной введения общеевропейских стандартов защиты персональных данных в праве Европейского Союза. Подтверждение этому можно найти в тексте Директивы 95/46 СЕ Европейского Парламента и Совета «О защите физических лиц при автоматизированной обработке персональных данных и беспрепятственных потоков этих данных», где цель ее принятия определяется не только необходимостью защиты фундаментальных прав и свобод человека, но и потребностями свободной конкуренции и обеспечения деятельности государственных органов. Европейская Комиссия обращает внимание на важность именно последних интересов, которые вызвали принятие этого акта на уровне ЕС. Об этом говорится также в первом докладе по имплементации Директивы[2].

По делу *Фишера* Европейский Суд справедливости подтвердил, что принципы обращения с персональными данными, которые зафиксированы в Директиве 95/46, вследствие их вне-

1. Рекомендації Ради Організації Економічного Співробітництва і Розвитку стосовно Керівних принципів, що регулюють захист приватності і транскордонні потоки персональних даних // Пазюк А.В. Захист прав людини стосовно обробки персональних даних: міжнародні стандарти. – К. : МГО Прайвесі Юкрейн, 2000. – 88 с.
2. First Report On the Implementation of the Data Protection Directive (95/46/EC). – Brussels: Commision of the European Communities, 2003. – COM (2003) 265 final.

дрения в национальное законодательство государств-членов Евросоюза, являются *общими принципами права Сообщества*[1]. А в следующем деле Суд также указал, что нормы Директивы ЕС 95/46 имеют прямое действие, т.е. частное лицо может делать на них ссылку в национальных судах, чтобы исключить применение несовместимых с этими положениями норм внутригосударственного права[2].

В Декларации «О защите личных данных в глобальном мире: универсальное право, уважающее многообразие», принятой Ассамблеей уполномоченных по защите приватности, в Монтре, 14 – 16 сентября 2005 г., содержится призыв усилить международное признание принципов универсального характера, а также сотрудничество с правительственными органами и международными организациями для принятия универсальной конвенции для защиты приватности индивидов в отношении обработки персональных данных[3].

Обеспечение обязательств, предусмотренных Конвенцией 108, а также состояние нормативно-правовой базы Украины, которая не в полной мере обеспечивала защиту прав человека в соответствии со статьями 3, 32, 34 Конституции Украины в части защиты персональных данных, обусловило принятие Закона Украины «О защите персональных данных»[4]. До принятия этого Закона в стране действовало более двух десятков законов, регулирующих общественные отношения, связанные со сбором, хранением, использованием и распространением идентифицирующей личность информации, однако все они не соо-

1. ЕСС, дело *Королева против Министра сельского хозяйства, рыболовства и продовольствия, на стороне Тревор Роберт Фишер и Пенни Фишер (The Queen v Minister of Agriculture, Fisheries and Food, ex parte Trevor Robert Fisher and Penny Fisher)*, дело С-369/98, решение от 14 сентября 2000 г.

2. ЕСС, дело *Аудиторы и др. против Австрийской радиовещательной компании (Rechnungshof and Others v Osterreichischer Rundfunk)*, дела С-465/00, С-138/01, С-139/01, решение от 20 мая 2003 г.

3. Montreux Declaration 'The protection of personal dara and privacy in globalised world: a universal right respecting diversities'. [Electronic source]. – 2005. – Access mode : http://www.privacyconference2005.org/fileadmin/PDF/montreux_declaration_e.pdf

4. Закон Украины «О защите персональных данных» / / Ведомости Верховной Рады Украины от 27.08.2010 г. – № 34. – стр. 1188. – ст. 481.

тветствовали общеевропейским стандартам. При разработке Закона принимались во внимание Директива 95/46/ЕС Европейского парламента и Совета от 24 октября 1995 г. относительно защиты физических лиц в вопросах обработки персональных данных и свободного обращения этих данных и Директива 97/66/ЕС Европейского парламента и Совета от 15 декабря 1997 г. относительно обработки персональных данных и защиты приватности в телекоммуникационном секторе.

Так, согласно статье 2 Закона понятие «персональных данных» может касаться разнообразной идентифицирующей информации о лице, в частности, адреса, даты и места его рождения, образования, семейного и имущественного положения, национальности, вероисповедания, состояния здоровья. В соответствии с Законом собирать, обрабатывать, хранить и использовать персональные данные разрешено лишь после получения письменного (документированного) согласия лица. При этом распорядитель базы персональных данных может обрабатывать данные лишь с целью и в объеме, определенном договором, а в случае изменения цели обработки, требуется получение нового согласие лица на обработку его персональных данных с учетом измененной цели. Положениями статьи 8 указанного Закона предусмотрены такие права субъекта персональных данных:

а) знать о местонахождении базы персональных данных, которая содержит его персональные данные, и иметь к ней доступ;

б) получать информацию об условиях предоставления доступа к персональным данным;

в) предъявлять мотивируемое требование с запретом обработки своих персональных данных органами государственной власти, органами местного самоуправления при осуществлении их полномочий, предусмотренных законом;

г) на защиту своих персональных данных от незаконной обработки и случайной потери, уничтожения, повреждения в связи с умышленным сокрытием, непредставлением или несвоевременным их предоставлением, а также на защиту от предоставления сведений, которые являются недостоверными или позорят честь, достоинство и деловую репутацию физического лица;

д) прибегать к средствам правовой защиты в случае нарушения законодательства о защите персональных данных.

Благодаря принятию указанного Закона, основополагающие принципы защиты персональных данных, предусмотренные Конвенцией № 108, были внедрены во внутригосударственное законодательство Украины.

Выводы

Нормы и принципы защиты персональных данных и их беспрепятственной трансграничной передачи составляют международно-правовой институт. Целью принятия международно-правовых актов в этой сфере является защита права человека на справедливое обращение с его персональными данными, а также обеспечение свободной конкуренции в частном секторе и деятельности государственных органов.

Внедрение в национальную правовую систему международных норм и принципов защиты персональных данных способствует обеспечению реализации и защиты прав и свобод человека в информационной сфере, устраняет барьеры для трансграничного информационного обмена государственными органами и частным сектором.

3.2. Международно-правовое регулирование трансграничной передачи персональных данных.

Ключевые слова: ограничение трансграничного информационного обмена – принципы защиты данных – контролер файлов – надзорная инстанция по защите данных – внутренний аудит – эквивалентность защиты данных.

Проблема обеспечения беспрепятственного оборота персонифицированной информации между различными юрисдикциями начала возникать в 60-х годах двадцатого века. В пункте 18 Тегеранского воззвания и резолюции XI о правах человека и научно-техническом прогрессе от 12 мая 1968 г., принятых Международной конференцией по правам человека, выражена обеспокоенность возникшими рисками и угрозами правам и свободам человека, связанными с научными открытиями и техническим прогрессом. Генеральная Ассамблея ООН в 1968 г. в своей резолюции 2450 (XXIII) предложила Генеральному секретарю предпринять меры для изучения проблем в области прав человека, возникающих в связи с научно-техническим прогрессом. Указанным вопросам было уделено внимание в докладах Генерального секретаря «Применение электроники, которая может затронуть права человеческой личности, а также допустимые пределы такого применения электроники в демократическом обществе»[1], а также «Уважение к частной жизни человека и неприкосновенности и суверенитету наций в условиях прогресса техники звукозаписи и других средств»[2].

Несогласованность национальных подходов имела следствием появление запретов на передачу персональных данных через границы, что стало барьером для внешнеэкономических отношений партнеров по бизнесу в разных странах. В 1978 г. правительственный комитет Великой Британии докладывал об отказе со стороны властей Швеции разрешить экспорт персональных данных на основаниях, что национальное законодательство Великой Британии в то время не содержало положений, которые бы гарантировали защиту приватности персональ-

1. Документ E/CN.4/1142; Add 1-2. – 1973.
2. Документ E/CN.4/1116; Add 1-3. – 1974.

ных данных. В свою очередь, в декабре 1990 г., регистратор баз персональных данных Великой Британии запретил передачу данных в США, обосновав свое решение тем, что законодательство США не предоставляет адекватного уровня защиты в частном секторе экономики[1].

Решить эту проблему на национальном уровне было невозможно ввиду существующего различия в национальных подходах. Растущий трансграничный обмен информацией требовал принятия неотложных мер на международном уровне. Усилия, направленные на создание международных стандартов для согласования национальных положений по защите персональных данных, были осуществлены, в частности, такими международными организациями, как Совет Европы, Организация Экономического Сотрудничества и Развития (ОЭСР) и Организация Объединенных Наций. Начиная с 70-х г. двадцатого века, созданные этими организациями группы экспертов занимаются разработкой и совершенствованием стандартов в области защиты персональных данных с целью гармонизации национального законодательства, ликвидации несогласованных положений в вопросе передачи данных через границы.

В отличие от ОЭСР, организации созданной на основе общего экономического интереса государств-членов, основной задачей Совета Европы была и остается защита прав человека и основных свобод. На Совете Европы лежит политическая ответственность за развитие права на уважение частной жизни, которое гарантировано статьей 8 Европейской Конвенции о защите прав человека и основных свобод 1950 года, а также права на свободу информации, гарантированного статьей 10 этой же Конвенции.

1. Michael J. Privacy and Human Rights. – Paris : UNESCO, 1994. – P. 35.

3.2.1. Деятельность Совета Европы.

Комитет Совета Европы по правовым вопросам сформировал Комиссию экспертов по вопросам приватности и компьютерам в 1971 г. Первые шаги были сделаны в направлении установления специальных принципов и норм для предотвращения неправомерного сбора и обработки персональных данных в электронных базах данных. Комиссия подготовила проекты двух резолюций: одной — для применения в частном секторе (№ 22), второй — в публичном (№ 29). Комитет Министров утвердил первую в 1973 г., вторую — в 1974 г. При подготовке этих документов стало ясно, что для достижения эффективности в защите приватности необходимо укрепить существующие национальные нормы, используя международные инструменты. Такое же предложение прозвучало во время конференции Европейских министров юстиции в 1972 г., что была отмечено в ее резолюции № 3.

Комитет Совета Европы по правовым вопросам учел указанное предложение и начал разработку проекта будущей конвенции. В 1976 г. для этого была сформирована новая Комиссия экспертов по защите данных. Собиралась она четыре раза на пленарные заседания и подготовила проект в мае 1979 г., а окончательный вариант Конвенции — в апреле 1980 г. В том же году Парламентская Ассамблея Совета Европы приняла Рекомендацию № 890, в которой указывалось на необходимость эффективной защиты конфиденциальности персональных данных и было предложено включить соответствующее положение в текст Европейской Конвенции о защите прав человека и основных свобод.

