ПРАВО

Ключевые международные договоры и региональные подходы к вопросу защиты персональных данных

Абрамова Анна Г.
Аспирант Российско-Армянского университета
Глава юридического департамента в ООО «АСК-Консалт» (Ереван, РА)
ORCID iD: 0009-0005-9237-5620
anna.yakhshibekian@gmail.com

УДК: 341; **EDN:** EAQUQW;
DOI: 10.58587/18292437-2023.6-43
Ключевые слова: персональные данные, GDPR, АСЕАН, АТЭС, конвенция, интернет, Европейский Союз, киберугроза, киберпреступность, Будапештская Конвенция

Հիմնական միջազգային պայմանագրեր և տարածաշրջանային մոտեցումներ անձնական տվյալների պաշտպանության հարցում

Աբրամովա Աննա Գ.
Հայ-Ռուսական Համալսարանի ասպիրանտ
Իրավաբանական վարչության ղեկավար «ԱՍԿ-Կոնսալտ» ՍՊԸ (Երևան, ՀՀ)

Ամփոփագիր՝ Այս հոդվածը խորապես ուսումնասիրում է անձնական տվյալների պաշտպանության միջազգային իրավական դաշտը, այս հարցի վերաբերյալ տարածաշրջանային օրենսդրական մոտեցումները, տարբեր տարածաշրջաններում տվյալների պաշտպանությունը կարգավորող օրենքները, ինչպես նաև ընդգծում է դրանց նշանակությունը և որոշակի իրավական բացերը: Հեղինակը լուսաբանում է հիմնական աղբյուրները, ինչպիսիք են GDPR-ը, APEC-ի գաղտնիության շրջանակը և անձնական տվյալների պաշտպանության ASEAN-ի շրջանակը: Բացի այդ, հոդվածը ներկայացնում է անձնական տվյալների խախտման դեպք, որը տեղի է ունեցել այս միջազգային պայմանագրերի և կոնվենցիաների համատեքստում:
Հանգուցաբառեր՝ անձնական տվյալներ, GDPR, ASEAN, APEC, կոնվենցիա, ինտերնետ, Եվրամիություն, կիբեր սպառնալիք, կիբերհանցագործություն, Բուդապեշտի կոնվենցիա

Key international treaties and regional approaches to the issue of personal data protection

Abramova Anna G.
PhD student at Russian-Armenian University
Head of Legal Department at "ASK-Consult" LLC (Yerevan, RA)

Abstract: This article conducts an in-depth exploration of the international legal framework for personal data protection, regional legislative approaches to this matter, laws governing data protection in different regions, as well as underscores their significance and certain legal gaps. The author illuminates key sources, such as the GDPR, the APEC Privacy Framework, and the ASEAN Framework on Personal Data Protection. Additionally, the article presents a case of a personal data breach incident that occurred within the context of these international treaties and conventions.
Keywords: personal data, GDPR, ASEAN, APEC, convention, Internet, European Union, cyber threat, cyber crime, Budapest Convention

Введение

В эпоху цифровых технологий Интернет занимает центральное место в повседневной жизни всех людей, меняя способы нашего общения, обмена информацией и ведения предпринимательской деятельности / бизнеса.

Однако, удобство онлайн-мира сопряжено с проблемами, связанными с защитой личных данных, которые беспрепятственно передаются через сеть интернет. Обеспечение конфиденциальности и безопасности личных данных стало глобальной проблемой, что привело к созданию и разработке международных договоров, а также региональных документов направленных на защиту персональных данных.

В данной статье рассматриваются международные правовые основы, регулирующие защиту персональных данных, и правовые подходы, принятые в конкретных регионах мира для решения этой проблемы. В статье подчеркиваются правовые пробелы и неоднозначности, присутствующие в рамках договоров и конвенций, а также рассматривается практический пример серьезной утечки данных, произошедшей в рамках действия этих международных договоров, что подчеркивает практические последствия этих правил.

