

ӘЛ-ФАРАБИ АТЫНДАҒЫ ҚАЗАҚ ҰЛТТЫҚ УНИВЕРСИТЕТІ  
КАЗАХСКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ ИМЕНИ АЛЬ-ФАРАБИ  
AL-FARABI KAZAKH NATIONAL UNIVERSITY

---

ХАЛЫҚАРАЛЫҚ ҚАТЫНАСТАР ФАКУЛЬТЕТІ  
ФАКУЛЬТЕТ МЕЖДУНАРОДНЫХ ОТНОШЕНИЙ  
FACULTY OF INTERNATIONAL RELATIONS

## «ФАРАБИ ӘЛЕМІ»

атты студенттер мен жас ғалымдардың  
халықаралық ғылыми конференция  
МАТЕРИАЛДАРЫ

*Алматы, Қазақстан, 6-8 сәуір 2023 жыл*

МАТЕРИАЛЫ  
международной научной конференции  
студентов и молодых ученых

## «ФАРАБИ ӘЛЕМІ»

*Алматы, Казахстан, 6-8 апреля 2023 года*

MATERIALS  
Of International Scientific Conference  
Of Students and Young Scientists

## «FARABI ALEMI»

*Almaty, Kazakhstan, April 6-8, 2023*

Алматы  
«Қазақ университеті»  
2023

**Бас редактор**

доктор Ph.D., ассоциированного профессора Жекенова Д.К.

**Ответственный редактор:**

к.и.н., и.о. доцента Омарова У.А.

**Редколлегия:**

доктор Ph.D. Парпиева С.М., доктор Ph.D., и.о. доцента Ермекбаев А.А., доктор Ph.D., и.о. доцента Баймагамбетова З.М., к.филол.н., и.о. доцента Смагулова А.С., ст. преподаватель Байтукаева Д.У., ст. преподаватель Мадиева Д.Б.

«ФАРАБИ ӘЛЕМІ» атты студенттер мен жас ғалымдардың халықаралық ғылыми конференциясының материалдары. Алматы, Қазақстан, 6-8 сәуір, 2023 жыл. – Алматы: Қазақ университеті, 2023. – 611 б.

**ISBN978-601-04-6354-7**

Ғылыми басылымда студенттер мен жас ғалымдарға арналған халықаралық ғылыми конференция материалдары енгізілген.

Бұл жинақ ғылыми қызметкерлерге, оқытушыларға, студенттерге, магистранттар мен докторанттарға арналады.

а) Армения аумағында Еуразиялық экономикалық одақ органдарының, сондай-ақ ЕурАзЭҚ пен Кеден одағының бұрынғы органдарының актілерін қолдану міндеті;

ә) Армения аумағында Шарттың күшіне енгеннен кейін қабылданған Еуразиялық экономикалық комиссияның арнаулы және өзге де шараларды қолдану туралы шешімдерінің тікелеу қолданылуын қамтамасыз ету міндеті.

Осы конституциялық талаптарды ескере отырып, АР Конституциялық соты келесілерге көзі жетті:

а) 2014 жылғы Шарт бойынша Армения Республикасымен қабылданып жатқан міндеттемелердің АР Конституциясының конституциялық құрылыс негіздерінде бекітілген негіз қалаушы принциптеріне теңдей құндылығы;

ә) қабылдап жатқын міндеттемелердің үйлесімділігі, атап айтқанда, БҰҰ, Еуропа Кеңесі мен Дүниежүзілік сауда ұйымы шеңберінде орнатылған нормалар мен принциптерге сәйкестігі;

б) Одақ органдарының шешім қабылдау тәртібі мен олардың міндетті болуының сипаты;

в) Шарттан шығу процедураларының халықаралық құқық нормалары мен принциптеріне сәйкестігі.

Жоғарыда келтірілген жекелеген міндеттемелердің орындалуын қамтамасыз ету жағынан АР Конституциялық соты Арменияның қатысуы бар халықаралық органдар шешімдерінің орындалуын қамтамасыз етудің құқықтық шарттарын АР Ұлттық Жиыны реттеп қойған деген қорытынды жасады.

Сонымен қатар, АР Конституциялық соты АР «Халықаралық шарттары туралы» Заң толық көлемде әрекет ететінін белгіледі. Осымен бірге, АР Конституциялық соты Одаққа Армения мүшелігінің құқықтық кепілдіктерін күшейту жағынан бірқатар заңнамалық актілерге өзгерістер енгізу қажеттігін басып айтты. Осының негізінде жиырмаға жуық заңнамалық актілер тиісті өзгерістерге ұшырады.