Конвенция Совета Европы № 108 «О защите лиц относительно автоматизированной обработки персональных данных» была открыта для подписания 28 января 1981 и вступила в действие 1 октября 1985 г., после того, как пять государств-членов Совета Европы выразили свое желание быть связанными положениями Конвенции. Ими стали Швеция, Франция, Норвегия, Испания и ФРГ. Все эти страны, за исключением Испании, имели национальные акты о защите данных в момент ратификации.

Украина подписала Конвенцию в 2005 г., а ратифицировала в 2010 г. после принятия Закона о защите персональных данных от 1 июня 2010 г. № 2297−VI[1]. По состоянию на август 2012 г. участницами Конвенции являются 44 государства, еще две страны подписали ее, но не ратифицировали — Россия и Турция.

Конвенция о защите лиц относительно автоматизированной обработки персональных данных (Конвенция № 108) является одним из первых международных инструментов, который благодаря своему обязательному характеру закрепил минимальные стандарты в области защиты информационной приватности.

Конвенция состоит из семи глав, которые условно можно объединить в три части, содержащие общие принципы, специальные правила по передаче данных через границы и механизмы сотрудничества между государствами-участниками Конвенции.

Центральной частью Конвенции 108 является Глава 2, которая содержит основные принципы защиты персональных данных и составляет стержень этого документа. Это принципы качества данных, правомерности и законности обработки, ограничения целью использования, адекватности, точности, ограничения идентификации (статья 5) и прочее. Статья 6 Конвенции предусматривает особый режим обработки определенных категорий данных, в частности данных о расовой принадлежности, политических взглядах или религиозных либо других убеждениях, а также персональных данных, касающихся здоровья или половой жизни, криминальных поступков, — учитывая угрозу их использования для дискриминации индивидов по тому или иному признаку. Следует отметить, Конвенция лишь указывает на цель, которая должна быть достигнута путем применения этих принципов, но оставляет каждому государству-участнику право определять способ, которым они должны быть внедрены в национальное законодательство.

Статья 8 Конвенции предусматривает гарантии субъекту данных в отношении эффективной реализации права на при-

1. Закон Украины «О защите персональных данных» // Ведомости Верховной Рады Украины от 27.08.2010 г. − № 34. − стр. 1188. − ст. 481.

ватность персонифицированной информации, включая такие правовые возможности:

— быть осведомленным о существовании баз персональных данных, условиях их обработки, в том числе о личности «контролера файла»;

— получать подтверждение обработки и знакомиться с самой информацией, которая обрабатывается;

— требовать исправления или уничтожения персональных данных, обрабатываемых с нарушением указанных принципов и, наконец,

— обращаться за правовой защитой в случае нарушения соответствующих прав контролером файла.

Разработчики Конвенции внедрили в ее текст определенные стандарты, выработанные Европейской Комиссией и Судом по правам человека в части оценки правомерности применения государствами ограничений основных прав и свобод человека. В частности, статья 9 Конвенции позволяет отступление от провозглашенных принципов, а также ограничение соответствующих прав субъекта данных, если это предусматривается национальным законодательством и является в демократическом обществе мерой, направленной на: а) защиту государственной безопасности и общественного спокойствия, финансовых интересов государства или на борьбу с уголовными преступлениями; б) защиту субъекта данных или прав и свобод других лиц. Возможность применения ограничений предусматривается также для реализации других общественных интересов. Это касается использования персональных данных для целей статистики или научных исследований.

Предложенные в Главе 3 Конвенции № 108 требования касаются вопросов трансграничной передачи данных и призваны согласовать, сбалансировать одновременно существующие требования по беспрепятственной передаче персонифицированной информации и защиты приватности. Провозглашается, что трансграничные потоки данных между государствами-членами Конвенции не могут быть объектом любого специального контроля. Однако, в отношении определенных категорий персональных данных, которые имеют специальный режим в соответствии с национальным законодательством, Конвенция все же предусматривает возможность отступления от требований в

отношении беспрепятственной передачи данных в страны-участницы Конвенции, если только этой категории данных не предоставляется эквивалентная защита в этой стране. Такая же возможность ограничения трансграничной передачи данных остается в случае реэкспорта данных в третьи страны, не являющиеся участницами Конвенции.

Международно-правовой механизм взаимодействия между государствами-участниками в делах, касающихся отдельных индивидов, детализируется в четвертом разделе Конвенции № 108. С этой целью каждая страна обязуется назначить национальные органы, ответственные за международное сотрудничество в этой области. Лицам, проживающим на территории стран-участниц Конвенции, гарантируется возможность подать запрос в целях реализации своих прав через посредство таких органов. На практике, такими органами выступают национальные надзорные инстанции в области защиты персональных данных.

Взаимная помощь, которую члены Конвенции оказывают друг другу, в частности представление информации о своем законодательстве и административной практике в области защиты данных, сведений об особенностях автоматизированной обработки, а также помощь субъектам данных, проживающим за границей, предоставляются на безвозмездной основе. В пятой главе Конвенции выписан механизм конвенционального сотрудничества через создание Консультативного комитета, в состав которого входят представители и заместители представителей, назначенные государствами-членами Конвенции.

С принятием Конвенции № 108 в 1981 г. деятельность Совета Европы в этой области не остановилась. Проектная группа по защите данных (CJ–PD), в состав которой входят эксперты из каждого государства–члена Конвенции, подготовила серию секторальных рекомендаций, которые в значительной степени расширяют и конкретизируют провозглашенные в Конвенции принципы.

Поскольку условия и методы работы с данными зависят от назначения последних, то рекомендации рассчитаны на их применение в следующих секторах: здравоохранении[1], научно-

1. Recommendation № Rec(81)1 of the Committee of Ministers to member states on regulations for automated medical data banks (adopted by the

исследовательском[1], рекламном бизнесе[2], социального обеспечения[3], полицейском[4], трудоустройства[5], финансовом[6], телекоммуникационных услуг[7], в статистике[8], во время передачи госу-

Committee of Ministers on 23 January 1981 at the 328th meeting of the Ministers' Deputies). – Council of Europe, 1981; Recommendation № Rec(97)5 of the Committee of Ministers to member states on the protection of medical data (adopted by the Committee of Ministers on 13 February 1997 at the 584th meeting of the Ministers' Deputies). – Council of Europe, 1997

1. Recommendation № Rec(83)10 of the Committee of Ministers to member states on the protection of personal data used for scientific research and statistics (adopted by the Committee of Ministers on 23 September 1983 at the 362nd meeting of the Ministers' Deputies). – Council of Europe, 1983.
2. Recommendation № Rec(85)20 of the Committee of Ministers to member states on the protection of personal data used for the purposes of direct marketing (adopted by the Committee of Ministers on 25 October 1985 at the 389th meeting of the Ministers' Deputies). – Council of Europe, 1985.
3. Recommendation № Rec(86)1 of the Committee of Ministers to member states on the protection of personal data used for social security purposes (adopted by the Committee of Ministers on 23 January 1986 at the 392nd meeting of the Ministers' Deputies). – Council of Europe, 1986.
4. Recommendation № R (87) 15 of the Committee of Ministers to member states on the protection of personal data used in the police sector (adopted by the Committee of Ministers on 17 September 1987 at the 410th meeting of the Ministers' Deputies). – Council of Europe, 1987.
5. Recommendation № R (89) 2 of the Committee of Ministers to member states on the protection of personal data used for employment purposes (adopted by the Committee of Ministers on 18 January 1989 at the 423rd meeting of the Ministers' Deputies). – Council of Europe, 1989.
6. Recommendation № R (90) 19 of the Committee of Ministers to member states on the protection of personal data used for payment and related operations (adopted by the Committee of Ministers on 13 September 1990, at the 443rd meeting of the Ministers' Deputies). – Council of Europe, 1990.
7. Recommendation № R (95) 4 of the Committee of Ministers to member states on the protection of personal data collected and processed in the area of telecommunication services, with particular reference to telephone services (adopted by the Committee of Ministers on 7 February 1995 at the 528th meeting of the Ministers' Deputies). – Council of Europe, 1995.
8. Recommendation № R (97) 18 of the Committee of Ministers to member states on the protection of personal data collected and processed for statistical purposes (adopted by the Committee of Ministers on 30 September 1997 at the 602nd meeting of the Ministers' Deputies). – Council of Europe, 1997.

дарственным органам третьих стран[1], защиты приватности в Интернете[2], страхования[3] и в контексте профилирования[4].

Указанный способ адаптации принципов приватности в новых условиях работы с персональными данными оказался удачным вследствие того, что процедура принятия рекомендаций и их утверждения Комитетом Министров является более простой, нежели внесение изменений в текст Конвенции, что потребовало бы их ратификации каждым государством-участником Конвенции.

В 2001 г. был открыт для подписания Дополнительный протокол к Конвенции, который вступил в силу после 5 ратификаций в 2004 г.[5] Целью принятия этого документа является введение института надзорной инстанции по вопросам защиты персональных данных. В этом же протоколе установлено правило, принципиально меняющее подход к регулированию вопросов трансграничной передачи данных. Так, статья 12 Конвенции в действующей редакции устанавливает правило, согласно которому запрещается применение ограничений на экспорт данных в другую страну, которая предоставляет эквивалентную защиту.

1. Recommendation № R (91) 10 of the Committee of Ministers to member states on the communication to third parties of personal data held by public bodies (adopted by the Committee of Ministers on 9 September 1991 at the 461st meeting of the Ministers' Deputies). – Council of Europe, 1991.

2. Recommendation № Rec(99)5 of the Committee of Ministers to member states on the protection of privacy on the Internet (adopted by the Committee of Ministers on 23 February 1999 at the 660th meeting of the Ministers' Deputies). – Council of Europe, 1999.

3. Recommendation № Rec(2002)9 of the Committee of Ministers to member states on the protection of personal data collected and processed for insurance purposes (adopted by the Committee of Ministers on 18 September 2002 at the 808th meeting of the Ministers' Deputies). – Council of Europe, 2002.

4. Recommendation CM/Rec(2010)13 on the protection of individuals with regard to automatic processing of personal data in the context of profiling (adopted by the Committee of Ministers on 23 November 2010 at the 1099th meeting of the Ministers' Deputies). – Council of Europe, 2010.

5. По состоянию на август 2012 года Дополнительный протокол ратифицирован 33 странами, еще 9 стран подписали, но не ратифицировали. Украина подписала и ратифицировала его в 2010 году вместе с Конвенцией.

То есть, здесь не предполагается предъявление требований к странам-участницам Конвенции ограничивать экспорт персональных данных; решение этого вопроса остается на усмотрение государств. В то же время, статья 2 дополнительного протокола устанавливает правило, согласно которому передача персональных данных получателю, который находится под юрисдикцией государства, не являющегося участником Конвенции, допускается при условии, что государство обеспечивает адекватный уровень защиты для предлагаемой передачи данных. Аналогичный подход в регулировании трансграничных потоков данных был избран Европейским Союзом, что свидетельствует о стремлении европейских стран ввести общеевропейские стандарты в области защиты персональных данных на основе Конвенции Совета Европы № 108.

