ДИАЛОГ

АНАЛИЗ ЗАРУБЕЖНЫХ ПРАКТИК ЗАЩИТЫ ПРАВ ЧЕЛОВЕКА В ЦИФРОВОМ ПРОСТРАНСТВЕ

ВВЕДЕНИЕ

В настоящий момент в России на государственном уровне ведется активное осмысление процессов, связанных с цифровизацией. Так, 10 декабря 2020 года состоялась встреча членов Совета по развитию гражданского общества и правам человека при Президенте РФ с Президентом, где, помимо прочего, обсуждалась проблема обеспечения прав человека в цифровом пространстве. По итогу Правительству РФ совместно с СПЧ Президентом была поручена разработка проекта концепции обеспечения защиты прав и свобод человека и гражданина в цифровом пространстве Российской Федерации и проекта "дорожной карты" по ее реализации, которые должен включать в себя мероприятия по повышению цифровой грамотности граждан и обучению их навыкам информационной безопасности и "цифровой гигиены". Согласно поручению Президента, проект концепции обеспечения прав человека в цифровом пространстве должен быть представлен до 1 августа. В связи с поручением Президента особую актуальность приобретает рассмотрение имеющегося опыта зарубежных практик в данной сфере.

Эта озабоченность темой цифровизации понятна: в последние десятилетия она постоянно расширяется, увеличивается ее влияние на все сферы жизни общества. Согласно отчету Digital 2021, выполненному международным агентством We Are Social, специализирующимся на исследованиях медиа, и компанией Hootsuite, занимающейся анализом социальных сетей, количество пользователей Интернета в мире составляет более 4,66 млрд человек - это свыше 59,5% населения планеты. 4,2 млрд. человек - 53,6% населения Земли - так или иначе охвачены социальными сетями. Расширяется "мобилизация" человечества: 5,22 млрд человек - 66,6% населения планеты - пользуются мобильными телефонами. Новые медиа привели к многократному увеличению интенсивности коммуникации. Обмен огромными массивами информации никогда прежде не был настолько простым. С этим связаны как масса преимуществ, так и большое число рисков.

В дигитальную эпоху социальные отношения меняются как в национальном, так и в транснациональном аспекте: одна из особенностей цифровизации заключается в том, что ее влияние возможно оценить лишь в трансграничном, транснациональном масштабе. В частности, это приводит к постепенному изменению таких основ международного права, как права человека.

Под правами человека обычно подразумевают универсальные, естественные и неотъемлемые права, по умолчанию присущие отдельному человеку по отношению к государству. Эти права лежат в основе международных договоров или признаны в нормах международного права. В их основе лежит принцип, согласно которому каждый человек с рождения обладает набором неприкосновенных, неотъемлемых прав, которые защищают его как личность от любого произвольного или нечеловеческого обращения, превращающего его в простой предмет чуждого действия. Оформление этих прав происходило постепенно. Вирджинский билль о правах и Декларация независимости США 1776 года; французская Декларация прав человека и гражданских свобод 1789 года; наконец, Устав ООН 1945 года и Всеобщая декларация прав человека 1948 года.

Условно права человека делятся на несколько поколений. К правам “первого поколения” относят базовые политические права свободы и участия: право на жизнь; запрет пыток и рабского труда; личная свобода и безопасность. К правам “второго поколения” относят экономические, социальные и культурные права,такие как права на труд, социальное обеспечение, питание, жилье, воду, здравоохранение и образование. В настоящий момент ведется работа над конкретизацией прав “третьего поколения”: к ним относят права на развитие, мир, экологичную среду. Дигитализация так или иначе затрагивает права всех поколений, радикально меняя реальность человеческой коммуникации.