Сонымен, ЕАЭО құқығының Армения Республикасында жүзеге асырылуы үшін барлық жағдай жасалған, соның ішінде, имплементацияның жалпы және арнайы тетіктері орнатылып қолданылуда.

### ***Пайдаланылған әдебиеттер тізімі:***

*Конституция Республики Армения от 5 июля 1995 года (с изменениями и дополнениями от 27 ноября 2005 года и 6 декабря 2015 года) [Электронный ресурс] - Режим доступа: <https://www.president.am/ru/constitution-2015/>*

*Закон Республика Армения «О международных договорах Республики Армения» от 22 февраля 2007 года [Электронный ресурс] - Режим доступа: <http://www.parliament.am/legislation.php?sel=show&ID=2953&lang=rus>*

*Бирюков П.Н. Имплементация права ЕАЭС в Республике Армения и РФ [Электронный ресурс] - Режим доступа: <http://www.law.vsu.ru/news/2019/docs/biryukov-2019-09-22.pdf>*

*Прогноз основных показателей экономического развития государств – членов ЕАЭС на 2020 – 2023 годы, Евразийская экономическая комиссия, 14 января 2021 г. [Электронный ресурс] - Режим доступа: [http://www.eurasiancommission.org/ru/act/integr\\_i\\_makroec/dep\\_makroec\\_pol/economyPrognoz/Pages/Sred\\_prog.asp](http://www.eurasiancommission.org/ru/act/integr_i_makroec/dep_makroec_pol/economyPrognoz/Pages/Sred_prog.asp)*

## **РАЗРЕШЕНИЕ ЮРИДИЧЕСКИХ ВОПРОСОВ, КАСАЮЩИХСЯ ПЕРСОНАЛЬНЫХ И НЕПЕРСОНАЛЬНЫХ ДАННЫХ В ОТНОШЕНИИ С GDPR**

***Бисалиев Марлен***

*Докторант 2-го курса специальности «Международное право»*

*Казахского национального университета им. аль-Фараби*

***Научный руководитель: д.ю.н., профессор Шакиров К.Н.***

## **Введение**

Стремительное развитие технологий привело к беспрецедентному росту сбора и обработки персональных данных. Эта тенденция приносит многочисленные проблемы и опасения по поводу конфиденциальности, защиты персональных данных и правовых последствий управления ими. Настоящая публикация направлена на всестороннее понимание вопросов, обусловленных применением персональных данных, и законов, связанных с их обращением. Правовые вопросы, затрагивающие личные и неличные категории данных, сложны, многогранны и имеют серьезные последствия с точки зрения конфиденциальности информации об отдельных лицах, а также защиты данных и соответствия меняющимся правилам.

Персональные данные, как это определено в Общем регламенте по их защите (General Data Protection Regulation - GDPR) [1], касаются любой информации, относящейся к идентифицированному или идентифицируемому физическому лицу, в то время как неперсональные данные относятся к информации, которую нельзя отследить до исследования данных физического лица. Различие между этими двумя типами данных имеет решающее значение, поскольку оно определяет объем и применимость законов о защите данных, а также обязанности контролеров и обработчиков данных.

Личные персональные данные — это информация, которая может быть использована для идентификации определенного индивида, например имя, фамилия, дата рождения, адрес электронной почты или номер телефона. Такие данные могут прямо или косвенно указывать на конкретного человека и могут быть использованы для его определения или контакта.

Неличные персональные данные — это информация, которая не связана с определенным индивидом и не может быть использована для его идентификации. Такие данные могут включать агрегированную статистику, анонимные данные или информацию, относящуюся к группе людей, но не к конкретному человеку. Неличные данные обычно используются для анализа трендов, исследования и статистики, но не для определения личности человека.

Идентифицируемые лица — это индивиды, которые могут быть определены с использованием личных данных. Это может включать их имена, номера телефонов, адреса электронной почты, идентификационные номера и другие уникальные идентификаторы, которые позволяют определить их личность.

Идентифицирующие лица — это организации или индивиды, которые собирают, обрабатывают или используют личные данные для определения личности идентифицируемых лиц. Это могут быть государственные органы, коммерческие организации или иные структуры, занимающиеся обработкой персональных данных и обязанные соблюдать законы о защите данных и конфиденциальности.

