Организация Объединенных Наций A/77/196

Генеральная Ассамблея

Distr.: General
20 July 2022
Russian
Original: Spanish

Семьдесят седьмая сессия
Пункт 69 b) предварительной повестки дня
Поощрение и защита прав человека: вопросы прав человека, включая альтернативные подходы в деле содействия эффективному осуществлению прав человека и основных свобод

Право на неприкосновенность частной жизни

Записка Генерального секретаря

Генеральный секретарь имеет честь препроводить Генеральной Ассамблее доклад, подготовленный Специальным докладчиком по вопросу о праве на неприкосновенность частной жизни Аной Браян Нугререс, представленный в соответствии с резолюцией 28/16 Совета по правам человека.

22-11362 (R) 180822 190822

Резюме

Принципы, лежащие в основе неприкосновенности частной жизни и защиты персональных данных, представляют собой структурную часть правовых систем в этой области, поскольку они выполняют двойную функцию: толкования и интеграции нормативно-правовой базы. Они являются наиболее ценным и полезным средством, позволяющим контролерам и обработчикам данных обеспечить надлежащую обработку личной информации, особенно в условиях риска неправомерного использования информационно-коммуникационных технологий.

В частности, мы рассмотрим следующие принципы: законность, правомерность и легитимность; согласие; транспарентность; цель; добросовестность; пропорциональность; минимизация; качество; ответственность и безопасность — как основополагающие принципы правовой системы в целом, регулирующей неприкосновенность частной жизни и защиту персональных данных. Мы проведем сравнительное исследование формулировок принципов, содержащихся в семи международных нормативных документах, как будет видно из нижеследующего текста. Мы выделим их общие элементы в целях работы над концепцией гармонизации на глобальном уровне и решения проблем защиты неприкосновенности частной жизни и персональных данных как основных прав человека, которые в силу своего сквозного характера способствуют реализации других основных прав человека, таких как право на свободу, равенство, честь и человеческое достоинство в цифровую эпоху.

Принципы, лежащие в основе неприкосновенности частной жизни и защиты персональных данных

I. Введение

1. В области неприкосновенности частной жизни и защиты данных существуют руководящие принципы, которые представляют собой руководство для толкования, помогают заполнить пробелы в законодательстве и имеют фундаментальное значение для определения путей решения проблем, возникающих при обработке персональных данных с использованием информационно-коммуникационных технологий.

2. Национальные и международные нормы в этой области носят общий характер. По этой причине они должны быть внедрены в различные виды деятельности по обработке персональных данных, осуществляемой контролерами и обработчиками, занятыми в различных секторах, государственном или частном, на национальном или международном уровне и независимо от используемых технологий[1]. Основной задачей является эффективное применение соответствующих нормативных актов, поскольку в демократической системе правления простого признания и разработки законов, касающихся основных прав, недостаточно. Эти закрепленные права должны сопровождаться эффективными гарантиями их реализации, независимо от контекста.

3. В связи с этим руководящие принципы, которые мы собираемся проанализировать, являются наиболее ценным и полезным средством обеспечения надлежащей обработки личной информации.

4. Принципы, лежащие в основе неприкосновенности частной жизни и защиты персональных данных, не следует рассматривать лишь как рекомендации, поскольку они имеют более высокий статус, чем рекомендации. В силу этого статуса они являются структурной частью правовых систем в этой области. Эти принципы обязывают контролеров и обработчиков действовать надлежащим образом при обработке персональных данных, а также принимать меры в связи с рисками неправомерного использования информационно-коммуникационных технологий, искусственного интеллекта и других технологических разработок, что, в свою очередь, позволит субъектам данных сохранять контроль над своей личной информацией.

5. Эти принципы тесно взаимосвязаны. Поэтому их следует рассматривать не только по отдельности, но и как часть комплекса, к которому они относятся, в целях обеспечения надлежащего управления личной информацией и уважения соответствующих основных прав и свобод.

6. Необходимо учитывать специальные категории персональных данных, в частности конфиденциальные данные. В настоящее время существует единое мнение, что на такие данные должны распространяться ограничения на обработку, так как они требуют большей защиты, поскольку затрагивают наиболее личную сферу жизни человека; как следствие, их обработка может представлять больший риск для основных прав и свобод.

---

[1] «Технологическая нейтральность имеет особое значение в связи со скоростью технологических инноваций и помогает обеспечить, чтобы законодательство оставалось способным учитывать будущие изменения и не устаревало слишком быстро». Comisión de las Naciones Unidas para el Derecho Mercantil Internacional, *Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firmas electrónicas* (Viena, 2009).

7. Согласно международным нормативным документам, в большинстве стран конфиденциальные данные, как правило, не должны обрабатываться, за исключением случаев, прямо установленных нормами. Смысл существования этого правила заключается в необходимости устранения риска дискриминации в отношении субъектов данных.

8. Считается целесообразным, чтобы в законодательстве были указаны категории конфиденциальных персональных данных, а также определена сфера их защиты и исключения из нее; при рассмотрении данных, относящихся к этой категории, государства вправе принимать во внимание свой контекст (культурный, социальный или политический) и местные реалии.

9. Обработка конфиденциальных персональных данных должна быть разрешена, если их защита надлежащим образом гарантирована законом. Такие гарантии должны включать, в частности, необходимость применения руководящих принципов в отношении неприкосновенности частной жизни и защиты данных.

10. Для обеспечения начала разработки принципов неприкосновенности частной жизни и защиты персональных данных на глобальном уровне в настоящем докладе проанализированы руководящие принципы, содержащиеся в семи международных нормативных документах по данному вопросу.

11. В этих документах были выделены основные общие аспекты и выявлены некоторые особенности для достижения консенсуса, который позволит гармонизировать усилия по надлежащей обработке персональных данных, отвечающей требованиям защиты этого права, а также неприкосновенности частной жизни и уважения человеческого достоинства в цифровую эпоху.

II. Нормативный анализ

12. В нижеследующих разделах мы проанализируем принципы законности, правомерности и легитимности; согласия; транспарентности; цели; добросовестности; пропорциональности; минимизации; качества; ответственности и безопасности. Для целей настоящего анализа основополагающими являются следующие документы:

- Общий регламент Европейского союза по защите данных (Общий регламент)[2]
- Модернизированная Конвенция Совета Европы о защите частных лиц в отношении обработки данных личного характера (модернизированная Конвенция 108)[3]
- Резолюция 45/95 Генеральной Ассамблеи Организации Объединенных Наций под названием «Руководящие принципы регламентации компьютеризованных картотек, содержащих данные личного характера» (Руководящие принципы Организации Объединенных Наций)
- Стандарты защиты персональных данных для иберо-американских государств, принятые Иберо-американской сетью по защите данных (Иберо-американские стандарты)[4]

[2] Регламент (ЕС) 2016/679 Европейского парламента и Совета от 27 апреля 2016 года.

[3] URL: https://rm.coe.int/1680078c46.

[4] Red Iberoamericana de Protección de Datos, “Estándares de Protección de Datos de los Estados Iberoamericanos”. URL: https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf.

- Рекомендации Совета, касающиеся Руководства по защите неприкосновенности частной жизни и трансграничной передаче персональных данных Организации экономического сотрудничества и развития (ОЭСР) (Руководство ОЭСР)[5]
- Рамочная основа неприкосновенности частной жизни Азиатско-Тихоокеанского экономического сотрудничества (АТЭС) (Рамочная основа неприкосновенности частной жизни АТЭС)[6]
- Обновленные принципы Межамериканского юридического комитета по неприкосновенности частной жизни и защите персональных данных, с аннотациями, принятые Генеральной Ассамблеей Организации американских государств (ОАГ) (Принципы ОАГ)[7]

Принцип законности, правомерности и легитимности

13. В соответствии с этим принципом обработка персональных данных на протяжении всего их жизненного цикла должна осуществляться контролером или обработчиком согласно соответствующим законам и с соблюдением признанных на международном уровне прав человека. Это означает, что посредством надлежащей и, следовательно, законной обработки персональных данных будет обеспечено и уважение к частной жизни, а также к другим правам и достоинству человека как субъекта данных.

14. Соблюдение права на защиту персональных данных, которое признано в качестве права, обеспечивающего защиту других прав[8], гарантирует, что надлежащая обработка данных, касающихся физического лица, будет, в свою очередь, гарантировать соблюдение других его основных прав.

15. Хотя законность должна быть основой всех действий по обработке на протяжении всего жизненного цикла персональных данных, то есть от их сбора до удаления, акцент обычно делается на первом действии по обработке, а именно на сборе данных, поскольку если это действие выполняется незаконно, это повлияет на законность других действий по обработке, которые следуют за ним[9].

16. В модернизированной Конвенции 108 относительно легитимности обработки данных говорится, что обработка должна преследовать законную цель на всех этапах и осуществляться в соответствии с законом (ст. 5.1).