Этим также объясняется заинтересованность Европейского Союза в присоединении к Конвенции № 108. 22 июля 1997 г. Совет ЕС своим решением уполномочил Комиссию ЕС начать процесс переговоров с целью присоединения Европейского Сообщества к Конвенции № 108. В письме, датированном 22 октября 1997 г., Генеральный секретарь Европейской Комиссии сообщил Генеральному секретарю Совета Европы о таком стремлении Европейских Сообществ. Оно было реализовано путем внесения соответствующих изменений в Конвенцию в 1999 г.

Модернизация Конвенции

Процесс модернизации Конвенции № 108 начался по случаю 5–й годовщины провозглашения международного Дня защиты данных (28 января 2011 г.), когда Генеральный секретарь Совета Европы открыл консультации с общественностью, направленные на изучение проблем применения правительством, гражданским обществом и частным сектором. Модернизация и развитие Конвенции № 108 планируются в качестве приоритетной задачи Совета Европы в течение двухгодичного периода 2012–2013 гг.

Процесс пересмотра преследует две основные цели: 1) разобраться с проблемами защиты приватности, возникшими в результате применения новых ИКТ; 2) укрепить механизм выполнения Конвенции.

В процессе достижения указанных целей должны быть соблюдены такие условия: 1) сохранение общего технологически нейтрального характера Конвенции с применением механизмов конкретизации в дополнительных секторальных инструментах «мягкого» права (мнениях и рекомендациях); 2) обеспечение согласованности и совместимости с правовой основой Европейского Союза; 3) подтверждение потенциала Конвенции в качестве универсального стандарта и его открытого характера[1].

Суть Конвенции № 108 заключается в защите человеческого достоинства — человек не должен рассматриваться как объект, подвергающийся обработке «бездушной» машиной. Отсюда следует, что решения в отношении человека не могут приниматься исключительно на результатах, полученных при автоматизированной обработке персональных данных. Человек имеет право заявить о своих правах и опротестовать такое обращение с данными о его личности. Последние поправки к Конвенции вносились в 2001 году, а самой Конвенции более 30 лет. За это время появилось много новых угроз приватности, которые привнесены развитием информационных технологий. Особую актуальность этот вопрос приобретает при пользовании Интернетом, в частности такими распространенными услугами, как социальные сети, блоги и другие интерактивные сервисы на основе *Web 2.0*. Очень часто, забывая о личной безопасности, пользователи своими действиями позволяют не только собирать и распространять о них информацию, но и от их имени общаться с неопределенным кругом лиц, предлагая установления контактов. И все это делается с помощью программ, которые безоговорочно распоряжаются «цифровой идентичностью», персональными данными, в том числе интимными изображениями и предпочтениями (социальным «портретом») подписчиков.

Предложенные рабочей группой Совета Европы поправки к Конвенции предусматривают распространение действия принципов и соответственно защиты прав в отношении обработки

1. Modernisation of Convention 108 : new proposals. The Consultative Committee on the Convention for the Protection of Individuals with regard to Automatic Processing of Personal data [Electronic source]. – Strasbourg, 27 April 2012. – Access mode : http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T–PD–BUR_2012_01Rev2FIN_en.pdf.

персональных данных на виртуальное пространство. Это вселяет надежду, что в социальных сетях появится правовой механизм противодействия нарушениям на основании законодательства о защите персональных данных, в том числе посредством государственного надзорного органа.

Далее приводится ряд положений, предложенных для включения в Конвенцию. К ним относится новый принцип *прозрачности (транспарентноси) процедур обработки*. Этот принцип возлагает на обработчиков обязанность предоставления субъектам данных полной информации о наличии или отсутствии обработки, сообщение на их запрос всей информации, а также полных сведений о происхождении и источниках информации, логических алгоритмах, использованных для автоматизированной обработки, немедленного сообщения при выявленных нарушениях. Вводится так называемый *внутренний аудит*, который предусматривает анализ рисков до начала обработки данных, который должен осуществляться как собственным, так и привлеченным сертифицированным персоналом.

Требования конкретизации нормативных предписаний для достижения установленного международным правом *баланса между приватностью и свободой выражения* сформулированы рабочей группой в виде предложения определить конкретные случаи: какие права субъекта данных и в каком объеме подлежат ограничению, если обработка персональных данных осуществляется для передачи информации, представляющей общественный интерес, в целях информирования общественности, а также художественного или артистического выражения.

Предлагается включить новые определения — «получатель данных», а также «поставщик (провайдер) услуг», чтобы расширить субъектный состав правовых отношений по обработке данных и тем самым возложить обязанности на лиц, получивших доступ к данным, вышедшим за пределы личной или бытовой сфер, в том числе через социальные сети.

Дополнительные полномочия предлагается предоставить национальным органам, которые заботятся о защите прав субъектов данных, в частности *проводить расследование и вступать в судебные процедуры*. Кстати, распространенной в европейских странах, а также в Канаде, Австралии является модель, когда, кроме административного органа защиты персональных дан-

ных, создается также парламентский или общественный орган (уполномоченное лицо), что способствует защите прав граждан в сфере обработки персональных данных. Ведь главной целью закона является не защита персональных данных, а прежде всего прав граждан, чьи данные собираются и используются как государственными органами, так и экономическими субъектами частного сектора. Нередко такое уполномоченное лицо способствует также осуществлению права на доступ к публичной информации, что позволяет улучшить транспарентность государственного управления. Изменениями к Конвенции предлагается возложить на государства-участники обязанность создать надлежащие условия для деятельности таких органов.

В отношении защиты персональных данных в контексте трансграничной передачи за рамки юрисдикции государств-сторон Конвенции предлагается рассмотреть дополнительные правовые механизмы. В частности, речь может идти о применении стандартных договорных условий и обязательных корпоративных правил при условии, что надзорными органами в месте конечной обработки данных осуществляются адекватные и эффективные меры контроля. Адекватный уровень защиты может быть обеспечен:

а) внутренним законодательством этого государства или этой организации, в частности применимыми положениями международных договоров; или

б) стандартными либо специальными правовыми механизмами, такими как нормы договоров, корпоративных правил или аналогичные инструменты, которые являются обязательными, а средства правовой защиты являются доступными и эффективными для субъекта данных, который раскрывает или делает персональные данные доступными для получателей за пределами национальной юрисдикции.

3.2.2. Руководящие принципы ОЭСР.

Не меньший интерес в вопросе унификации правил обращения с персональными данными представляет деятельность другой влиятельной международной организации — Организации Экономического Сотрудничества и Развития (ОЕСР), которая начала исследование вопросов, связанных с трансграничными потоками данных, в 1969 году. Группа по вопросам применения компьютеров, а позже Комиссия по базам данных, проанализировала и подготовила доклады по различным аспектам, касающимся конфиденциальности персональных данных, в частности, цифрового формата информации, трансграничных потоков данных, управления информационной деятельностью.

В 1977 г. Комиссия ОЭСР по базам данных совместно с Комитетом экспертов Совета Европы в Вене провела международный симпозиум, где состоялся обмен мнениями и опытом людей, представлявших различные интересы, включая представителей политических и деловых кругов, пользователей международных сетей и заинтересованных международных организаций. Во время его проведения была выработана общая позиция относительно необходимости установления на международном уровне основополагающих принципов для регулирования международного обмена персональными данными.

В начале 1978 г. была сформирована новая группа по вопросам трансграничных потоков и защиты приватности во главе с председателем Австралийского комитета по правовой реформе, судьей Верховного Суда *М.Д. Керби*. Группа подготовила ряд докладов по ключевым проблемам обмена персональными данными и проанализировала различные подходы, которые выбрали страны-члены ОЭСР в законодательном регулировании этих вопросов[1].

Среди членов ОЭСР на момент принятия Руководящих принципов некоторые страны уже приняли нормативные акты, которые предусматривали соответствующее регулирование вопросов защиты информационной приватности. Так, например, Австрия, Канада, Дания, Франция, Люксембург, Норвегия,

1. Justice Michael D. Kirby. Transborder Data flows and the 'Basic Rules' of data privacy / / Stanford Journal of International Law. – 1980. – Vol. 16. – P. 27 – 66.

Швеция и США уже имели соответствующие законы, а Бельгия, Исландия, Нидерланды, Испания и Швейцария только подготовили законопроекты. Имеющиеся расхождения между странами касались сферы законодательного регулирования, а также внимания к определенным элементам защиты и контрольному механизму. В частности, отсутствовал консенсус в вопросах лицензирования и функционирования контрольного механизма — специального уполномоченного надзорного органа, категорий «уязвимых данных», понимания принципа прозрачности и индивидуального участия субъекта данных в процессах обработки данных. К этому же добавлялись традиционные различия между правовыми системами, из которых вытекали различные подходы к закреплению правил обращения с данными на регулятивном уровне. Указанные обстоятельства обусловили характер принятого документа.

Руководящие принципы, регулирующие защиту приватности и трансграничные потоки персональных данных — были приняты в виде рекомендации, устанавливающей обобщенные правила обращения с персональными данными. Руководящие принципы вступили в действие 23 сентября 1980 г. после их принятия как Рекомендации Совета ОЭСР на 523-м заседании[1].

Названные Рекомендации являются минимальными стандартами, которые созданы в результате консенсуса между позициями стран-членов ОЭСР в этом вопросе. Документ состоит из пяти частей. Первая содержит ряд дефиниций и определяет сферу применения Руководящих принципов. Вторая часть состоит из восьми основных положений (пункты 7 − 14), которые являются стержнем Руководящих принципов: 1) ограничение целью; 2) качество данных; 3) определение цели; 4) ограничение использования; 5) гарантии безопасности; 6) траснпарентность; 7) индивидуальное участие; 8) ответственность.

Часть 3 представляет принципы международного применения, связанные с взаимоотношениями стран-членов ОЭСР в этом вопросе, которые в тексте документа обозначаются как «свободный поток и законные ограничения».

1. Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transbordaer Flows of Personal data, adopted by the Council 23 September 1980. − Paris: OECD, 1981.

Руководящие принципы рекомендуют государствам-членам принять все разумные и необходимые меры для обеспечения ускорения темпов и безопасности трансграничных потоков персональных данных, включая транзит через территорию государства-члена ОЭСР. С этой целью государства должны воздерживаться от ограничений трансграничного обмена персональными данными с другим государством–членом, кроме случаев, когда последнее еще не в достаточной степени придерживается Руководящих принципов или когда реэкспорт таких данных нарушает его внутреннее законодательство по защите персональных данных. Как и Конвенция Совета Европы № 108, Руководящие принципы предусматривают возможность применения ограничений передачи данных по определенным категориям персональных данных, которые имеют специальный национальный правовой режим.