Изучение зарубежного опыта в сфере прав человека в цифровом пространстве способствует отбору наиболее успешных практик, внедрение которых позволит России максимально эффективно использовать возможности, появляющиеся в дигитальную эпоху. Цифровые технологии за счет формирования новых каналов коммуникации позволяют государственным институтам более оперативно реагировать на запросы граждан, учитывать их мнение при выработке своей политики, что способствует увеличению доверия граждан к ним. Развитие уже существующих и создание принципиально новых систем, способных оперативно обеспечивать государственную власть обратной связью от граждан, в конечном счете значительно увеличивает эффективность функционирования государства.

Последние десятилетия международные дебаты по правам человека в контексте дигитализации были сосредоточены, преимущественно, на проблемах национальной и транснациональной безопасности, информационной войны и терроризма. Между тем, распространение цифровых способов управления, в основном, на национальном уровне привело к созданию принципиально новых систем государственного контроля, автоматизации дискриминации и насилия. Все это поднимает разнообразные критические вопросы, касающиеся возможности демократии и равенства в цифровом обществе. Однако сводить проблематику влияния дигитализации до темы цензуры и государственного контроля некорректно: проблемная область значительно шире, ее сложность обусловлена тем, что различные права человека в принципе конфликтуют друг с другом и потому должны быть уравновешены. Интернет-среда с ее сверхбыстрой коммуникацией часто выступает катализатором этой конфликтности. Для выработки взвешенной политики в данной области требуется комплексное взаимодействие самых разных акторов: государственных и надгосударственных институтов, IT-гигантов, НКО, профильно занимающихся защитой прав человека в Интернете.

В данном исследовании анализируются ключевые зарубежные практики, связанные с защитой прав человека в цифровом пространстве. В первой главе рассматривается деятельность основных профильных международных организаций, как межправительственных, так и общественных; во второй - комплекс практик, связанных с правом на доступ к Интернету; в третьей - практики, связанные с базовыми правами человека (правом на жизнь, свободу и личную неприкосновенность - ст. 3 Всеобщей декларации прав человека; правом на достойное обращение - ст. 5 Декларации; правом на защиту от дискриминации - ст. 7 Декларации); в четвертой - практики, связанные с правом на неприкосновенность частной жизни - ст. 12. Декларации; в пятой - практики, связанные с правом на свободный доступ к информации и на ее распространение - ст. 19 Декларации.

МЕЖДУНАРОДНЫЕ ОРГАНИЗАЦИИ

В данном разделе рассматриваются наиболее значимые практики как правительственных, так и неправительственных международных организаций, связанные с проблематикой прав человека в цифровом пространстве.

В настоящий момент на международном уровне различными как правительственными, так и неправительственными организациями ведется активная дискуссия по вопросам, связанным с защитой прав человека в цифровом пространстве. Увеличивается число организаций, профильно занимающихся данной проблематикой. Однако деятельность большинства таких организаций является сугубо декларативной, сводящейся к проведению различных образовательных мероприятий, организации публичных обсуждений и подготовке тематических исследований. Можно констатировать, что в настоящий момент деятельность международных организаций в сфере защиты прав человека в цифровом пространстве не является значимым фактором профильной политики: ключевые решения, затрагивающие данную сферу, почти всегда принимаются на национальном уровне и отражают приоритеты и интересы данных государств.

ООН

Организация Объединенных Наций неоднократно заявляла о необходимости защиты и продвижения прав человека в Интернете. Работа в этом направлении активизировалась после того, как пост Генерального секретаря организации занял Антониу Гутерриш. **В 2018 году была опубликована Стратегия Генерального секретаря в отношении новых технологий, которая заявила несколько определяющих принципов и обязательств работы ООН в цифровом пространстве**. В целом принципы и обязательства носят достаточно абстрактный характер и имеют декларативную функцию.

В качестве основных принципов приведены следующие положения:

- Защита и продвижение общечеловеческих ценностей;
- Способствование обеспечению инклюзивности и транспарентности;
- Работа в партнерстве;
- Наращивание имеющегося потенциала;
- Постоянное развитие;

Гутерреш заявил, что в современном мире ООН должна взять на себе не только обязательства по координации регулирования Интернет-пространства различными государствами, но также активно начать заниматься мониторингом равномерного распределения информационных технологий и защитой прав человека в данной сфере.