Проблемы с разграничением личных и неличных данных возникают в первую очередь из-за широкого определения «идентифицируемых» лиц в соответствии с GDPR и растущей сложности методов анализа данных, которые часто могут выявить личную информацию из, казалось бы, неличных данных. Эти проблемы привели к юридическим неясностям и сложностям, что потребовало более тонкого подхода к определению и обработке этих категорий данных.

Кроме того, обработка анонимизированных, псевдонимизированных и деидентифицированных данных добавляет еще один уровень сложности в правовую среду. Хотя эти методы направлены на то, чтобы скрыть личность людей в наборе данных, они все же могут быть подвержены рискам повторной идентификации, что еще больше стирает границы между личными и неличными данными. В результате юридические вопросы между личными и неличными персональными данными вращаются вокруг достижения тонкого баланса между защитой частной жизни, обеспечением соблюдения правил их защиты, что требует всестороннего понимания различий между личными и неличными данными и

принятия контекстно-зависимых основ и подходов, основанных на оценке возникающих при этом рисков.

### **Проблематика и обсуждение**

Известные зарубежные ученые в области изучения юридических вопросов защиты персональных данных М. Финк и Ф. Паллас [2], исследуя проблемы разграничения личных и неличных данных в соответствии с GDPR, подчеркивают важность этого различия, поскольку объем и требования GDPR распространяются только на персональные данные. Текущий подход к определению персональных данных в соответствии с GDPR проблематичен из-за расширенного определения «идентифицируемых» лиц. GDPR считает данные персональными, если они могут быть прямо или косвенно связаны с идентифицируемым лицом. Это широкое определение часто создает двусмысленность при определении того, следует ли классифицировать конкретные данные как личные или неличные. Авторы предлагают подход, основанный на оценке рисков, чтобы лучше различать персональные и неперсональные данные. Этот подход учитывает вероятность идентификации на основе имеющихся средств и ресурсов, а также потенциальный вред, который может быть нанесен в результате идентификации. Сосредоточив внимание на риске идентификации, этот подход обеспечивает более практичную и контекстно-зависимую основу для определения применимости положений GDPR. В этой связи, М. Финк и Ф. Паллас подчеркивают необходимость более тонкого понимания персональных данных в соответствии с GDPR. Их подход, основанный на оценке риска, предлагает многообещающую альтернативу текущему определению, обеспечивая большую ясность и гибкость в применении регулирования персональных данных, сохраняя при этом надежную защиту данных для физических лиц.

Другие юристы-исследователи Н. Черкуи и Т. Чирвасе [3], анализируя различия между обработкой персональных и неличных данных и последствия этих различий для конфиденциальности и защиты данных, утверждают, что, хотя неперсональные данные не имеют прямого отношения к идентифицируемому лицу, по-прежнему крайне важно учитывать их потенциальное влияние на конфиденциальность. Н. Черкуи и Т. Чирвасе подчеркивают важность понимания различных типов данных и их потенциального использования. Они обсуждают правовые рамки, регулирующие обработку персональных данных, такие как GDPR, и подчеркивают, что на неперсональные данные не распространяются строгие требования. Однако авторы утверждают, что обработка неличных данных все еще может иметь серьезные последствия для конфиденциальности, особенно в отношении агрегации данных, анонимизации и повторной идентификации. Авторами рассматриваются проблемы обеспечения конфиденциальности в эпоху больших данных и расширенной аналитики данных, при этом они отмечают, что кажущиеся неличными данные могут раскрывать конфиденциальную информацию о людях в сочетании с другими источниками данных, что приводит к потенциальным рискам для конфиденциальности. Они подчеркивают, что различие между личными и неличными данными часто размыто и требует тщательного анализа в каждом конкретном случае. Н. Черкуи и Т. Чирвасе призывают к более широкому взгляду на защиту данных, который учитывает потенциальные риски для конфиденциальности, связанные с обработкой неличных данных. Они предлагают регулирующим органам и организациям принять более комплексный подход к защите данных, учитывая последствия обработки персональных и неличных данных. В заключение в публикации подчеркивается важность понимания и устранения последствий обработки неличных данных для конфиденциальности, ибо необходим более комплексный подход к защите данных, учитывая потенциальные риски для конфиденциальности, связанные с обработкой личных и неличных данных.