Вопросы внедрения основных принципов изложены в четвертой части. Здесь же конкретизируется, что принципы должны применяться на не дискриминационной основе. Внедрение принципов в национальную правовую систему требует установления законодательных, административных или иных процедур или институтов. Согласно Руководящим принципам, от государств потребуется: 1) принятия соответствующего внутреннего законодательства; 2) поощрение и поддержка саморегуляции; 3) обеспечение реализации индивидами своих прав; 4) введение санкций (мер ответственности) за нарушения изложенных принципов.

Пятая часть посвящена вопросам сотрудничества государств-членов, которое осуществляется через обмен информацией, устранение несовместимых национальных процедур для защиты персональных данных. Рекомендация не возлагает на страны-члены ОЭСР таких обязательств, как Конвенция Совета Европы № 108 на ее участников. Вместе с тем, Руководящие принципы ограничивают возможность применения исключений из установленных в них правил, которые определенным образом усиливают этот документ. К тому же Руководящие принципы распространяют свое действие не только на автоматизированные файлы данных, как Конвенция Совета Европы, но и на данные, обработка которых несет угрозу приватности и индивидуальным свободам независимо от методов и средств обраще-

ния с ними. Группа экспертов аргументировала такой подход попыткой избежать возможных пробелов в регулировании, причиной которых является проблема разграничения на техническом уровне процессов автоматизированной и неавтоматизированной обработки данных, в частности в «смешанных» системах.

Кроме того, Руководящие принципы более конкретно определяют права субъекта данных. Так, принцип 13 регламентирует «индивидуальное участие» субъекта данных в процессе доступа и содержит право на получение данных, которые его касаются. Субъекту данных дается право обжаловать любой отказ в предоставлении такой информации и получить обоснование такого отказа.

Ряд документов был принят ОЭСР в развитие провозглашенных принципов и их адаптации к требованиям времени. Вопрос свободной передачи данных получил свое дальнейшее развитие в Декларации о трансграничных потоках данных, которая была подготовлена Комитетом по информации, компьютерам и коммуникациям в марте и утверждена министрами стран–членов в апреле 1985 года[1]. Принимая Декларацию, страны–члены ОЭСР подтвердили свое стремление обеспечить свободный обмен информацией и разработать общие политические подходы к вопросам трансграничной передачи данных, в частности о передаче информации в торговой сфере, внутрикорпоративного обмена данными, компьютеризированных информационных услуг, научного и технологического обмена.

В ноябре 1992 г. Совет ОЭСР принял Рекомендацию о Руководящих принципах безопасности информационных систем[2]. Этот документ предусматривает принятие странами национальных положений для обеспечения целостности и конфиденциальности информационных систем и информации, которая в них обрабатывается, через принятие комплекса организационных и технических защитных мероприятий.

Вопросам гармонизации политики стран-членов ОЭСР в сфере применения криптографической защиты информации

1. Declaration on Transborder Data Flows – OECD. – Paris : OECD, 1985.

2. Recommendation of the Council concerning Guidelines for the Security of Information Systems – Paris : OECD, 1992.

посвящена Рекомендация о Руководящих принципах относительно политики в области криптографии, принятая в марте 1997 г.[1] Документ устанавливает принципы, направленные на регламентирование прав пользователей по выбору криптографических методов, свободного проектирования таких методов и средств, возможность взаимодействия информационных сетей, их значение для защиты персональных данных и устранения барьеров в международной торговле.

В октябре 1998 г. в Оттаве (Канада) на заседании министров 29 стран-членов ОЭСР, посвященном электронной коммерции, рассматривался вопрос защиты приватности в глобальных информационных сетях. Среди его результатов — принятие Декларации о защите приватности в глобальных сетях. В документе отмечается необходимость защиты приватности в глобальных информационных сетях для обеспечения уважения основных прав, построения доверия и предотвращения установления излишних ограничений для трансграничной передачи данных[2]. В Декларации отмечается важность принятия на национальном уровне комплексной программы мероприятий для обеспечения приватности, в частности предупреждение пользователей сетей о проблеме приватности в информационном пространстве, их обучение, содействие развитию технологий, гарантирующих конфиденциальность информационного обмена.

Развитие информационных технологий и глобализация информационных потоков требует пересмотра ранее установленных принципов с целью их адаптации к требованиям времени. Перед ОЭСР возникает необходимость пересмотреть ранее достигнутый между странами-членами консенсус по этому вопросу. Это непростая задача осложняется существующими различиями в стандартах между европейскими и неевропейскими странами-членами ОЭСР, прежде всего между Европейским Союзом и США.

1. Guidelines for Cryptography Policy. – Paris : OECD, 1997.
2. OECD Ministerial Declaration on Privacy on Global Networks // I–Ways. – 1998. – 4th Quarter. – P. 48.

3.2.3. Руководящие принципы ООН регламентации компьютеризированных картотек, содержащих данные личного характера.

Вопросам унификации правил обращения с персональными данными, посвятила свое внимание также Генеральная Ассамблея ООН, которая 14 декабря 1990 г. приняла Руководящие принципы регламентации компьютеризированных картотек, содержащих данные личного характера, рассчитанные на их внедрение государствами в свое национальное законодательство, а также на применение межправительственными организациями[1].

Руководящие принципы ООН воспроизводят основные общепризнанные принципы защиты приватности: принцип соблюдения законности и справедливости во время обработки; принцип точности (проверки соответствия и точности); принцип конкретизации цели обработки; принцип доступа к персональным данным, включая право на возражение против обработки, внесения изменений в персональные данные и восстановления нарушенных прав; принцип недискриминации и защиты уязвимых данных; полномочия делать исключения в интересах национальной безопасности, общественного порядка, здоровья или нравственности, а также защиты прав и свобод других лиц; принцип безопасности; принцип надзора и санкций, а также беспрепятственной трансграничной передачи между странами с эквивалентной защитой. Приведенные принципы, как это указывается в тексте документа, должны распространяться на все публичные и частные компьютеризированные файлы, а также могут применяться к картотекам, т.е. персональным данным, обрабатываемым вручную. Однако Руководящие принципы не признаются международным сообществом как универсальные международно-правовые стандарты, поскольку рассчитаны преимущественно на внутреннее применение органами Организации Объединенных Наций, а не для регулирования вопросов трансграничной передачи данных. Так что вопрос разработки универсальных международных договоренностей в этой сфере стоит крайне актуально.

1. Guidelines for the Regulation of Computerized Personal Data Files, adopted by General Assembly resolution 45/95 of 14 December 1990 // Human Rights : A Compilation of International Instruments, Vol. I (Second Part). – New York and Geneva : Centre for Human Rights, Geneva, 1994. – P. 540 – 543.

В связи с этим, для рассмотрения Комиссией международного права (КМП) были разработаны предложения, целью которых является выработка общих принципов сопутствующих защите личных данных. В документе КМП указывается: «Как явствует из общего анализа ныне действующих норм и правил, при различиях в подходе налицо общность интересов по ряду ключевых принципов. Прецеденты и другой соответствующий материал, включая международные договоры, законодательство, судебные решения и правовые акты, не имеющие обязательной силы, указывают на возможность выработки комплекса положений, дающих предметное описание вопросов, имеющих отношение к защите данных в свете современной практики. Такая работа была бы полезна для подготовки свода международно-приемлемых руководящих принципов оптимальной практики и помогла бы правительствам в разработке законодательства. Она также помогла бы частному сектору в разработке моделей саморегулирования. Выработка принципов защиты неприкосновенности частной жизни «третьего поколения» вполне согласовывалась бы с усиливающимися призывами к международной реакции в этой области. Хотя эта область имеет технический и специализированный характер, именно здесь практика государств еще не стала широкой или полностью сформировавшейся. Используя свои методы работы, Комиссия тем не менее могла бы выявить складывающиеся тенденции в юридической теории и практике, которые, скорее всего, сформируют глобальный правовой режим, который мог бы возникнуть в конечном итоге»[1].

Выводы

Закрепленные в различных международных документах и национальных законах принципы справедливого обращения с информацией персонального характера являются унифицированными по содержанию, но в значительной степени отличаются правовыми механизмами их обеспечения.

1. Защита личных данных при трансграничном перемещении информации [Электронный ресурс] / Организация Объединенных Наций. Доклад Комиссии международного права. Пятьдесят восьмая сессия. (A/61/10). Приложение Е. Нью-Йорк : ООН, 2006. – С. 504 – 535. – Режим доступа: http://untreaty.un.org/ilc/reports/2006/russian/annexes.pdf

Унификация и кодификация принципов защиты персональных данных позволит создать международно-правовой режим, обеспечивающий повсеместную защиту прав и свобод человека в этой сфере и беспрепятственную трансграничную передачу персональных данных.

3.3. Международно-правовое регулирование трансграничной передачи персональных данных в целях международной борьбы с преступностью.

3.3.1. Трансграничная передача персональных данных в секторе полиции.

Ключевые слова: полицейские файлы – транснациональная преступность – международная борьба с преступностью – Интерпол.

Международное сотрудничество в целях борьбы с преступностью невозможно без обмена информацией правоохранительными органами и, прежде всего, персональными данными в отношении лиц, имеющих отношение к преступлениям в качестве подозреваемых, обвиняемых, потерпевших или свидетелей.

Украина принимает активное участие в международном сотрудничестве в сфере борьбы с преступностью и как следствие, в международном информационном обмене в указанной сфере. Это сотрудничество осуществляется в рамках значительного количества международных договоров, предусматривающих использование доказательств в уголовном судопроизводстве[1].

Кроме того, Министерство внутренних дел Украины заключает межведомственные договора с полицейскими учреждениями других стран о сотрудничестве и координации совместных правоохранительных мероприятий, а количество указанных соглашений уже давно превысило полсотни[2].

1. См. : Збірник документів – Україна в міжнародно-правових відносинах. Боротьба із злочинністю та взаємна правова допомога. Книга 1. – К. : Юрінком, 1996. – 1085 с.
2. См. : Правові основи міжнародної діяльності МВС України (в двох томах). – К. : МВС України, 1997. – 720 с.

Украина вступила в Интерпол (Международную организацию уголовной полиции) в 1992 г. на 61-й сессии Генеральной Ассамблеи этой Организации[1]. В 1993 г. на Министерство внутренних дел Украины было возложено выполнение функций Национального центрального бюро Интерпола в Украине с целью координации деятельности правоохранительных органов Украины в борьбе с преступностью, имеющей транснациональный характер или выходящей за рамки страны, а также обеспечения взаимодействия с Генеральным секретариатом и соответствующими органами государств-членов Интерпола в борьбе с такими преступлениями[2].

В связи с этим актуальным является урегулирование вопросов обращения с персональными данными, которые собираются, используются и передаются в процессе международного обмена в рамках взаимодействия правоохранительных органов разных стран. В законодательстве Украины эти вопросы урегулированы на уровне подзаконных актов, которые не предусматривают эффективных гарантий защиты прав субъектов данных, что не соответствует требованиям международно-правовых актов в сфере защиты персональных данных[3]. А.С. Мацко справедливо отмечает, что «законодательные и другие меры, которые могут оказаться необходимыми для реализации положений договора во внутреннем правопорядке в большой мере отсутствуют»[4].