На 73-й сессии ООН в январе 2019 года была принята резолюция о "Праве на неприкосновенность частной жизни в цифровую эпоху". Резолюция среди прочего подтверждала, что права, которыми люди обладают за пределами Интернета, включая право на неприкосновенность частной жизни, должны соблюдаться и в Интернете, а также содержала целый ряд призывов для государств-членов, среди которых наиболее важными являются:

- Защита права на неприкосновенность частной жизни в Интернете;
- Предоставление лицам, чье право на неприкосновенность частной жизни было нарушено, эффективной защиты и поддержки;
- Разработка превентивных мер и средств правовой защиты граждан, чье право на неприкосновенность частной жизни было нарушено;
- Предоставление коммерческим предприятиям действенных указаний относительно того, как именно следует соблюдать права человека.

Кроме призыва к государствам, **в резолюции ООН также имеются призывы к частным компаниям**. В частности, отмечается, что IT-компании должны:

- Понятным и доступным образом информировать клиентов о сборе, использовании, передаче и хранении данных;
- Обеспечить, чтобы права человека (например, право на неприкосновенность частной жизни) учитывались при разработке, использовании, оценке и регулировании технологий автоматического принятия решений и машинного обучения.

В целом в резолюции в значительной мере развивались положения, приведенные в записке Генерального секретаря организации от 2015 года, в которой отмечалась важность применения норм международного права при использовании различных информационных технологий. Однако, если в записке 2015 года права человека упоминались лишь один раз, то в документе 2019 года задача охраны основных прав и свобод человека в Интернете поставлена во главу угла.

К вопросу развития современного цифрового пространства Антониу Гутерреш повторно обратился в 2019 году, когда в июне объявил о запуске "Стратегии борьбы с проявлениями ненависти". Ее реализация невозможна без активной политики в Интернет-пространстве, в котором, по словам Гутерреша "...*проявления ненависти достигают более широкой аудитории, чем когда-либо ранее*". В рамках этой стратегии ООН подчеркивает важность частно-государственного сотрудничества в вопросе предотвращения распространения разжигающего ненависть контента в Интернете.

На фоне пандемии коронавируса, ускорившей переход многих областей общественной жизни в онлайн, вопрос защиты прав человека в Интернет-пространстве получил особую актуальность. **В июне 2020 года ООН представила "Дорожную карту по цифровому сотрудничеству", в которой были обозначены приоритетные направления цифровизации и меры по укреплению межгосударственного цифрового сотрудничества на следующее десятилетие**.

К ним относится:

- Обеспечение к 2030 году доступа в Интернет для каждого взрослого человека;
- Создание цифровых общественных благ, включая программное обеспечение с открытым исходным кодом, открытые данные, стандарты и контент;
- Обеспечение всеобщего охвата населения цифровыми технологиями, сокращение цифровых разрывов;
- Наращивание потенциала в области цифровых технологий с помощью развития умений и навыков населения;
- Защита прав человека в цифровой среде через выработку соответствующих регуляторных рамок и законодательства;
- Поддержка глобального сотрудничества в области искусственного интеллекта;
- Обеспечение доверия и безопасности в цифровой среде;
- Создание эффективной архитектуры глобального цифрового сотрудничества, в том числе в целях преодоления последствий пандемии коронавируса.

