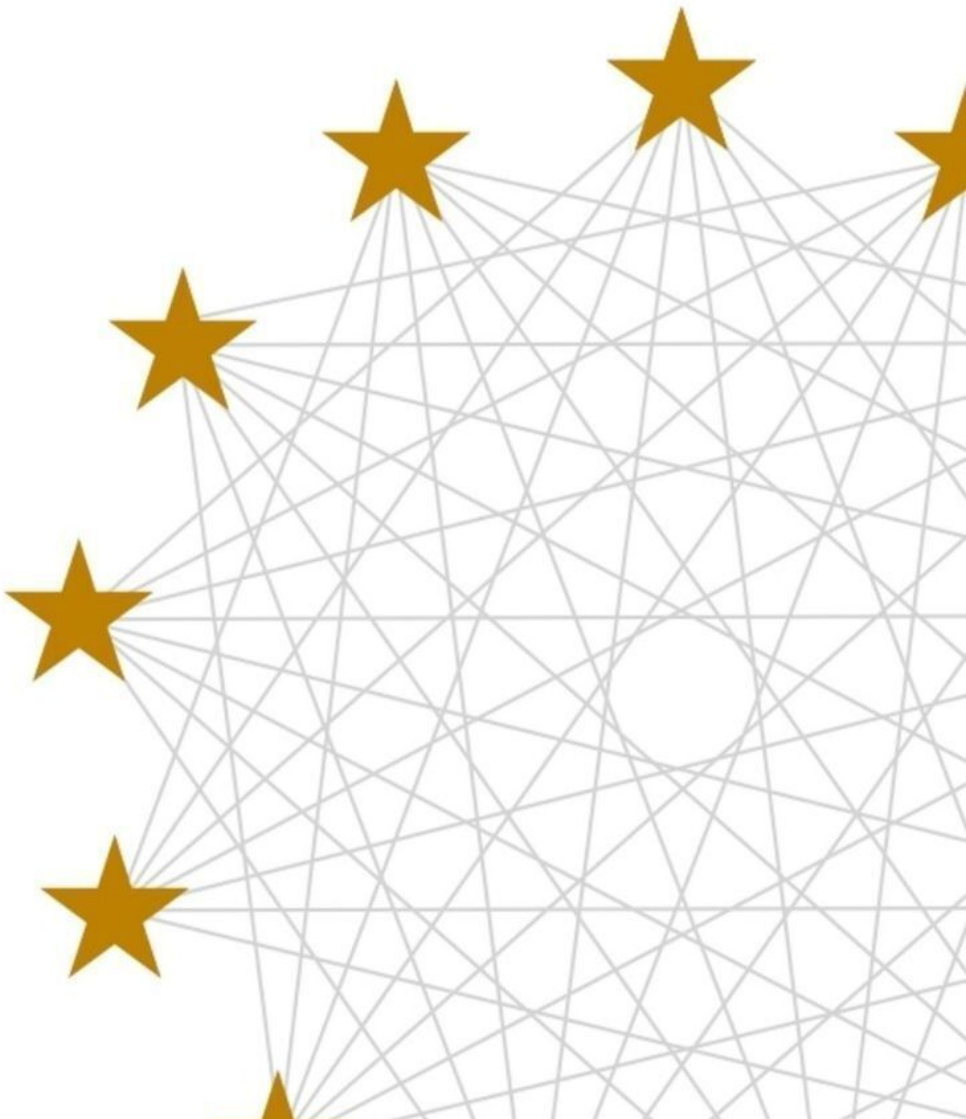
Мария Беляева Сергей Руднев

РУКОВОДСТВО ПО GDPR

Комментарии надзорных органов, критерии и сравнение, выводы и решения европейских судов.



Мария Беляева

Руководство по GDPR

«Издательские решения»

Беляева М.

Руководство по GDPR / М. Беляева — «Издательские решения»,

ISBN 978-5-00-517769-8

В 2018 году Евросоюзом принят законодательный акт, определяющий права граждан и иных субъектов данных при обработке их персональных данных.В руководстве приведены принципы и критерии европейского законодательства по защите данных, механизмы применения норм права, надзор за соблюдением прав субъектов, а также сравнение законодательных практик ЕС и РФ в области защиты данных, рабочие кейсы, выводы и решения надзорных органов ЕС, Суда Европейского Союза и Европейского суда по правам человека.

ISBN 978-5-00-517769-8

Содержание

Руководство по GDPR

Мария Беляева
Сергей Руднев

ISBN 978-5-0051-7769-8
Создано в интеллектуальной издательской системе Ridero

Предисловие

Право человека на защиту своих данных, неприкосновенность жилища и тайна переписки является одним из основных прав в цивилизованном обществе. Евросоюз наиболее последовательно стремится унифицировать законодательные базы стран содружества, соблюдение прав человека, принципы обработки и защиты персональных данных.

Изложенные материалы помогут Вам разобраться в требованиях европейского законодательства и получить представление о механизмах обработки и защиты персональных данных в ЕС. В книге приведен сравнительный анализ европейских и российских законодательных актов по защите персональных данных, рабочие кейсы, выводы и решения надзорных органов ЕС, Суда Европейского Союза и Европейского суда по правам человека.

Понимание процессов применения законодательства ЕС и стран Евросоюза может подтолкнуть Вас к изучению дополнительных материалов по теме обработки персональных данных и защиты неотъемлемых прав человека.

Приятного чтения!

Глава 1

Европейский Союз: о*сновные права физических лиц на защиту персональных данных. История развития права.*

Законодательные акты ЕС, в которых закреплены понятия прав физического лица, объектов и субъектов права.

Ограничение права на защиту персональных данных.

Преследуемые цели в защите прав физических лиц, принципы достижения целей и их влияние на правоприменительную практику.

Законодательная и судебная власть ЕС и РФ в области защиты данных.

Право на неприкосновенность частной жизни и защиту персональных данных физических лиц

Право на неприкосновенность частной жизни и право на защиту персональных данных в ЕС тесно связаны между собой, но являются отдельными правами. Право на неприкосновенность частной жизни впервые было упомянуто в 1948 году во Всеобщей декларации прав человека. С юридической точки зрения, данное право является одним из наиболее защищенных прав человека.

В 1950 году право на неприкосновенность частной жизни было подтверждено Европейской конвенцией по правам человека, юридически обязательным документом для ратифицировавших ее сторон. Европейская конвенция по правам человека предусматривает, что каждый человек имеет право на уважение личной и семейной жизни, жилища и переписки. Вмешательство в это право со стороны государственных органов запрещено за исключением случаев, когда вмешательство осуществляется в соответствии с законом, преследует важные и законные общественные интересы и необходимо в демократическом обществе.

Всеобщая декларация прав человека и Европейская конвенция по правам человека были приняты задолго до развития технологий и современного состояния информационного общества. Наравне с комфортом, повышением качества жизни и производительностью труда технологии привнесли с собой и новые риски для современного общества. В свою очередь, это потребовало создания новых регулирующих правил, в том числе и в отношении права физического лица на неприкосновенность и уважение частной жизни. Новые правила призваны регулировать сбор и использование личной информации на законодательном уровне. Возникновение концепции конфиденциальности данных предопределило разработку законодательных норм для защиты персональных данных.

В 80-х годах прошлого века некоторые государства закрепили на законодательном уровне правила, регулирующее обработку персональных данных государственными органами и крупными компаниями. Позднее инструменты защиты данных были внедрены на европейском уровне и с годами защита данных превратилась в отдельную норму, которая не определяется правом на неприкосновенность частной жизни. В правовом поле Европейского Союза защита данных признана в качестве основного права, отдельного от фундаментального права на неприкосновенность частной жизни. Такое разделение поднимает вопрос о взаимоотношениях и различиях между этими двумя правами.

Право на неприкосновенность частной жизни и право на защиту персональных данных тесно связаны. Они защищают основные ценности человека, такие как автономия физического лица и человеческое достоинство, предоставляя субъекту персональную сферу, в которой он может развивать свою личность, свободно мыслить и формировать свое мнение.

Таким образом, они являются важной предпосылкой для осуществления других основных свобод, таких как свобода выражения мнений, свобода мирных собраний и ассоциаций, свобода вероисповедания.

Два права различаются по своей формулировке и содержанию. Право на неприкосновенность частной жизни состоит из общего запрета на вмешательство с учетом некоторых критериев общественного интереса, которые в определенных случаях могут оправдывать вмешательство. Право на защиту персональных данных создает систему сдержек и противовесов для защиты физических лиц при обработке их персональных данных. Обработка должна соответствовать основным компонентам защиты персональных данных, а именно независимому надзору и соблюдению прав субъектов данных.

Статья 8 Хартии основных прав ЕС содержит определение основного права на защиту личных данных и утверждает основные ценности, связанные с этим правом. Нормы Хартии предусматривают обработку персональных данных в соответствии с определенными целями, на справедливой основе, с согласия соответствующего лица или на ином законном основании.

Физические лица должны иметь право доступа к своим личным данным и возможность их корректировки, соблюдение таких прав должно контролироваться независимым органом.

Право на защиту личных данных, возникающее при обработке персональных данных, применяется чаще и имеет более широкую трактовку в силу своего правового значения, чем право на неприкосновенность частной жизни. Любая операция по обработке персональных данных подлежит защите. Защита касается всех видов персональных данных и обработки, независимо от степени конфиденциальности. Для срабатывания механизма защиты не требуется факта нарушения права, защита данных является превентивной мерой.

Право на неприкосновенность частной жизни возникает в ситуациях, когда личные интересы или «частная жизнь» человека были скомпрометированы. Понятие «частная жизнь», в прецедентном праве ЕС, включает в себя конфиденциальные данные, профессиональную жизнь, а также информацию, которая может нанести ущерб репутации человека в обществе и иные сведения, относящиеся к понятию «частная жизнь». Оценка того, имеет ли место вмешательство в «частную жизнь» или нет, зависит от контекста и фактов каждого индивидуального случая.

Например, работодатель регистрирует информацию, касающуюся имен и вознаграждений, выплачиваемых работникам. Простая запись этой информации не может рассматриваться как нарушение неприкосновенности частной жизни, но в случае передачи такой информации третьим лицам, неприкосновенность частной жизни будет нарушена. В любом случае работодатель обязан соблюдать правила защиты данных, поскольку запись информации работников представляет собой обработку персональных данных.

Международная правовая база

Организация Объединенных Наций

Организация Объединенных Наций не признает право на защиту личных данных в качестве основного права, хотя право на неприкосновенность частной жизни является основополагающим правом в международном правопорядке.

Всеобщая декларация прав человека об уважении частной и семейной жизни является международным документом, закрепляющим право человека на защиту своей частной сферы от вторжений третьих лиц, особенно со стороны государства. Несмотря на то, что Декларация не имеет статуса юридического документа, она имеет особый статус в качестве основополагающего инструмента международного права. Декларация послужила основой при разработке других документов по правам человека в ЕС.

Международный пакт о гражданских и политических правах вступил в силу в 1976 году. Он провозглашает, что никто не может нарушать неприкосновенность частной жизни, жилища или переписки, а также незаконно посягать на честь и репутацию человека. Международный пакт о гражданских и политических правах является международным договором, обязывающим 169 участников уважать и обеспечивать осуществление гражданских прав физических лиц, включая конфиденциальность.

Организация Объединенных Наций приняла две резолюции по вопросам конфиденциальности под общим названием «Право на неприкосновенность частной жизни в цифровую эпоху». Резолюции были приняты как ответ на разработку новых технологий и откровений о массовом наблюдении, предпринятом в США (откровения Эдварда Сноудена). Резолюции решительно осуждают массовое наблюдение и подчеркивают влияние, которое такое наблюдение может оказать на основные права, на неприкосновенность частной жизни и свободу выражения мнений, а также на функционирование динамичного и демократичного общества. Хотя резолюции и не имели юридического статуса, они вызвали важные международные политические дебаты о конфиденциальности, новых технологиях и надзоре на высоком уровне. Организация Объединенных Наций ввела должность Специального докладчика по вопросам права на неприкосновенность частной жизни с мандатом по защите этого права. Конкретные задачи докладчика включают сбор информации о национальной практике и опыте в отношении конфиденциальности и проблем, возникающих в связи с новыми технологиями, обмен передовым опытом и популяризацию защиты права.

В то время как в предыдущих резолюциях основное внимание уделялось негативным последствиям массового надзора и ответственности государств за ограничение полномочий разведывательных органов, более поздние резолюции отражают ключевые тезисы в обсуждение вопросов конфиденциальности в рамках Организации Объединенных Наций. В резолюциях, принятых в 2016 и 2017 годах, подтверждается необходимость ограничить полномочия спецслужб и осудить массовое наблюдение. Тем не менее они также прямо заявляют, что «расширяющиеся возможности коммерческих организаций по сбору, обработке и использованию персональных данных могут представлять риск для осуществления права на неприкосновенность частной жизни в эпоху цифровых технологий». В дополнение к ответственности государственных органов в резолюциях указывается на ответственность частного сектора за соблюдение прав человека и содержится призыв к компаниям информировать пользователей о сборе, использовании, обмене и хранении персональных данных, а также принимать прозрачные политики обработки данных.

Европейская конвенция по правам человека

Совет Европы был образован после Второй мировой войны в целях обеспечения верховенства закона, демократии, прав человека и социального развития в объединенных государствах Европы. С этой целью в 1950 году была принята Европейская конвенция по правам человека, которая вступила в силу в 1953 году.

Стороны, ратифицировавшие Конвенцию, принимают на себя международное обязательство соблюдать ее. Все государства – члены Совета Европы в настоящие время имплементировали положения Европейской конвенции по правам человека в свое национальное законодательство. Государство должно уважать права, предусмотренные в Конвенции, при осуществлении какой-либо деятельности или полномочий. Существуют прецедентные решения Европейского суда по правам человека о вмешательстве государства в личную жизнь человека, в которых Суд утверждает, что деятельность государства по наблюдению за физическими лицами представляет собой нарушение неприкосновенности частной жизни.

В целях соблюдения международных обязательств, в рамках Европейской конвенции о правах человека в 1959 году был создан Европейский суд по правам человека. Европейский суд по правам человека обеспечивает соблюдение государствами своих обязательств, согласно Европейской конвенции по правам человека, занимается рассмотрением жалоб физических лиц и групп лиц, негосударственных организаций или юридических лиц, утверждая своим решением факт нарушения Конвенции. Европейский суд по правам человека также может рассматривать межгосударственные дела, возбужденные одним или несколькими государствами-членами Совета Европы против другого государства, принявшего на себя международные обязательства по соблюдению Конвенции.

По состоянию на 2020 год в состав Совета Европы входят 47 договаривающихся сторон, 28 из которых являются государствами Евросоюза. Заявитель в Европейский суд по правам человека не обязательно должен быть гражданином одной из договаривающихся сторон, хотя предполагаемые нарушения должны иметь место в пределах юрисдикции одного из государств, ратифицировавших Конвенцию.