1 См. : Постановление Кабинета Министров Украины № 555 от 30.09.1992 «О вступлении Украины в Интерпол» [Электронный ресурс]. – Режим доступа : http://zakon2.rada.gov.ua/laws/show/555–92–%D0%BF.

2. См. : Постановление Кабинета Министров Украины №220 от 25.03.1993 г. «О Национальном центральном бюро Интерпола в Украине» // СП Украины. – 1994. – № 2. – ст. 25.

3. См. : Інструкція про порядок використання правоохоронними органами можливостей НЦБ Інтерполу в Україні у попередженні, розкритті та розслідуванні злочинів, затверджена спільним наказом МВС, СБУ, ДМС, Генпрокуратури, Держприкордону, ДПА України від 09.01.1997 № 3/1/2/5/2/2 // Офіційний вісник України. – 1997. – № 9. – Стор. 77.

4. Мацко А. С. Міжнародна діяльність Інтерполу по боротьбі з транснаціональною злочинністю. Наукова доповідь, 27.09.2012. – К .: КНУ ім. Т.Шевченка, ІМВ, «Міжнародно-правові читання», 2012. – С. 25.

В связи с этим требуется принятие закона, который внедрит международно-правовые принципы обращения с персональными данными в полицейском секторе во внутригосударственное законодательство Украины с целью защиты прав и свобод человека и обеспечения законности в деятельности правоохранительных органов.

Выводы

Международно-правовые документы в области защиты права на приватность относят полицейские файлы к категории сведений, обработка которых несет повышенный риск правам и свободам субъектов данных, что требует принятия дополнительных превентивных мер и гарантий соблюдения законности.

Сотрудничество в целях борьбы с транснациональной преступностью должно опираться на адаптированные для полицейского сектора международно-правовые принципы защиты персональных данных, соблюдение которых гарантируется государствами, принимающими участие в информационном обмене полицейскими файлами.

3.3.2. Правовые стандарты Совета Европы в отношении использования персональных данных в секторе полиции.

Ключевые слова: принцип контроля – уязвимость данных – классификация данных – принцип соразмерности – принцип законности – доступ к полицейским файлам.

Требования в отношении использования персональных данных в секторе полиции детализируются в Рекомендации № R (87) 15 Комитета Министров Совета Европы государствам-членам. Одобренная в 1987 г. на 410-й встрече заместителей министров, она не потеряла своей актуальности и на сегодняшний день. Сам текст Рекомендации содержит всего восемь принципов, развернутое толкование которых добавляется в пояснительной записке. Не случайно, что *первым принципом* является принцип контроля над обработкой персональных данных. Речь идет о внедрении механизма надзора за соблюдением полицией

установленных законом требований к обработке персонифицированной информации. Такой надзор должен осуществляться независимым органом государственной власти, деятельность которого не связана с работой полиции. На этот же надзорный орган может быть возложена функция регистрации баз данных персональных данных, обрабатываемых полицией. Процедура уведомления призвана, во-первых, ввести предварительный контроль над законностью обработки той или иной категории персональных данных, во-вторых, упростить процедуру и повысить эффективность надзора с помощью полученных при этом сведений об органе и его должностных лицах, ответственных за обработку и последующую передачу данных.

Учитывая все более активное внедрение новых информационных технологий в деятельность полиции, независимый надзорный орган должен выполнять важную роль предварительной проверки новых средств или устройств, которые используются для обработки персональных данных, а следовательно, могут нести большой риск для прав человека. В частности, речь может идти о технологии негласного слежения или сбора информации посредством сопоставления информации из различных баз данных, что является потенциально опасным.

Принцип 2 Рекомендации посвящается вопросам сбора сведений о лицах правоохранительными органами и адаптирует требования статьи 5 Конвенции Совета Европы 1981 г. к условиям деятельности полиции. В частности, очерчиваются границы сбора персональных данных. Они могут собираться для предотвращения реальной опасности или прекращения уголовного преступления. Для негласного сбора персональных данных, в том числе с использованием технических средств, в национальном законодательстве должны быть введены подробные правила и гарантии от злоупотреблений.

Отдельное внимание уделяется сбору так называемых «уязвимых данных», которые раскрывают расовую или этническую принадлежность, религиозные убеждения, политические взгляды или философские убеждения, сексуальное поведение и т.д. Их сбор разрешается только в случае «исключительной необходимости для целей особого запроса», т.е. когда существуют серьезные основания полагать, что преступление совершено или может быть совершенным лицом, которое может быть

идентифицировано с помощью таких уязвимых данных. При этом разъясняется, что сведения о сексуальном поведении могут собираться исключительно для расследования уже совершенных преступлений.

Чем больше уязвимость данных, тем больше риск нарушения прав лиц при обработке персональных данных, а значит, тем сильнее должны быть правовые гарантии защиты от нарушений. Оценка уязвимости данных, следовательно, и всех обстоятельств их обработки, должна предшествовать самой обработке. Этот принцип является определяющим для построения всей правовой конструкции отношений по обработке персональных данных в правоохранительной деятельности, поскольку напрямую связан с институциональным принципом соразмерности, который в сфере правоохранительной деятельности означает пропорциональность применяемых ограничений прав граждан степени общественной опасности преступления.

К процедуре хранения данных также предъявляются требования, которые предоставляют гарантии предотвращения нарушений прав лиц во время их дальнейшего использования. Эти же требования способствуют не только защите прав человека, но и улучшают эффективность правоохранительной деятельности, что подтверждается опытом европейских стран. В частности, *Принцип 3* Рекомендации предусматривает необходимость внедрения системы классификации данных, различая подтвержденные данные от и неподтвержденные, а также данные, полученные из надежных источников и ненадежных. Кстати, именно такая система классификации успешно используется уже не одно десятилетие в Соединенном Королевстве[1].

Кроме того, рекомендуется, чтобы данные о совершенных преступлениях или о подготовке к совершению преступлений хранились отдельно от данных, собранных для административных целей, в том числе об административных правонарушениях. Тем самым будет обеспечиваться, во-первых, принцип соб-

1. David Wolstenholme. Police Requirements and Practices in the Information Society. The case in the United Kingdom // ADACS/DGI (2000) 3 Sem. : Data protection in Police Sector. Council of Europe Regional Seminar under the activities for the development and consolidation of democratic stability. – Strasbourg, 2000.

людения цели сбора во время хранения, во-вторых, исключаться ошибочное их использования вследствие смешивания.

В этой связи интересным является прецедентное право Европейского Суда справедливости, в котором нашел свое отражение вышеуказанный принцип. Европейский Суд признал факт дискриминации в отношении лиц, не являющимися гражданами ФРГ, персональные данные которых собирались в целях статистического учета миграции населения. Одновременно, Суд установил нарушение принципов Директивы ЕС 95/46, поскольку объем собираемых данных, включавший сведения о привлечении лиц к уголовной ответственности, явно выходил за рамки статистической цели сбора данных[1].

Кроме того, Европейский Суд справедливости в своем прецедентном праве дал четкую установку, что следует разграничивать сбор и хранение персональных данных в рамках уголовного расследования и гражданско-правового судопроизводства. Оценивая конкурирующие интересы, такие как сохранение приватности при использовании программ файлового обмена (англ. *file exchange programme*) для противоправной передачи фонограмм пользователями Интернета и доступ к персональным данным указанных пользователей как потенциальных нарушителей прав интеллектуальной собственности в рамках гражданского судопроизводства, Европейский Суд призвал Мадридский коммерческий суд № 5, обратившийся за разъяснением, учесть при вынесении решения значимость каждого из фундаментальных прав и положения законодательства Евросоюза в отношении услуг информационного общества, гармонизации авторского права и обеспечения прав интеллектуальной собственности. Последнее предусматривает раскрытие персональных данных пользователей Интернета исключительно в контексте уголовного судопроизводства[2].

Четвертый принцип закрепляет требование использования данных, собранных в полицейских целях, т.е. для предотвращения или пресечения преступлений или поддержания обще-

1. См.: ЕСС, дело *Хюбер против ФРГ (Huber v. Federal Republic of Germany)*, дело C-524/06, решение от 16 декабря 2008 г.

2. *Музыкальный проюдюсер [Испании] «Промусикай» против Телефоника САУ (Productores de Musica de Espaca (Promusicae) v. Telefynica de Espaca SAU)*, дело C-275/06, решение от 29 января 2008 г.

ственного порядка, только в этих целях. Это не означает, что данные из полицейских файлов не могут передаваться другим органам, поскольку указанную функцию определенным образом выполняют также другие государственные органы и учреждения. Случаи, которые составляют не правило, а исключение из него, конкретизируются в *принципе 5.*

Одним из требований для легитимной передачи данных полицейской организацией другим органам и учреждениям является наличие процедуры санкционирования, во время которой уполномоченным органом проверяется ее целесообразность и законность.

При отсутствии такой санкции передача разрешается, если это необходимо для выполнения государственным органом возложенных на него по закону функций в интересах лица, которого касается информация (субъекта данных), а также когда это необходимо для предотвращения серьезной реальной опасности (нависшей угрозы).

Международная передача полицейских данных разрешается только между органами полиции. Правовым основанием для таких передач является наличие соответствующих договоренностей между государствами. Речь также идет о соответствии национального законодательства получателя данных принципам, изложенным в Рекомендациях. Обеспечение этого требования возлагается на полицейское учреждение, которое передает данные в страну, в которой уровень правовой защиты не является адекватным. При этом предусматривается возможность применения оговорок со стороны передающей стороны по процедуре обработки и использования персональных данных получателем для удовлетворения информационного запроса.

Важной гарантией законности обработки персональных данных в целях борьбы с преступностью, восстановления ограниченных и защиты нарушенных прав граждан в правоохранительной деятельности является, во-первых, право на ознакомление с полицейскими файлами заинтересованных лиц, во-вторых, право на исправление неточных данных, в-третьих, право на обжалование неправомерных действий. Эти вопросы регламентируются в *шестом принципе.*

Не требует дополнительных пояснений утверждение, что сбор, систематизация и анализ сведений о лицах, готовящих

или совершивших преступления, равно как и о лицах, жизнь, здоровье или имущество которых стали объектом посягательств, являются ключевыми элементами правоохранительной деятельности. В то же время, в интересах правоохранительной деятельности — не уведомлять лиц о негласном сборе персонифицированной информации, держать полученные сведения о лице недоступными для общественности, поскольку разглашение может навредить следствию, сделать невозможным достижение результата оперативно-розыскных мероприятий и следственных действий вообще. Латентный характер обработки сведений о лице в целях борьбы с преступностью входит в противоречие с принципом прозрачности, который является существенным для эффективной реализации права человека на приватность. Не имея представления о сборе персональных данных, заинтересованное лицо не может защитить свои права.