Именно после принятия данной “дорожной карты” была реализована высказанная Гутеррешем в 2018 году идея создания поста посланника Генерального секретаря ООН по технологиям, который должен заниматься содействием развитию механизмов глобального цифрового сотрудничества и взаимодействием между системой ООН и технологической индустрией. В настоящий момент рано говорить о результатах работы посланника по технологиям (должность была учреждена лишь в январе 2021 года), но можно сказать, что принципы и направления, которые используются в “Дорожной карте”, имеют высокую актуальность и соответствуют проблемам, которые решают государства на национальном уровне. Кроме того, впервые у ООН появились не только рекомендации, но и набор мер, направленных на решение обозначенных проблем в Интернет-пространстве. В свою очередь, посланник Генерального секретаря ООН по технологиям в будущем может стать одним главных из инструментов организации в деле продвижения собственной политике в Интернет-пространстве, в том числе в области защиты прав человека.

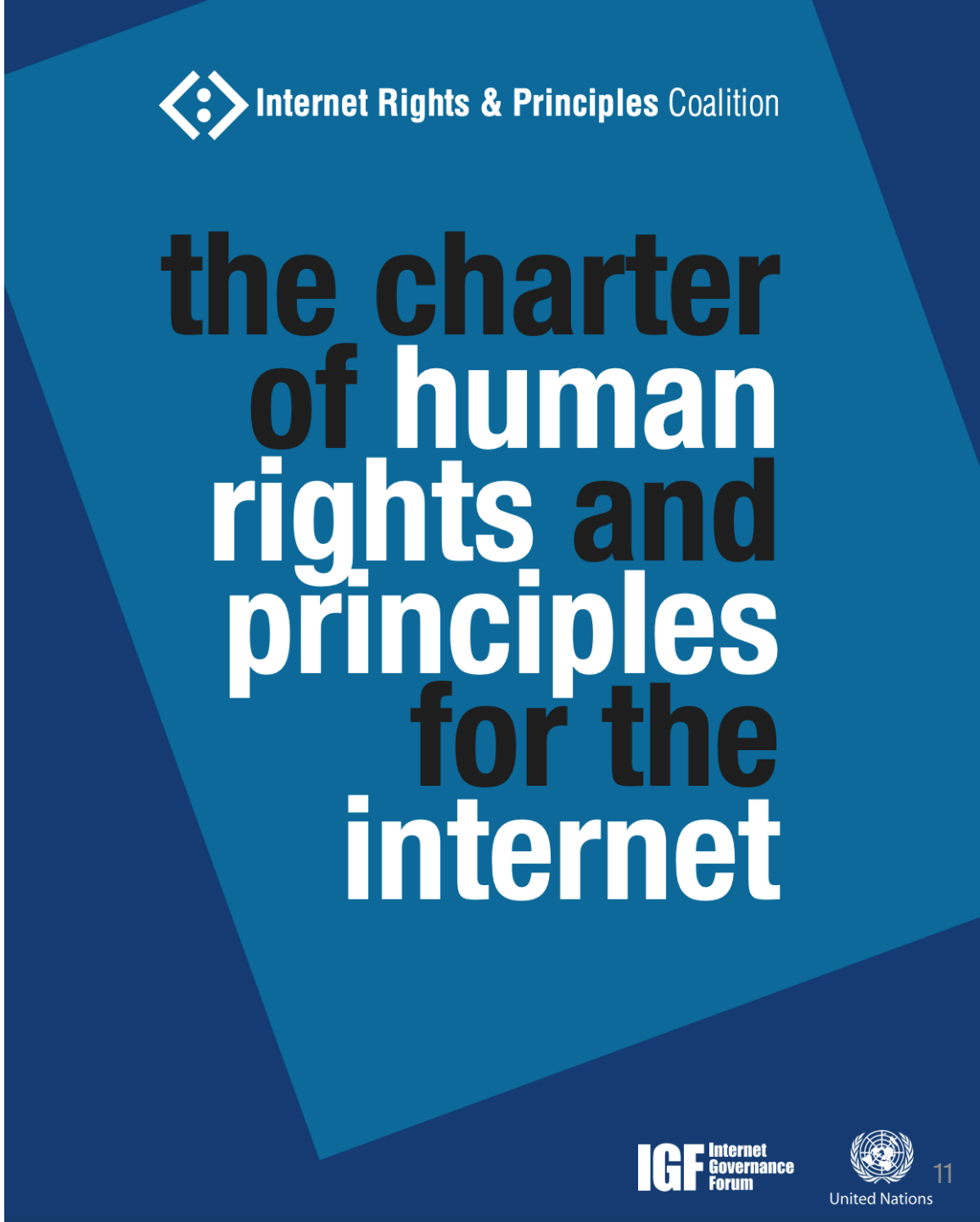
Активная политика ООН в направлении обеспечения прав человека в Интернет-пространстве является, помимо прочего, ответом на запрос со стороны различных правозащитных организаций. Так, еще в 2014 году Human Rights Watch опубликовала доклад “Права человека в цифровую эпоху”, в котором призвала ООН к ряду решительных действий, направленных на более активную защиту прав граждан в Интернете. В частности, Human Rights Watch предлагала ООН создать должность специального посланника по праву человека на приватность, углубив основные принципы резолюции “О праве на неприкосновенность личной жизни в эпоху цифровых технологий” 2014 года. Стоит отметить, что многие положения из этого документа позднее были использованы в “Дорожной карте по цифровому сотрудничеству”: например, право уважать и защищать право на неприкосновенность личной жизни, в том числе в контексте цифровой связи.