Право на защиту персональных данных является частью прав, охраняемых согласно статье 8 Европейской конвенции о правах человека, которая гарантирует право на уважение частной и семейной жизни, жилища и тайны переписки и устанавливает условия, при которых ограничения этого права допускается.

Европейский суд по правам человека рассмотрел множество споров, связанных с вопросами защиты данных. К ним относятся перехват сообщений, различные формы наблюдения со стороны как частного, так и государственного секторов и защита от хранения персональных данных государственными органами. Уважение частной жизни не является абсолютным правом, поскольку осуществления права на неприкосновенность частной жизни может поставить под угрозу другие права, такие как свобода выражения мнений и доступ к информации и наоборот. Следовательно, Суд стремится найти баланс между различными правами. Суд пояснил, что статья 8 Европейской конвенции о правах человека не только обязывает государства воздерживаться от любых действий, которые могут нарушать это право Конвенции, но и накладывает обязательства по активному обеспечению эффективного соблюдения неприкосновенности частной и семейной жизни.

Конвенция Совета Европы

С началом стремительного развития информационных технологий в 60-х годах прошлого столетия возникла потребность в более детализированных правилах защиты персональных данных. В период с 60-е по 80-е годы Комитеты Совета Европы приняли несколько профильных резолюций о защите персональных данных. В 1981 году Совет Европы утвердил единый

документ о защите данных физических лиц в отношении автоматической обработки персональных данных – Конвенция 108. Конвенция о защите данных физических лиц в отношении автоматической обработки персональных данных была и остается единственным юридически обязывающим международным документом по защите данных.

Положения Конвенция 108 распространяются на любые операции по обработке персональных данных, осуществляемых как в частном, так и в государственном секторе, включая обработку данных судебными и правоохранительными органами. Цели Конвенции направлены на защиту операций по обработке персональных данных и регулирование трансграничной передачи данных.

Принципы, изложенные в Конвенции 108, касаются, в частности, справедливого и законного сбора данных и применения автоматизированной обработки в определенных целях. Принципы раскрываются в следующих требованиях:

– запрет на использование обработки для целей, несовместимых с законными целями;

– запрет на хранение персональных данных дольше, чем это необходимо для целей законной обработки;

– принцип качества данных, который включает в себя понятия адекватности и актуальности данных;

– соразмерность обрабатываемых данных заявленным целям и их точность.

Принципы Конвенции 108 указывают на запрет обработки специальных категорий персональных данных в отсутствии адекватных правовых гарантий и обязательств по обеспечению безопасности персональных данных, к таким данным относятся:

– этническое происхождение,

– политические взгляды,

– данные о здоровье,

– вероисповедание,

– сексуальная жизнь,

– информация о наличии судимости.

Конвенция также закрепляет право человека знать, какая информация хранится о нем, и право на внесение в нее исправлений. Ограничение прав и свобод субъекта данных возможно только в случае угрозы государственной безопасности. Положения Конвенции 108 направлены на регулирование потоков персональных данных между сторонами, ратифицировавшими Конвенцию, и диктуют определенные ограничения для передачи в страны, где правовое регулирование не обеспечивает адекватной защиты данных.

На сегодняшний день участниками Конвенции 108 является 51 страна. К ним относятся все государства – члены Совета Европы (47 стран), Уругвай (первая неевропейская страна, присоединившаяся в августе 2013 года), Маврикий, Сенегал и Тунис, которые присоединились в 2016 и 2017 годах. Российская Федерация ратифицировала Конвенцию и некоторые протоколы в марте 1998 года. Протоколы 6, 12, 13, и 16 не были ратифицированы РФ.

Следует отметить, что Конвенция 108 открыта для присоединения и является обязательным документом для государств, которые ее ратифицировали. Она не подлежит судебному надзору со стороны Европейского суда по правам человека, но ее требования учитываются Судом в контексте статьи 8 Европейской конвенции по правам человека. Практика Европейского Суда указывает, что защита личных данных является важной частью права на неприкосновенность частной жизни. В своей деятельности судебные органы руководствуются принципами Европейской конвенции по правам человека при определении факта вмешательства в основные права.

Для модернизации общих принципов и правил, изложенных в Конвенции 108, Комитеты Совета Европы приняли несколько рекомендаций, не имеющих статуса юридического доку-

мента, но тем не менее оказывающих влияние на развитие законодательства о защите данных в Европе.

На протяжении многих лет единственным документом ЕС в части использования персональных данных в правоохранительном секторе были рекомендации полицейского департамента. Положения, содержащиеся в рекомендациях, касаются способов хранения данных и необходимости осуществления регулирования для доступа к данным субъектов. В последующем данные принципы легли в основу законодательных актов по защите данных в ЕС.

В 2001 году был принят дополнительный протокол к Конвенции 108. В рамках протокола были введены положения о трансграничных потоках данных государств, не являющихся сторонами Конвенции (так называемые третьи страны) и об обязательном создании надзорных органов по защите данных.

В 2011 году по итогам публичных консультаций были закреплены две основные цели: усиление защиты конфиденциальности пропорционально развитию технологий и укрепление механизма последующей деятельности в рамках Конвенции. Процесс модернизации был направлен на достижение этих целей и завершился принятием протокола о внесении изменений в Конвенцию 108 (Протокол СДСЕ №223). Работы проводились параллельно с другими реформами международных инструментов защиты данных, а также с реформой правил защиты данных ЕС.

Регуляторы на уровне Совета Европы и ЕС приложили все усилия для обеспечения последовательности и совместимости между двумя правовыми системами. Модернизация позволила сохранить общий и гибкий характер Конвенции 108, и усилила ее потенциал как универсального инструмента в области законодательства о защите данных. Модернизированная Конвенция поддерживает важные принципы и предоставляет новые права субъектам данных, нацелена на повышение уровня ответственности организаций, обрабатывающих персональные данные и поднадзорность таких действий. Лица, чьи персональные данные обрабатываются, имеют право на получение информации о причинах такой обработки и право на возражение против такой обработки. В целях соблюдения прав субъектов данных Конвенция устанавливает право физического лица возражать против принятия решения на основе исключительно автоматизированной обработки без учета мнения субъекта данных. Одним из ключевых аспектов Конвенции 108 является эффективное соблюдение правил защиты данных независимыми надзорными органами ратифицировавших ее сторон. Статьи Конвенции 108 прямо указывают на эффективность полномочий, функций и независимость надзорных органов при осуществлении свой деятельности.

Ограничение права на защиту персональных данных

Право на защиту персональных данных, в соответствии со статьей 8 Хартии основных прав ЕС, не является абсолютным правом, «но оно должно рассматриваться с точки зрения его применения в обществе». В статье 52 (1) Хартии говорится, что ограничения на права, аналогичные изложенным в статьях 7 и 8 Хартии основных прав ЕС, могут налагаться при условии, что:

– подобные ограничения предусмотрены законом;

– уважают суть этих прав и свобод;

– связаны с соблюдением принципа соразмерности;

– соответствуют целям, представляющим общий интерес, признанный в ЕС;

– существует необходимость защищать такие права.

Аналогичным образом Европейская конвенция о правах человека гарантирует защиту данных физических лиц при обработке. Осуществление данного права может быть ограничено для достижения законных целей.

Требования к обоснованному вмешательству в соответствии с Европейской Конвенцией о правах человека

Обработка персональных данных может представлять собой вмешательство в право субъекта данных на неприкосновенность частной жизни. Вопреки правовому порядку ЕС Европейская конвенция о правах человека не признает защиту персональных данных как фундаментальное право.

Действие статьи 8 Европейской конвенции о правах человека не распространяется на операции по обработке персональных данных, если не установлено, что частная жизнь человека была скомпрометирована.

В прецедентном праве Европейского суда по правам человека понятие «частная жизнь» охватывает также аспекты профессиональной деятельности и общественного поведения. Несмотря на широкое толкование понятия «частная жизнь», не все виды обработки сами по себе могут поставить под угрозу права, защищаемые статьей 8 Европейской конвенции о правах человека.

При рассмотрении дел о несоблюдении права на неприкосновенность частной жизни Европейскому суду по правам человека необходимо, установить являлось ли вмешательство оправданным. Право на неприкосновенность частной жизни не является абсолютным, но коррелирует с другими законными интересами и правами, будь то права других лиц (частные интересы) или общества в целом (общественные интересы).

Вмешательство может быть оправдано, если оно:

• осуществлено в соответствии с законом.

Согласно прецедентному праву, Европейский суд по правам человека осуществляет вмешательство на основании положений национального законодательства, которое определяет такое вмешательство. Закон должен быть «доступен для заинтересованных лиц и предсказуем в отношении его последствий». Прецедентным правом предусмотрено, что «правило сформулировано с достаточной точностью, для того чтобы дать возможность любому лицу определить свое поведение в той или иной ситуации». Кроме того, применение нормы закона в данном контексте будет зависеть от конкретного случая;

• преследовало законные цели.

Законные цели, которые могли бы оправдать вмешательство, в соответствии со статьей 8 (2) Европейской Конвенции о правах человека:

– интересы национальной безопасности;
– интересы общественной безопасности;
– интересы экономического благосостояния государства;
– предотвращение беспорядков и преступлений;
– охрана здоровья или нравственных устоев;
– защита прав и свобод других лиц;
• необходимо в демократическом обществе.

Европейский суд по правам человека заявил, что «понятие необходимости подразумевает, что вмешательство соответствует насущной социальной необходимости и соразмерно преследуемой законной цели».

При оценке необходимости вмешательства Европейский суд по правам человека изучает необходимость такого вмешательства и соответствие преследуемой цели. Также принимается во внимание, пытается ли вмешательство решить проблему, которая в случае бездействия может иметь негативные последствия для общества; есть ли доказательство того, что вмешательство может смягчить пагубный эффект и наличие общественного интереса.

Для определения соразмерности решения Европейский суд по правам человека всесторонне рассматривает необходимость и последствия подобного вмешательства. В прецедентном праве Европейского суда по правам человека пропорциональность рассматривается в рамках понятия необходимости. Соразмерность требует, чтобы вмешательство в права было пропорционально достижению законной цели.

Важными факторами, которые учитываются при определении соразмерности, являются:
– оценка масштаба вмешательства (количество затронутых лиц);
– меры предосторожности, введенные ограничения негативных последствий для физических лиц.

Условия для законных ограничений в соответствии с Хартией основных прав ЕС

Структура и формулировки Хартии основных прав ЕС отличаются от выводов прецедентного права Европейского суда по правам человека. Хартия не использует понятие вмешательства в гарантированные права, но содержит положения об ограничении при осуществлении прав и свобод, признанных Хартией.

Согласно статье 52 (1) ограничения на осуществление прав и свобод, признанных в Хартии, и, соответственно, права на защиту персональных данных, допустимы только в том случае, если они:
– предусмотрены законом;
– уважают суть права на защиту (в контексте закона);
– соответствуют принципам необходимости и пропорциональности;
– соответствуют целям, представляющим общий интерес, признанный Союзом, или;
– существует необходимость защищать права и свободы других лиц.

Поскольку защита персональных данных является отдельным фундаментальным правом в правовом порядке ЕС, защищенным в соответствии со статьей 8 Хартии, любая обработка сама по себе представляет собой вмешательство в это право.

Неважно, относятся ли рассматриваемые персональные данные к личной жизни человека, специальным категориями данных или нет. Чтобы вмешательство было законным, оно должно соответствовать всем условиям, перечисленным в статье 52 (1) Хартии:
• предусмотрено законом.

Ограничение прав на защиту персональных данных должно быть предусмотрено законом. Законодательство четко определяет объем и способ осуществления полномочий компе-

тентными органами по защите физических лиц от произвольного вмешательства, аналогично «законному вмешательству» прецедентного права Европейского суда по правам человека. Формулировка «предусмотрено законом», используемая в Хартии, должна интерпретироваться в соответствии с прецедентным правом Европейского суда по правам человека;

• уважение сути права.

В правопорядке ЕС любое ограничение основных прав, защищаемых Хартией, должно уважать суть этих прав. Это означает, что масштабные и навязчивые ограничения не могут быть оправданы, если лишают человека фундаментального права на защиту. Если сущность права скомпрометирована, ограничения признаются незаконными, без необходимости дополнительной оценки того, служит ли такое ограничение целям общего интереса и удовлетворяют ли они критериям необходимости и соразмерности;

• необходимость и пропорциональность.

Статья 52 (1) Хартии предусматривает, что при условии соблюдения принципа пропорциональности, ограничения на осуществление основных прав и свобод, признанных Хартией, могут устанавливаться только в случае необходимости.

В случае ограничения прав на уважение частной жизни и защиту личных данных, требуется оценка их соразмерности в отношении целей налагаемых ограничений. Суд Европейского Союза определяет применение «отступлений и ограничений в той степени, в которой они необходимы».

Соразмерность означает, что преимущества, вытекающие из ограничения, должны перевешивать недостатки, которые последние создают для осуществления основных прав, о которых идет речь. Чтобы уменьшить издержки и риски для осуществления прав на неприкосновенность частной жизни и защиту данных важно, чтобы ограничения содержали соответствующие гарантии.

Аналогичный подход в отношении принципа необходимости используется Европейским супервизором по защите данных. С помощью набора правовых инструментов (специально разработанных чек-листов) производится оценка соответствия предлагаемых мер законодательству ЕС в части защиты данных. Государственные деятели и законодатели ЕС, ответственные за подготовку и тщательное изучение законодательных мер, используют данные инструменты с целью унификации подхода в вопросах обработки персональных данных, а также соотношения с другими правами и свободами, закрепленными в Хартии;

• цели общественного интереса.

Для законного использования ограничений в части осуществления прав, признанных Хартией, они должны соответствовать целям общественного интереса, признанного в Европейском Союзе или необходимости защиты прав и свобод третьих лиц, которое часто пересекается с другими основными правами.

Что касается целей, представляющих общественный интерес, то к ним относятся цели ЕС, закрепленные в статье 3 Договора о Европейском Союзе:

– содействие миру и благополучию граждан ЕС;

– социальная справедливость и защита;

– создание зоны свободы, безопасности и правосудия, в которой обеспечивается свободное передвижение физических лиц в сочетании с надлежащими мерами по предупреждению и борьбы с преступлениями;

– а также другими целями и интересами, защищаемыми положениями договоров ЕС.

Общий регламент по защите данных ЕС 2016/679 в отношении использования ограничений, ссылается на статью 52 (1) Хартии. В статье 23 (1) Общего регламента перечисляется ряд целей общественного интереса, которые считаются законными для ограничения прав физических лиц при условии, что ограничения учитывают суть права на защиту данных и являются необходимым и пропорциональным:

– национальная безопасность и оборона;
– предупреждение преступлений;
– защита важных экономических и финансовых интересов ЕС и государств Евросоюза;
– общественное здравоохранение и социальное обеспечение и др.