Итак, требуется выработка правового механизма, который позволит учесть интересы лица, чьи права ограничиваются в ходе негласного сбора и обработки персональных данных. В частности, в этом принципе речь идет о контроле со стороны общественности через орган надзора за обработкой персональных данных, осуществляемой правоохранительными органами. То есть, не должно существовать тайных файлов или баз данных, о которых не знает общественность. Все они должны быть легализованы, а их использование урегулировано в законодательстве, доступном для общественности. Право на доступ к персональным данным, которые содержатся в полицейских файлах, должно гарантироваться. Однако пределы осуществления этого права напрямую будут зависеть от последствий, которые повлечет разглашение соответствующей информации. Если разглашение той или иной информации, полученной как гласными, так и негласными средствами, может навредить следствию, — последняя не должна сообщаться. В других случаях, как в интересах граждан, так и в интересах правоохранительных органов предоставлять заинтересованному лицу доступ к информации с правом исправления или дополнения достоверных данных. При этом персональные данные, собранные с нарушением закона, должны быть уничтожены по требованию субъекта данных.

Национальное законодательство должно предусматривать процедуру контроля над соблюдением законности в случае отказа в доступе к полицейским файлам. Эту функцию должен выполнять независимый орган, будь–то надзорная инстанция или суд.

Принцип 7 Рекомендаций предусматривает, что персональные данные, которые собирались с определенной целью, после достижения цели или невозможности, или нецелесообразности ее достижения, должны уничтожаться. Такими основаниями могут быть отказ в возбуждении уголовного дела, осуждение лица, реабилитация, амнистия или другие аналогичные случаи. Национальное законодательство должно определять сроки хранения тех или иных данных в зависимости от цели их сбора или характера самих данных.

Последний, *восьмой принцип*, призван обеспечить целостность данных путем адекватных технических и организационных мероприятий для предотвращения, предупреждения или прекращения несанкционированного доступа, передачи, преобразования или уничтожения персональных данных и от любой другой незаконной обработки вследствие неосторожности и преднамеренных действий третьих лиц.

Следовательно, внедрение этих предписаний в законодательство, регулирующее правоохранительную деятельность, позволяет сбалансировать субъективные интересы лиц, которых касается персонифицированная информация, а также интересы общества в безопасности. Тем самым обеспечивается принцип пропорциональности применения ограничений и, вместе с ним, законность.

Выводы

Принципы обработки персональных данных в полицейском секторе адаптируют общие требования защиты приватности, содержащиеся в международно-правовых актах, к условиям деятельности полиции. Учитывая существенный риск для прав человека, в национальное законодательство необходимо внедрить общедоступные и подробные правила обращения с персональными данными в правоохранительной деятельности и гарантии от злоупотреблений.

3.3.3. Обращение с персональными данными полицейскими учреждениями Европы: Шенгенская Конвенция и Конвенция Европол.

Ключевые слова: Шенгенская Конвенция – Шенгенская информационная система – категории персональных данных – Конвенция Европола – информационная система Европола – адекватный уровень защиты – Евроюст.

Шенгенская Конвенция

Вопросы защиты конфиденциальности персональных данных в связи с их обработкой полицейскими учреждениями приобрели особую важность для Европейского Союза после ликвидации таможенных границ между странами–членами Шенгенской Конвенции.

Первая договоренность «О постепенной отмене проверок на общих границах» объединила группу из пяти европейских стран (Францию, Германию, Бельгию, Люксембург и Нидерланды). Подписанная 14 июня 1985 г., она заложила фундамент для дальнейшего сотрудничества европейских стран в области создания территории без внутренних границ. Эта договоренность получила название Шенгенского Соглашения от названия города в Великом Герцогстве Люксембург, где произошло подписание соглашения.

Процесс ликвидации внутренних границ и создания общих правил паспортного контроля был продлен подписанием Конвенции 19 июня 1990 г. «О применении Шенгенского соглашения», которая вступила в силу в 1995 г.

Шенгенское пространство распространилось почти на все страны-члены Европейского Союза и уже в 1997 г. включало 13 стран ЕС, за исключением Великой Британии и Ирландской Республики. С 25 марта 2001 г. в Шенгенское пространство вошли еще две страны Северного (Скандинавского) паспортного союза — Исландия и Норвегия.

Введенное Амстердамским Договором пространство свободы, безопасности и правосудия позволило включить Шенгенское Соглашение в организационную структуру Европейского Союза. Этим же Договором, который вступил в силу 1 мая

1999 г., полномочия Исполнительного Комитета Шенгенской Конвенции были переданы Совету Европейского Союза.

С целью содействия деятельности правоохранительных органов особенно учитывая трудности, возникающие из–за предоставления гражданам европейских и неевропейских стран свободы свободного передвижения в Шенгенском пространстве, была создана комплексная информационная система для обмена сведениями о лицах, а также об украденных или утерянных вещах. Информационная система состоит из сети, к которой подключены национальные подразделения, информационного центра, а также операционной системы удовлетворения запросов национальных подразделений под названием «Сирен» (фр. «Supplement d'Information Requis a l'Entree Nationale»).

Эта операционную система с сентября 2001 г. заменена на новую — «Сиснет», в которой дополнительно обрабатываются сведения об иммиграции. Функции поддержки этой системы обеспечивает Французская Республика; службы технического обеспечения располагаются в Страсбурге.

Ликвидация контроля при пересечении внутренних границ внутри Шенгенского пространства компенсируется общим контролем над пересечением ее внешних границ, который осуществляется национальными подразделениями в общем порядке, определенном Шенгенской Конвенцией. Во время такого контроля проверяются как граждане стран Шенгенского пространства, так и граждане других стран. Он включает проверку идентифицирующих личность документов, а для граждан других стран — еще и наличие официального разрешения на въезд, и отсутствие оснований для задержания этого лица в любой из стран, входящих в Шенгенское пространство.

Информация, необходимая для проведения контроля, предоставляется упомянутой информационной системой, в которой содержатся сведения обо всех ордерах на задержание, выданных в странах-участницах, а также об отказах на въезд не гражданам. Информация в системе содержится в состоянии постоянного обновления в режиме реального времени. В случае отсутствия разрешения на въезд, не гражданин лишается доступа на территорию Шенгенского пространства. При наличии оснований для задержания, предусмотренных Шенгенской Конвенцией, лицо подлежит задержанию на границе. Такими

основаниями могут быть: судебный ордер на арест или экстрадицию этого лица под юрисдикцию другой Шенгенской страны (статья 95), сведения об исчезновении лица или о необходимости предоставления ему специальной защиты (статья 97); сведения о необходимости дачи этим лицом показаний в суде или отбывания наказания в виде лишения свободы (статья 98).

Шенгенская информационная система содержит следующие категории персональных данных (статья 94): фамилия, имя, а также другие имена (псевдонимы, прозвища), которыми пользуется человек и которые могут быть зарегистрированы; особенности внешнего вида, его постоянные характеристики, первые буквы отчества; дату и место рождения; пол; национальность, наличие оружия; агрессивность (готовность к совершению насилия) основания для внесения сведений в систему, меры, которые надлежит предпринимать в отношении лица, в случае его идентификации во время контроля.

В информационную систему заносятся сведения об иностранцах, в отношении которых сделан информационный запрос с целью отказа в допуске. Шенгенские страны решают вопрос по запросу на основании своих национальных положений с соблюдением соответствующих процессуальных норм. Статья 96 Конвенции довольно расплывчато определяет основания для принятия таких решений, оставляя это на усмотрение странам. Такими основаниями являются: угроза общественному порядку или национальной безопасности; иностранец является объектом депортации, принудительного возвращения или высылки, действие которых не отменено и не остановлено, вследствие несоблюдения национальных правил о въезде и пребывании иностранцев.

Введенная информация используется для осуществления негласного слежения или специального контроля при наличии следующих оснований: имеется объективная информация о подготовке к совершению или совершении преступления данным лицом: общая оценка этого лица, осуществленная на основании его предыдущих преступлений, свидетельствует о вероятности повторения особенно опасных преступлений; получение сведений необходимо для предотвращения серьезной угрозы внутренней и внешней безопасности государства.

В рамках негласного слежения для органа, направившего информационный запрос, может собираться и передаваться информация, полученная национальными правоохранительными органами во время проведения профилактических и предупредительных мероприятий внутри страны. Негласно собранная информация может включать следующие сведения: о факте обнаружения лица или транспортного средства, в отношении которых направлен информационный запрос; о месте, времени и основаниях для принятия мер; о маршруте и месте назначения поездки; о сопровождающих лицах или пассажирах транспортного средства, об используемом транспортном средстве и перевозимых грузах; об обстоятельствах, при которых было обнаружено лицо или транспортное средство. В соответствии с процедурой специального контроля, лица, транспортные средства и предметы могут быть подвергнуты обыску в соответствии с национальными процессуальными нормами для получения указанной информации.

Вопросам контроля над безопасностью персональных данных и соблюдения прав лиц, относительно которых осуществляется их обработка в Шенгенской информационной системе, посвящается третья глава в разделе IV Конвенции (ст.ст. 102−118), а также отдельный Раздел VI под названием «Защита персональных данных» (ст.ст. 126 −130).

Принципы правомерности обработки персональных данных, провозглашенные Конвенцией Совета Европы о защите лиц относительно автоматизированной обработки персональных данных 1981 г. № 108, а также в Рекомендации № R (87) 15 Комитета Министров Совета Европы, инкорпорированы в Шенгенскую Конвенцию. В частности, статья 126 Шенгенской Конвенции требует от каждой из стран-членов принятия национальных положений по защите персональных данных, которые должны гарантировать уровень правовой защиты не ниже, чем стандарты, внедренные Конвенцией Совета Европы № 108. Эта же статья запрещает любую передачу персональных данных в страны, уровень защиты в которых не соответствует требованиям Конвенции Совета Европы № 108. Кроме того, на сторону, которая получает данные, возлагается обязательство использовать их исключительно в целях, предусмотренных Конвенцией. При этом такие данные могут использоваться лишь судебными органами. Перед

передачей данных осуществляется проверка достоверности. Неточные данные подлежат уточнению или уничтожению, о чем уведомляются все их получатели.

Лица, которых касается информация содержащаяся в информационной системе, могут осуществлять свое право на доступ к таким сведениям в каждой стране Шенгенского пространства в соответствии с положениями национального законодательства по месту обращения. В случае обжалования факта внесения персональных данных в указанную систему или обращения относительно внесения уточнения или уничтожения персональных данных решение принимается национальным надзорным органом после получения объяснения от компетентного органа, ответственного за внесение данных. Такое решение носит обязательный характер на территории всех шенгенских стран.

Если при сообщении недостоверных или частично неточных данных были нарушены права субъектов данных, нанесен ущерб и т.д., компенсация причиненного заинтересованным лицам ущерба в полном объеме осуществляется в соответствии с национальными положениями стран–участниц. Конечную ответственность в порядке регресса несет сторона, которая сообщила недостоверные данные, что привело к причинению вреда.