17. Согласно Руководящим принципам Организации Объединенных Наций, принцип правомерности и законности требует, чтобы сбор и обработка личной информации осуществлялись правомерными и законными способами.

18. Различные международные нормативные документы диверсифицируют или включают в себя другие принципы защиты данных, которые связаны с принципом законности и дополняют его.

---

[5] URL: https://digital.report/rekomendatsii-soveta-kasayushhiesya-rukovodstva-po-zashhite-neprikosnovennosti-chastnoy-zhizni-i-transgranichnoy-peredache-personalnyih-dannyih/.

[6] URL: https://www.apec.org/publications/2017/08/apec-privacy-framework-(2015).

[7] Informe del Comité Jurídico Interamericano, “Principios Actualizados del Comité Jurídico Interamericano sobre la Privacidad y la Protección de Datos Personales, con anotaciones”. 9 de abril de 2021.

[8] Статья 1 модернизированной Конвенции 108.

[9] Пункт 7 Руководства ОЭСР; принцип 1 Обновленных принципов Юридического комитета; статья 1 Руководящих принципов.

19. Так, в статье 6 и пунктах 39 и 40 Общего регламента предусматривается, что принцип правомерности обработки данных соблюдается, когда обработка осуществляется на одном из правовых оснований, установленных законом.

20. Согласно Иберо-американским стандартам принцип легитимности предполагает, что обработка персональных данных может осуществляться только на условиях, установленных законом (ст. 11).

21. В соответствии с Рекомендациями Совета ОЭСР сбор данных должен осуществляться законным и честным образом и с ведома или согласия субъекта данных (ст. 7).

22. Законность обработки персональных данных основывается на наличии ряда законных оснований, установленных действующими нормативными актами. По итогам анализа положений рассмотренных международных нормативных документов была составлена таблица 1, в которой представлены признанные на международном уровне законные основания.

Таблица 1
Законные основания для обработки данных

	Модернизированная Конвенция Совета Европы о защите частных лиц в отношении обработки данных личного характера	*Руководящие принципы регламентации компьютеризованных картотек, содержащих данные личного характера, Организации Объединенных Наций*	*Стандарты защиты персональных данных Иберо-американской сети по защите данных*	*Общий регламент Европейского союза по защите данных*	*Руководство по защите неприкосновенности частной жизни и трансграничной передаче персональных данных ОЭСР*	*Рамочная основа неприкосновенности частной жизни АТЭС*	*Обновленные принципы ОАГ по неприкосновенности частной жизни и защите персональных данных, с аннотациями*
	Статья	*Статья*	*Статья*	*Статья*	*Пункт*	*Принцип*	*Принцип*
Согласие субъекта данных	5.2		11.1 a)	6.1 a)	10 a)	III.24	1
Согласие субъекта данных для цели, несовместимой с той, для которой был разрешен сбор данных		3 b)					
Закон	5.3		14.1		10 b)	IV.25 c)	1
Юридическое обязательство контролера			11.1 f)	6.1 c)			1
Договорные отношения или преддоговорные действия			11.1 e)	6.1 b)		IV.25 b)	1
Государственный интерес			11.1 h)	6.1 e)			1
Законный интерес контролера			11.1 i)	6.1 f)			1
Жизненно важные интересы субъекта данных или третьей стороны			11.1 g)	6.1 d)			1
Признание или защита прав субъекта данных в государственном органе			11.1 d)				1
Постановление суда, решение или мандат государственного органа			11.1 b)				1

23. Ниже указаны допустимые основания для обработки персональных данных, в порядке частоты упоминания таких оснований в проанализированных международных нормативных документах.

24. Шесть документов включают согласие субъекта данных в качестве одного из законных оснований для обработки персональных данных, что делает его наиболее часто упоминаемым основанием в проанализированных нормативных актах.

25. Согласно Руководящим принципам Организации Объединенных Наций, согласие устанавливается не в качестве общего допустимого основания, а для осуществления деятельности по обработке данных в целях, отличных от тех, для которых был разрешен сбор. С учетом вышесказанного, а также статьи 1 Руководящих принципов, которой регулируется анализируемый принцип, персональные данные должны обрабатываться законными и правомерными способами в соответствии с целями Устава Организации Объединенных Наций, что предполагает обеспечение определенной гласности или информирование субъекта данных.

26. За согласием субъекта данных следует верховенство права или правовые положения внутреннего законодательства каждой страны-члена, о чем говорится в пяти проанализированных документах.

27. В четырех документах в качестве законного основания фигурируют договорные отношения и преддоговорные действия; признание этого основания в рамках гражданских и коммерческих отношений, а также электронной торговли приобретает особую актуальность в экономическом контексте цифровой эпохи.

28. В трех документах в качестве законных оснований признаются юридическое обязательство контролера, государственный интерес, законный интерес контролера и жизненно важные интересы субъекта данных или третьей стороны, а в двух документах говорится о признании или защите прав субъекта данных в государственном органе и постановлении суда, решении или мандате государственного органа.

29. Для обеспечения уважения права на защиту персональных данных, неприкосновенности частной жизни и человеческого достоинства, независимо от нормативного контекста, контролеру и, где это применимо, обработчику для управления персональными данными необходимо иметь одно из допустимых оснований.

Принцип согласия

30. Согласие — это явное или подразумеваемое волеизъявление, в результате которого у лица появляется юридическое обязательство. Когда субъект данных дает свое согласие, право контроля над его персональными данными, принадлежащими ему как субъекту данных, проявляется напрямую.

31. Принцип согласия тесно связан с принципом законности, поскольку оно является наиболее распространенным, признанным на международном уровне допустимым основанием для обработки персональных данных.

32. В соответствии с принципом согласия субъект данных должен указать, что согласен с тем, что его персональные данные могут собираться, записываться, преобразовываться, сообщаться, передаваться и в целом подвергаться любой обработке, включая удаление, что предоставляет контролеру возможность

распоряжаться данными в течение всего их жизненного цикла и определять его границы[10].

33. В проанализированных нормативных документах согласие является одним из наиболее важных законных оснований для обработки персональных данных, поскольку оно конкретно предусмотрено в качестве такового в шести из них[11], с различными характерными элементами.

34. Упомянутые ниже элементы являются средством определения параметров, в рамках которых может быть дано согласие как способ наиболее точно отразить волеизъявление субъекта данных.

35. В таблице 2 ниже сравниваются характеристики, содержащиеся в семи проанализированных международных нормативных документах.

Таблица 2
Характеристики согласия

	Модернизированная Конвенция Совета Европы о защите частных лиц в отношении обработки данных личного характера	*Руководящие принципы регламентации компьютеризованных картотек, содержащих данные личного характера, Организации Объединенных Наций*	*Стандарты защиты персональных данных Иберо-американской сети по защите данных*	*Общий регламент Европейского союза по защите данных*	*Руководство по защите неприкосновенности частной жизни и трансграничной передаче персональных данных ОЭСР*	*Рамочная основа неприкосновенности частной жизни АТЭС*	*Обновленные принципы ОАГ по неприкосновенности частной жизни и защите персональных данных, с аннотациями*
	Статья (статьи)	*Статья (статьи)*	*Статья (статьи)*	*Статья (статьи)*	*Пункт*	*Принцип*	*Принцип*
Свободное	5.2			4.11			2
Выраженное	5.2		12	4.11			2
Информированное	5.2			7.3 и 4.11	Пункт 52 объяснительного меморандума		2
Недвусмысленное	5.2		12	4.11			2
Отзываемое			12.2	7.3			2

36. Как можно видеть, в модернизированной Конвенции 108 (ст. 5.2), Общем регламенте[12] и Обновленных принципах ОАГ (принцип 2) дается наибольшее число характеристик типа согласия, необходимого для защиты персональных данных, чтобы наиболее точно отразить волеизъявление субъекта данных.

37. Исходя из анализа характеристик, упомянутых в текстах, согласие такого типа должно быть свободным, выраженным, информированным, недвусмысленным и отзываемым. Мы видим, что такая характеристика, как возможность отзыва согласия, априори отсутствует в модернизированной Конвенции 108 (а также в Руководящих принципах Организации Объединенных Наций (ст. 4), Руководстве ОЭСР и Рамочной основе неприкосновенности частной жизни АТЭС (ст. 21–23 и 26)); вместе с тем ее можно найти в этих текстах в разделах,

[10] Пункт 32 Общего регламента.

[11] Как отмечалось в предыдущем разделе, посвященном принципу законности, правомерности и легитимности, в Руководящих принципах Организации Объединенных Наций согласие устанавливается только в качестве законного основания для осуществления деятельности по обработке данных в целях, отличных от тех, для которых был разрешен сбор.

[12] Статьи 4.11, 6.3 a) и b), 6.1 a), b), c), d) и e), 7 и 8.

касающихся прав субъектов данных[13]. Возможность отзыва представлена как коррелят полномочия на согласие, имеющий противоположный смысл и действующий после выдачи согласия.