Важно определить и раскрыть цели общественного интереса, преследуемого ограничением достаточно подробно, так как необходимость ограничения будет оцениваться с учетом данного параметра. Четкое описание цели ограничения и предлагаемых мер имеет важное значение для оценки того, является ли такое ограничение необходимым. Преследуемая цель, необходимость и пропорциональность являются основополагающими параметрами, рассматриваемыми при принятии решений.

Хартия основных прав ЕС и Европейская конвенция по правам человека

Несмотря на использование различных формулировок, условия для законного ограничения прав в статье 52 (1) Хартии основных прав ЕС схожи с приведенными в статье 8 (2) Европейской конвенции по защите прав человека, касающейся права на уважение частной жизни. В своем прецедентном праве Суд Европейского Союза и Европейский суд по правам человека часто ссылаются на суждения друг друга, и находятся в постоянном диалоге в поисках гармоничного толкования правил защиты данных. Статья 52 (3) Хартии гласит, что «так как Хартия содержит права, которые соответствуют правам, гарантированным Европейской конвенцией по правам человека, значение и объем этих прав, должен быть такой же, как установленный настоящей конвенцией».

Тем не менее статья 8 Хартии по содержанию не соответствует статье 8 (1) Европейской конвенции по правам человека.

Однако ввиду диалога и тесного сотрудничества между двумя судами, при анализе законодательства Суд Европейского Союза может принимать во внимание критерии законного ограничения в соответствии со статьей 8 Европейской конвенции по правам человека в интерпретации Европейского суда по правам человека. Возможен и противоположный сценарий, при котором Европейский суд по правам человека может ссылаться на условия законного ограничения в соответствии с Хартией.

В любом случае следует также принять во внимание, что в Европейской конвенции по правам человека не существует прямого эквивалента статьи 8 Хартии, которая касается защиты персональных данных и, в частности, прав субъекта данных, перечня законных оснований для обработки и надзора со стороны независимого органа. Некоторые положения статьи 8 Хартии, могут быть заложены в прецедентном праве Европейского суда по правам человека, разрабатываемом в соответствии со статьей 8 Европейской конвенции по правам человека и затрагивающем Модернизированную Конвенцию 108. Эта взаимосвязь правовых систем позволяет поддерживать конструктивный диалог между Судом Европейского Союза и Европейским судом по правам человека по вопросам, связанным с защитой данных.

Закон о защите данных ЕС

Право ЕС состоит из основного и вторичного права. Договор о Европейском Союзе и Договор о функционировании Европейского Союза были ратифицированы всеми государствами Евросоюза и образуют «основной» закон ЕС. Регламенты, директивы и решения, принятые институтами ЕС, составляют «вторичный» закон.

Защита данных в «основном» законодательстве ЕС

Изначально соглашения европейских сообществ не содержали каких-либо ссылок на права человека или их защиту, так как европейское экономическое сообщество создавалось как региональная организация, ориентированная на экономическую интеграцию и создание общего рынка.

Основополагающим принципом, лежащим в основе развития европейских сообществ, является принцип наделения компетенциями. Согласно этому принципу ЕС действует только в пределах полномочий, предоставленных ему государствами-членами, как это отражено в договорах ЕС. В отличие от Совета Европы договоры ЕС не содержат четкой компетенции в вопросах основных прав.

Суд Европейского Союза при рассмотрении дел о нарушениях прав человека в областях, попадающих под действие законодательства ЕС, предоставляет важную интерпретацию договоров ЕС. В целях предоставления защиты для основных прав физических лиц, Суд имплементировал основные права в общие принципы европейского права. Согласно заявлению Суда, эти принципы отражают право на защиту данных в национальных законодательствах стран ЕС. Европейский Суд заявил о соответствии национального права стран Евросоюза требованиям защиты основных прав субъектов данных.

В 2000 году Европейским парламентом была принята Хартия основных прав ЕС. Хартия включает в себя весь спектр гражданских, политических, экономических и социальных прав европейских граждан, объединяя конституционные и международные обязательства, общие для государств – членов ЕС. Права, описанные в Хартии разделены на шесть частей:

– достоинство;
– свободы;
– равенство;
– солидарность;
– права граждан;
– справедливость.

Юридически обязательным документом, одним из основных законов ЕС (статья 6.1 Договора о Европейском Союзе), Хартия стала после подписания Лиссабонского договора 1 декабря 2009 года. Положения Хартии адресованы институтам и органам ЕС, что обязывает последних при исполнении своих обязанностей уважать закрепленные в Хартии права. Положения Хартии также учитываются государствами Евросоюза в рамках европейского законодательства.

Хартия декларирует не только уважение частной и семейной жизни (статья 7), но и закрепляет право на защиту личных данных (статья 8). Статья 8 Хартии содержит законодательное обоснование и поддержку сформированной ранее Директивы о защите данных. Хартия прямо упоминает право на защиту данных (статья 8.1), ссылается на ключевые принципы защиты данных (статья 8.2) и обязывает надзорные органы контролировать реализацию этих принципов. Право на защиту личных данных является одним из основных прав в законодательстве ЕС. Учреждения и органы ЕС обязаны гарантировать и уважать это право, как и государства Евросоюза при применении законодательства ЕС (статья 51).

Ратификация Лиссабонского договора является важной вехой в развитии закона о защите данных. Договор не только повысил статус Хартии до статуса основного юридически обязательного документа, но и обеспечил право на защиту данных. Это право предусмотрено в статье 16 Договора о функционировании Европейского Союза, где приведено описание общих принципов ЕС. Норма Договора создает новую правовую основу, предоставляя ЕС полномочия принимать законы по вопросам защиты данных.

Это важное событие, так как правила защиты данных в ЕС, в частности, Директива о защите данных, изначально базировалась на правовой структуре внутреннего рынка и необходимости унификации национального законодательства для свободного перемещения данных в ЕС. Договор о функционировании Европейского Союза обеспечивает независимую правовую основу для современного, комплексного подхода к защите данных, который охватывает все вопросы компетенции ЕС, включая сотрудничество правоохранительных и судебных органов по уголовным делам.

Статья 16 Договора о функционировании Европейского Союза также подтверждает, что соблюдение правил защиты данных, принятых в соответствии с ней, должно быть предметом контроля независимых органов. Положения Договора о функционировании Европейского Союза послужили правовой основой для проведения всеобъемлющей реформы правил защиты данных в 2016 году, принятия Общего регламента по защите данных ЕС и Директивы о защите данных для органов полиции и уголовного правосудия.

Общий регламент по защите данных ЕС 2016/679

С 1955 года до середины 2018 года основным правовым документом ЕС по защите данных была Директива 95/46/ЕС Европейского Парламента и Совета Европы от 24 октября 1995 года о защите физических лиц в отношении обработки персональных данных и о свободном передвижении таких данных. Директива о защите данных вступила в силу уже после принятия некоторыми государствами ЕС национальных законодательных актов в части защиты данных. Возникла необходимость согласования подобных инициатив в целях обеспечения высокого уровня защиты и свободного потока личных данных между государствами Евросоюза. Свободное перемещение физических лиц, товаров, капитала и услуг на внутреннем пространстве требует свободного потока данных, реализация которого позволит государствам ЕС рассчитывать на единый высокий уровень защиты данных.

Директива дополняет принципы защиты данных, содержащиеся в Конвенции 108 и национальном законодательстве. В частности, внесение в Директиву нормы о независимом надзоре, как инструменте, используемом в целях эффективного соблюдения правил защиты данных, стало важным вкладом в функционирование европейского законодательства о защите данных. Данная норма была имплементирована в Конвенцию 108 в качестве best practices.

В соответствии с правовой системой ЕС положения Директивы должны быть имплементированы в национальное право государств Евросоюза. Страны ЕС по своему усмотрению проводят интеграцию положений в свое национальное право. Несмотря на то что цели Директивы были направлены на обеспечение полной гармонизации (и адекватности уровня защиты данных), на практике в странах Европейского Союза она была внедрена по-разному. Это привело к установлению различных правил защиты данных по всему ЕС с определениями и нормами, по-разному интерпретируемыми в национальном законодательстве. Совокупность данных факторов послужили причиной реформирования европейского законодательства по защите данных.

Реформа привела к созданию Общего регламента по защите данных ЕС 2016/679 в апреле 2016 года. Дискуссии о необходимости модернизации правил защиты данных ЕС начались в 2009 году, когда Европейская комиссия инициировала обществен-

ные консультации о будущей правовой базе для обеспечения основного права физических лиц на защиту личных данных. Предложение о регулировании было опубликовано в январе 2012 года, положив начало длинному процессу переговоров между Европейским Парламентом и Советом Европы. После принятия Общего регламента по защите данных был предусмотрен двухлетний переходный период. Общий регламент по защите данных вступил в силу в мае 2018 года, тем самым отменив действие Директивы 95/46/ЕС.

В соответствии с законодательством ЕС, нормы Регламента имеют прямое применение без необходимости имплементации в национальное право. Таким образом, Общий регламент по защите данных предусматривает единый набор правил на всей территории ЕС. Это создает среду правовой определенности, от которой выигрывают как экономические «операторы», так и частные лица (субъекты данных).

Несмотря на то, что Общий регламент по защите данных ЕС 2016/679 является самостоятельным документом, ожидается, что государства Евросоюза внесут необходимые изменения в национальное законодательство в части защиты данных. Регламент имеет глобальное экстерриториальное действие. Его требования распространяются на организации в ЕС, а также на контроллеров и процессоров за его пределами, предлагающие товары и услуги субъектам данных в Евросоюзе или осуществляющие профилирование данных граждан ЕС. Определенная доля организаций, расположенных за пределами ЕС, имеют ключевую долю на европейском рынке и миллионы клиентов из ЕС. Соблюдение этими организациями правил защиты данных имеет важное значение для обеспечения защиты субъектов данных, а также для обеспечения равных условий.

Защита данных в правоохранительных органах Директива 2016/680

Общей регламент по защите данных обеспечивает экстерриториальность защиты данных. Поскольку действие отмененной Директивы о защите данных распространялось на внутреннее пространство ЕС и деятельность его государственных институтов, то было необходимо соблюдать баланс между защитой данных и другими законными интересами, в том числе при обработке персональных данных правоохранительными органами.

Первым правовым документом ЕС, регулирующим этот вопрос, было решение 2008/977 JHA Совета Европы. Его действие распространяется на обмен данными между полицейскими и судебными органами ЕС в рамках сотрудничества по уголовным делам. Обработка персональных данных в обеспечении деятельности правоохранительных органов не регулируется нормами решения 2008/977 JHA.

Одновременно с Общим регламентом по защите данных вступила в силу Директива 2016/680 о защите физических лиц в отношении обработки персональных данных компетентными органами в целях предотвращения, расследования, выявления преступлений или судебного преследования за совершение уголовных преступлений или исполнения уголовных наказаний, а также о свободном перемещении таких данных – Директива о защите данных для органов полиции и уголовного правосудия.

В то время как Общей регламент по защите данных устанавливает общие правила для защиты физических лиц в отношении обработки их персональных данных и для обеспечения свободного перемещения таких данных в пределах ЕС, в Директиве изложены конкретные правила защиты данных в областях судебной власти и сотрудничества правоохранительных органов. Директива 2016/680 применяется, когда компетентный орган обрабатывает персональные данные в целях предотвращения, расследования, выявления или преследования за совершение уголовных преступлений. Если компетентные органы обрабатывают персональные данные для

целей, отличных от вышеупомянутых, применяется общий режим в соответствии с Общим регламентом по защите данных.

В отличие от решения Совета Европы 2008/977 JHA, положения Директивы 2016/680 затрагивают внутреннюю обработку персональных данных правоохранительными органами в том числе и за пределами ЕС, и нацелены на достижение баланса между правами физических лиц и законными целями обработки, связанной с национальной безопасностью.

Директива подтверждает право на защиту персональных данных и основные принципы, которые должны охватывать обработку данных в строгом соответствии с правилами и принципами Общего регламента по защите данных. Права субъектов данных и обязанности, налагаемые на контроллеров (например, в части безопасности данных, защиты данных по умолчанию, уведомления о нарушении в отношении персональных данных субъектов), идентичны правам и обязанностям Общего регламента по защите данных. Контроллер обязан назначить сотрудника для контроля за соблюдением правил защиты данных, информирования и консультационной поддержки организаций и работников, а также для сотрудничества с надзорными органами.

Директива также учитывает и осуществляет контроль над технологиями обработки, которые могут стать обременительными для субъектов данных (например, использование профилирования правоохранительными органами). В целом, все решения, основанные исключительно на автоматизированной обработке, включая профилирование, должны быть запрещены. Кроме того, такой вид обработки не применим к «специальным» категориям данных.

В настоящее время обработка персональных данных правоохранительными структурами и органами уголовного правосудия находится под контролем независимых надзорных органов.

Директива о конфиденциальности и электронных средствах связи

С целью обеспечения прав пользователей на неприкосновенность частной жизни и соблюдения конфиденциальности была разработана и внедрена Директива 2002/58/ЕС. Положения Директивы о конфиденциальности и электронных средствах связи устанавливают правила безопасности в части обработки персональных данных и защиты конфиденциальности в электронных сообщениях.

Операторы услуг электронной связи обязуются ограничить доступ к персональным данным всем, кроме уполномоченных лиц, и принять меры для предотвращения уничтожения, потери или случайного повреждения данных. В случае наличия возможного риска при использовании сервисов, оператор связи обязан проинформировать пользователя сервиса о наличии такого риска. В случае нарушения, несмотря на предпринятые меры защиты, операторы обязаны уведомить компетентный национальный орган, которому поручен контроль за выполнением Директивы. Операторам также вменяется в обязанность уведомлять субъектов данных о нарушениях, которые могут оказать негативное влияние на конфиденциальность данных. Для обеспечения конфиденциальности сообщений требуется, чтобы прослушивание, хранение или любой вид наблюдения или перехвата сообщений и метаданных, по умолчанию был запрещен. Директива также запрещает нежелательные спам-сообщения, если только субъекты данных не дали на это свое согласие. На электронных устройствах субъекта данных должны быть определены правила хранения файлов cookie. Данные обязательные нормы указывают на то, что конфиденциальность сообщений в значительной степени связана с защитой права на уважение частной жизни и персональных данных, закрепленные в статьях 7 и 8 Хартии основных прав ЕС соответственно.

В январе 2017 года для модернизации Директивы о конфиденциальности и электронных средствах связи комиссия Совета Европы опубликовала предложения о регулировании, касающегося уважения частной жизни и защиты личных данных в электронных сообщениях.

Цель реформы заключается в унификации правил, регулирующих электронные коммуникации в соответствии с требованиями Общего регламента по защите данных. Новый Регламент распространяется на все государства ЕС, что позволит обеспечить одинаковый уровень защиты электронных сообщений. Прозрачность, правовая определенность и внедрение единого набора правил на территории ЕС коррелируют права субъектов данных, телекоммуникационных операторов и организаций.