Помимо этого организация призвала ООН к новому взгляду на Интернет как на совершенно новое общественное явление, отметив, что существующие национальные и территориальные принципы плохо подходят для Интернета. Потому ООН как независимая международная организация должна в вопросе защиты прав граждан в Интернете ориентироваться не только на отдельные государства, но и на гражданское общество отдельных стран (в частности, в пример приводятся китайские активисты, которые испытывают давление со стороны государства). Несмотря на подобные призывы, ООН в данном вопросе продолжает играть умеренную роль, лишь в последние несколько лет перейдя от мониторинга ситуации к более активному участию.

THE INTERNET RIGHTS & PRINCIPLES COALITION

Коалиция по правам и принципам в Интернете - это международная сеть частных лиц и организаций, работающих над защитой прав человека в онлайн-среде и разработкой политики в Интернете в целом. Коалиция основана на базе Форума ООН по управлению Интернетом, в рамках которого обсуждаются вопросы, относящиеся к Интернет-пространству. **Основная миссия Коалиции заключается в переводе основных прав человека, сформулированных во Всеобщей декларации прав человека, в онлайн-пространство**.

Главным документом, разработанным Коалицией, является Хартия прав человека и принципов в Интернете от 2011 года. В Хартии содержится более подробная версия универсальных стандартов в области прав человека, адаптированная под специфику онлайн-пространства. Хартия основывается на Женевской Декларации принципов Всемирного Саммита по информационно-коммуникационным технологиям и информационному обществу и Тунисской программе развития информационного общества. **Цель документа - построение ориентированного на людей информационного общества, которое уважает и поддерживает основные права, закрепленные во Всеобщей декларации прав человека**.



В документе определяются десять ключевых прав и принципов управления Интернетом:

1. **Универсальность и равенство:** все люди рождаются свободными и равными в своем достоинстве и правах, которые должны уважаться, защищаться и реализовываться в онлайн-среде;

2. **Права и социальная справедливость:** Интернет - это пространство для поощрения, защиты и осуществления прав человека и продвижения социальной справедливости. Каждый обязан уважать права человека в онлайн-среде;

3. **Равный доступ к Интернету:** каждый имеет право на доступ и использование безопасного и открытого Интернета;

4. **Свобода слова и ассоциаций:** у каждого пользователя есть право свободно искать, получать и распространять информацию в Интернете без цензуры или иного вмешательства. Каждый человек имеет право свободно общаться в Интернете в социальных, политических, культурных или иных целях;