38. В Руководстве ОЭСР характеристика информированного согласия в принципе не вытекает из формулировки статей, которыми предусматривается, что сбор данных должен осуществляться, если возможно, с ведома или согласия субъекта данных. Однако в объяснительном меморандуме к Руководству отмечается, что, хотя согласие субъекта данных может быть установлено или не установлено в качестве обязательного условия, минимальным требованием должна быть его осведомленность[14]. Поэтому, если согласие является обязательным условием для сбора персональных данных, оно должно быть информированным, поскольку осведомленность субъекта данных является минимальным требованием, которое должно быть выполнено.

39. Характеристика волеизъявления, посредством которого разрешается обработка данных, не всегда фигурирует в статьях, регулирующих принцип согласия, но следует отметить, что в некоторых документах, например в статье 4 Общего регламента, ряд таких характеристик устанавливается в определениях и пояснениях.

40. В Руководящих принципах Организации Объединенных Наций и Рамочной основе неприкосновенности частной жизни АТЭС характеристики согласия не устанавливаются.

41. Должно ясно следовать, что, если согласие является допустимым основанием для обработки персональных данных, оно должно быть получено до начала деятельности, на которую оно предоставляется.

42. Принцип согласия напрямую связан с принципом транспарентности, поскольку юридически действительное согласие субъекта данных подразумевает, что он надлежащим образом проинформирован об условиях, которые будут применяться к его личной информации.

43. Следует особо упомянуть о согласии на обработку персональных данных несовершеннолетних и о том, как этот вопрос отражен в различных документах. Что касается защиты персональных данных, то дети и подростки считаются уязвимой группой, особенно восприимчивой к последствиям обработки касающейся их информации, а потому необходимо обеспечить их комплексную защиту и благополучие.

44. В Иберо-американских стандартах (ст. 13), Общем регламенте (ст. 8), а также в Принципах ОАГ (принцип 2, с аннотациями) для получения согласия несовершеннолетних требуется разрешение со стороны обладателей родительских прав или их законных представителей, которые будут нести ответственность за последствия обработки данных. В этой связи в вышеупомянутых документах также предусматривается, что внутренним правом каждого государства может устанавливаться минимальный возраст, по достижении которого несовершеннолетние могут самостоятельно давать согласие с соблюдением надлежащих гарантий.

[13] Статья 9 модернизированной Конвенции 108; статья 4 Руководящих принципов.

[14] Объяснительный меморандум (пункт 52).

Принцип транспарентности

45. Один из принципов, касающихся обработки персональных данных, заключается в том, что данные должны обрабатываться контролером транспарентным по отношению к субъекту данных образом. Этот принцип подразумевает, что контролер должен информировать субъекта данных об условиях обработки, которым будет подвергаться его личная информация с момента сбора, чтобы субъект данных был в состоянии осуществлять надлежащий контроль над данными.

46. В таблице 3 ниже приведена информация, которую, согласно проанализированным международным нормативным документам, контролеры должны предоставлять субъектам данных.

Таблица 3

Информация, которая должна быть предоставлена субъектам данных

	Модернизированная Конвенция Совета Европы о защите частных лиц в отношении обработки данных личного характера	*Руководящие принципы регламентации компьютеризованных картотек, содержащих данные личного характера, Организации Объединенных Наций*	*Стандарты защиты персональных данных Иберо-американской сети по защите данных*	*Общий регламент Европейского союза по защите данных*		*Руководство по защите неприкосновенности частной жизни и трансграничной передаче персональных данных ОЭСР*	*Рамочная основа неприкосновенности частной жизни АТЭС*	*Обновленные принципы ОАГ по неприкосновенности частной жизни и защите персональных данных, с аннотациями*
				Когда данные получены от субъекта	*Когда данные не получены от субъекта*			
	Статья (статьи)	*Статья (статьи)*	*Статья (статьи)*	*Статья (статьи)*		*Пункт*	*Принцип*	*Принцип*
Личность и адрес контролера и/или представителя	8.1 a)		16.2 a)	13.1 a)	14.1 a)	12	21 d)	2
Существование и/или основные характеристики обработки			16.1			12	21 a)	
Правовое основание или база	8.1 b)			13.1 c)	14.1 c) и 14.2 b)			2
Цели или задачи обработки	8.1 b)		16.2 b)	13.1 c)	14.1 c)	12	21 b)	2
Категории обрабатываемых данных	8.1 c)				14.1 d)			
Происхождение данных, если они не получены непосредственно от субъекта данных			16.2 e)		14.2 f)			
Получатели или категория получателей	8.1 d)		16.2 c)	13.1 e)	14.1 e)		21 c)	2
Информация о правах и способах их реализации	8.1 e)		16.2 d)	13.2 b) и c)	14.2 c) и d)		21 e)	2
Право на подачу жалобы в надзорный орган				13.2 d)	14.2 e)			

	Модернизированная Конвенция Совета Европы о защите частных лиц в отношении обработки данных личного характера	*Руководящие принципы регламентации компьютеризованных картотек, содержащих данные личного характера, Организации Объединенных Наций*	*Стандарты защиты персональных данных Иберо-американской сети по защите данных*	*Общий регламент Европейского союза по защите данных*		*Руководство по защите неприкосновенности частной жизни и трансграничной передаче персональных данных ОЭСР*	*Рамочная основа неприкосновенности частной жизни АТЭС*	*Обновленные принципы ОАГ по неприкосновенности частной жизни и защите персональных данных, с аннотациями*
				Когда данные получены от субъекта	*Когда данные не получены от субъекта*			
	Статья (статьи)	*Статья (статьи)*	*Статья (статьи)*	*Статья (статьи)*		*Пункт*	*Принцип*	*Принцип*
Является ли сообщение юридическим или договорным требованием или необходимо для заключения договора, и обязан ли субъект данных предоставить свои персональные данные, а также последствия их непредоставления				13.2 e)				
Наличие автоматизированных решений, включая профилирование, содержательная информация о применяемой логике, значении и предполагаемых последствиях такой обработки				13.2 f)	14.2 g)			
Информация о цели, если планируется дальнейшая обработка с целью, отличной от той, для которой были собраны данные				13.3	14.4			
Контактная информация сотрудника, ответственного за защиту данных				13.1 b)	14.1 b)			
Срок хранения или критерии для его определения				13.2 a)	14.2 a)			

	Модернизированная Конвенция Совета Европы о защите частных лиц в отношении обработки данных личного характера	*Руководящие принципы регламентации компьютеризованных картотек, содержащих данные личного характера, Организации Объединенных Наций*	*Стандарты защиты персональных данных Иберо-американской сети по защите данных*	*Общий регламент Европейского союза по защите данных*		*Руководство по защите неприкосновенности частной жизни и трансграничной передаче персональных данных ОЭСР*	*Рамочная основа неприкосновенности частной жизни АТЭС*	*Обновленные принципы ОАГ по неприкосновенности частной жизни и защите персональных данных, с аннотациями*
				Когда данные получены от субъекта	*Когда данные не получены от субъекта*			
	Статья (статьи)	*Статья (статьи)*	*Статья (статьи)*	*Статья (статьи)*		*Пункт*	*Принцип*	*Принцип*
Предусмотрены ли сообщение или передача, а также нормативные акты, которыми они разрешены				13.1 f)	14.1 f)			
Передаваемая информация								2
Цели передачи			16.2 c)					

47. Как можно заметить, среди семи проанализированных международных нормативных документов Руководящие принципы не регулируют принцип транспарентности; следовательно, далее мы проанализируем повторяющиеся ссылки в остальных шести документах на информацию, которая, согласно им, должна быть предоставлена субъектам персональных данных в соответствии с принципом транспарентности.

48. В шести документах указано, что должны быть раскрыты личность и адрес контролера или его представителя, а также цели или задачи обработки. Эти данные составляют основу транспарентных действий.

49. В пяти документах требуется информирование о правах субъекта данных и способах их реализации, а также о получателях или категории получателей. В отношении наличия у субъекта информации о принадлежащих ему как субъекту правах указывается на важность того, чтобы субъект находился в надлежащем положении для осуществления своего права контроля над касающейся его личной информацией.

50. В трех документах требуется информирование о правовом основании или базе для обработки, а также о существовании и/или основных характеристиках обработки.

51. Принцип транспарентности должен соблюдаться независимо от правового основания для обработки. Могут возникнуть исключительные ситуации, связанные со своевременностью предоставления информации субъекту данных[15] или с теми случаями, когда субъект данных не является источником, из которого собирается его или ее личная информация[16]; такие исключительные ситуации должны использоваться для обеспечения максимально возможной транспарентности и добросовестности.

52. В двух документах требуется информирование о категории обрабатываемых данных и о происхождении данных, если они не были получены непосредственно от субъекта данных.

53. Настоящий анализ также включает информацию, которая согласно только одному международному нормативному документу должна быть сообщена субъекту персональных данных, чтобы обеспечить лучшие условия для осуществления им своего права контроля.