Предлагаемые правила конфиденциальности электронных сообщений также распространяются на новых поставщиков услуг и сервисов, когда как положения старой Директивы касались только традиционных поставщиков телекоммуникационных услуг. Широко распространенные сервисы для отправки сообщений или звонков такие как Skype, WhatsApp, Facebook (организация запрещена на территории РФ), Viber (и подобные) подпадают под юрисдикцию Общего регламента по защите данных и должны обеспечить соответствие требованиям по защите данных, конфиденциальности и безопасности. На момент написания этой книги процесс обсуждения модернизации Директивы еще не был окончен.

Регламент №45/2001

Для защиты физических лиц в отношении обработки персональных данных учреждениями и органами ЕС был разработан Регламент ЕС №45/2001, контроль за исполнением которого возложен на Европейского супервизора по защите данных.

Европейский супервизор наделен полномочиями по надзору и обязанностью контролировать обработку персональных данных в учреждениях и органах ЕС, а также рассматривать и расследовать жалобы на предполагаемые нарушения правил защиты данных. Он также предоставляет консультации учреждениям и органам ЕС по различным вопросам: начиная от предложений по новому законодательству и заканчивая разработкой внутренних правил, касающихся обработки данных. В январе 2017 года Европейская комиссия представила предложения по новому регламенту обработки данных институтами ЕС, который отменит действующее положение.

Как и в случае с Директивой о конфиденциальности и электронных средствах связи, реформа Регламента №435/2001 позволит актуализировать и унифицировать документ в соответствии с положениями Общего регламента по защите данных ЕС 2016/679.

Роль Суда Европейского Союза

Суд Европейского Союза обладает юрисдикцией для определения выполнения государствами ЕС своих обязательств в соответствии с европейским законодательством о защите данных и обеспечения его эффективного и единообразного применения во всех государствах Евросоюза.

С момента принятия Директивы о защите данных в 1995 году накопился значительный объем прецедентного права, в котором разъясняется сфера охвата и значения принципов защиты данных, а также фундаментальное право на защиту данных, закрепленное в статье 8 Хартии основных прав ЕС. Несмотря на то что Директива была отменена и вступил в законную силу Общий регламент по защите данных, прецедентное право остается актуальным для толкования и применения принципов защиты данных ЕС.

Взаимодействие с другими правами и законными интересами

Право на защиту персональных данных не является абсолютным правом, условия законного ограничения этого права были подробно изложены выше. Одним из критериев законного ограничения прав субъекта, признанных как в соответствии с законодательством Совета Европы, так и в ЕС, является защита прав и свобод других субъектов при вмешательстве в защиту данных. Там, где защита данных взаимодействует с другими правами, как Европейский суд по правам человека, так и Суд Европейского Союза неоднократно заявляли, что для сохранения баланса с другими правами необходимо при применении и толковании статьи 8 Европейской конвенции по правам человека и статьи 8 Хартии основных прав ЕС.

В целях соблюдения баланса правовых систем государства ЕС могут внедрить необходимые нормы закона для согласования права на защиту данных с другими правами субъектов данных. По этой причине в Общем регламенте по защите данных существует ряд областей права, в котором предусмотрено отступление на национальном уровне.

Что касается свободы выражения мнений, то Общий регламент по защите данных требует от государств Евросоюза законодательно согласовать «право на защиту персональных данных с правом на свободу выражения мнений и получения/распространения информации, включая обработку в целях журналистики, академического, художественного и литературного выражения». Государства ЕС могут также принять законы для совмещения защиты данных с публичным доступом к официальным документам и обязательствами сохранения профессиональной тайны, защищенными как форма права на уважение частной жизни.

Свобода самовыражения

Право, которое в наибольшей степени взаимодействует с правом на защиту данных, – право на свободу выражения мнения.

Свобода выражения мнений защищена статьей 11 Хартии Основных прав («Свобода выражения мнений и информации»). Это право включает «свободу придерживаться своего мнения, получать и распространять информацию и идеи без вмешательства со стороны публичных властей и независимо от государственных границ». Свобода информации, как в соответствии со статьей 11 Хартии, так и в соответствии со статьей 10 Европейской конвенции по правам человека, защищает право не только передавать, но и получать информацию.

Ограничение свободы выражения мнений должно соответствовать критериям, предусмотренных статьей 52 (1) Хартии основных прав ЕС. В соответствии со статьей 52 (3) Хартии, «значение и объем этих прав должны быть таким же, как и установленные указанной конвенцией». Ограничения, которые могут на законных основаниях быть наложены на право, гарантированное статьей 11 Хартии, не могут превышать ограничения, предусмотренные статьей 10 (2) Европейской конвенции по правам человека. Такие права включают, в частности, право на неприкосновенность частной жизни и права на защиту персональных данных.

Взаимосвязь между защитой личных данных и свободой выражения мнений регулируются статьей 85 «Обработка, свобода выражения и информации» Общего регламента по защите данных ЕС 2016/679. Согласно этой статье, государства ЕС должны согласовывать право на защиту персональных данных с правом на свободу выражения мнений и информации. Исключения и отступления от норм Общего регламента по защите данных могут быть сделаны для целей журналистики или для академического, художественного или литературного выражения, так как они необходимы для баланса права на защиту персональных данных с правом выражения мнения и информации.

В прецедентном праве Европейского суда по правам человека одним из важнейших критериев, касающихся сбалансированности этих прав, является вопрос о том, удовлетворяет ли данное решение интересы широкой общественности.

Право на свободу выражения мнения и право на защиту персональных данных не всегда конфликтуют друг с другом. Есть случаи, когда эффективная защита данных гарантирует свободу выражения мнений.

Право на получение информации, которое также является частью свободы выражения мнений, зачастую определяет прозрачность действий правительства для функционирования демократического общества. Прозрачность – цель интереса общественности, которая может оправдать вмешательство в право на защиту данных, если это необходимо и соразмерно. В результате за последние два десятилетия право на доступ к документам, находящимся в распоряжении государственных органов, было признано важным правом каждого гражданина ЕС и любого физического и юридического лица, проживающего или имеющего зарегистрированное юридическое лицо на территории государств Евросоюза.

Законодательство Совета Европы ссылается на принципы, закрепленные в «Конвенции Совета Европы по доступу к официальным документам» (CETS 205).

В соответствии с законодательством ЕС право на доступ к документам гарантируется Регламентом 1049/2001 ЕС и касается публичного доступа к документам Европейского парламента, Совета Европы и к документам Комиссии ЕС. Документы Комиссии (Положение о доступе к документам), статья 42 Хартии основных прав ЕС и статья 15 (3) Договора о функционировании Европейского Союза расширили право на доступ «к документам учреждений, органов и агентств Союза независимо от их формы».

Это право может вступать в конфликт с правом на защиту данных, если доступ к документу может раскрыть личные данные других лиц. Статья 86 Общего регламента по защите данных четко предусматривает, что персональные данные в официальных документах, находящихся в распоряжении государственных органов, могут быть раскрыты соответствующими институтами в соответствии с законодательством ЕС или государства Евросоюза.

Подобные запросы о доступе к документам или информации должны быть соотнесены с правом на защиту лиц, чьи данные содержатся в запрашиваемых документах.

Подход Европейского суда по правам человека в отношении конфиденциальности и доступа к документам оценивается с учетом следующих критериев:

– цель запроса информации;
– характер запрашиваемой информации;
– роль заявителя;
– готовность и доступность информации.

Профессиональная тайна

Профессиональную тайну можно понимать, как особый этический долг, который влечет за собой юридическое обязательство, присущее определенным профессиям и функциям, основанным на вере и доверии. Лица и учреждения, выполняющие эти функции, обязаны не разглашать конфиденциальную информацию, полученную ими в ходе выполнения своих обязанностей. Профессиональная тайна прежде всего относится к врачебной тайне и привилегированным отношениям между адвокатом и клиентом, во многих юрисдикциях также признается обязательство профессиональной тайны в финансовом секторе.

Профессиональная тайна не является фундаментальным правом, но защищается как форма права на неприкосновенность частной жизни. Суд Европейского Союза постановил, что в некоторых случаях «превалирует запрет разглашения определенной информации, которая классифицируется как конфиденциальная, для защиты основного права на уважение частной

жизни, закрепленное в статье 8 Европейской конвенции по правам человека и статьей 7 Хартии основных прав ЕС». Европейский суд по правам человека также принимает решения о том, являются ли ограничения профессиональной тайны нарушением статьи 8 Европейской конвенции о правах человека.

Взаимодействие между правом на профессиональную тайну и правом на защиту данных неоднозначно. С одной стороны, правила защиты данных и гарантии, установленные в законодательстве, обеспечивают право на профессиональную тайну. Правила для контроллеров и процессоров, направленные на реализацию надежных мер безопасности, в том числе касаются сохранности конфиденциальных личных данных, защищенных профессиональной тайной. Кроме того, Общий регламент по защите данных ЕС позволяет обрабатывать данные о состоянии здоровья, которые представляют собой специальную категорию персональных данных, но при этом делают обязательным применение усиленных мер по защите прав субъектов данных, в том числе при обеспечении профессиональной тайны.

С другой стороны, обязательство сохранения профессиональной тайны, налагаемое на контроллеров и процессоров в отношении определенных персональных данных, могут ограничивать права субъекта данных, в частности, право на получение информации. Несмотря на то что Общий регламент по защите данных содержит обширный список информации, которая должна быть предоставлена субъекту данных в соответствии с правовыми системами ЕС и национальным законодательством, требование о раскрытии данных не применяется в случае, если данные были получены от третьих лиц и существует обязательство по сохранению профессиональной тайны.

Общий регламент по защите данных предусматривает возможность принятия государствами ЕС специальных правил для защиты профессиональных или эквивалентных обязательств в отношении примирения права на защиту персональных данных и профессиональной тайны.

В рамках Общего регламента по защите данных предусмотрено, что государства Евросоюза могут принимать правила о полномочиях надзорных органов в отношении контроллеров и процессоров, на которых распространяется обязанность соблюдения профессиональной тайны. Эти правила относятся к возможности получения доступа к помещению контроллера или процессора, его системам и оборудованию для обработки и хранения таких данных, если такие данные были получены в ходе деятельности по соблюдению профессиональной тайны. Таким образом, надзорные органы, на которые возложена защита данных, обязаны соблюдать профессиональную тайну и обязательства, которые связывают контроллеров и процессоров. Статья 54 (2) Общего регламента по защите данных четко предусматривает, что надзорные органы обязаны соблюдать профессиональную тайну в отношении такой конфиденциальной информации, в том числе после прекращения их полномочий.

Кроме того, государства Евросоюза обязаны уведомлять Комиссию ЕС о правилах, которые они принимают для согласования норм защиты данных и о принципах, установленных в национальных законодательствах касательно обязательств по сохранению профессиональной тайны.

Свобода вероисповедания и убеждений

Свобода вероисповедания и убеждений защищена статьей 9 Европейской конвенции о правах человека и статьей 10 Хартии основных прав ЕС. Личные данные, раскрывающие религиозные или философские убеждения, считаются специальными категориями персональных данных в соответствии с законодательством ЕС и Совета Европы, а их обработка и использования подлежат усиленным мерам защиты.

Согласно Общему регламенту по защите данных ЕС и Модернизированной Конвенции 108, персональные данные, обрабатываемые для целей научных и исторических исследований, могут храниться в течение более длительных периодов времени. Кроме того, независимо от первоначальной цели обработки, последующее использование персональных данных для научных исследований не должно считаться несовместимой целью. Однако в целях защиты прав и свобод субъектов данных при такой обработке должны быть приняты соответствующие меры предосторожности. Законодательство ЕС или национальное право страны Евросоюза может предусматривать отступление от прав субъекта, таких как право на доступ, исправление, ограничение обработки и возражений против такой обработки, в случае обработки их персональных данных в целях научных, исторических или статистических исследований.

Защита интеллектуальной собственности

Интеллектуальная собственность охватывает не только художественные, литературные или музыкальные произведения, но также патенты, товарные знаки и смежные права.

Право на защиту интеллектуальной собственности закреплено в статье 1 Первого Протокола к Европейской конвенции по правам человека, а также в статье 17 (1) Хартии основных прав ЕС. Одним из аспектов права, который особенно важен для защиты данных, является защита интеллектуальной собственности, прямо упомянутая в статье 17 (2) Хартии основных прав ЕС. Некоторые нормативные документы ЕС, такие как Директива ЕС №92/100/ЕЕС, №93/83/ЕЕС и другие, направлены на эффективную защиту интеллектуальной собственности, в частности авторского права. Защита интеллектуальной собственности также должна быть сбалансирована с другими основными правами, в частности с правом на защиту данных.

Защита данных и экономические интересы

Некоторые компании полагают, что нормативные требования в части защиты личных данных, на практике, приведут к чрезмерно обременительным обязательствам. Таким образом, возникает вопрос о том, могут ли экономические интересы контроллеров/процессоров или общественности превалировать над ограничением права на защиту данных.

Предоставление физическим лицам большего контроля над своими личными данными является одним из приоритетов законодательства ЕС о защите данных. Существует дисбаланс между возможностями компаний, которые обрабатывают и имеют доступ к огромным объемам персональных данных, и возможностями физических лиц, которым эти персональные данные принадлежат. Суд Европейского Союза использует индивидуальный подход при корреляции права на защиту данных и экономических интересов, таких как интересы третьих сторон в отношении акционерных обществ и компаний с ограниченной ответственностью.

В правовых системах ЕС, законодательных актах и рекомендациях соответствующих органов огромное значение придается достижению целей законодательного регулирования. Суд Европейского Союза и Европейский суд по правам человека призваны соблюдать баланс принципов и прав при достижении целей законодательства.

Таким образом, мы можем говорить о том, что правовые системы ЕС направлены на соблюдение основных прав субъектов данных и общественности и ни одна норма закона не должна трактоваться вразрез с указанными целями и принципами.

Ключевые моменты

Право на защиту персональных данных:

– Конвенция Совета Европы является первым и единственным международным, юридически обязательным документом, касающимся защиты данных. Конвенция прошла модернизацию, завершившуюся принятием поправки к Протоколу СДСЕ №223, далее Модернизированная Конвенция 108;

– в соответствии с законодательством ЕС защита данных была признана в качестве отдельного фундаментального права (статья 16 Договора о функционировании ЕС, а также статья 8 Хартии основных прав ЕС);

– право человека на защиту в отношении обработки персональных данных является частью права на неприкосновенность частной и семейной жизни, жилища и переписки (тайна личной переписки) в соответствии со статьей 8 Европейской конвенции по правам человека;

– Общий регламент по защите данных вступил в силу в мае 2018 года, отменив Директиву о защите данных;

– при обработке персональных данных государственными органами для правоохранительных целей применяется Директива (ЕС) 2017/680.