Итальянский ученый-юрист в области фундаментальных прав человека К. Ирти [4] исследует различные категории данных и их влияние на конфиденциальность и защиту данных в программных сервисах. Автором представлен углубленный анализ различий

между личными и неличными данными, анонимными, псевдонимизированными и обезличенными данными, при этом подчеркивается важность понимания этих классификаций для надлежащего управления конфиденциальностью и защитой данных. Объясняя определения и правовые рамки, регулирующие персональные данные, таких как GDPR, он выделяет особые требования к контролерам и обработчикам данных при обработке персональных данных. Затем автор углубляется в оценку неличных данных, которые не имеют прямого отношения к идентифицируемым лицам и не подпадают под такие же строгие правила конфиденциальности. В его публикации также рассматриваются нюансы анонимных, псевдонимизированных и деидентифицированных данных, которые представляют собой различные методы сокрытия личности людей при наборе данных. К. Ирри подчеркивает, что, хотя эти методы могут помочь защитить конфиденциальность, они не являются надежными и могут быть подвержены рискам повторной идентификации, особенно в эпоху применения больших данных и расширенной аналитики. Автор также обсуждает проблемы и обязанности поставщиков программных услуг в управлении различными типами данных. Автором подчеркивается важность принятия соответствующих технических и организационных мер для защиты конфиденциальности и соблюдения правил защиты данных, таких как шифрование, контроль доступа и методы минимизации данных и предлагается всесторонний анализ различных категорий данных и их содержания для конфиденциальности и защиты в индустрии программных услуг, что подчеркивает важность понимания этих классификаций и принятия эффективных мер для обеспечения соблюдения правил конфиденциальности и поддержания доверия пользователей.

Нидерландские ученые-юристы, специализирующиеся на защите персональных данных в индустрии здравоохранения Д. Грус и Е.-В. ван Вин [5] обсуждают сложности, связанные с анонимными данными в контексте верховенства закона и правил защиты данных, таких как GDPR. В публикации подчеркивается важность понимания юридических последствий и потенциальных рисков анонимных данных. В свою очередь, Д. Грус и Е.-В. ван Вин начинают с разъяснения концепции анонимных данных, которая относится к данным, которые были обработаны таким образом, что они больше не могут быть прямо или косвенно связаны с идентифицируемым лицом. Согласно GDPR, обезличенные данные не подпадают под действие правил защиты персональных данных, поскольку не представляют угрозы для конфиденциальности физических лиц. Однако авторы утверждают, что процесс анонимизации не всегда прост и может быть сопряжен с потенциальными рисками повторной идентификации, особенно в связи с достижениями в области анализа данных и растущей доступностью дополнительных источников данных. Они подчеркивают, что методы анонимизации следует оценивать в каждом конкретном случае с учетом конкретного контекста и потенциальных рисков, дополнительно рассматривая юридические проблемы и ответственность, связанные с использованием анонимных данных. Авторы утверждают, что организации должны тщательно учитывать последствия анонимизации для верховенства закона такие, как потенциальное влияние на прозрачность, подотчетность и справедливость. Они также подчеркивают важность внедрения соответствующих мер безопасности и технологий повышения конфиденциальности для минимизации рисков повторной идентификации и обеспечения соблюдения правил защиты данных. Ими критически анализируются сложности, связанные с анонимными данными и верховенством закона, подчеркивается необходимость более тонкого понимания методов анонимизации, их правовых последствий и важности принятия эффективных мер для минимизации рисков, связанных с анонимными данными.

В статье нидерландского ученого-юриста в области имущественного права С. ван Эрпа [6] подчеркивается важность создания общего словаря для понимания концепций владения данными в европейском праве собственности, а также утверждается, что отсутствие согласованной терминологии и определений в отношении владения данными может привести к путанице, юридическим проблемам и потенциальному неправомерному

использованию данных. С. ван Эрп начинает с обсуждения растущего значения данных в современной цифровой экономике и сложностей, связанных с владением данными, особенно с появлением таких технологий, как Интернет вещей (IoT), большие данные и облачные вычисления. Автор подчеркивает, что существующие правовые рамки, такие как GDPR, в первую очередь сосредоточены на защите данных и конфиденциальности, но недостаточно решают вопрос владения данными, а отсутствие четкого и единого понимания владения данными может привести к двусмысленности и несоответствиям в юридических толкованиях и применениях. Например, личные данные, неличные данные и права на интеллектуальную собственность могут частично совпадать или конфликтовать в определенных ситуациях, что затрудняет определение того, кто имеет право на доступ, контроль или получение прибыли от данных. Чтобы решить эту проблему, С. ван Эрп предлагает разработать общий словарь по владению данными, который охватывает различные аспекты, включая их создание, сбор, обработку, хранение и передачу. Автор предлагает, чтобы общий словарь был основан на существующих правовых принципах и рамках, при этом учитывались уникальные характеристики данных и их потенциальное использование в эпоху цифровых технологий. Им подчеркивается, что установив в общем словаре четкие и последовательные определения и концепции, заинтересованные стороны могут лучше понять свои права и обязанности в отношении владения персональными и другими данными, что в конечном итоге будет способствовать созданию более справедливой и прозрачной цифровой экосистемы.