54. В данном случае речь идет о Стандартах для иберо-американских государств в отношении целей, с которыми осуществляется передача данных, и Общем регламенте, в котором упоминаются следующие пункты: контактная информация сотрудника, ответственного за защиту данных; срок хранения или критерии для его определения; предусмотрены ли сообщение или передача, а также нормативные акты, которыми они разрешены; право на подачу жалобы в надзорный орган; является ли сообщение юридическим или договорным требованием или необходимо для заключения договора, и обязан ли субъект данных предоставить свои персональные данные, а также последствия их непредоставления; наличие автоматизированных решений, включая профилирование, содержательная информация о применяемой логике, значении и предполагаемых последствиях такой обработки; информация о цели, если планируется дальнейшая обработка с целью, отличной от той, для которой были собраны данные.

55. Среди требований, о которых говорится исключительно в Общем регламенте, следует упомянуть только одно, которое направлено на то, чтобы субъект данных понимал, каким образом будет обрабатываться информация о нем,

[15] Статья 22 Рамочной основы неприкосновенности частной жизни АТЭС.

[16] Статья 8.3 модернизированной Конвенции 108.

например, будет ли использоваться искусственный интеллект, и согласно которому ему должна быть предоставлена «содержательная информация о применяемой логике» и «значении и предполагаемых последствиях»[17].

56. Информация, с которой субъект данных должен быть ознакомлен согласно принципу транспарентности, должна предоставляться простым, ясным, разборчивым, доступным и понятным языком[18]; при этом особое внимание следует проявлять в случае детей и подростков[19].

57. Следует добавить, что особое значение имеет должная осмотрительность контролера при работе с личной информацией, поскольку контролер должен руководствоваться транспарентной политикой в отношении обработки персональных данных[20].

Принцип цели

58. Принцип цели направляет и ограничивает все действия по обработке персональных данных, от сбора до удаления. Цель, как правило, определяется контролером, однако она не будет признана действительной, если она не связана с одним из законных оснований для обработки данных.

59. С начала сбора цель должна соответствовать определенным характеристикам, которые изложены в проанализированных международных нормативных документах. Так, цель должна быть явной, конкретной, законной и релевантной. После обеспечения соответствия характеристикам, установленным нормативными документами для определения цели или целей, эти характеристики будут ограничивать деятельность по обработке, которой будут подвергаться персональные данные.

60. Согласно рассматриваемому принципу, собранные данные могут быть использованы исключительно в рамках той цели, для которой они были собраны. Он служит для ограничения различных действий по обработке данных, от сбора до хранения, изменения, сообщения и передачи, а также любого обращения с данными, вплоть до их удаления.

61. Поэтому, как указано в различных нормативных документах[21], любая деятельность по обработке не должна выходить за рамки того, что разрешено для изначально определенных целей, за исключением случаев, когда это прямо разрешено действующими нормативными актами, и с соблюдением необходимых гарантий. Пример этого можно найти в Рамочной основе неприкосновенности частной жизни[22], где упоминается возможность использования данных для других целей, совместимых с первоначально установленными целями.

---

[17] Agencia Española de Protección de Datos. *Adecuación al Reglamento General de Protección de Datos de tratamientos que incorporan inteligencia artificial: una introducción*. Febrero 2020, pág. 24. URL: https://www.aepd.es/sites/default/files/2020-02/adecuacion-rgpd-ia.pdf.

[18] Статья 16.3 Иберо-американских стандартов; статья 12.1 Общего регламента; статья 21 Рамочной основы неприкосновенности частной жизни АТЭС.

[19] Статья 16.3 Иберо-американских стандартов; статья 12.1 Общего регламента.

[20] Статья 16.4 Иберо-американских стандартов; пункт 12 Руководства ОЭСР; статья 21 Рамочной основы неприкосновенности частной жизни АТЭС.

[21] Статья 5.4 b) модернизированной Конвенции 108; статья 3 Руководящих принципов Организации Объединенных Наций; статья 17 Иберо-американских стандартов; статья 5.1 b) Общего регламента; пункт 9 Руководства ОЭСР; статьи 24 и 25 Рамочной основы неприкосновенности частной жизни АТЭС; принцип 1 Обновленных принципов ОАГ.

[22] Статья 25, раздел IV Рамочной основы неприкосновенности частной жизни АТЭС.

62. Принцип цели упоминается во всех проанализированных текстах[23]; в них излагаются его характеристики и последствия применения его на практике. Он тесно связан с принципом законности, или правомерности, поскольку им устанавливается законность целей в качестве необходимой характеристики.

63. В международных нормативных документах указаны характеристики, которым должна соответствовать цель, чтобы обеспечить возможность обработки персональных данных; как показано в таблице ниже, цели должны быть явными, конкретными, законными и релевантными.

Таблица 4
Характеристики цели

	Модернизированная Конвенция Совета Европы о защите частных лиц в отношении обработки данных личного характера	*Руководящие принципы регламентации компьютеризованных картотек, содержащих данные личного характера, Организации Объединенных Наций*	*Стандарты защиты персональных данных Иберо-американской сети по защите данных*	*Общий регламент Европейского союза по защите данных*	*Руководство по защите неприкосновенности частной жизни и трансграничной передаче персональных данных ОЭСР*	*Рамочная основа неприкосновенности частной жизни АТЭС*	*Обновленные принципы ОАГ по неприкосновенности частной жизни и защите персональных данных, с аннотациями*
	Статья (статьи)	*Статья (статьи)*	*Статья (статьи)*	*Статья (статьи)*	*Пункт*	*Принцип*	*Принцип*
Явная	5.4 b)	3	17	5.1 b)	9	24 и 25	1
Конкретная	5.4 b)	3	17	5.1 b)	9	24 и 25	
Законная	5.4 b	3	17	5.1 b)		24 и 25	1
Релевантная	5.4 b	3	17	5.1 b)	9	24 и 25	

64. Законность не упомянута в качестве характеристики целей обработки данных только в пункте 9 Руководства ОЭСР. Это может быть связано как с простой проблемой редакции, так и с опущением того, что в принципе представляется подразумеваемым при анализе всего нормативного документа.

65. Что касается Принципов ОАГ, то, хотя все характеристики целей прямо не изложены в тексте принципа 1, подразумевается, что они охвачены аннотацией к этому принципу.

66. Что касается специфики обработки в зависимости от цели, то следует отметить, что Общий регламент (ст. 5.1), Иберо-американские стандарты (ст. 17.3), модернизированная Конвенция 108 (ст. 5.4 b)) и Принципы ОАГ (принцип 4) предусматривают возможность использования данных для целей, отличных от тех, для которых они были собраны, при условии, что такие цели являются статистическими, историческими или научными.

67. Как было указано выше, законная цель или цели, послужившие основанием для обработки, ограничивают действия контролера и обработчика, если таковой имеется, а потому, как только цель будет исчерпана или достигнута, законность продолжения обработки будет утрачена, если иное прямо не предусмотрено в применимом законодательстве, которое в таком случае послужит новым допустимым основанием.

[23] Статья 5.4 b) модернизированной Конвенции 108; статья 3 Руководящих принципов Организации Объединенных Наций; статья 17 Иберо-американских стандартов; статья 5.1 b) Общего регламента; статья 9 Руководства ОЭСР; статьи 24 и 25 Рамочной основы неприкосновенности частной жизни АТЭС; принцип 1 Принципов ОАГ.

Принцип добросовестности

68. Этот принцип означает, что личная информация должна обрабатываться в точном соответствии со всеми условиями, послужившими основанием для ее сбора, а также с использованием средств обработки, способствующих достижению цели.

69. Ниже мы проанализируем международные нормативные документы, в которых регламентируется этот принцип.

70. В статье 1 Руководящих принципов Организации Объединенных Наций предусматривается принцип законности и лояльности. Он направлен на то, чтобы обеспечить, чтобы данные не обрабатывались незаконными или нелояльными методами и не использовались в целях, противоречащих принципам Устава Организации Объединенных Наций. В общем смысле это означает, что не должно быть произвольной дискриминации в отношении субъекта данных, что обработка данных должна осуществляться в соответствии с национальными и международными принципами и нормами, а также что права отдельных лиц должны неукоснительно соблюдаться.

71. В Иберо-американских стандартах этот принцип фигурирует как принцип добросовестности (ст. 15). В соответствии с ним контролер обязан отдавать приоритет защите интересов субъекта данных и воздерживаться от обработки данных обманным или мошенническим путем. Обработка данных, которая приводит к несправедливой или произвольной дискриминации их субъектов, считается недобросовестной.

72. Аналогичным образом статьей 5.1 a) Общего регламента устанавливается, что одним из принципов, который должен соблюдаться при обработке персональных данных, является принцип добросовестности, а также принципы правомерности и транспарентности по отношению к субъекту данных.