Ограничение права на защиту персональных данных:

– право на защиту персональных данных не является абсолютным правом, оно может быть ограничено, если это необходимо, для целей общего интереса или для защиты прав и свобод других лиц;

– условия ограничения прав на уважение частной жизни и защиту персональных данных перечислены в статье 8 Европейской конвенции о правах человека и статье 52 (1) Хартии основных прав ЕС. Соответствующие условия были разработаны и интерпретированы в рамках прецедентного права Европейского суда по правам человека и Суда Европейского Союза;

– в соответствии с Общим регламентом по защите данных обработка персональных данных представляет собой законное вмешательство в право на неприкосновенность частной жизни и может осуществляться, только если оно соответствует закону, основным правам и свободам; преследует законные цели; необходимо и соразмерно целям демократического общества;

– правовой порядок ЕС налагает аналогичные условия на ограничения в осуществлении основных прав, защищаемых Хартией основных прав ЕС. Любое ограничение любого основного права, в том числе защиты персональных данных, может быть законным, только если оно соответствует закону, основным правам и свободам; пропорционально и соразмерно цели обработки; преследует цель общего интереса, признанного в ЕС или необходимостью защищать права других субъектов данных.

Взаимодействие с другими правами и законными интересами:

– право на защиту данных часто взаимодействует с другими правами, такими как свобода выражения мнений, право на получение и распространение информации;

– взаимодействие с другими правами зачастую противоречит конкретному праву. Существуют ситуации, когда право на защиту персональных данных эффективно обеспечивает соблюдение иного права. Например, свобода выражения мнений является составляющим компонентном неприкосновенности частной жизни, ее защита обеспечивается фундаментальным правом;

– необходимость защиты прав и свобод других лиц является одним из критериев, используемых для оценки законного ограничения права на защиту персональных данных;

– суды обязаны соблюдать баланс при использовании двух правовых систем;

– Общий регламент по защите данных ЕС требует, чтобы государства Евросоюза согласовывали право на защиту персональных данных с правом на свободу выражения мнения, получения и распространения информации;

– государства ЕС обязаны внедрять конкретные нормы в национальном законодательстве для обеспечения права на защиту персональных данных с публичным доступом к официальным документам.

Выдержки из решений Суда Европейского Союза и Европейского суда по правам человека

Неприкосновенность частной жизни

Судом Европейского Союза рассматривалось дело о соответствии законодательству Директивы 2006/24/ЕС в части основных прав на защиту личных данных и неприкосновенности частной жизни. Директива обязывала поставщиков услуг электронной связи или сетей общего пользования хранить данные цифровой связи граждан сроком до двух лет для обеспечения доступа к этим данным в целях предотвращения, расследования и судебного преследования серьезных преступлений. Мера касалась только метаданных, данных о местоположении и информации, необходимой для идентификации абонента или пользователя и не распространялась на содержание электронных сообщений.

Суд Европейского Союза посчитал это вмешательством в основополагающее право на защиту персональных данных. Кроме того, Суд установил, что Директива нарушала право на неприкосновенность частной жизни в целом. Предоставляемые персональные данные позволяли «сделать точные выводы о частной жизни лиц, такие как поведенческие привычки, постоянные или временные места жительства, ежедневные или иные перемещения, социальные отношения этих лиц и часто посещаемая ими социальная среда». Вмешательство в эти два права является достаточно серьезным и широкомасштабным.

Суд Европейского Союза объявил Директиву 2006/24/ЕС недействительной. Хотя она преследовала законную цель, вмешательство в право на защиту личных данных было достаточно серьезным и не ограничивалось строгой необходимостью.

Вмешательство в права субъекта данных, осуществляемые в соответствии с законодательством

В деле *Rotaru против Румынии* заявитель утверждал о нарушении его права на неприкосновенность частной жизни в связи с получением и использованием Румынской разведывательной службой файла, содержащего личную информацию субъекта. Европейский суд по правам человека установил, что хотя национальное законодательство Румынии разрешает сбор, запись и архивирование в закрытых файлах информации, затрагивающей вопросы национальной безопасности, оно не устанавливает каких-либо ограничений на осуществление таких полномочий, оставляя данный вопрос на усмотрение властей. Например, национальное законодательство не определяет тип информации, которую можно обрабатывать, обстоятельства и категории субъектов данных, в отношении которых могут быть приняты меры наблюдения или процедуры, которым необходимо следовать.

Таким образом, Европейский суд по правам человека пришел к выводу, что национальное законодательство не соответствовало принципам предсказуемости в соответствии со статьей 8 Европейской конвенции о правах человека и данная норма была нарушена.

В деле *Taylor-Sabori против Соединенного Королевства* заявитель был объектом надзора правоохранительных органов. Используя «клон» пейджера заявителя, полиция смогла перехватить отправленные ему сообщения. Заявитель был арестован и обвинен в продаже запрещенного наркотического вещества. Часть обвинения строилась на расшифрованных сообщениях личного средства коммуникации.

Однако на момент судебного разбирательства в британском законодательстве не было положения, регулирующего перехват электронных сообщений. Таким образом, вмешательство

в его права не было произведено «в соответствии с законом». Европейский суд по правам человека пришел к выводу, что это нарушает статью 8 Европейской конвенции о правах человека.

Преследуемые законные цели

В деле *Peck против Соединенного Королевства* заявитель пытался покончить жизнь самоубийством на улице, порезав запястья. Полиции, которая наблюдала за происходящим через камеры уличного видеонаблюдения, удалось спасти пострадавшего. Впоследствии отснятый материал был передан в средства массовой информации и был опубликован без маскировки лица заявителя.

Европейский суд по правам человека установил, что не было соответствующих или достаточных причин, которые оправдывали прямое раскрытие материалов властям и общественности без получения согласия заявителя или сокрытия его личности. Суд пришел к выводу, что имело место нарушение статьи 8 Европейской конвенции о правах человека.

Необходимость вмешательства в демократическом обществе

Дело *Khelili против Швейцарии*. Во время проверки полиция обнаружила у заявителя при себе визитные карточки следующего содержания: «Милая, симпатичная женщина, бальзаковского возраста хотела бы встретиться с мужчиной для приятного времяпрепровождения, телефона нет». Заявитель утверждала, что после задержания полиция внесла ее данные в карточку учета как лица, занимающегося проституцией, хотя она отрицала такой род занятий.

Заявитель просила удалить слово «проститутка» из карточки учета полиции. Европейский суд по правам человека признал, что сохранение личных данных лица на том основании, что это лицо может преступить закон, не является соразмерными действиями. Утверждение о незаконном занятии проституцией выглядело расплывчатым и не подкреплялось конкретными фактами. Заявитель никогда не была осуждена за занятие незаконной проституцией и потому факт внесения рода занятий в полицейскую карточку не удовлетворял «насущной социальной потребности» в рамках трактовки статьи 8 Европейской конвенции о правах человека.

Касательно серьезности вмешательства в права заявителя и того факта, что власти должны доказать точность хранящихся данных, Суд постановил, что формулировка «проститутка» в материалах полиции на протяжении многих лет не было необходимым в демократическом обществе. Суд пришел к выводу, что имело место нарушение 8 Европейской конвенции о правах человека.

По делу *S. and Marper против Соединенного Королевства* оба заявителя были арестованы и обвинены в уголовных преступлениях. Полиция взяла их отпечатки пальцев и образцы ДНК, как это предусмотрено Законом о полиции и обстоятельствами уголовного дела. Заявители не были осуждены за преступления: один был оправдан в зале суда, уголовное дело в отношении второго было прекращено. Тем не менее их отпечатки, профили и образцы ДНК были сохранены в базе данных полиции и национальное законодательство разрешило их хранение без ограничения по срокам.

Соединенное Королевство утверждало, что задержание помогло установить личности предполагаемых преступников, и, таким образом, преследовало законную цель предупреждения и раскрытия уголовных преступлений. Однако Суд постановил, что вмешательство в право заявителей на неприкосновенность частной жизни неоправданно. Он напомнил, что основные принципы защиты данных требуют, чтобы сохранение персональных данных было пропорционально по отношению к цели сбора и что сроки хранения должны быть ограничены. Суд согла-

сился с тем, что расширение базы данных полиции с целью включения в нее профилей ДНК не только осужденных, но и подозреваемых в совершении уголовных преступлений могло бы способствовать выявлению и предотвращению преступлений в Соединенном Королевстве. Тем не менее фундаментальное право субъектов было нарушено. Учитывая огромное количество генетической и медицинской информации, содержащейся в клеточных образцах, вмешательство в право заявителя на частную жизнь было чрезмерным. Отпечатки пальцев и образцы могут быть взяты у арестованных и храниться в базе полиции неограниченное количество времени, в случае если арестованный впоследствии будет осужден.

Также Суд уделил особое внимание тому факту, что заявителю на момент ареста было 11 лет. Сохранение личных данных несовершеннолетнего, который не был осужден, может оказать негативное влияние на его социальное развитие и интеграцию в обществе. Суд единогласно постановил, что их хранение представляет собой несоразмерное вмешательство в право на личную жизнь, которое не может считаться необходимым в демократическом обществе.

В деле *Leander против Швеции* Суд постановил, что тайный контроль за физическими лицами, кандидатами на важные должности в сфере национальной безопасности, само по себе не противоречит целям, установленным в демократическом обществе. Специальные гарантии, установленные в национальном законодательстве для защиты интересов субъекта данных, привели к выводу Европейский суд по правам человека о том, что шведская система контроля персонала отвечает требованиям статьи 8 (2) Европейской конвенции о правах человека.

Принимая во внимание, имеющиеся у него широкие полномочия в определении целей, государство-ответчик, имело право считать, что в случае заявителя интересы национальной безопасности преобладали над интересами физического лица. Суд пришел к выводу, что не было нарушения статьи 8 Европейской конвенции о правах человека.

Уважение сути права

Дело *Schrems* касалось защиты физических лиц в отношении передачи их личных данных в третьи страны – в данном случае, Соединенные Штаты. *Schrems*, австрийский гражданин, был пользователем Facebook (организация запрещена на территории РФ) в течение нескольких лет. Заявитель подал жалобу в ирландский орган по надзору за защитой данных, для того чтобы осудить передачу его личных данных с целью хранения и последующей обработки из ирландского филиала Facebook (организация запрещена на территории РФ) в Facebook Inc. (организация запрещена на территории РФ), серверы которого расположены на территории США. Он утверждал, что в свете разоблачений Эдварда Сноудена в 2013 году, касающихся деятельности по надзору службами США, законодательство и судебная практика США не обеспечивают достаточной защиты личных данных.

Передача данных на территорию США основывалась на решении Комиссии ЕС об адекватности, разрешающим передачу данных американским компаниям. Компании-получатели гарантировали защиту данных, передаваемые из ЕС, в соответствии с так называемым правилом безопасной гавани (англ. Safe Harbor) – юридический принцип, согласно которому некоторые виды поведения не рассматриваются как нарушение более общего принципа или правила.

Дело, переданное в Суд Европейского Союза, рассматривалось в части соответствия решения Комиссии положениям Хартии ЕС. Суд напомнил, что защита основных прав в ЕС требует, чтобы ограничения этих прав применялись только в той степени, в которой они строго необходимы. Суд Европейского Союза рассматривал законодательство, разрешающее государственным органам доступ к общему содержанию электронных сообщений, как «нарушающее суть основного права на уважение частной жизни, гарантируемое статьей 7 Хартии». Это право было бы лишено смысла, если бы государственным органам США было разрешено получать

доступ к электронным сообщениям без какого-либо объективного обоснования конкретных целей национальной безопасности или предупреждения преступлений, которые касаются конкретных лиц, поскольку подобная практика не является следствием злоупотребления властью.

Кроме того, Суд Европейского Союза отметил, что «законодательство, не предусматривающее какой-либо возможности для лица использовать средства правовой защиты для получения доступа к своим персональным данным или для получения возможности исправления или удаления таких данных» несовместимо с фундаментальным правом на эффективную судебную защиту (статья 47 Хартии). В октябре 2015 года Суд Европейского Союза признал правило Safe Harbor недействительным.

Принципы необходимости и пропорциональности

В деле *Volker и Markus Schecke* Суд Европейского Союза пришел к выводу, что обязательство публиковать личные данные физических лиц, которые получали помощь от определенных фондов, нарушает принцип соразмерности. Данные предоставлялись без проведения различия на основании соответствующих критериев, таких как периоды, в течение которых лица получали помощь, частота такой помощи, ее характер и объем.

В связи с этим Суд Европейского Союза посчитал необходимым объявить недействительными некоторые положения Регламента Совета ЕС №1290/205 и объявить Регламент 259/2008 недействительным в целом.

Цели общественного интереса

Дело *Schwarz против города Бохум* (Германия) касалось ограничения права на неприкосновенность частной жизни и права на защиту персональных данных, возникающих при получении и хранении отпечатков пальцев в целях оформления паспортов гражданам ЕС. Заявитель обратился в функциональный центр г. Бохум для получения паспорта, но отказался предоставить отпечатки пальцев. На этом основании в выдаче паспорта ему было отказано. Заявитель обратился в немецкий суд с иском о выдаче паспорта без предоставления отпечатков пальцев. Немецкий суд передал дело в Суд Европейского Союза и направил запрос касательно применения статьи 1 (2) Регламента 252/2004 о стандартах безопасности и биометрических данных в паспортах и проездных документах, выданных государствами ЕС.

Суд Европейского Союза постановил, что отпечатки пальцев представляют собой персональные данные, поскольку объективно содержат уникальную информацию о лицах, которая позволяет их точно идентифицировать, а снятие и хранение отпечатков пальцев является обработкой персональных данных. В данном случае, обработка персональных данных, которая регулируется статьей 1 (2) Регламента 2252/2004, представляет собой угрозу правам на уважение частной жизни и защиту данных. Однако статья 52 (1) Хартии основных прав ЕС допускает ограничение осуществление этих прав при условии, что ограничения предусмотрены законом, уважают суть этих прав, и соответствуют принципам соразмерности, а также необходимы и действительно соответствуют целям, представляющим общественный интерес, признанный в ЕС.

Во-первых, Суд Европейского Союза отметил, что ограничение, возникающее в связи с получением и хранением отпечатков пальцев при выдаче паспортов, должно рассматриваться как предусмотренное законом, так как эти операции предусмотрены статьей 1 (2) Регламента 2252/2004.

Во-вторых, последняя редакция Регламента была разработана с целью предотвращения подделки паспортов и их использования в мошеннических целях. Таким образом, норма ста-

тьи 1 (2) направлена на предотвращение, в частности, незаконного въезда в ЕС, а потому преследует цель общественного интереса, признанного в ЕС.

В-третьих, в имеющихся у Суда Европейского Союза материалах дела не было заявлено, что ограничения, накладываемые на осуществление этих прав, не соответствуют сущности прав.