Рассмотрим основные *три договора и конвенции* в сфере защиты персональных данных.

I. Конвенция 108 и ее модернизация

Конвенция о защите частных лиц при автоматической обработке персональных данных, известная как Конвенция 108, является одним из первых международных документов, посвященных защите данных. Он был принят Советом Европы в 1981 году, а затем модернизирован в 2018 году [**3**] с учетом проблем, возникающих в эпоху Интернета. Конвенция 108+ рассматривает такие принципы, как права субъектов данных, передача персональных данных и надзор за правомерным использованием данных. Данная конвенция представляет собой основополагающую веху в международном законодательстве о защите данных, подчеркивая важность прав субъектов данных и принципов справедливости, прозрачности и подотчетности.

II. Общий регламент защиты персональных данных (GDPR)

Вероятнее всего, самым влиятельным международным регламентом по защите данных является Общий регламент по защите персональных данных (GDPR), который вступил с силу в Европейском Союзе в 2018 году [**9**]. GDPR имеет экстерриториальное применение [**9**, recital 115] и затрагивает организации по всему миру, которые обрабатывают персональные данные граждан ЕС. Он устанавливает строгие требования к защите данных, включая согласие, переносимость данных и право быть забытым (на забвение) [**9**, art. 17(2)]. GDPR представляет собой веху в защите данных, подчеркивая принципы минимизации обрабатываемых данных, ограничения целей и внесение должной подотчетности [**9**, recital 156]. Он устанавливает высокие стандарты защиты персональных данных граждан стран ЕС во всем мире и предусматривает значительные штрафы за их несоблюдение.

III. Конвенция о киберпреступности (Будапештская конвенция)

Будапештская конвенция, принятая в 2001 году, уделяет основное внимание киберпреступности, но включает положения, касающиеся защиты персональных данных в контексте расследований киберпреступлений. В этом договоре особое внимание уделяется международному сотрудничеству в борьбе с киберугрозами и защите персональных данных во время трансграничных расследований [**4**]. Это подчеркивает необходимость международного сотрудничества в борьбе с киберпреступностью, признавая важность защиты данных даже в контексте уголовных расследований.

Региональные подходы к защите персональных данных.

1) Европейский Союз – GDPR

Европейский Союз посредством GDPR установил глобальный стандарт защиты данных. Как мы уже указали выше, этот нормативный акт не только обеспечивает комплексную защиту личных данных, но также влияет на предприятия и организации по всему миру. Он ввел гармонизированную систему защиты данных в ЕС, включая строгие правила уведомления об утечке данных, оценки воздействия на защиту данных и трансграничной передачи данных. GDPR не только подчеркивает принципы защиты данных, но также требует от контролеров и обработчиков данных демонстрировать соответствие, возлагая на организации ответственность за данные, которые они обрабатывают [**9**, art. 44].

2) Рамочное соглашение Азиатско-Тихоокеанского экономического сотрудничества (АТЭС) [**1**]

Рамочная соглашение АТЭС – это необязательный гибкий инструмент, направленный на усиление защиты персональных данных в странах-членах сообщества. Основное внимание уделяется обеспечению совместимости режимов защиты данных в Азиатско-Тихоокеанском регионе. Хотя Рамочное соглашение по защите конфиденциальности АТЭС не имеет обязательной юридической силы, она поощряет страны-участницы внедрять принципы конфиденциальности и механизмы сотрудничества. Это подчеркивает важность сотрудничества и последовательности в защите данных в Азиатско-Тихоокеанском регионе, признавая экономическую и социальную значимость потоков данных.