73. В Руководстве ОЭСР в рамках принципа ограничения сбора данных упоминается честность (п. 7). В данной статье рассматриваются два вопроса: a) ограничения на сбор данных; b) требования к методам сбора данных; именно в рамках последнего вопроса указывается, что данные должны быть получены законным и честным образом.

74. Вместе с тем в статье 24 Рамочной основы неприкосновенности частной жизни АТЭС в некоторой степени упоминается принцип добросовестности: в ней указано, что методы сбора данных должны быть законными и справедливыми.

75. Как и в предыдущем случае, в модернизированной Конвенции 108 этот принцип прямо не упоминается, но о его установлении можно судить по статье 5.4 a), где говорится, что при обработке данные должны использоваться справедливо, причем это условие относится не только к первому действию по обработке — сбору данных, но и к любому действию, связанному с обработкой данных.

76. Наконец, в Принципах ОАГ этот принцип установлен как часть первого принципа, «законные цели и добросовестность», согласно которому «персональные данные должны собираться только для законных целей и добросовестными и законными средствами». В данном случае добросовестность прямо предусмотрена в отношении средств, используемых для сбора персональных данных.

77. В Принципах ОАГ указано, что «добросовестность контекстуальна и зависит от обстоятельств» и что она требует, чтобы людям предлагался соответствующий выбор относительно того, как и когда они предоставляют свои данные,

что исключает их получение путем мошенничества, обмана и под ложным предлогом.

78. Добросовестность должна соблюдаться в ходе всех действий по обработке персональных данных; в международных нормативных документах, в которых особое внимание уделяется деятельности по сбору данных, подчеркивается, что некорректный или незаконный способ действий в самом начале процесса может обозначить и определить последующие действия по обработке.

79. Не должно быть никаких сомнений в том, что добросовестная обработка должна быть характерной чертой деятельности контролера и обработчика на протяжении всего жизненного цикла персональных данных, независимо от контекста и используемой технологии. Добросовестная деятельность предполагает ответственность, этику и соблюдение норм, применимых в свете принципов.

Принцип пропорциональности

80. Принцип пропорциональности накладывает ограничения на обработку персональных данных. В силу этого принципа персональные данные, а также действия по их обработке должны быть ограничены исключительно достижением целей, для которых они были собраны[24].

81. Следует помнить, что этот принцип должен соблюдаться на всех этапах обработки, начиная с момента принятия решения о проведении обработки, чтобы первый этап сбора был начат надлежащим и законным образом.

82. С этим принципом тесно связаны принцип цели, согласно которому данные должны обрабатываться способом, совместимым с целью, для которой они были собраны, и принцип минимизации, согласно которому данные должны быть сведены к минимуму, необходимому для достижения установленной цели.

83. Одно из требований принципа пропорциональности заключается в том, что контролер должен провести оценку, чтобы выбрать из различных операций по обработке, которые могут быть использованы для достижения разрешенной цели, ту, которая является наименее инвазивной для частной и личной жизни. Такая оценка становится особенно необходимой, когда прибегают к использованию определенных информационно-коммуникационных технологий, которые могут представлять риск для основных прав.

84. Этот принцип упоминается во всех проанализированных международных нормативных документах, либо конкретно, как, например, в статье 18 Иберо-американских стандартов, либо в рамках других принципов. В Руководящих принципах Организации Объединенных Наций он включен в принцип цели (ст. 3 a)); в модернизированной Конвенции 108 — в принцип законности обработки и качества данных (ст. 5.1 и 5.4 c)); в Общем регламенте — в принцип минимизации данных (ст. 5.1 c)); в Рамочной основе неприкосновенности частной жизни АТЭС — в принцип ограничения сбора данных (ст. 24); в Руководстве ОЭСР — в принцип конкретизации целей (п. 9); наконец, в Принципах ОАГ — в принцип актуальности и необходимости (принцип 3) и принцип ограниченного обращения и хранения (принцип 4).

[24] Статьи 5.1 и 5.4 c) модернизированной Конвенции 108; статья 18.1 Иберо-американских стандартов; статья 24 Рамочной основы неприкосновенности частной жизни АТЭС; статья 5.1 c) Общего регламента; статья 3 a) Руководящих принципов Организации Объединенных Наций; пункт 9 Руководства ОЭСР; принципы 3 и 4 Принципов ОАГ.

85. Из таблицы 5 видно, что в Иберо-американских стандартах, Общем регламенте, Руководящих принципах Организации Объединенных Наций и Принципах ОАГ упоминается актуальность данных по отношению к цели. Вместе с тем в модернизированной Конвенции 108, Иберо-американских стандартах, Общем регламенте и Принципах ОАГ упоминается, что данные должны соответствовать цели.

86. Во всех проанализированных международных нормативных документах, за исключением Руководящих принципов Организации Объединенных Наций, так или иначе утверждается, что данные должны быть ограниченными и не должны быть чрезмерными по отношению к цели, для которой они были собраны. В Иберо-американских стандартах, Общем регламенте, Рамочной основе неприкосновенности частной жизни АТЭС и Принципах ОАГ утверждается, что данные должны быть ограничены тем, что необходимо в связи с целью.

87. Вместе с тем в модернизированной Конвенции 108 упоминается, что данные не должны быть чрезмерными по отношению к цели, для которой они обрабатываются; делается также ссылка на то, что данные должны соответствовать поставленной задаче и что обработка данных должна быть пропорциональна преследуемой законной цели. В Руководстве ОЭСР упоминается, что использование данных должно быть ограничено выполнением целей, указанных на момент сбора данных, или других целей, которые не являются несовместимыми с этими целями.

Таблица 5
Ограничения, определяющие принцип пропорциональности

	Модернизированная Конвенция Совета Европы о защите частных лиц в отношении обработки данных личного характера	*Руководящие принципы регламентации компьютеризованных картотек, содержащих данные личного характера, Организации Объединенных Наций*	*Стандарты защиты персональных данных Иберо-американской сети по защите данных*	*Общий регламент Европейского союза по защите данных*	*Руководство по защите неприкосновенности частной жизни и трансграничной передаче персональных данных ОЭСР*	*Рамочная основа неприкосновенности частной жизни АТЭС*	*Обновленные принципы ОАГ по неприкосновенности частной жизни и защите персональных данных, с аннотациями*
	Статья	*Статья*	*Статья*	*Статья*	*Пункт*	*Принцип*	*Принцип*
Соответствие цели	5.4 c)		18.1	5.1 c)			3
Актуальность по отношению к цели	5.4 c)						
Релевантность по отношению к цели		3.a)	18.1	5.1 c)			3
Ограниченность и не чрезмерность по отношению к цели	5.4 c)		18.1	5.1 c)	9	24	3

88. Анализируемый принцип буквально отражен в ряде международных нормативных документов, в которых прямо упоминаются «персональные данные», например в Иберо-американских стандартах, Рамочной основе неприкосновенности частной жизни АТЭС, Общем регламенте и Руководящих принципах Организации Объединенных Наций; в других, например в Руководстве ОЭСР, упоминается «обработка» таких данных; в иных, например в модернизированной Конвенции 108 и Принципах ОАГ, упоминаются как персональные данные, так и обработка, которой они будут подвергаться.

89. Несмотря на вышесказанное и с учетом полных текстов международных нормативных документов, в целом принцип пропорциональности должен

соблюдаться как в отношении собираемых персональных данных, так и в отношении действий по обработке, которым они будут подвергнуты, а именно: в обоих случаях данные должны быть соответствующими, актуальными, релевантными и ограниченными законными целями, для которых они были собраны.

Принцип минимизации

90. Минимизация — это принцип, согласно которому данные всегда должны быть ограничены тем, что необходимо для достижения установленной цели.

91. В этом смысле данный принцип тесно связан с принципом цели, который служит параметром для ограничения объема обрабатываемых данных.

92. Общий регламент является единственным документом, в котором принцип минимизации регулируется в конкретной форме; в его статье 5.1 c) указано, что персональные данные должны быть соответствующими и релевантными и ограничиваться тем, что необходимо в связи с целями, для которых они обрабатываются. В других проанализированных документах[25] содержание этого принципа охвачено в рамках принципа пропорциональности или какого-либо другого принципа.

93. Принцип минимизации также связан с определенными обязательствами, которые Общий регламент устанавливает для контролера и обработчика, такими как неприкосновенность частной жизни по замыслу и по умолчанию. Минимизация как превентивная мера помогает снизить риск нарушения безопасности и его влияние на базы данных.

94. Как указано в статье 25.2 Общего регламента, «контролер должен принимать соответствующие технические и организационные меры для обеспечения того, чтобы по умолчанию обрабатывались только те персональные данные, которые необходимы для каждой конкретной цели обработки; это обязательство распространяется на объем собранных персональных данных, степень их обработки, срок их хранения и их доступность».

95. Принцип минимизации должен соблюдаться особенно тщательно с учетом все более частого использования информационно-коммуникационных технологий для обработки персональных данных.