В-четвертых, хранение отпечатков пальцев на носителе с высокой степенью защиты, как предусмотрено Регламентом 252/2004, требует использования высокотехнологичных решений. Такое хранение может снизить риск подделки паспортов и облегчить работу органов, ответственных за проверку подлинности паспортов на границе ЕС. Хотя данный метод не гарантирует 100% защиты от мошеннических действий и подделки документов, достаточного того, что он в значительной степени снижает вероятность наступления таких событий.

В свете вышеизложенного Суд Европейского Союза постановил, что взятие и хранение отпечатков пальцев, упомянутое в статье 1 (2) Регламента 2252/2004, это адекватное ограничение для достижения целей, преследуемых настоящим Регламентом.

Суд Европейского Союза признал необходимость такой обработки и отметил, что снятие отпечатков ограничивалось двумя пальцами, данное действие не носило интимный характер и проводилось в присутствии третьих лиц. Данная операция также не вызывает какого-то целенаправленного физического или психического дискомфорта у пострадавшего лица, операция может быть приравнена к фотосъемке. Следует также отметить, что единственной реальной альтернативой снятия отпечатков пальцев, как установил Суд Европейского Союза, является сканирование радужной оболочки глаз. Суд Европейского Союза не нашел подтверждения, что сканирование радужной оболочки глаз несет меньше ограничений в правах, признанных статьями 7 и 8 Хартии основных прав ЕС. Кроме того, что касается эффективности этих двух методов, то общепризнанным является факт использования технологии снятия отпечатков пальцев вместо сканирования радужной оболочки глаза, в связи с недостаточным технологическим обеспечением. К тому же сканирование сетчатки является дорогостоящей альтернативой и поэтому практически не используется для этих целей.

Соответственно, Суд Европейского Союза признал снятие отпечатков пальцев эффективной и соразмерной мерой ограничения права.

Свобода самовыражения

В деле *Tietosuojavaltuutettu против Satakunnan Markkinapörssi Oy и Satamedia Oy*, Суду Европейского Союза было предложено определить взаимосвязь между защитой данных и свободой прессы. Суд должен был изучить вопрос о распространении компанией через сервис SMS-сообщений данных о налогах 1,2 миллиона субъектов данных, законно полученных от финских налоговых органов. Финский надзорный орган по защите данных принял решение, обязывающее компанию прекратить распространение этих данных. Компания обжаловала это решение в национальном суде, который запросил у Суда Европейского Союза разъяснения относительно толкования Директивы о защите данных (DPD – финское национальное право). В частности, Суд Европейского Союза должен был проверить, может ли обработка персональных данных рассматриваться в контексте деятельности, осуществляемой в журналистских целях (налоговые органы предоставили пользователям мобильных устройств налоговые данные третьих лиц). После того, как был сделан вывод о том, что деятельность компании заключалась в «обработке персональных данных» в значении статьи 3 (1) Директивы о защите данных (DPD), Суд Европейского Союза проанализировал статью 9 Директивы об обработке персональных данных и свободе выражения.

Суд отметил важность права на свободу выражения мнений в каждом демократическом обществе и постановил, что такое понятие, как журналистика, имеет широкую трактовку.

Также Суд отметил, что для достижения баланса между двумя основными правами отступления и ограничения права на защиту данных должны применяться только в той мере, в которой это строго необходимо.

В этих обстоятельствах Суд Европейского Союза постановил, что действия компаний в отношении данных из документов, которые являются общественным достоянием в соответствии с национальным законодательством, могут быть классифицированы как «журналистские действия», если их целью является раскрытие общественности информации, мнения или идей, независимо от среды, используемой для их передачи. Он также постановил, что данная деятельность не ограничивается передачей посредством СМИ и может осуществляться в целях получения прибыли. В данном конкретном случае Суд Европейского Союза оставил рассмотрение на уровне национального суда.

Это же дело было рассмотрено Европейским судом по правам человека после того, как национальный суд на основании указаний Суда Европейского Союза принял решение о том, что постановление надзорного органа о прекращении публикации всей налоговой информации является оправданным вмешательством в свободу выражения мнения компании. Суд пришел к выводу, что хотя вмешательство в право компании распространять информацию имело место, вмешательство соответствовало закону, преследовало законную цель и было необходимо в демократическом обществе.

Суд напомнил о критериях прецедентного права, которыми должны руководствоваться национальные органы власти и сам Европейский суд по правам человека при сопоставлении свободы выражения мнений с правом на неприкосновенность частной жизни. В отношении вопросов, представляющих общественный интерес, существует мало возможностей для ограничения права на получение и распространение информации, поскольку общественность имеет право на получение информации «и это является важнейшим правом в демократическом обществе». Тем не менее статьи в прессе, нацеленные исключительно на то, чтобы удовлетворить любопытство конкретного читателя относительно деталей личной жизни человека, не могут являться предметом общественного интереса. Отступление от правил защиты в журналистских целях предназначено для того, чтобы журналисты могли получать, собирать и обрабатывать данные для возможности осуществления журналистской деятельности.

Суд установил, что общественность не интересовалась массовым распространением таких необработанных данных газетами в неизменном виде. Информация о налогообложении могла бы позволить любопытным представителям общественности классифицировать субъектов данных в соответствии с их экономическим статусом и удовлетворить общественную жажду информации о частной жизни других людей. Это не может рассматриваться с позиции удовлетворения общественного интереса.

Баланс права на защиту данных и свободу выражения мнений

В деле *Axel Springer AG против Германии* Европейский суд по правам человека постановил, что судебное решение, запрещающее компании-заявителю публиковать статью об аресте и осуждении известного актера, нарушило статью 10 Европейской конвенции по правам человека.

Европейский суд по правам человека перечислил критерии, которые следует учитывать при сопоставлении права на свободу выражения мнения с правом на уважение частной жизни, как это установлено в прецедентном праве:

– представлял ли интерес тот случай, когда рассматриваемая статья была представлена общественности?

– было ли заинтересованное лицо публичной фигурой?

– как была получена информация и является ли она достоверной?

Европейский суд по правам человека установил, что арест и осуждение актера являются публичными судебными фактами, а потому представляют общественный интерес. Актер был достаточно известен, и информация об аресте была предоставлена прокуратурой, ее точность и достоверность не оспаривались сторонами. Поэтому наложенные ограничения на публикацию не были пропорциональны законной цели защиты личной жизни заявителя.

Суд пришел к выводу, что имело место нарушение статьи 10 Европейской конвенции по правам человека.

Дело *Coudec and Hachette Filipacchi Associés против Франции* касалось публикации во французском еженедельнике интервью с г-жой *Coste*, которая утверждала, что принц Монако *Albert* был отцом ее ребенка. В интервью также рассказывалось об отношениях г-жи *Coste* с принцем и о том, как он отреагировал на рождение ребенка, а также фото принца с ребенком. Принц *Albert* возбудил дело против издательской компании за нарушение его права на неприкосновенность частной жизни. Французские суды постановили, что публикация статьи нанесла необратимый ущерб принцу *Albert* и обязали издателя возместить убытки и опубликовать подробности решения на обложке журнала.

Издатели журнала передали дело в Европейский суд по правам человека, утверждая, что решение французских судов неоправданно нарушает их право на свободу выражения мнений. Европейский суд по правам человека должен был соотнести право принца *Albert* на неприкосновенность частной жизни с правом издателя на выражение мнения и правом общественности на получение информации. Право г-жи *Coste* поделиться своей историей с общественностью и заинтересованность ребенка в официальном установлении отношений с отцом также стали критериями при рассмотрении дела.

Европейский суд по правам человека постановил, что публикация интервью представляет собой вмешательство в личную жизнь принца и продолжил изучение необходимости вмешательства. Он указал, что публикация касается общественного деятеля и вопроса общественного интереса, поскольку граждане Монако заинтересованы в том, чтобы знать о существовании ребенка принца, так как будущее наследственной монархии «неразрывно связано с существованием потомков» и, таким образом, это вызывает обеспокоенность общественности. Суд также отметил, что эта статья позволила г-же *Coste* и ее ребенку осуществить свое право на свободу выражения мнений. Национальные суды не смогли должным образом учесть принципы и критерии, разработанные в прецедентном праве Европейского суда по правам человека в отношении баланса права на неприкосновенность частной жизни и права на свободу выражения мнений.

Суд пришел к выводу, что Франция нарушила статью 10 Европейской конвенции по правам человека о свободе выражения мнений.

Интересы широкой общественности

В деле *Mosley против Соединенного Королевства* национальная еженедельная газета опубликовала интимные фотографии заявителя, известного деятеля, который впоследствии подал гражданский иск против издателя и получил компенсацию за ущерб. Несмотря на присужденную денежную компенсацию, заявитель продолжал жаловаться на то, что остается жертвой нарушения его права на неприкосновенность частной жизни. Заявителю было отказано в подаче иска о вынесении судебного запрета до публикации данных фотографий из-за отсутствия каких-либо правовых требований (поскольку факт публикации уже случился).

Европейский суд по правам человека отметил, что распространение подобных материалов предназначается для развлечения и не преследует иных целей. Несомненно, заявитель был в выигрышной позиции в контексте статьи 10 Европейской конвенции по правам чело-

века и аналогичным требованиям статьи 8 Европейской конвенции о правах человека в части защиты информации частного и интимного характера. Тем не менее особое внимание следует уделять изучению ограничений, которые могут выступать в роли цензуры до публикации. Европейский суд по правам человека пришел к выводу, что юридически обязательное предварительное уведомление не требовалось в соответствии со статьей 8 Европейской конвенции о правах человека. Соответственно норма статьи 8 не была нарушена.

В деле *Bohlen против Германии* заявитель, известный певец и художественный продюсер, опубликовал автобиографическую книгу и впоследствии был вынужден удалить некоторые отрывки по решению суда. Эта история широко освещалась в национальных СМИ. Табачная корпорация начала юмористическую рекламную кампанию, содержащую отсылки на данное событие, и использовала имя заявителя без его согласия. Заявитель безуспешно требовал возмещения убытков от рекламной кампании, ссылаясь на нарушение его прав в соответствии со статьей 8 Европейской конвенции о правах человека.

Европейский суд по правам человека определил баланс между правом на уважение частной жизни и правом на свободу выражения мнений, и постановил, что нарушения статьи 8 Европейской конвенции о правах человека не было. Заявитель был публичным лицом, и реклама не содержала подробностей его частной жизни. Кроме того, отсылка была сделана на широко освещаемое событие, и носила юмористический характер без признаков унижения или негативного отношения к заявителю.

В деле *Biriuk против Литвы* заявитель утверждал в Европейском суде по правам человека, что Литва не выполнила своего обязательства по обеспечению уважения ее права на частную жизнь. Крупное издание совершило серьезное нарушение ее права на неприкосновенность частной жизни, а национальные суды, рассматривавшие дело, присудили ей денежную сумму за нанесенный моральный вред. Согласно положениям национального закона о предоставлении информации населению, национальный суд определил незначительный размер компенсации материального вреда, причиненного незаконным распространением в СМИ информации о личной жизни человека. Дело было связано с публикацией на первой полосе крупнейшей литовской газеты статьи о том, что заявитель был ВИЧ-положительным.

Европейский суд по правам человека напомнил, что защита личных данных, в том числе медицинских, имеет основополагающее значение для права на уважение частной жизни в рамках Европейской конвенции о правах человека. Конфиденциальность данных о здоровье особенно важна, так как разглашение медицинских данных может существенно повлиять на личную и семейную жизнь человека, его или ее занятость, а также участие в жизни общества. Суд придает особое значение распространению медицинским персоналом информации о ВИЧ-статусе заявителя, что свидетельствует о факте нарушения врачебной тайны. Таким образом, не было никакого законного вмешательства в право заявителя на частную жизнь.

Однако при рассмотрении вопроса о том, оправдывает ли существование общественного интереса к такого рода публикациям, Суд установил, что основной целью публикации было увеличение продаж газеты за счет удовлетворения любопытства читателей. Такая цель не может представлять интерес общественности. Европейский суд по правам человека установил, что имело место нарушение статьи 8 Европейской конвенции о правах человека.

Право на доступ к информации

В деле *Счетной палаты против австрийской общественной телерадиокомпании* Суд Европейского Союза проверил соответствие некоторых австрийских законов законодательству ЕС о защите данных. Законодательство обязывало государственный орган собирать и передавать информацию об именах работников различных государственных учреждений и их дохо-

дах для публикации в ежегодном отчете, доступном для широкого круга лиц. Некоторые субъекты данных отказывались передавать свои данные для публикации, ссылаясь на право защиты данных.

Суд Европейского Союза напомнил, что Хартия основных прав ЕС не была обязательным документом в тот период, когда формировался принцип права. Суд постановил, что сбор данных о профессиональном доходе человека и передача таких сведений третьей стороне представляет собой нарушение права на неприкосновенность частной жизни. Европейского Союза отметил, что австрийское законодательство преследовало законную цель по сдерживанию заработной платы государственных служащих в разумных пределах, что напрямую связано с экономическим благосостоянием страны. Однако заинтересованность Австрии в обеспечении наилучшего использования государственных средств должна быть сбалансирована с серьезностью вмешательства в право на неприкосновенность частной жизни.

Оценка необходимости публикации данных о доходах физических лиц и соразмерности преследуемой цели была оставлена на усмотрение национального суда. Суд Европейского Союза призвал национальный суд рассмотреть вопрос о том, не могла ли такая цель быть достигнута с учетом баланса права. Примером может служить передача персональных данных только контролирующим государственным органам, а не широкой общественности.

Защита профессиональной тайны

В деле *Pruteanu против Румынии* заявитель выступал в качестве адвоката коммерческой компании, которой запретили проводить банковские операции по обвинению в мошенничестве. В ходе расследования дела румынские суды уполномочили органы прокуратуры перехватывать и записывать телефонные разговоры партнера компании в течение определенного периода. Записи включали его разговоры с адвокатом.

Г-н *Pruteanu* утверждал, что это нарушало его право на уважение личной жизни и переписки. В своем решении Европейский суд по правам человека подчеркнул статус и важность отношений адвоката со своими клиентами, которые являются профессиональной тайной. В данном случае адвокат также может подать жалобу на вмешательство в его право на уважение частной жизни и переписки. Суд Европейского Союза постановил, что имело место нарушение статьи 8 Европейской конвенции по правам человека.

В деле *Brito Ferrinho Bexiga Villa-Nova против Португалии* заявитель и адвокат, отказались раскрывать свои личные банковские выписки налоговым органам на основании профессиональной и банковской тайн. Прокуратура начала расследование по факту налогового мошенничества и потребовала приостановить разрешение на сохранение профессиональной тайны. Национальные суды вынести соответствующее решение о приостановлении, поскольку общественные интересы преобладали над личными.

При рассмотрении дела Европейский суд по правам человека постановил, что доступ к банковским выпискам заявителя представлял собой вмешательство в его право на неприкосновенность частной жизни. Вмешательство имело законную основу, поскольку оно основывалось на нормах уголовно-процессуального кодекса и преследовало законную цель. Однако рассматривая необходимость и соразмерность вмешательства, Европейский суд по правам человека указал на то обстоятельство, что разбирательство по вопросам конфиденциальности было проведено без участия или ведома заявителя.