3) Рамочное соглашение Ассоциации государств Юго-Восточной Азии (ASEAN) по защите персональных данных

ASEAN также признала важность защиты персональных данных, приняв Рамочное соглашение ASEAN по защите персональных данных. Эта структура, призванная согласовать усилия по защите данных государств-членов ASEAN, направлена на облегчение трансграничных потоков данных при одновременной защите личных данных. Основное внимание уделяется таким ключевым принципам, как согласие, достоверность персональных данных, ограничение целей и подотчетность [**2**, с. 3]. Рамочное соглашение ASEAN представляет собой совместную попытку обеспечить единообразие стандартов защиты данных во всех государствах-членах, обеспечивая при этом свободный поток данных.

Сравнение ключевых международных договоров и региональных подходов выявляет как общие черты, так и различия. Несмотря на то, что за последнее время имел место заметный прогресс с сфере защиты данных, в частности,

GDPR устанавил высокие стандарты защиты данных, а региональные структуры, такие как АТЭС и ASEAN, обеспечили гибкость и сотрудничество, правовые пробелы и неясности, тем не менее, сохранились, включая согласование региональных и международных стандартов, решение проблемы трансграничной передачи данных и обеспечение эффективного правоприменения.

Сравнительный анализ ***подчеркивает*** различные подходы к защите данных.

- В то время как GDPR характеризуется своим всеобъемлющим и предписывающим характером, что делает его одним из самых строгих и подробных регламентов в мире, Конвенция 108 и Будапештская конвенция используют более принципиальный подход. Они устанавливают общие принципы и ориентиры, оставляя более широкий простор для национальных правительств и организаций для адаптации и применения согласно своим особенностям. Это более гибкий подход, который позволяет странам-участницам более полно учитывать свои уникальные потребности и условия. Такое разнообразие поднимает вопросы о совместимости и гармонизации стандартов защиты данных, особенно в глобализированной цифровой среде.
- Проблемы в согласовании региональных и международных стандартов могут усложнить работу транснациональных организаций, работающих в разных регионах. Экстерриториальное действие GDPR, например, вынуждает многие организации соблюдать строгие требования регламента, даже если они базируются не в ЕС. *Релевантный случай, который подчеркивает практические последствия нарушения данных международных соглашений, - это инцидент с утечкой данных Equifax, произошедший в 2017 году. Несмотря на то, что Equifax - это американская кредитная агентство, оно подпадает под экстратерриториальное воздействие GDPR из-за обработки персональных данных граждан Европейского союза. В результате этой утечки была раскрыта личная информация почти 147 миллионов человек, и возникли сложные вопросы о передаче данных через границы, обязательствах и механизмах обеспечения соблюдения законодательства* [**5**]. *Этот инцидент подчеркивает необходимость беспрепятственной координации между международными договорами по защите данных, особенно в случаях, связанных с многонациональными организациями.*
- Трансграничная передача данных остается центральной проблемой в международной сфере защиты данных. Организациям приходится решать сложности передачи данных в глобально связанном мире. Международные договоры и региональные соглашения стремятся решить эти проблемы, но практические решения и усилия по гармонизации все еще находятся на стадии разработки. *Практичный пример, который иллюстрирует сложности трансграничной передачи данных и усилия по их решению, можно найти в контексте Европейского Союза и Соединенных Штатов.*

Когда Соединенные Штаты и Европейский Союз пересматривали свои соглашения о передаче данных, такие как "Щит конфиденциальности" (Privacy Shield) [**8**]*, возникли вопросы о том, как обеспечивать адекватную защиту данных европейских граждан, когда их данные передаются в Соединенные Штаты.*

Суд Европейского Союза в своем решении в 2020 году признал, что Privacy Shield не обеспечивает достаточной гарантии защиты данных европейских граждан в Соединенных Штатах [**7**]. *Это решение возникло из-за опасений относительно массовой сборки данных и недостаточных механизмов защиты субъектов данных от доступа органов государственной безопасности в Соединенных Штатах.*

Это практический пример того, как проблемы трансграничной передачи данных могут стать источником непонимания и недовольства субъектов данных и регулирующих органов. Этот случай показывает, что, несмотря на усилия по заключению международных соглашений, реализация их положений и гармонизация стандартов по-прежнему вызывают сложности и требуют постоянной коррекции и согласования.