Принцип качества

96. Принцип качества подразумевает, что данные должны быть достоверными, точными, полными и обновленными, что обязывает контролеров принимать для обеспечения этого соответствующие меры. В некоторых международных нормативных документах этот принцип также упоминается как принцип точности[26] или целостности[27].

97. Как следует из таблицы 6 ниже, персональные данные должны быть достоверными, полными и точными на протяжении всего процесса обработки и должны обновляться по мере необходимости либо должностным лицом (контролером или обработчиком), либо по запросу субъекта данных.

---

[25] Статья 18 Иберо-американских стандартов; статья 3 Руководящих принципов Организации Объединенных Наций; статьи 5.1 и 5.4 c) модернизированной Конвенции 108; статья 24 Рамочной основы неприкосновенности частной жизни АТЭС; пункт 9 Руководства ОЭСР; принципы 3 и 4 Принципов ОАГ.

[26] Статья 2 Руководящих принципов Организации Объединенных Наций и принцип 7 Принципов ОАГ.

[27] Статья 27 Рамочной основы неприкосновенности частной жизни АТЭС.

Таблица 6
Характеристики качества данных

	Модернизированная Конвенция Совета Европы о защите частных лиц в отношении обработки данных личного характера	*Руководящие принципы регламентации компьютеризованных картотек, содержащих данные личного характера, Организации Объединенных Наций*	*Стандарты защиты персональных данных Иберо-американской сети по защите данных*	*Общий регламент Европейского союза по защите данных*	*Руководство по защите неприкосновенности частной жизни и трансграничной передаче персональных данных ОЭСР*	*Рамочная основа неприкосновенности частной жизни АТЭС*	*Обновленные принципы ОАГ по неприкосновенности частной жизни и защите персональных данных, с аннотациями*
	Статья (статьи)	*Статья (статьи)*	*Статья (статьи)*	*Статья (статьи)*	*Пункт*	*Принцип*	*Принцип*
Достоверность/точность	5.4 d)	2	19.1	5.1 d)	8	27	7
Обновленность	5.4 d)	2	19.1	5.1 d)	8	27	7
Полнота		2	19.1		8	27	7

98. В статье 5.4 d) модернизированной Конвенции 108 говорится о том, что данные должны быть точными и обновленными. В статье 2 Руководящих принципов Организации Объединенных Наций говорится об обязательстве проверять точность и соответствие данных, сохранять их максимальную полноту, чтобы избежать ошибок из-за пропусков, и периодически обновлять данные.

99. В пяти международных нормативных документах, упомянутых ниже, анализируемый принцип напрямую увязывается с принципом цели обработки.

100. Статьей 19 Иберо-американских стандартов контролеру вменяется в обязанность принятие «необходимых мер для поддержания точности и полноты и обновления персональных данных таким образом, чтобы достоверность данных не была изменена, как того требует достижение целей, послуживших основанием для их обработки».

101. В Общем регламенте указано, что персональные данные должны быть точными и при необходимости должны обновляться, а также что должны быть приняты все разумные меры для того, чтобы персональные данные, которые являются неточными в отношении целей обработки, были удалены или исправлены (ст. 5.1 d)).

102. В Руководстве ОЭСР (п. 8) и в Рамочной основе неприкосновенности частной жизни АТЭС (ст. 27) указано, что данные должны быть точными, полными и обновленными. Между тем в Принципах ОАГ в отношении принципа точности данных отмечается, что данные «должны всегда быть точными, полными и обновленными в той мере, в какой это необходимо для целей их обработки, причем это не должно сказываться на их достоверности» (принцип 7).

103. Качество обрабатываемой личной информации является жизненно важным для успешного достижения целей, послуживших основанием для ее сбора, а также для ее дальнейшей обработки. Обеспечение качества данных является признаком ответственности за достижение разрешенных целей.

104. Для надлежащего соблюдения принципа качества контролеры и обработчики должны внедрить в своих организациях меры, гарантирующие, что персональные данные, которые они собирают и обрабатывают, являются достоверными, точными, полными или целостными и обновленными, с тем чтобы разрешенные цели достигались при должном соблюдении прав субъектов личной информации, что должно быть в их интересах. Вышеуказанное должно выполняться независимо от шагов, которые субъект данных решит предпринять в

целях обеспечения качества касающейся его информации при ее обработке другим лицом.

Принцип ответственности

105. Принцип ответственности можно проанализировать с двух точек зрения: с одной стороны, контролеры и обработчики данных должны внедрить механизмы для соблюдения принципов защиты данных и неприкосновенности частной жизни, обеспечивая и гарантируя права и свободы субъектов данных; с другой стороны, контролеры и обработчики данных должны быть в состоянии гарантировать и продемонстрировать соблюдение этих принципов.

106. Проанализировав международные нормативные документы, мы обнаружили, что этот принцип закреплен в статье 20 Иберо-американских стандартов, в соответствии с которой контролер должен внедрить все необходимые механизмы для соблюдения принципов и обязательств, изложенных в Стандартах, и несет ответственность за обработку персональных данных перед субъектом данных и надзорным органом. Для этого могут использоваться стандарты, национальная или международная передовая практика, схемы саморегулирования, системы сертификации или любой другой механизм, который контролер сочтет подходящим для этих целей. Вышеуказанное актуально также в случаях, когда данными занимается обработчик, и при передаче данных.

107. В статье 20.3 Иберо-американских стандартов приводятся примеры механизмов, которые контролер может использовать для соблюдения принципа ответственности; их следует постоянно анализировать и оценивать в целях определения их эффективности с точки зрения соответствия применимому национальному законодательству.

108. В Общем регламенте этот принцип фигурирует под термином проактивной ответственности (ст. 5.2). Его можно определить как необходимость или обязанность контролера принимать соответствующие технические и организационные меры, чтобы гарантировать и продемонстрировать, что обработка персональных данных соответствует Регламенту (ст. 24), в частности принципам правомерности, добросовестности и транспарентности; ограничения цели; минимизации данных; точности; ограничения срока хранения; целостности и конфиденциальности (ст. 5.1). Для этого контролер должен установить процедуры, с помощью которых можно обеспечить применение норм и продемонстрировать их эффективное применение и осуществление третьим лицам (ст. 5.2).

109. Общим регламентом устанавливается ряд мер по обеспечению соблюдения этого принципа, в том числе: внедрение защиты данных по замыслу и по умолчанию (ст. 25); ведение реестра действий по обработке (ст. 30); принятие мер безопасности (ст. 32); направление уведомлений о нарушениях безопасности в надзорный орган и субъектам данных (ст. 33 и 34); проведение оценки воздействия на защиту данных (ст. 35) и назначение сотрудника, ответственного за защиту данных (ст. 37).

110. Из вышеупомянутых мер одна, а именно оценка воздействия на защиту данных, включенная в Общий регламент, является обязательной (ст. 35, пункты 1, 3 и 4), когда обработка влечет за собой высокий риск для свобод и прав субъектов информации[28]; это особенно актуально при внедрении новых технологий обработки данных физических лиц.

[28] Статья 35 Общего регламента: «3. Оценка воздействия на защиту данных, упомянутая в пункте 1, требуется, в частности, в случае:
а) систематической и всесторонней оценки персональных аспектов физических лиц,

111. Указанная оценка должна быть проведена контролером до обработки персональных данных, чтобы помочь в принятии соответствующих решений и обеспечить защиту данных по замыслу и по умолчанию[29].

112. Принцип проактивной ответственности требует от организаций анализа того, какие данные они обрабатывают, для каких целей и какого рода операции по обработке они выполняют. Исходя из этой информации они должны четко определить, как они будут осуществлять меры, предусмотренные Общим регламентом, обеспечивая, чтобы эти меры и процедуры соответствовали требованиям по защите данных, и как они могут продемонстрировать это субъектам данных и надзорному органу. Этот принцип требует добросовестного, внимательного и активного отношения со стороны организаций ко всем выполняемым ими операциям по обработке персональных данных[30].

113. В том же ключе в Принципах ОАГ подчеркивается важность принятия, внедрения и демонстрации мер безопасности с акцентом на ответственности за безопасность персональных данных и за сообщение и передачу данных на международном уровне; при этом контролеры берут на себя задачу обеспечения постоянного уровня защиты в соответствии с принципами, изложенными в этом документе (принцип 10).

114. Руководство ОЭСР возлагает ответственность за соблюдение норм и решений по защите частной жизни на контролера, который должен действовать в соответствии с установленными принципами (ст. 14).

115. В Рамочной основе неприкосновенности частной жизни АТЭС при рассмотрении этого принципа основное внимание уделяется передаче данных (ст. 32). Таким образом, когда личная информация должна быть передана другому лицу или организации, как внутри страны, так и на международном уровне, контролеры должны получить согласие субъекта данных или, если согласие не получено, убедиться в том, что получатель будет защищать информацию последовательным образом, путем принятия разумных мер для обеспечения защиты информации после передачи в соответствии с принципами.