И.М. Берияйн, А.Д. Санчес и Х.К. Парилья [7], исследуя юридические и этические последствия обработки данных умерших людей, подчеркивают отсутствие четких правил и руководств по обработке таких данных и предлагают нормативную базу для устранения этого пробела. Авторы, отмечая растущее значение данных в сегодняшнюю цифровую эпоху увеличения объема информации, оставленной умершими людьми, подчеркивают, что существующие правовые рамки, такие как GDPR, в первую очередь сосредоточены на защите данных живых людей, оставляя данные умерших людей в серой зоне регулирования. И.М. Берияйн, А.Д. Санчес и Х.К. Парилья утверждают, что отсутствие четких правил обращения с данными умерших людей может привести к потенциальному неправомерному использованию, нарушению конфиденциальности и конфликтам между заинтересованными сторонами, такими как члены семьи, исследователи или коммерческие организации. Авторы подчеркивают, что данные умерших могут по-прежнему иметь значительную ценность и нести в себе потенциальные риски, что требует комплексного и взвешенного подхода к их обработке. Для решения этой проблемы в статье предлагается нормативная база для обработки данных об умерших лицах с учетом различных вовлеченных интересов и проблем. Авторы предполагают, что эта структура должна основываться на таких принципах, как уважение желаний умершего человека, защита прав и интересов членов семьи и учет общественных благ, таких как научные исследования или сохранение исторической памяти. В публикации подчеркивается необходимость нормативной базы для управления данными об умерших лицах, решения правовых и этических проблем, возникающих в этой недостаточно регулируемой области. Установив четкие правила и принципы, заинтересованные стороны могут лучше справляться со сложностями обработки данных умерших людей, уважая их желания, защищая интересы своих близких и способствуя общественному спокойствию.

### **Предложения**

Чтобы уменьшить юридические недостатки в обработке персональных и неличных данных, политики, организации и отдельные лица могут принять ряд мер. Эти предложения направлены на создание более надежной правовой базы и продвижение практики ответственного обращения с данными.

Четкие определения и рекомендации. Директивные органы должны разработать четкие определения и руководящие принципы для проведения различия между личными и

неличными данными. Эта мера поможет организациям и отдельным лицам понять свои обязанности и обязанности, уменьшив двусмысленность и возможность неправильного толкования.

**Риск-ориентированный подход.** Принятие риск-ориентированного подхода к обработке данных, при котором организации оценивают потенциальные риски, связанные со сбором, хранением и использованием персональных и неличных данных. Такой подход может помочь организациям выявить и смягчить потенциальные юридические недостатки.

**Минимизация данных.** Внедрение принципов минимизации данных в деятельность по обработке данных, собирая только необходимые данные и сохраняя их как можно быстрее. Такой подход снижает риск юридических недостатков за счет сведения к минимуму объема персональных данных, которые могут быть случайно перемешаны с неличными данными.

**Методы анонимизации и псевдонимизации.** Поощрение обоснованных методов анонимизации и псевдонимизации для защиты личных данных от повторной идентификации. Однако организации также должны знать об ограничениях и потенциальных рисках этих методов.

**Комплексная политика конфиденциальности.** Организации должны разработать всеобъемлющие политики конфиденциальности, которые прямо касаются обработки личных и неличных данных, предоставляя четкую информацию о методах сбора, обработки, хранения и обмена данными.

**Назначение сотрудника по защите данных (DataProtectionOfficer).** Назначьте DPO в организациях, работающих с большими объемами персональных данных, чтобы обеспечить соблюдение правил защиты данных и снизить риск юридических недостатков.

**Обучение и осведомленность сотрудников.** Проводите регулярные программы обучения и повышения осведомленности сотрудников, чтобы сотрудники понимали юридические различия между личными и неличными данными и свои обязанности при обработке таких данных.