5. **Конфиденциальность и защита данных:** каждый человек имеет право на конфиденциальность в Интернете. Это право включает в себя свободу от слежки и возможность использования шифрования для поддержания собственной анонимности. Каждый человек также имеет право на защиту персональных данных, включая контроль за сбором, хранением, обработкой, удалением и раскрытием персональных данных;

6. **Жизнь, свобода и безопасность:** права на жизнь, свободу и безопасность должны уважаться, защищаться и полностью соблюдаться в Интернете;

7. **Разнообразие:** следует поощрять культурное и языковое разнообразие в Интернете, а также поддерживать технические и политические инновации для содействия плюрализму выражения мнений;

8. **Сетевое равенство:** каждый человек должен иметь открытый доступ к контенту Интернета, свободный от дискриминационного определения приоритетов, фильтрации или контроля трафика по коммерческим, политическим или иным основаниям;

9. **Стандарты и регулирование:** коммуникационные системы и базы данных в Интернете должны основываться на принципах открытости, обеспечивающих полную функциональную совместимость, инклюзивность и равные возможности для всех пользователей;

10. **Система управления:** права человека и социальная справедливость должны формировать нормативную базу для развития и регулирования Интернета. Это должно происходить транспарентным и многосторонним образом, основанным на принципах открытости, инклюзивного участия и подотчетности.

Отдельная группа прав в Хартии представлена гражданскими и политическими правами человека, среди которых выделяются свобода вероисповедания, свобода онлайн-протестов, собраний и союзов, свобода средств массовой информации, свобода от языка вражды и цензуры, а также право на информацию, онлайн-неприкосновенность, защиту цифровых данных, медицинские и социальные услуги, правовую защиту и справедливое судебное разбирательство в отношении действий, связанных с Интернетом. К социальным и культурным правам в онлайн-среде относятся право на образование в Интернете, благоприятные и справедливые условия труда в Сети, онлайн-участие в управлении своей страной.

Хартия прав человека и принципов в Интернете может быть использована в качестве образцового примера перенесения принципов Всемирной Декларации ООН в онлайн-пространство. Хартия представляет собой *“основу”* для защиты и продвижения прав человека в онлайн-среде.

Проблема доступа к Интернету - одна из ключевых, рассматривающихся в Хартии прав человека и принципов в Интернете. Доступ к Интернету становится необходимым условием для полноценного осуществления целого ряда прав человека, включая право на свободу слова, образование, свободу мирных собраний и ассоциаций, участие в процессе принятия социально-политических решений, а также права на труд и отдых. Расширение доступа к Интернету, согласно Хартии, подразумевает соблюдение следующих принципов:

- **Высокое качество обслуживания**: предоставляемые услуги по обеспечению доступа к Интернету должны совершенствоваться в соответствии с развитием технологических возможностей;
- **Свобода выбора системы и использования программного обеспечения**;
- **Цифровая инклюзивность**: все люди, вне зависимости от своих особенностей, должны иметь равный доступ к цифровым средствам массовой информации, коммуникационным платформам и устройствам для управления и обработки информации;
- **Нейтральность и равенство в Интернете:** отсутствие особых привилегий или, наоборот, препятствий для равного доступа и использования Сети.

КОАЛИЦИЯ FREEDOM ONLINE

Коалиция Freedom Online - межправительственная коалиция, занимающаяся поддержкой основных цифровых прав человека – свободы выражения мнений, ассоциаций, собраний и конфиденциальности. Организация была создана в 2011 году на международной онлайн-конференции в Гааге по инициативе Министерства иностранных дел Нидерландов. На сегодняшний день Коалиция насчитывает 32 государства-члена, среди которых США, Великобритания, Германия, Австралия, Япония, Гана. **Основная миссия Коалиции заключается во включении вопросов свободы Интернета в повестку международной политики для достижения конкретных политических изменений в данной сфере**.