116. Модернизированная Конвенция 108 требует от контролеров или обработчиков принятия технических и организационных мер, учитывающих последствия права на защиту персональных данных на всех этапах обработки (ст. 10.1 и 10.3). В пояснительном докладе к Конвенции указаны определенные меры, которые может быть необходимо принять контролеру или обработчику, включая следующие: обучение сотрудников; установление надлежащих процедур уведомления; указание срока, в который данные должны быть удалены; установление конкретных договорных положений, делегирующих обработку данных в

которая основана на автоматизированной обработке, включая профилирование, и на основании которой принимаются решения, порождающие юридические последствия для физических лиц или существенно влияющие на них аналогичным образом; b) масштабной обработки специальных категорий данных, упомянутых в пункте 1 статьи 9, или упомянутых в статье 10 персональных данных, относящихся к судимостям и уголовным преступлениям; или c) масштабного систематического наблюдения за общедоступной территорией».

[29] Directrices sobre la evaluación de impacto relativa a la protección de datos y para determinar si el tratamiento “entraña probablemente un alto riesgo” a efectos del Reglamento (UE) 2016/679.WP.248. Abril 2017. Pág. 16.

[30] Agencia Española de Protección de Datos Personales, “¿Qué es el principio de responsabilidad proactiva?”, https://www.aepd.es/es/preguntas-frecuentes/2-rgpd/3-principios-relativos-al-tratamiento/FAQ-0208-que-es-el-prinipio-de-responsabilidad-proactiva.

целях обеспечения соблюдения Конвенции; установление внутренних процедур, позволяющих проверять и демонстрировать соблюдение Конвенции[31].

117. Наконец, следует отметить, что данный принцип конкретно предусмотрен всеми проанализированными международными нормативными документами, за исключением Руководящих принципов Организации Объединенных Наций, и только в Иберо-американских стандартах и Общем регламенте устанавливаются механизмы или меры, которые должны быть внедрены для обеспечения соблюдения этого принципа, как видно из таблицы 7 ниже.

Таблица 7
Принцип ответственности и механизмы обеспечения его соблюдения

	Модернизированная Конвенция Совета Европы о защите частных лиц в отношении обработки данных личного характера	*Руководящие принципы регламентации компьютеризованных картотек, содержащих данные личного характера, Организации Объединенных Наций*	*Стандарты защиты персональных данных Иберо-американской сети по защите данных*	*Общий регламент Европейского союза по защите данных*	*Руководство по защите неприкосновенности частной жизни и трансграничной передаче персональных данных ОЭСР*	*Рамочная основа неприкосновенности частной жизни АТЭС*	*Обновленные принципы ОАГ по неприкосновенности частной жизни и защите персональных данных, с аннотациями*
	Статья (статьи)	*Статья (статьи)*	*Статья (статьи)*	*Статья (статьи)*	*Пункт*	*Принцип*	*Принцип*
Конкретно предусмотрен принцип ответственности	10.1		20	5.2	14	32	10
Устанавливаются механизмы или меры, которые должны быть внедрены для обеспечения соблюдения этого принципа			20.3	5.1, 24, 25, 30, 32, 33, 34, 35 и 37			

118. По сути, принцип ответственности направлен на улучшение соблюдения принципов и всех нормативных актов по защите данных и неприкосновенности частной жизни, которые контролеры и обработчики обязаны соблюдать в ходе всех осуществляемых ими действий по обработке данных, и обеспечение наличия объективных элементов, на которых основано подлинное соблюдение принципа и достижение законных целей в атмосфере доверия и уважения к соответствующим основным правам.

Принцип безопасности

119. Безопасность имеет основополагающее значение для защиты данных; защита данных невозможна без безопасности.

120. Для соблюдения этого принципа необходимо выявить, оценить и задокументировать риски, которые могут возникнуть в течение жизненного цикла данных, чтобы принять необходимые меры безопасности и иметь возможность гарантировать конфиденциальность, целостность и доступность персональных данных, избегая материализации рисков.

121. Все проанализированные международные нормативные документы включают этот принцип в более или менее описательной форме, указывая на

[31] Traducción Núm. 058/2019. Informe Explicativo del Convenio, *Artículo 10, No. 85.* URL: https://rm.coe.int/informe-explicativo-de-convenio/1680968479.

необходимость принятия соответствующих, достаточных, своевременных, разумных или надлежащих мер безопасности для предотвращения различных видов рисков, таких как, в частности, несанкционированный доступ, потеря, изменение, уничтожение или раскрытие персональных данных[32].

122. В таблице 8 подробно описаны виды мер безопасности и рисков, указанные в каждом из международных нормативных документов. Также отмечается, в каких из них установлены руководящие принципы для определения мер и обязанность уведомлять о нарушениях безопасности.

Таблица 8
Принцип безопасности

	Модернизированная Конвенция Совета Европы о защите частных лиц в отношении обработки данных личного характера	*Руководящие принципы регламентации компьютеризованных картотек, содержащих данные личного характера, Организации Объединенных Наций*	*Стандарты защиты персональных данных Иберо-американской сети по защите данных*	*Общий регламент Европейского союза по защите данных*	*Руководство по защите неприкосновенности частной жизни и трансграничной передаче персональных данных ОЭСР*	*Рамочная основа неприкосновенности частной жизни АТЭС*	*Обновленные принципы ОАГ по неприкосновенности частной жизни и защите персональных данных, с аннотациями*
Вид мер безопасности	Соответствующие меры безопасности Ст. 7.1	Соответствующие меры Ст. 7	Достаточные административные, физические и технические меры Ст. 21.1	Соответствующие технические и организационные меры Ст. 5.1 f)	Разумные меры безопасности п. 11	Соответствующие меры Ст. 28	Разумные и надлежащие технические, административные или организационные гарантии безопасности Принцип 6
Вид риска	Такие риски, как случайный или несанкционированный доступ, уничтожение, потеря, использование, изменение или раскрытие персональных данных Ст. 7.1	Естественные риски, такие как случайная потеря или уничтожение в результате стихийного бедствия, и связанные с деятельностью человека риски, такие как несанкционированный доступ, противозаконное использование данных или заражение компьютерным вирусом Ст. 7	Повреждение, потеря, изменение, уничтожение, доступность и вообще любое незаконное или несанкционированное использование персональных данных Ст. 22.1	Несанкционированная или незаконная обработка, а также случайная потеря, уничтожение или повреждение Ст. 5.1 f)	Такие риски, как потеря или несанкционированный доступ, уничтожение, использование, изменение или раскрытие данных п. 11	Потеря или несанкционированный доступ; уничтожение, использование, изменение или несанкционированное раскрытие; или иное неправомерное использование Ст. 28	Несанкционированная или незаконная обработка, включая доступ, потерю, уничтожение, повреждение или раскрытие, даже если это произошло в результате случайности Принцип 6

[32] Вся эта информация отражена в представленной в данном разделе таблице, где показаны виды мер безопасности и рисков, содержащиеся в упомянутых там статьях (статья 7.1 модернизированной Конвенции 108; статья 7 Руководящих принципов Организации Объединенных Наций; статья 21.1 Иберо-американских стандартов; статья 5.1 f) Общего регламента; пункт 11 Руководства ОЭСР; статья 28 Рамочной основы неприкосновенности частной жизни АТЭС; принцип 6 Принципов ОАГ).

	Модернизированная Конвенция Совета Европы о защите частных лиц в отношении обработки данных личного характера	*Руководящие принципы регламентации компьютеризованных картотек, содержащих данные личного характера, Организации Объединенных Наций*	*Стандарты защиты персональных данных Иберо-американской сети по защите данных*	*Общий регламент Европейского союза по защите данных*	*Руководство по защите неприкосновенности частной жизни и трансграничной передаче персональных данных ОЭСР*	*Рамочная основа неприкосновенности частной жизни АТЭС*	*Обновленные принципы ОАГ по неприкосновенности частной жизни и защите персональных данных, с аннотациями*
Руководящие принципы для определения мер			Ст. 21.2	Ст. 32		Ст. 28	
Уведомление надзорного органа о нарушениях безопасности	Ст. 7.2		Ст. 22	Ст. 33	п. 15 c)	Ст. 54	
Уведомление затронутых субъектов данных о нарушениях безопасности			Ст. 22	Ст. 34	п. 15 c)	Ст. 54	

123. Меры безопасности должны быть пропорциональны величине риска, должны периодически пересматриваться и обновляться, а также могут подвергаться проверке в целях их улучшения и предотвращения их устаревания[33].

124. В Принципах ОАГ установлено, что данные меры безопасности должны постоянно проверяться и обновляться (принцип 6), а в Иберо-американских стандартах указано, что контролер должен периодически выполнять действия по обеспечению мониторинга, пересмотра, поддержки и постоянного улучшения мер безопасности, применимых к обработке персональных данных (ст. 21.3). Вместе с тем в Рамочной основе неприкосновенности частной жизни АТЭС упоминается, что меры безопасности должны подвергаться периодическому пересмотру и переоценке (ст. 28).