Таким образом, заявитель не имел возможности оспорить снятие статуса конфиденциальности или каких-либо средств правовой защиты. Из-за отсутствия процессуальных гарантий и эффективного судебного контроля за мерой, приостанавливающей обязанность соблю-

дения конфиденциальности, Европейский суд по правам человека пришел к выводу, что имело место нарушение статьи 8 Европейской конвенции по правам человека.

Свобода вероисповедания и убеждений

В деле *Sinak Isik против Турции* заявитель был членом религиозной общины алевитов, чья вера находится под влиянием суфизма и других исламских верований и рассматривается некоторыми учеными, как отдельная религия, а другими – как часть исламской религии. Заявитель жаловался на то, что, несмотря на его возражения, в удостоверении личности содержалась строка с указанием его религии как «ислам», а не «алеви». Национальные суды отклонили его ходатайство о смене удостоверения личности на том основании, что «алеви» обозначает подгруппу ислама, а не отдельную религию. Заявитель пожаловался в Европейский суд по правам человека на то, что вынужден был раскрыть веру без его согласия, потому что это было обязательным при оформлении удостоверения личности и это нарушало его право на свободу вероисповедания и убеждений. Кроме того, формулировка «ислам» в удостоверении личности не соответствовало вере заявителя.

Европейский суд по правам человека подтвердил, что свобода вероисповедания влечет за собой свободу исповедовать религию вместе с другими индивидами, как публично и в кругу лиц, разделяющих ту же веру, а также в частном порядке и одному. Действующее в то время национальное законодательство обязывало физических лиц иметь при себе удостоверение личности – документ, который должен был быть предъявлен по требованию любого государственного органа, с обязательным указанием религии субъекта данных. По мнению Европейского Суда, сам факт обращения с вопросом удаления записи о вероисповедании может привести к раскрытию информации об отношении субъектов к религии.

Кроме того, наличие поля для внесения данных о вероисповедании субъекта может также внести дисбаланс в обществе: владельцы удостоверений личности с пустым полем будут выделяться среди тех, у кого есть удостоверение с заполненным полем. Европейский суд по правам человека пришел к выводу, что внутренне законодательство нарушает статью 9 Европейской конвенции о правах человека.

Защита интеллектуальной собственности

Дело *Promusicae против Telefónica de España* касалось отказа испанского провайдера раскрыть некоммерческой организации личные данные определенных лиц, которым провайдер предоставлял доступ. Организация добивалась раскрытия персональных данных с целью возбуждения гражданского дела против лиц, которые использовали программу обмена файлами. Права на использование файлов принадлежало компании *Promusicae*.

Испанский суд передал в Суд Европейского Союза запрос о том, должны ли такие персональные данные передаваться в соответствии с законодательством ЕС в контексте гражданского судопроизводства для обеспечения эффективной защиты авторских прав. Испанский суд сослался на Директивы 2000/31, 2001/29 и 2004/48, которые также рассматриваются в свете статей 17 и 47 Хартии основных прав ЕС. Суд Европейского Союза пришел к выводу, что эти три директивы, а также Директива о цифровой конфиденциальности (Директива 2002/58) не запрещают государствам Евросоюза устанавливать обязательство о раскрытии персональных данных в контексте гражданского судопроизводства для обеспечения эффективной защиты авторских прав.

При рассмотрении дела рассматривался вопрос о согласовании права на неприкосновенность частной жизни с правом на защиту собственности и правом на эффективные средства правовой защиты.

Суд Европейского Союза пришел к следующему выводу: «при имплементации упомянутых выше Директив государства должны позаботиться о том, чтобы найти сбалансированное решение для защиты основных прав в соответствии с нормами законодательства ЕС. Кроме того, органы власти и суды государств Евросоюза должны не только толковать свое национальное право в соответствии с этими Директивами, но также следить за тем, чтобы не были нарушены основные принципы законодательства ЕС, например, принцип соразмерности (пропорциональности).

Дело *Bonnier Audio AB и другие против Perfect Communication Sweden AB* касалось соблюдения баланса прав при защите интеллектуальной собственности и личных данных. Заявители, пять издательских компаний, обладающих авторскими правами на 27 аудиокниг, возбудили дело в шведском суде. Заявители утверждали, что были нарушены авторские права посредством доступа к FTP-серверу с аудиокнигами. Заявители просили Интернет-провайдера раскрыть персональные данные субъекта на основании IP-адреса, с которого были отправлены файлы. Интернет-провайдер оспорил решение, поскольку оно нарушало Директиву 2006/24 (Директива хранения данных – аннулирована в 2014 году).

Шведский суд направил запрос в Суд Европейского Союза с целью установить, ограничивает ли Директива 2006/24 применение национального положения, основанного на статье 8 Директивы 2004/48 (Директива по защите интеллектуальной собственности).

Статья 8 Директивы по защите интеллектуальной собственности позволяет выдать судебный приказ, в рамках которого Интернет-провайдеры обязаны передавать правообладателям информацию об Интернет-пользователях, с чьих IP-адресов были совершены правонарушения в области интеллектуальной собственности. Запрос основывался на предположении, что заявитель предоставил четкие доказательства нарушения определенного авторского права и что такая мера согласована с основными правами.

Суд Европейского Союза постановил, что Директива 2006/24 касается исключительно обработки и хранения данных, сгенерированных поставщиками услуг электронной связи с целью расследования, выявления и преследования уголовных преступлений и их передачи компетентным национальным органам. Таким образом, национальное законодательство, имплементирующее Директиву по защите интеллектуальной собственности, не ограничивается нормами Директивы 2006/24.

Что касается предоставления персональных данных, о которых просят заявители, Суд Европейского Союза постановил, что такое действие представляет собой обработку персональных данных и подпадает под действие Директивы 2002/58 (Директива о цифровой конфиденциальности). Суд Европейского Союза отметил, что передача этих данных требуется в гражданском судопроизводстве в интересах правообладателей для обеспечения эффективной защиты авторских прав и, таким образом, подпадает под действие основных целей в контексте применения Директивы 2004/48.

Защита данных и экономические интересы

В деле *Google против Испании* Суд Европейского Союза указал, что при определенных условиях субъекты данных имеют право обращаться в поисковые системы с запросом об удалении своих индексов из результатов поиска. В заключении Суд Европейского Союза указал на тот факт, что использование поисковых систем и результатов поиска позволяет установить подробный профиль человека. Эта информация может касаться аспектов частной жизни, что представляет собой серьезное вмешательство в основные права субъектов данных на неприкосновенность частной жизни и защиту персональных данных.

Суд Европейского Союза проверил оправданность такого вмешательства. Что касается экономической заинтересованности поисковой системы в проведении обработки, то Суд Европейского Союза постановил, что «вмешательство не может быть оправданно только с точки зрения экономической заинтересованности в результате обработки таких данных» и что «как правило, основные права в соответствии со статьями 7 и 8 Хартии основных прав ЕС имеют приоритет над такими экономическими интересами и интересами общественности при использовании поисковой системы для профилирования пользователей».

Законодательная база

Право на защиту данных

Европейское законодательство

– статья 16 Договора о функционировании Европейского Союза, статья 8 Хартии основных прав Европейского Союза;

– Регламент ЕС 2016/679 о защите физических лиц в отношении обработки персональных данных и о свободном перемещении таких данных и отмена Директивы 95/46/ЕС (Общее положение о защите данных), OJ 2016 L 119;

– Директива ЕС 2016/680 о защите физических лиц в отношении обработки персональных данных компетентными органами в целях предотвращения, расследования, выявления или преследования уголовных преступлений или исполнения уголовных наказаний, а также о свободе движения таких данных и отмена Рамочного решения Совета 2008/977/JHA (Защита данных для органов полиции и юстиции), OJ 2016 L 119;

– Директива 2002/58/ЕС, касающаяся обработки персональных данных и защиты конфиденциальности в секторе электронных коммуникаций (Директива о конфиденциальности и электронных коммуникациях), OJ 2002 L 201;

– Регламент ЕС №45/2001 о защите отдельных лиц в отношении обработки персональных данных учреждениями и органами Сообщества и о свободном перемещении таких данных (Регламент о защите данных учреждений ЕС), OJ 2001 L 8.

Закон Совета Европы

– статья 8 Европейской конвенции по правам человека (право на неприкосновенность частной и семейной жизни, жилища и корреспонденции);

– Конвенция 108 – Модернизированная Конвенция о защите физических лиц в отношении автоматической обработки персональных данных.

Российская Федерация

– Европейская конвенция по правам человека;
– Модернизированная Конвенция 108 с оговорками в части пунктов 2a и 2c;
– статья 2, п. 2 статьи 17, статья 23, п. 1 статьи 24 Конституции РФ;
– статья 2 Федерального закона от 27.06.2006 №152-ФЗ «О персональных данных».

Ограничение права на защиту данных

Европейское законодательство

– статья 52 (1) Хартии основных прав ЕС;
– статья 23 Общего регламента по защите данных ЕС 2016/679;
– Суд Европейского Союза, объединенные дела C-92/09 и C-93/09.

Закон Совета Европы

– статья 8 (2) Модернизированной Конвенции 108;
– статья 11 Европейского суда по правам человека;
– дело *Marper против Соединенного Королевства* [GC], №30562/04 и 30566/04, 2008 г.

Российская Федерация

– Судебное решение.

Свобода самовыражения

Европейское законодательство

– Суд Европейского Союза, C-131/12, *Google Испания SL, Google Inc. против Агентства Испании по защите прав (AEPD)*.

Закон Совета Европы

– Европейский суд по правам человека, *Axel Springer AG против Германии [GC]*, №39954/08, 2012 г;

– Европейский суд по правам человека, *Mosley против Великобритании*, №48009/08, 2011 г;

– Европейский суд по правам человека, *Bohlen против Германии*, №53495/09, 2015 г.

Российская Федерация

– статьи 17 и 29 Конституции РФ.

Доступ к информации

Европейское законодательство

– Суд Европейского Союза, C-28/08 P, *Европейская комиссия против Bavarian Lager Co. Ltd [GC]*, 2010;

– Суд Европейского Союза, C-615 / 13P*, ClientEarth, PAN Europe против EFSA*, 2015.

Закон Совета Европы

– Европейский суд по правам человека, *Magyar Helsinki Bizottság против Венгрии [GC]*, №18030/11, 2016.

Российская Федерация

– статья 8 Федерального закона от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– статья 14 Федерального закона от 27.06.2006 №152-ФЗ «О персональных данных».

Профессиональная тайна

Европейское законодательство

– статья 90 Общего регламента по защите данных ЕС 2016/679.

Закон Совета Европы

– Европейский суд по правам человека, *Pruteanu против Румынии*, №30181/05, 2015.

Российская Федерация

– п. 5 статьи 9 от 27.07.2006 №149-ФЗ Федерального закона «Об информации, информационных технологиях и о защите информации» и перечень федеральных законов.

Свобода религии или убеждений

Европейское законодательство

– статья 91 Общего регламента по защите данных ЕС 2016/679.

Закон Совета Европы
– прецедентное право отсутствует.

Российская Федерация
– статья 28 Конституции РФ;
– статья 3 Федерального закона от 26.09.1997 125-ФЗ «О свободе совести и о религиозных объединениях».

Свобода искусств и наук

Европейское законодательство
– прецедентное право отсутствует.

Закон Совет Европы
– Европейский суд по правам человека, *Vereinigung bildender Künstler против Австрии*, №68345/01, 2007.

Российская Федерация
– статья 44 Конституции РФ.

Защита собственности

Европейское законодательство
– Суд Европейского Союза, C-275/06 *Promusicae против Telefónica de España SAU [GC]*, 2008.

Закон Совета Европы
– прецедентное право отсутствует.

Российская Федерация
– часть четвертая Гражданского кодекса РФ.

Экономические интересы и защита данных

Европейское законодательство
– Суд Европейского Союза, *C-131/12, Google Spain SL, Google Inc. против Agencia Española de Protección de Datos (AEPD),* 2014;
– Суд Европейского Союза, C-398/15*, Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce против Salvatore Manni*, 2017.

Закон Совета Европы
– прецедентное право отсутствует.

Российская Федерация
– судебное решение.

Законодательная практика РФ

Право на защиту данных:

– в соответствии с пунктом 1 статей 23 и 24 Конституции РФ гражданин Российской Федерации имеет право на неприкосновенность частной жизни, личную и семейную тайну защиту своей части и доброго имени. Ограничения по решению суда могут быть наложены на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Конституционно критерии таких ограничений не закреплены, критерии и условия ограничения такого права указаны на уровне федерального законодательства;

– Российская Федерация ратифицировала Европейскую конвенцию по правам человека Федеральным законом от 30.03.1998 «О ратификации Конвенции и о защите прав человека и основных свобод и Протоколов к ней» с ограничениями, указанными в федеральном законе. Модернизированная Конвенция 108 была ратифицирована Российской Федерацией 15 мая 2013 года с оговорками по подпунктам «а», «с» пункта 2 статьи 3 и подпункту «а» пункта 2 статьи 9;

– в соответствии с Конституцией РФ защита персональных данных не является конституционным правом гражданина и защищается на федеральном уровне;

– регулирование правил обработки персональных данных в Российской Федерации и правил защиты информации были приняты в 2006 году;

– с 2006 года федеральные законодательства по регулированию правил обработки персональных данных и регулирование защиты данных периодически дополняются;

– регулирование доступа к информации, правил ее защиты, требований к обработке персональных данных и ограничений указано более чем в 20 федеральных законах и подзаконных актах, единого документа нет, что существенно затрудняет их правоприменение.

Ограничение права на защиту персональных данных:

– право на защиту персональных данных не является абсолютным правом в соответствии с Конституцией РФ. Оно может быть ограничено, в соответствии с федеральным законодательством и решением судов Российской Федерации;

– условия ограничения прав на уважение частной жизни и защиту персональных данных перечислены в статье 8 Федерального закона от 12.08.1995 №144-ФЗ «Об оперативно-розыскной деятельности»;

– в соответствии с пунктом 6 статьи 16 Федерального закона от 27.07.2007 №149-ФЗ «Об информации, информационных технологиях и защите информации» Российская Федерация вправе ограничить принятыми оговорками подпункта. а пункта 2 статьи 9 указанными при ратификации Модернизированной Конвенции 108 Российская Федерация вправе ограничить на уровне федерального законодательства использование отдельных средств защиты информации и осуществление отдельных видов деятельности в области защиты информации.

Взаимодействие с другими правами и законными интересами:

Взаимодействие с другими правами и законными интересами в Российской Федерации реализовано на уровне Конституции РФ, нормативно-правовых актов федерального значения и решений судов. Критерии таких взаимодействий основываются на решении органов власти и судебных решениях, выносимых в строгом соответствии с законом и внутренним убеждением судьи (п. 3, статьи 8 главы 3 Кодекса судейской этики).