Все государства-члены коалиции подписали учредительный документ FOC (Freedom Online: Joint Action for Free Expression on the Internet). **В нем главный принцип организации сформулирован следующим образом: *"Права человека в оффлайн-пространстве являются такими же в Интернете"*.** В 2021 году Коалиция Freedom Online продолжает работу в области цифровой интеграции, кибербезопасности и искусственного интеллекта посредством дипломатического сотрудничества с государствами-участниками и с иными стейкхолдерами (государствами, IT-компаниями, институтами гражданского общества); формирования глобальных норм соблюдения цифровых прав человека; проведения различных онлайн- и оффлайн-мероприятий (ежегодная конференция FOC, региональные тематические мероприятия).

Одним из ключевых направлений работы международной коалиции Freedom Online является борьба с угрозами для свободы слова в Интернете. В совместном заявлении организация призывает всех вовлеченных акторов "воздержаться" от введения ограничений контента в Интернете, нарушающих международное право в области прав человека. Члены Коалиции подчеркивают, что необходимо создавать благоприятные условия для свободного выражения мнений и доступа к информации в Интернете, а именно:

- Государства не должны ограничивать, модерировать онлайн-контент или манипулировать им, нарушать работу социальных сетей с целью лишения пользователей доступа к определенной информации, использовать технологии интернет-цензуры, противоречащие их международным обязательствам;
- Государства должны конструктивно сотрудничать с IT-компаниями в целях повышения прозрачности их процессов модерации контента. Правительствам следует также поощрять компании к принятию справедливых механизмов правовой защиты;
- Вовлеченные акторы должны вместе работать над общим подходом к управлению Интернетом, направленным на оценку, реагирование и, при необходимости, исправление поддерживаемых рядом государств усилий по ограничению онлайн-контента.

Также FOC обращает внимание на рост числа мероприятий, направленных на блокирование доступа к законному онлайн-контенту, давления на рядовых пользователей Интернета и IT-компании. Утверждается, что такие мероприятия зачастую совершаются под предлогом обеспечения безопасности или общественного порядка, однако фактически это происходит незаконно. Эксперты коалиции отмечают, что тактика ограничения свободы слова в онлайн-пространстве снижает доверие интернет-пользователей к действиям государства, подрывает экономические и социальные преимущества Интернета, а также негативно сказывается на соблюдении прав человека в целом.

Особое внимание коалиция Freedom Online уделяет проблеме доступа к Интернету. **По мнению организации, политика ограничения мобильной связи и интернет-услуг для конкретных групп граждан ограничивает цифровые права человека, а также значительно обесценивает преимущества Интернета.** Преднамеренные сбои в работе сети, нарушая доступ граждан к онлайн-услугам, подрывают позитивный экономический эффект от развития Интернета. Такие действия, по мнению членов Коалиции, не согласуются с целями устойчивого развития, в частности с целью расширения доступа граждан к информационно-коммуникационным технологиям. Коалиция призывает все правительства *“положить конец таким нарушениям прав на свободу выражения мнений и мирных собраний”*.

По мнению экспертов коалиции, государствам следует:

- Поддерживать и развивать уважающее права человека законодательство с учетом принципа недопустимости ограничения коммуникационных сетей;
- Законодательно определить случаи, в которых доступ к сети может быть ограничен;
- Способствовать повышению транспарентности органов государственной власти;
- Включить вопросы, связанные с преднамеренными сетевыми сбоями, в обсуждаемую международную повестку;
- Развивать диалог со всевозможными заинтересованными акторами по теме обеспечения стабильного доступа граждан к Сети;
- Выпускать публичные заявления, в которых освещаются случаи сетевых сбоев, а также информировать об их возможных последствиях;