125. Некоторыми международными нормативными документами, например модернизированной Конвенцией 108 (ст. 7.2), Иберо-американскими стандартами (ст. 22), Общим регламентом (ст. 33), Руководством ОЭСР (п. 15 c)) и Рамочной основой неприкосновенности частной жизни АТЭС (ст. 54), предусмотрена обязанность уведомлять надзорный орган о нарушениях безопасности. Кроме того, эти международные нормативные документы, за исключением модернизированной Конвенции 108, также устанавливают обязанность сообщать о нарушениях безопасности затронутым субъектам данных.

126. Следует подчеркнуть важность уведомления надзорных органов или, в зависимости от обстоятельств, затронутых субъектов данных. С одной стороны, это позволяет таким органам проследить за тем, чтобы в случае нарушения безопасности были приняты соответствующие меры и чтобы нарушение было локализовано в кратчайшие возможные сроки; с другой стороны, это гарантирует, что субъекты данных, затронутые нарушением безопасности, будут осведомлены о произошедшем нарушении и о возможном последующем ущербе.

127. Испанское агентство по защите данных отмечает, что упомянутый в Общем регламенте принцип безопасности «налагает на лиц, обрабатывающих данные,

[33] Принцип 6 Принципов ОАГ.

обязанность анализа рисков, направленного на определение технических и организационных мер, необходимых для гарантии целостности, доступности и конфиденциальности обрабатываемых ими персональных данных[34]».

128. Иберо-американскими стандартами защиты (ст. 21.2), Общим регламентом (ст. 32) и Рамочной основой неприкосновенности частной жизни АТЭС (ст. 28) устанавливаются руководящие принципы или факторы для определения мер безопасности, которые должны быть приняты, о чем говорится ниже, но ни одним из них не устанавливается, какие конкретные меры должны быть приняты, поскольку эти меры было бы невозможно определить таким образом, чтобы они не устаревали.

129. В Общем регламенте указано, что при определении соответствующих мер по обеспечению уровня безопасности сообразно риску контролер и обработчик должны учитывать следующие факторы: «состояние техники, затраты на реализацию, характер, объем, контекст и цели обработки, а также риски различной вероятности и серьезности для прав и свобод физических лиц» (ст. 32).

130. В Иберо-американских стандартах также учитываются эти факторы и добавляются следующие: «осуществляемая или предполагаемая международная передача данных», «число субъектов данных», «возможные последствия нарушения для субъектов данных и предыдущие нарушения» (ст. 21.2).

131. В Рамочной основе неприкосновенности частной жизни АТЭС упоминается, что меры безопасности должны быть пропорциональны вероятности и серьезности ущерба, который может быть нанесен, степени конфиденциальности информации и условиям, на которых она хранится (ст. 28). В отличие от других международных нормативных документов, в ней обязанность устанавливать и поддерживать меры безопасности, принимая во внимание вышеупомянутые факторы, возлагается только на контролера, а не на обработчика данных.

132. В Принципах ОАГ принцип безопасности сформулирован не так, как указано выше. Вместе с тем в них указано, что «меры, принимаемые для защиты персональных данных, должны выбираться с учетом, среди прочих факторов: i) потенциального воздействия на права субъектов данных, в частности потенциальной ценности данных для третьей стороны, не уполномоченной на их обработку; ii) затрат на их осуществление; iii) целей обработки; iv) характера обрабатываемых персональных данных, в частности конфиденциальных данных» (принцип 6, с аннотациями).

133. Из проанализированных международных нормативных документов только в Общем регламенте приводятся примеры технических и организационных мер для обеспечения уровня безопасности, соответствующего риску, а именно: «a) псевдонимизация и шифрование персональных данных; b) способность обеспечить постоянную конфиденциальность, целостность, доступность и устойчивость систем и услуг по обработке данных; c) возможность быстрого восстановления доступности и доступа к персональным данным в случае физического или технического инцидента; d) процесс регулярной проверки, оценки и анализа эффективности технических и организационных мер по обеспечению безопасности обработки» (ст. 32.1).

134. Кроме того, в статье 32.3 Общего регламента указано, что для демонстрации соответствия этим требованиям может использоваться соблюдение кодекса поведения или внедрение механизма сертификации.

[34] Agencia Española de Protección de Datos, “Principios”, 25 de noviembre de 2021, https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/principios.

135. Все контролеры и обработчики должны принимать меры для обеспечения безопасности и защиты персональных данных от таких рисков, как несанкционированный доступ, потеря, изменение, уничтожение, раскрытие или повреждение. Если такие меры безопасности не принимаются, личная информация становится уязвимой для вышеупомянутых рисков, что может привести к серьезному ущербу для прав субъектов данных. Поэтому во всех проанализированных международных нормативных документах рассматривается необходимость установления различных видов мер в отношении рисков, которые могут возникнуть; в некоторых случаях в них приводятся руководящие принципы для определения надлежащих мер безопасности, хотя и без указания конкретных мер, которые должны быть приняты, поскольку невозможно обновлять документы с такой частотой, чтобы они отражали развитие технологий и возможные нарушения.

136. Многообразие технологий, а также их динамичная трансформация, увеличивающая возможности сбора и обработки данных, должны приниматься во внимание для обеспечения ответственной и этичной оценки рисков и надлежащих мер безопасности контролерами данных в контексте их законных полномочий как таковых, а также неоспоримой необходимости сохранения должной конфиденциальности персональных данных, обрабатываемых под их ответственность.

137. Обеспечение целостности, доступности и конфиденциальности персональных данных является первостепенной задачей и обязанностью контролеров и обработчиков данных, позволяющей избежать серьезных нарушений прав субъектов данных; вместе с тем нарушения, если они происходят, должны оказывать как можно меньшее влияние на права субъектов данных; также должны быть установлены руководящие принципы, которым необходимо следовать в случае нарушений, например обязательное уведомление надзорного органа и затронутых субъектов прав.

III. Выводы

138. Руководящие принципы в отношении неприкосновенности частной жизни и защиты персональных данных представляют собой структурную часть правовых систем в этой области. Они являются руководством для толкования и помогают заполнить пробелы в законодательстве. Они обязывают контролеров и обработчиков действовать надлежащим образом при обработке персональных данных.

139. Законность должна быть основой всех действий по обработке на протяжении всего жизненного цикла персональных данных, и для ее обеспечения требуется наличие ряда законных оснований, установленных действующими нормативными актами.

140. Принцип согласия тесно связан с законностью, поскольку он является наиболее распространенным, признанным на международном уровне допустимым основанием для обработки персональных данных.

141. Принцип транспарентности должен соблюдаться независимо от правового основания для обработки.

142. Принцип цели закреплен во всех проанализированных нормативных документах. Цель должна быть явной, конкретной, законной и релевантной. Она будет ограничивать деятельность по обработке, которой будут подвергаться персональные данные.

143. Принцип добросовестности требует, чтобы личная информация обрабатывалась в точном соответствии со всеми условиями, послужившими основанием для ее сбора, и с использованием средств обработки, способствующих достижению цели.

144. В силу принципа пропорциональности персональные данные, а также действия по их обработке должны быть ограничены исключительно достижением законных целей, для которых они были собраны.

145. Качество обрабатываемой личной информации является жизненно важным для успешного достижения целей, послуживших основанием для ее сбора, а также для ее дальнейшей обработки.

146. Принцип ответственности направлен на улучшение соблюдения обязательных принципов и нормативных актов и обеспечение наличия объективных элементов, на которых основано подлинное соблюдение принципа и достижение законных целей в атмосфере доверия и уважения к соответствующим основным правам.

147. Без безопасности не будет ни защиты данных, ни неприкосновенности частной жизни. Обеспечение целостности, доступности и конфиденциальности персональных данных является первостепенной задачей и предполагает большую ответственность. Для обеспечения ответственной и этичной оценки рисков и надлежащих мер безопасности необходимо принимать во внимание многообразие технологий, а также их динамичную трансформацию.

148. Существует много общего в том, как в международных нормативных документах рассматриваются принципы неприкосновенности частной жизни и защиты персональных данных.

149. Выявленные общие элементы могут служить основой для продвижения к глобальному консенсусу, который позволит согласованно и надлежащим образом решать различные проблемы, возникающие при обработке данных, касающихся отдельных лиц, в частности в области международной передачи данных, использования информационно-коммуникационных технологий и искусственного интеллекта; права человека заслуживают равного уважения как в виртуальной, так и в физической среде.

150. Необходимо продолжать добиваться баланса между различными интересами, связанными с обработкой персональных данных в нынешнюю глобальную и цифровую эпоху, стремясь к сотрудничеству и согласованию норм регулирования.