С целью осуществления внутреннего контроля любое обращение с целью получения персональных данных подлежит регистрации в базе (национальной составляющей информационной системы). Такие же правила распространяются на неавтоматизированную (ручную) обработку и передачу персональных данных.

Гарантировать соблюдение правил обращения с персональными данными и, соответственно, прав субъектов данных должны национальные органы, уполномоченные осуществлять независимый надзор. В случае отсутствия гарантии, передача данных в такие страны запрещается. Персональные данные, внесенные в Шенгенскую информационную систему, используются не только в целях контроля при пересечении границ Шенгенского пространства, но и в правоохранительной деятельности полицейских учреждений и судебных органов европейских стран.

Конвенция Европола

Сотрудничество полицейских учреждений Европейского Союза приобрело определенные институциональные формы с созданием Европейского полицейского учреждения, сокращенное название которого — Европол. Первая официальная ссылка на Европол содержится в Маастрихтском договоре 1992 г., в статье K. 1.9 которой страны-члены ЕС определяют объектом общего интереса такие сферы: сотрудничество полиции с целью предотвращения и пресечения терроризма, незаконного оборота наркотиков и других серьезных форм международной преступности, включая при необходимости аспекты сотрудничества таможенных учреждений, — учитывая организацию общеевропейской системы обмена информацией через Европейское полицейское учреждение (Европол). После подписания Конвенции Европола в июле 1995 г. понадобилось еще три года, чтобы парламенты всех стран-членов ЕС ее ратифицировали. Вступив в силу 1 октября 1998 г., Конвенция позволила Европолу начать свою деятельность с 1 июля 1999 г.

Сферами, на которые распространяется компетенция Европола (к ним присоединяются новые) являются: предотвращение и пресечение терроризма, незаконный оборот наркотиков; торговля людьми (в том числе производство и распространение детской порнографии), преступления, связанные с нелегальной иммиграцией; противозаконное обращение радиоактивных и ядерных веществ; торговля похищенными автомобилями; подделка денег и других средств платежа; отмывание денег, добытых преступным путем, связанных с международной преступностью.

Европол имеет следующие основные задачи: улучшить обмен информацией между полицейскими учреждениями стран-членов Европейского Союза; получать, классифицировать и анализировать информацию и сведения; сообщать незамедлительно компетентным учреждениям стран–членов ЕС информацию, а также об установленных связях между уголовными поступками; оказывать помощь в расследованиях, осуществляемых национальными полицейскими подразделениями; поддерживать компьютеризированные системы собранной информации и т.п.

Одной из уникальных характеристик Европола является то, что в рамках этого учреждения постоянно поддерживается связь с национальными подразделениями через офицеров связи, назначенных странами–членами для работы в составе центрального аппарата Европола. Кроме того, достигается определенная централизация правоохранительной деятельности на европейском уровне благодаря организации подразделений-представительств Европола, которые служат промежуточными звеньями для обмена информацией с национальными полицейскими органами.

Для выполнения своих задач Европол содержит информационную систему, в которой собираются, сортируются и анализируются сведения, которые могут быть использованы для расследования преступлений. Основное преимущество наличия общей информационной системы заключается в том, что полученные от национальных подразделений разрозненные данные после их обработки в системе позволяют на ранних стадиях расследования выявлять связи, которые не могли быть установлены во время их первоначального анализа национальными подразделениями. Информационная система Европола, в частности, содержит следующие виды персональных данных (статья 9): фамилия, девичья фамилия, а также другие имена (псевдонимы, прозвища), дата и место рождения; национальность; пол; особенности внешнего вида.

Кроме того, информационная система Европола используется для обработки дополнительной информации относительно обстоятельств совершения или подготовки к совершению преступлений, средств совершения преступлений; подразделений, осуществлявших расследование, а также материалов расследования; подозреваемого членства в преступной группе; предъявленных обвинениях.

Введенные данные должны касаться только лиц, которые готовятся совершить преступление, подозреваемых в совершении или причастности к преступлению, на которые распространяется компетенция Европол, а также обвиняемых в таком преступлении (статья 8).

Персональные данные, которые собираются и накапливаются в информационной системе, передаются в нее национальными подразделениями государств-членов Конвенции,

третьими государствами или международными организациями и органами, как по собственной инициативе, так и по запросу Европола.

Раздел IV Конвенции Европола содержит положения, регулирующие обработку персональных данных, в том числе принципы защиты приватности. Статья 14 возлагает на государства-члены обязательства привести национальное законодательство в соответствие с требованиями защиты персональных данных в области правоохранительной деятельности, в частности теми, которые содержатся в Конвенции Совета Европы № 108, а также Рекомендации № R (87) 15 Комитета Министров Совета Европы. Невыполнение этого условия чревато запретом на передачу персональных данных.

Ответственность за соблюдение правил обращения с персональными данными возлагается на государство-члена Конвенции, полицейское учреждение которого вводит или передает данные, а также на Европол, если данные, полученные от третьих сторон, заносятся в информационную систему непосредственно офицерами Европола или полученные в результате проведенного офицерами Европола анализа. Поскольку предполагается разграничение ответственности между субъектами обработки, информационная система должна обеспечивать возможность их распознавания.

Статья 16 Конвенции Европола предусматривает механизм внутреннего контроля соблюдения законности при обработке персональных данных в информационной системе Европола. Один из десяти случаев использования персональных данных, а также каждое их исправление подлежат проверке с точки зрения их соответствия требованиям Конвенции, о чем составляется отчет.

Общим правилом обращения с данными, полученными из информационной системы Европола, является ограничение их использования уполномоченными органами государств–членов Конвенции в случаях, подпадающих под компетенцию Европола. Однако, они также могут быть ими использованы для борьбы с другими серьезными видами преступлений, выходящими за пределы компетенции Европола. При этом любое государство-член Конвенции или третья сторона (государство или международный орган) вправе ввести предостережения относитель-

но дальнейшего использования персональных данных. В этих случаях пользователь данных (Европол или государство-член Конвенции) должен согласовать с передающей стороной условия использования данных в каждом конкретном случае.

Статья 18 Конвенции Европола закладывает основы для сотрудничества с третьими государствами и организациями, предусматривая правила передачи персональных данных, содержащихся в информационной системе Европола, сторонам, которые не являются членами Конвенции.

Передача персональных данных третьим государствам и организациям разрешается, если это необходимо, в отдельных случаях в целях предотвращения или борьбы с преступлениями, которые входят в компетенцию Европола. При этом третье государство или организация должны обеспечивать адекватный уровень защиты приватности персональных данных. Это положение заимствовано из статьи 25 Директивы № 95/46 СЕ Европейского Парламента и Совета «О защите физических лиц при автоматизированной обработке персональных данных и беспрепятственного движения этих данных». Для оценки адекватности уровня защиты во внимание должны приниматься такие условия, как характер данных, цель предполагаемой обработки, ее продолжительность, а также какие положения законодательства применяются к передаче персональных данных. Необходимым условием для передачи данных на указанных выше основаниях является наличие в третьем государстве или организации механизма надзора за соблюдением законности использования персональных данных, который осуществляется уполномоченным органом.

Вопрос передачи персональных данных в третьи государства или организации детализируются в Акте Совета Европейского Союза от 12 марта 1999 г. Общим основанием для передачи персональных данных является соответствующее соглашение между руководящим органом Европола и третьим государством или организацией. Решение о заключении соглашения с третьим государством или организацией принимается единогласно Советом Европейского Союза на основании оценки возможности соблюдения правил обработки персональных данных третьим государством или организацией. В соглашении с третьим государством или организацией указываются получате-

ли данных (ответственный орган или организация), характер данных, цели передачи и использования. Каждый запрос на передачу данных также должен содержать указание на условия получения и использования данных.

Передаче данных третьему государству или организации предшествует получение согласия того государства–члена Конвенции Европола, которое занесло данные в информационную систему. О передаче персональных данных, которые введены в информационную систему непосредственно служащими Европола, решение также принимает Европол. От получателя данных (третьего государства или организации) требуется заверения, что заявленная цель использования персональных данных будет соблюдена. При отсутствии соглашения между Европолом и третьим государством или организацией, как исключение, разрешается санкционированная директором Европола передача, если это необходимо для защиты важных интересов государств–членов Конвенции или для предотвращения нависшей опасности, связанной с преступлением. О такой передаче немедленно сообщаются правление и общий надзорный орган Европола.

Исключительно под санкцию директора Европола могут передаваться «уязвимые данные», которые раскрывают расовое происхождение, политические взгляды, религиозные или иные убеждения, данные о здоровье, сексуальной жизни. Этим, в частности, обеспечивается требование статьи 6 Конвенции Совета Европы № 108 о предоставлении дополнительных гарантий к обработке персональных данных, которые могут, учитывая их характер, нести повышенный риск для безопасности, прав и свобод личности.

Как отмечалось выше, право заинтересованных лиц на доступ к своим персональным данным является важной гарантией законности, поскольку при этом лицо имеет право оспорить возможные неправомерные действия с персональными данными. Статья 19 Конвенции Европола определяет порядок доступа лиц к персональным данным, находящимся в информационной системе Европола. Обращения граждан должны адресоваться национальным компетентным органам в соответствии с требованиями национального права. В доступе к данным может быть отказано, если это необходимо для обеспечения

надлежащего выполнения Европолом своих функций, для обеспечения безопасности и общественного порядка или предотвращения преступления, а также для защиты прав и свобод других лиц.

Учитывая международный характер деятельности Европола и наличие различных источников информации, попадающей в информационную систему, в этой статье предусматривается процедура согласования позиций различных субъектов для решения вопроса о предоставлении доступа. В частности, учитывается мнение государств-членов Конвенции, третьих государств и организаций, которые предоставили персональные данные или заинтересованы в предоставлении их для ознакомления. При этом достаточно одного возражения любой из заинтересованных сторон, чтобы персональные данные не были сообщены.

Заинтересованное лицо, просьба которого о доступе или проверке данных не будет удовлетворена, вправе обратиться с апелляцией к общему надзорному органу. Этот орган принимает свое решение после получения заключения национального надзорного органа, который должен провести проверку соблюдения национального законодательства при рассмотрении обращения национальным подразделением полиции. Если данные введены в информационную систему непосредственно офицерами Европола, необходимые проверки проводятся также Европолом.

В случае, когда персональные данные являются неточными или введены в информационную систему или обрабатываются с нарушением требований правил обработки, предусмотренных Конвенцией Европола или национальным законодательством, они исправляются или уничтожаются. Об этом уведомляются всем получатели данных, государства или организации, которые ими владеют, а также субъект данных, который обратился с просьбой об исправлении своих персональных данных. Статья 22 Конвенции Европол содержит важную гарантию предотвращения сокрытия факта нарушения прав субъектов данных во время процедуры уничтожения персональных данных. Если есть основания полагать, что законные интересы субъекта данных могут быть утрачены в случае уничтожения неточных данных, файлы не уничтожаются, а маркируются специальными обозна-

чениями, чтобы их могли использовать. Это же правило применяется также в случаях возможного уничтожения данных в связи с истечением срока хранения.