Глава 2

Европейский Союз: основные аспекты концепции персональных данных, механизмы анонимизации, псевдонимизации и аутентификации.

Специальные категории персональных данных, персональные данные в контексте правонарушений и приговоров судов.

Концепция обработки данных, автоматизированная и ручная обработка персональных данных.

Контроллеры и совместные контроллеры, процессоры, взаимодействие контроллер – процессор, получатели и третьи лица, согласие.

Законодательство ЕС и РФ в области защиты данных.

В соответствии с законодательством ЕС и Совета Европы, персональные данные определяются как информация, относящаяся к идентифицированному или идентифицируемому физическому лицу. Это относится к информации о лице, чья личность либо идентифицирована, либо может быть установлена посредством дополнительной информации. Для определения является ли физическое лицо идентифицируемым, контроллер или другое лицо должны принять во внимание все разумные меры, которые могут быть использованы для прямой или косвенной идентификации личности (например, дополнительные атрибуты данных, позволяющие отличить одного субъекта от другого).

Основные аспекты концепции персональных данных

Субъект данных

В контексте Общего регламента по защите данных к персональным данным относится любая информация, относящаяся к идентифицированному или идентифицируемому лицу. В соответствии с законодательством ЕС физические лица (субъекты данных) являются единственными владельцем своих данных в контексте права на защиту данных. Действие Общего регламента по защите данных распространяется на субъектов данных в ЕС и не применяется к защите персональных данных умерших лиц.

Закон Совета Европы в части Модернизированной Конвенции 108 также регламентирует защиту физических лиц в отношении обработки их персональных данных. Терминология законодательства о защите данных, в части правовых систем ЕС, идентична.

Юридические лица имеют право на защиту данных. Европейский суд по правам человека принимает заявления от юридических лиц касательно нарушений их прав на защиту данных в соответствии со статьей 8 Европейской конвенции по правам человека.

В Пояснительном докладе к Модернизированной Конвенции 108 отмечается, что национальное законодательство может применяться для защиты законных интересов юридических лиц. Общий регламент по защите данных ЕС 2016/679 не распространяется на обработку данных юридических лиц, включая форму собственности и названия, а также контактных данных такого субъекта. Тем не менее Директива о конфиденциальности и электронных коммуникациях защищает конфиденциальность сообщений и законные интересы юридических лиц в отношении автоматизированной обработки и хранения данных субъектов.

Данные

Любые данные считаются персональными при условии, что они относятся к идентифицированному или идентифицируемому лицу. Персональные данные включают информацию, относящуюся к личной, профессиональной и общественной жизни субъекта данных.

Например, оценочный лист работника, хранящийся в его личном деле, представляет собой персональные данные работника. Мнение руководителя, зафиксированное в данном оценочном листе, будет считаться косвенной информацией о субъекте, а значит данные, такие как «лояльность работника» и факты, которые можно отнести к субъекту «работник отсутствовал 2 недели в течение года», будут считаться персональными данными работника.

Европейский суд по правам человека интерпретирует термин «персональные данные» как не ограничивающиеся вопросами личности субъекта, поскольку разделение вопросов частной и профессиональной жизни не всегда возможно. Данная интерпретация применяется и в Общем регламенте по защите данных.

Согласно законодательству ЕС и Совета Европы, информация содержит данные о субъекте, в случае если:

– лицо идентифицировано или может быть идентифицировано с помощью этой информации;

– субъект данных хотя и не идентифицирован, но может быть идентифицирован при последующей обработке.

Европейский суд по правам человека неоднократно заявлял, что понятие «персональные данные» в Европейской конвенции по правам человека идентично понятию в Модернизированной Конвенции 108, особенно в отношении идентифицированного или идентифицируемого лица.

В Общем регламенте по защите данных указано, что физическое лицо может быть идентифицировано в случае, если субъекта «можно идентифицировать прямо или косвенно, в частности, с помощью таких атрибутов, как имя, идентификационный номер, данные о местоположении, сетевой идентификатор (IP – адрес), по каждому из факторов или в совокупности, специфичных для физической, физиологической, генетической, психической, экономической, культурной или социальной идентичности субъекта». Имя субъекта данных является ярким примером такого описания и может непосредственно идентифицировать субъекта в связке с дополнительным атрибутом данных.

В некоторых случаях атрибуты, аналогичные имени, косвенно могут идентифицировать субъекта данных. Номер телефона, номер карточки социального страхования и регистрационный номер транспортного средства – все это примеры информации, которая может сделать субъект идентифицируемым. Также могут быть использованы и иные атрибуты, такие как – файлы персонального компьютера, файлы cookie и инструменты наблюдения за веб-трафиком для выделения субъектов путем определения их поведения и привычек. По мнению Рабочей группы по ст. 29 Общего регламента по защите данных, «без запроса имени и адреса лица его можно классифицировать на основе социально-экономических, психологических, философских или иных критериев и атрибутов». Определение персональных данных как в Совете Европы, так и в Европейском Союзе достаточно широкое и охватывает различные степени идентификации.

Так как многие имена не являются уникальными, в целях установления личности человека могут потребоваться другие атрибуты для гарантии точной идентификации субъекта. Иногда прямые и косвенные атрибуты могут быть объединены, чтобы провести точную идентификацию, например, дата и место рождения. Кроме того, в некоторых странах на государственном уровне введены персонализированные номера (аналог серии и номера паспорта гражданина РФ) для отождествления физических лиц. Переданные налоговые данные, данные на получение вида на жительство, сведения в административных документах, банковские данные и информация о здоровье могут быть отнесены к персональным данным. Биометрические данные, такие как отпечатки пальцев, цифровые отпечатки или радужная оболочка глаз, данные о местоположении и онлайн-атрибуты все чаще используются для идентификации субъектов в цифровом пространстве.

Для применения Общего регламента по защите данных не требуется фактической идентификации субъекта данных, достаточно, чтобы субъект был потенциально идентифицируемым. Субъект считается потенциально идентифицируемым, если имеется достаточно атрибутов данных, с помощью которых его можно прямо или косвенно идентифицировать. Согласно разделам 2 и 3 Общего регламента по защите данных все идентифицируемые данные, хранящиеся у обработчика, должны быть доступны субъекту данных, равно как и все сведения об обработке, включая третьих лиц, которым такие данные доступны.

Например, местный орган власти собирает данные об автомобилях на улицах города. По его указанию происходит автоматическая фотофиксация времени и местоположения автотранспортного средства с целью оформления штрафов, в случаях выявления нарушений. Субъект данных подает жалобу, заявляя, что местный орган власти не имеет правовых оснований в соответствии с законодательством о защите данных. Местный орган власти утверждает, что не осуществляет сбор персональных данных, поскольку номерные знаки

автомашин обрабатываются без других идентификаторов и орган власти не имеет доступа к реестру полиции для идентификации субъекта.

Данное утверждение не соответствует требованиям Общего регламента по защите данных. Принимая во внимание, что цель сбора данных состоит в конечной идентификации субъекта для наложения штрафных санкций, можно сделать вывод, что субъект данных будет идентифицирован. Следовательно, будет произведена обработка персональных данных в реестрах полиции. Общий регламент по защите данных предусматривает дополнительных получателей данных, кроме непосредственного обработчика, которые могут предпринять попытку идентификации личности. В данном контексте действия местных властей равносильны сбору данных об идентифицируемых лицах и требуют наличия правовой основы в соответствии с законодательством о защите данных.

Для определения критериев вероятности идентификации субъекта следует учитывать все объективные факторы, такие как стоимость и время, затраченное на идентификацию, а также принять во внимание физические и программные возможности.

В соответствии с законодательством Совета Европы, Пояснительный доклад к Модернизированной Конвенции 108 содержит следующую формулировку понятия «идентификация»: понятие «идентифицируемый» относится не только к гражданской или юридической идентичности человека как таковой, но и к тому, что может позволить «определить личность субъекта» средствами обработки и, как следствие, подвергнуть классификации. Такое «определение субъекта» может быть осуществлено с помощью доступа к его (ее) электронным устройствам или комбинации таких устройств (стационарные или мобильные гаджеты, камеры, игровые устройства и т. д.), а также с использованием идентификационного псевдонима (логина), биометрических или генетических данных, данных о местонахождении, IP-адреса или иного идентификатора. Субъект данных не будет считаться потенциально «идентифицируемым», если для его/ее идентификации требуется неоправданное количество времени, денег или иных ресурсов. Оправданность ресурсных затрат должна оцениваться в каждом индивидуальном случае с учетом следующих факторов: цели обработки данных, стоимости и преимущества идентификации данных, типа контроллера и используемых средства, а также технологий обработки.

Законодательство о защите данных не регулирует формы содержания или хранения персональных данных. Например, это могут быть устные сообщения, телевизионное или кабельное изображение (включая звук), информация в электронном виде, генетические материалы, ДНК (дезоксирибонуклеиновая кислота) и иные атрибуты данных.

Анонимизация

Согласно принципу минимизации в контексте ограничения объемов и сроков хранения данных, изложенному как в Общем регламенте по защите данных, так и в Модернизированной Конвенции 108, данные должны храниться «в форме, которая позволяет идентифицировать субъект данных не дольше, чем это необходимо для целей обработки персональных данных». В соответствии с этим принципом данные должны быть уничтожены или обезличены после достижения целей обработки.

Процесс обезличивания данных означает, что все идентифицируемые элементы исключаются из набора персональных данных, так чтобы субъекта данных невозможно было идентифицировать. В своем мнении Рабочая группа по статье 29 анализирует эффективность и границы применения различных методов обезличивания данных. Оптимальное решение принимается в каждом индивидуальном случае. Независимо от выбранного метода обезличивание должно быть необратимым, чтобы по оставшимся атрибутам нельзя было идентифици-

ровать данных субъекта. Риск повторной идентификации обезличенных субъектов необходимо рассматривать с учетом критериев: время, усилия, затраты и использование технологических ресурсов.

После процедуры обезличивания данных они перестают относиться к персональным данным и действие Общего регламента по защите данных на них более не распространяется.

Регламент предусматривает, что физическое или юридическое лицо, не обязано проводить обработку дополнительных данных для идентификации субъекта после процедуры обезличивания. Но в случае повторно проводимых операций, например, осуществление права доступа, исправления, удаления, ограничения обработки и операций по переносу данных, когда субъект данных предоставляет дополнительную информацию и совокупность атрибутов для идентификации, такой набор данных становится персональными данными.

Псевдонимизация

К персональной информации относятся следующие атрибуты: имя, дата рождения, пол, адрес и другие элементы, по совокупности которых вас могут идентифицировать. Процесс псевдонимизации личных данных означает, что идентифицируемые атрибуты заменяются псевдонимами.

Законодательство ЕС толкует псевдонимизацию как «обработку персональных данных таким образом, при котором персональные данные больше не могут быть соотнесены с конкретными субъектами данных без использования дополнительных атрибутов данных, при условии, что такие атрибуты хранятся отдельно и защищены организационными и техническими мерами от возможной попытки идентификации субъекта».

В отличие от обезличенных данных псевдонимизированные данные по-прежнему относятся к персональным данным, которые подпадают под юрисдикцию Общего регламента по защите данных.

Общий регламент по защите данных признает различные виды использования псевдонима в качестве соответствующей технической меры для усиления защиты данных и специально упоминается при проектировании систем защиты данных и при определении средств обработки с использованием механизмов защиты по умолчанию (by design and by default).

Псевдонимизация прямо не упоминается в правовых определениях Модернизированной Конвенции 108. Тем не менее в Пояснительном докладе Модернизированной Конвенции 108 указано, что «использование псевдонима или любого цифрового идентификатора не приводит к обезличиванию данных, так как субъект все еще может быть идентифицирован и выделен как субъект данных».

Один из способов псевдонимизации данных – шифрование. После того как данным был присвоен псевдоним, расшифровка данных возможна только при наличии ключа дешифрования. Без такого ключа идентификация крайне затруднительна. Однако для владельцев такого ключа, повторная идентификация не составит сложности. Несанкционированное использование ключей дешифрования представляет риск для обработки персональных данных. Таким образом, «псевдонимированные данные должны рассматриваться как персональные данные», подпадающие под юрисдикцию Модернизированной Конвенции 108.

Аутентификация

Данная процедура предназначена для подтверждения соотношения субъекта данных с определенной личностью, или с выполнением определенных действий, таких как: вход в зону безопасности или снятие денег с банковской карты. Аутентификация может быть достигнута путем сравнения биометрических данных, таких как фотография или отпечатки пальцев в удо-

стоверении личности с данными устанавливаемого лица. Например, путем запроса информации, которая должна быть известна только лицу с определенной личностью или посредством авторизации с использованием персонального идентификационного номера (ПИН). Так же может быть предъявлен определенный токен, который должен находиться исключительно у лица с определенной идентификационной информацией или авторизацией, такой как специальная чип-карта или ключ от сейфа. Электронная подпись также является средством идентификации и аутентификации субъекта в электронных сообщениях.

Специальные категории персональных данных

Обе правовые системы Европы предусматривают специальные категории персональных данных, обработка которых несет дополнительный риск для субъектов данных, и соответственно, такие категории нуждаются в усиленной защите. Данные из таких категорий обрабатываются по принципу «запрещено все, что не разрешено» и в строго ограниченных законом целях.

Согласно статье 6 Модернизированной Конвенции 108 и статье 9 Общего регламента по защите данных, специальными считаются следующие категории данных:

– персональные данные, раскрывающие расовое и этническое происхождение;

– персональные данные, раскрывающие политические взгляды, религиозные или иные убеждения, в том числе философские;

– персональные данные членов профсоюзов;

– генетические и биометрические данные человека, обрабатываемые с целью его идентификации;

– персональные данные о здоровье, сексуальной жизни или сексуальной ориентации.

Персональные данные в контексте правонарушений и приговоров судов

Под юрисдикцию Модернизированной Конвенции 108 подпадают персональные данные, относящиеся к преступлениям, уголовными разбирательствам и приговорам суда. К таким данным применяются соответствующие меры защиты, и они отнесены к специальным категориям персональных данных. В рамках Общего регламента по защите данных такие данные не выделены в специальную категорию, но рассматриваются в отдельной статье.

Статья 10 Общего регламента по защите данных указывает, что обработка таких данных может осуществляться только «под контролем официальных властей или в случае, когда такая обработка разрешена законодательством ЕС или государства Евросоюза, и предусматривает надлежащие гарантии прав и свобод субъекта данных».

В ЕС обработка личных данных в контексте правоприменения регулируется специальным правовым документом – Директивой 2016/680/ЕС. Директива устанавливает правила защиты данных, которые являются обязательными для компетентных органов при обработке персональных данных в контексте предотвращения, расследования, выявления и преследования по уголовным преступлениям.

Концепция обработки данных

Конец ознакомительного фрагмента.