- Эффективность механизмов правоприменения и регулирующих органов также различается, что влияет на соблюдение законов о защите данных. Хотя GDPR предусматривает значительные штрафы за несоблюдение требований, в некоторых региональных структурах отсутствуют карательные меры такого же уровня, что приводит к расхождениям в последствиях утечки данных и нарушений конфиденциальности в зависимости от стран и регионов.

Заключение

Основываясь на анализе, представленном выше, международно-правовое регулирование защиты персональных данных в эпоху Интернета является динамичной и развивающейся сферой. Ключевые договоры и конвенции, которые были рассмотрены в данной статье, обеспечивают прочную основу, но тем не менее данная сфера нуждается в постоянном

развитии и углублении. В многосторонних международных договорах подчеркиваются принципы прав субъектов данных, подотчетности и важность международного сотрудничества в защите данных.

Региональные подходы, в том числе Рамочное соглашение АТЭС по конфиденциальности и Рамочное соглашение ASEAN по защите персональных данных, обеспечивают гибкость и сотрудничество, отражая конкретные потребности и проблемы соответствующих регионов. Эти подходы отдают приоритет функциональной совместимости и согласованности стандартов защиты данных, признавая экономическую и социальную значимость потоков данных.

В заключение отметим, что защита персональных данных является глобальной проблемой, которая требует международного сотрудничества и региональной адаптации. Понимание взаимодействия между ключевыми договорами и региональными подходами имеет жизненно важное значение для достижения гармонизированного, но гибкого подхода к защите персональных данных в эпоху Интернета. Баланс интересов отдельных лиц, организаций и правительств в цифровом мире требует постоянного диалога и сотрудничества, чтобы гарантировать, что законы о защите данных остаются эффективными и актуальными.

Также, необходимо отметить, что международно-правовое регулирование защиты персональных данных в эпоху Интернета является динамичной и развивающейся сферой. Ключевые договоры и конвенции, такие как Конвенция 108 и GDPR, обеспечивают прочную основу, а региональные подходы ЕС, АТЭС и ASEAN адаптируют защиту данных к конкретным региональным потребностям. Детальное понимание этих инструментов и их последствий имеет решающее значение в цифровую эпоху, когда потоки данных пересекают границы, поэтому крайне важно найти баланс между личной конфиденциальностью и глобальным обменом данными. Новые технологии, такие как искусственный интеллект, блокчейн и биометрия, раздвигают границы традиционных законов о защите данных, что требует своевременного внесения поправок в существующие рамки.

Список использованной литературы:

1. APEC, Privacy Framework, 2005, APEC Secretariat // https://u.to/2uIVIA//
2. ASEAN Framework on personal data protection, 2016 // https://asean.org/wp-content/uploads/2012/05/10-ASEAN-Framework-on-PDP.pdf
3. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data // web: https://rm.coe.int/1680078b37
4. Convention on Cybercrime // https://rm.coe.int/1680081561
5. *Data Protection Agency (AEPD) v. EQUIFAX IBÉRICA,* S.L., decision in proceeding PS/00240/2019 // https://www.aepd.es/documento/ps-00240-2019.pdf
6. *Data Protection Comissioner v. Facebook Ireland ltd., Maximillian Schrems and other intervening parties [2020]*, Judgment of the Court (grand chamber) // https://u.to/WegVIA
7. EU-U.S. Privacy Shield Framework Principles, 2016 // https://u.to/1eUVIA
8. Fred H. Cate, Privacy in the Information Age 101-32, (1997)
9. Regulation (EU) 2016/679, General Data Protection Regulation // web: https://gdpr-info.eu/

Сдана/Հանձնվել է՝ 10.11.2023
Рецензирована/Գրախոսվել է՝ 01.12.2023
Принята/Ընդունվել է՝ 07.12.2023