Статья 21 Конвенции Европола регламентирует срок хранения и уничтожения персональных данных. По общему правилу, данные хранятся столько, сколько это требуется для выполнения Европолом своих задач. Первый срок ограничивается тремя годами, после чего данные пересматриваются на предмет возможности их длительного хранения. Государства–члены уведомляются за три месяца до приближении срока пересмотра данных. Данные, по которым решение о продлении срока хранения не принято, автоматически уничтожаются. Государство–член сообщает Европолу об уничтожении данных, которые были ранее введены в информационную систему. В случае необходимости Европол может не уничтожать такие данные, если он нуждается в их дальнейшем хранении. О таком решении сообщается заинтересованному государству–члену.

Национальные надзорные органы контролируют все операции, осуществляемые национальными полицейскими подразделениями с персональными данными, а также рассматривают обращения заинтересованных лиц о проверке правомерности действий с персональными данными. Статья 23 Конвенции предусматривает, что такой надзорный орган должен действовать совершенно независимо.

Положения статьи 25 Конвенции Европола, касающиеся технической и организационной защиты (безопасности) данных, почти тождественны по своему содержанию соответствующим положениям статьи 118 Шенгенской Конвенции. В частности, в обоих документах предусматривается контроль доступа к оборудованию, носителей и содержания данных, доступа к информационной системе, использования, передачи, ввода и транспортировки. Однако в дополнение к предусмотренным в Шенгенской Конвенции мерам безопасности Конвенция Европола указывает на необходимость обеспечения немедленного исправления систем, которые вышли из строя, а также неотложного сообщения об ошибочных операциях. Требуется также обеспечение целостности персональных данных в случае неправильного функционирования систем автоматизированной обработки.

Положение о технической и организационной защите (безопасности) персональных данных далее по тексту Конвенции Европола дополняются в статьях 31 и 32. Кроме того, Актом Совета Европейского Союза от 3 ноября 1998 г. утверждены правила о конфиденциальности в Европоле. Предполагается, что уровень технической и организационной защиты (безопасности) персональных данных на территории государств-членов Конвенции, должен быть не ниже уровня защиты, введенного Конвенцией Европола, указанными правилами о конфиденциальности в Европоле, а также «Руководящими принципами безопасности».

Для информации, находящейся в распоряжении Европола, кроме той, которая явно относится к открытой для общественности, по общему правилу устанавливается основной уровень защиты. Информация, которая по своему характеру требует дополнительных мер безопасности, классифицируется по уровням безопасности на три категории: «Европол 1», «Европол 2» и «Европол 3».

Внедрение такой системы маркировки информации не означает, что общественность лишена возможности контролировать деятельность Европола. Любое заинтересованное лицо также имеет право на доступ не только к своим персональным данным, но и к информации о деятельности Европола как и любой другой институции Европейского Союза. Это право закрепляется в Акте Совета ЕС от 20 декабря 1993 г. «О доступе общественности к документам Совета», который принят для обеспечения прозрачности в работе органов ЕС. Исключительными легитимными основаниями для отказа в предоставлении информации для ознакомления являются защита: общественных интересов (государственная безопасность, международные отношения, монетарная стабильность, расследование преступлений, проверка и исследования); лиц, их права на приватность; коммерческой и производственной тайны, финансовых интересов Европейских сообществ; конфиденциальности, о чем просит физическое или юридическое лицо, предоставившее информацию; конфиденциальности работы Совета ЕС и т.д. Таким образом, у граждан ЕС, а также граждан третьих государств есть возможность воспользоваться своим правом на доступ к информации, касающейся деятельности Европола,

если это не будет вредить законным интересам общества, других лиц и т.п.

Бесспорно, что заключение как Шенгенской Конвенции, так и Конвенции Европола положительно повлияло на урегулирование вопросов обработки персональных данных в правоохранительной деятельности на европейском региональном уровне. Однако отсутствие международных стандартов защиты конфиденциальности персональных данных в контексте правоохранительной деятельности, которые должны носить обязательный характер для государств-участников международного договора, оставляет много нерешенных вопросов, что негативно сказывается на правах и свободах человека.

Недостатки существующего международно-правового регулирования вопросов обработки персональных данных в правоохранительной деятельности на общеевропейском уровне были предметом внимания международного семинара, проведенного в декабре 1999 г. Советом Европы. По его результатам были предложены рекомендации для улучшения правового регулирования, как на национальном, так и международном уровнях[1].

В частности, на национальном уровне рекомендуется, чтобы законодательство по вопросам защиты персональных данных в правоохранительной деятельности основывалось как на общем законе о защите персональных данных, так и на специальных нормативно-правовых актах по вопросам обработки персональных данных различными звеньями правоохранительных (полицейских) учреждений.

Учитывая растущий объем трансграничной передачи персональных данных во время сотрудничества в области правоохранительной деятельности, рекомендуется, чтобы перед началом передачи качество данных тщательно оценивалось; осуществлялся эффективный надзор за законностью обработки; субъекты данных получали эффективную помощь даже за пределами национальных границ. Также отмечается необходимость совершенствования регулирования передачи данных в страны, которые не обеспечивают адекватной защиты персональных данных, усилив соответствующие требования к получателям.

1. Data protection in Police Sector. Council of Europe Regional Seminar under the activities for the development and consolidation of democratic stability // ADACS/DGI (2000) 3 Sem. – Strasbourg: 2000.

Подписанное 4 декабря 2009 г. в рамках Саммита Украина – ЕС Соглашение между Украиной и Европолом о стратегическом сотрудничестве способствует координации усилий государств–членов ЕС и Украины в предотвращении и противодействии любым формам международной преступности, проявлениям террористических угроз, торговли людьми, наркотиками и другими психотропными веществами, нелегальной миграции[1].

Стратегическое соглашение предусматривает обмен оперативной информацией между соответствующими службами МВД Украины и Европолом, но не предоставляет полномочий для передачи персональных данных (Статья 1).

С Европолом также достигнута договоренность о заключении Соглашения об оперативном сотрудничестве, что стало возможным благодаря ратификации Украиной Конвенции Совета Европы о защите лиц в связи с автоматизированной обработкой персональных данных и Дополнительного протокола к ней, а также принятия Закона Украины «О защите персональных данных».

Защита прав граждан в связи с обработкой персонифицированной информации в деятельности органов правосудия также находится в повестке дня институций Европейского Союза. В частности, Конвенция о взаимной помощи в уголовных делах стран-членов Европейского Союза предусматривает обмен персональными данными в рамках такого сотрудничества[2]. Для этого создана информационная сеть, управление которой осуществляет специальное подразделение по вопросам судебного сотрудничества – Евроюст (*Eurojust*)[3].

В декабре 2000 г. в состав Евроюста были назначены судья и прокуроры из стран-членов Европейского Союза, которые координируют правовые вопросы проведения трансграничных

1. Закон України «Про ратифікацію Угоди між Україною та Європейським поліцейським офісом про стратегічне співробітництво» від 05.10.2010 р. № 2576–VI // Відомості Верховної Ради України. – 2011. – N 6. – ст. 48.
2. Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty of European Union the Convention on Mutual Assistance in Criminal Matters between the member States of the European Union // Official Journal of the European Communities. – 2000. – C. 197.
3. Council Decision of 14 December 2000 setting up a Provisional Judicial Cooperation Unit // Official Journal of the European Communities. – 2000. – L 324.

расследований, включая терроризм, компьютерную преступность, отмывание денег и экологические правонарушения . Соглашение между Министерством юстиции Украины и Евроюстом было парафировано в Гааге 8 декабря 2011 г.

Выводы

Сотрудничество в правоохранительной сфере на основании общепризнанных принципов защиты персональных данных создает правовую основу для быстрого обмена информацией, координации действий в противодействии трансграничной преступности, содействия в сборе доказательств и привлечения к ответственности правонарушителей. Такое сотрудничество поднимает на более высокий уровень эффективность взаимодействия правоохранительных органов Европейского Союза и Украины в расследовании тяжких преступлений транснационального характера.

Контрольные вопросы и задания:

1. Дайте определение понятия «персональные данные».
2. Назовите цели принятия на международном уровне актов, направленных на регулирование защиты и беспрепятственной трансграничной передачи персональных данных.
3. Назовите основные международно-правовые акты, устанавливающие правила обращения с персональными данными.
4. Перечислите принципы обращения с персональными данными.
5. Укажите принципы использования персональных данных в секторе полиции.
6. Укажите правовые механизмы надзора за законностью негласной обработки персональных данных.
7. Укажите цели и правила обработки персональных данных в информационных системах – Шенгенской, Европола и Евроюста.
8. Укажите законодательные акты Украины, определяющие гарантии защиты приватности в контексте обработки персональных данных.

Литература

Защита личных данных при трансграничном перемещении информации [Электронный ресурс] / Организация Объединенных Наций. Доклад Комиссии международного права. Пятьдесят восьмая сессия. (A/61/10). Приложение E. – Нью-Йорк : ООН, 2006. – С. 504 – 535. – Режим доступа : http://untreaty.un.org/ilc/reports/2006/russian/annexes.pdf;

Мацко А. С. Міжнародна діяльність Інтерполу по боротьбі з транснаціональною злочинністю. Наукова доповідь, 27.09.2012. – К. : Київський Нац. університ. ім. Т. Шевченка, Інститут міжн. Відн. «Міжнародно–правові читання», 2012;

Пазюк А. В. Захист прав громадян у зв'язку з обробкою персональних даних у правоохоронній діяльності : європейські стандарти і Україна. — К. : МГО Прайвесі Юкрейн, 2001;

Пазюк А. В. Захист прав людини стосовно обробки персональних даних: міжнародні стандарти. – К. : МГО Прайвесі Юкрейн, 2000; Права людини та Інтернет. – К. : МГО Прайвесі Юкрейн, 2002;

Порівняльно-правове дослідження відповідності законодавства України законодавству ЄС у сфері персональних даних / В. М. Брижко, А. І. Радянська, М. Я. Швець. – К. : Тріумф, 2006;

Правові основи міжнародної діяльності МВС України (в двох томах). – К. : МВС України, 1997;

Радионов К. С. Интерпол : вчера, сегодня, завтра / К. С. Радионов. – М. , 1990;

Wolstenholme David. Police Requirements and Practices in the Information Society. The дело in the United Kingdom // ADACS/DGI (2000) 3 Sem. : Data protection in Police Sector. Council of Europe Regional Seminar under the activities for the development and consolidation of democratic stability. – Strasbourg, 2000.