**Регулярные аудиты и проверки соответствия.** Проводите регулярные аудиты и проверки соответствия, чтобы убедиться, что методы обработки данных соответствуют требованиям законодательства, а также выявлять и устранять потенциальные юридические недостатки.

**Взаимодействие с регуляторами.** Поощряйте открытый диалог и сотрудничество между организациями и регулируемыми органами для лучшего понимания правовой ситуации и содействия разработке передовых методов обработки персональных и неличных данных.

**Гармонизация международного права.** Директивные органы должны работать над гармонизацией международных законов о защите данных, обеспечивая единые стандарты обработки данных в разных юрисдикциях. Эта мера поможет уменьшить юридические недостатки и продвинуть глобальный подход к защите данных.

Внедряя эти предложения, заинтересованные стороны могут уменьшить правовые недостатки в обработке личных и неличных данных, способствуя созданию более прозрачной, ответственной и юридически совместимой экосистемы данных.

## **Заключение**

В заключение отметим, что устранение юридических недостатков в обработке персональных и неличных данных имеет первостепенное значение в современном мире, который все больше зависит от данных. Быстрое развитие технологий и растущий объем генерируемых, собираемых и обрабатываемых данных привели к многочисленным проблемам в защите частной жизни и обеспечении соблюдения правил защиты данных. Чтобы преодолеть эти проблемы, политики, организации и отдельные лица должны совместно работать над созданием надежной правовой базы и продвижением ответственных методов работы с данными.



Разрабатывая четкие определения и руководящие принципы, применяя подходы, основанные на оценке рисков, внедряя принципы минимизации данных и поощряя методы анонимизации и псевдонимизации, заинтересованные стороны могут уменьшить правовые недостатки и создать более прозрачную и юридически совместимую экосистему данных. Кроме того, организациям следует уделять первоочередное внимание обучению сотрудников, регулярным аудитам и проверкам соответствия, а также вести открытый диалог с регулирующими органами и политиками, чтобы способствовать лучшему пониманию правовой ситуации.

В конечном счете, необходимы согласованные усилия всех заинтересованных сторон для создания более устойчивой и юридически обоснованной среды для защиты данных, достижения баланса между внедрением инноваций на основе данных и защитой прав на неприкосновенность частной жизни. Признавая и устраняя юридические недостатки в отношении личных и неличных данных, перед учеными стоят задачи по созданию более безопасной и надежной цифровой экосистемы в сфере обработки персональных и иных видов на благо всех.

### **Список использованной литературы:**

1. *European Parliament and Council of the European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) // Official Journal of the European Union. – 2016.*
2. *Finck M., Pallas F. They who must not be identified—distinguishing personal from non-personal data under the GDPR //International Data Privacy Law. – 2020. – V. 10. – №. 1. – pp. 11-36.*
3. *Cherciu N., Chirvase T. Non-Personal Data Processing-Why Should We Take It Personally? //Eur. J. Privacy L. & Tech. – 2020. – pp. 183-192.*
4. *Irti C. Personal Data, Non-personal Data, Anonymised Data, Pseudonymised Data, De-identified Data //Privacy and Data Protection in Software Services. – 2022. – pp. 49-57.*
2. *Groos D., van Veen E. B. Anonymised data and the rule of law //Eur. Data Prot. L. Rev. – 2020. – V. 6. – pp. 498-508.*
3. *van Erp S. The need for a common vocabulary on "data ownership"//European Property Law Journal. – 2019. – V. 8. – №. 1. – pp. 1-3.*
2. *De Miguel Beriain I., Duardo Sánchez A., Castillo Parrilla J. A. What Can We Do with the Data of Deceased People? A Normative Proposal. – 2021. – pp. 785-806.*

## **THE NECESSITY OF THE KAZAKHSTAN GOVERNMENT TO PROVIDE AID TO PEOPLE WITH DISABILITIES AT THE BACKGROUND OF RUSSIAN-UKRAINE ARMED CONFLICT. VIEW FROM INTERNATIONAL LAW PERSPECTIVE**

*Agibaev Asset*

*3rd year doctoral student of the «International Law»*

*Al-Farabi Kazakh National University*

*Scientific advisor: Cand.of Legal Sciences, assoc. professor Omirzhanov E.T.*

### **Introduction**

In spite on numerous international conventions regulating norms of protection of civilian population in conditions of war, for instance Geneva Conventions of 1949 and their Additional Protocols of 1977, there are not so many specific provisions on treatment to people with disabilities during the armed conflicts.