APC
Association for Progressive Communications

Ассоциация прогрессивной коммуникации (APC) - это международная сеть организаций гражданского общества, занимающаяся расширением прав человека и поддержкой людей, работающих во имя мира, развития и защиты окружающей среды, посредством стратегического использования информационно-коммуникационных технологий. Ассоциация является активным участником международных дискуссий по вопросам политики в Интернете и обладает статусом первой категории при Экономическом и Социальном Совете ООН. **Миссия Ассоциации заключается в *“построении мира, в котором все люди имеют легкий и равный доступ к потенциалу ИКТ для улучшения жизни и создания более демократических и эгалитарных обществ”*.** Идея Ассоциации состоит в том, чтобы люди использовали Интернет и цифровые технологии *“для создания справедливого и устойчивого мира, ведущего к большей заботе о себе, друг о друге и о земле”*. В состав Ассоциации выходят 57 организаций и 33 индивидуальных члена, действующих в 73 странах, среди которых Нидерланды, Германия, Тунис, Индия, Южно-Африканская Республика, Бразилия, Аргентина и США.

57 **организаций**

33 **индивидуальных члена**

73 **страны, в которых организации и индивидуальные члены сети действуют**

На сегодняшний день Ассоциация руководствуется разработанным Стратегическим Планом 2020-2023. Основная цель Стратегического Плана - обеспечение развития Интернета и коллективное управление им как глобальным общественным благом. В документе выделены пять аспектов, имеющих непосредственное отношение к продвижению цифровых прав человека:

1. **Коллективная сила сообществ.**
   Партнерские отношения и союзы широких сообществ имеют решающее значение для развития Интернета. Ассоциация стремится развивать сотрудничество с организациями, которые работают над экологической справедливостью, сексуальными правами, правозащитной деятельностью в области цифровых прав, феминизацией Интернета, технологиями и альтернативной интернет-инфраструктурой;

2. **Цифровая инклюзивность для наиболее уязвимых групп.**
   Необходимо добиться изменений в предоставлении доступных цифровых услуг. Это включает в себя доступ к открытым цифровым технологиям и пространствам, свободным от цензуры, слежки, преследований и любых других форм нарушения прав человека. Для предоставления равного доступа к Интернету для всех граждан важно разрабатывать инклюзивные и справедливые экономические модели, направленные на общую цифровую интеграцию. Достичь этого можно регулированием цен на онлайн-услуги;

3. **Феминизация Интернета.**
   В последнее время в онлайн-пространстве большое распространение получили случаи гендерного насилия. По этой причине Ассоциация уделяет особое внимание разработке стратегии в направлении феминизации Интернета. Организация подчеркивает, что необходимо спонсировать тех, кто работает над развитием феминистских онлайн-технологий;

4. **Защита прав человека в онлайн и оффлайн-среде.**
   Права человека должны быть основой регулирования Интернета и цифровых технологий. Основное внимание следует уделять продвижению и осуществлению норм в области прав человека и привлечению государств к ответственности за их нарушения, в том числе в онлайн-среде. APC призывает государства поощрять, защищать и уважать права человека, что подразумевает борьбу с нарушениями со стороны частных субъектов, а также разрабатывать новые стандарты и нормативные акты, касающиеся Интернета, цифровых технологий и цифровых прав человека;

5. **Содействие управлению Интернетом как глобальным общественным благом.**
   Заинтересованные стороны “*должны более решительно*” выступать за инклюзивные и транспарентные механизмы управления Интернетом и публичные слушания по тематическим вопросам.

АСЕАН

Информационно-коммуникационные технологии (ИКТ), и в частности Интернет, стали основным стимулом развития социально-экономической системы. **В настоящее время государства-члены АСЕАН постепенно переходят к цифровой экономике, уделяя все большее внимание развитию онлайн-среды.** Первый Генеральный план АСЕАН в области ИКТ (2010-2015) определил шесть стратегических направлений в качестве своих ключевых целей:

1. Экономические преобразования;
2. Расширение прав и возможностей людей и их вовлечение в Интернет-среду;
3. Цифровые инновации;
4. Развитие цифровой инфраструктуры;
5. Развитие человеческого капитала;
6. Преодоление цифрового разрыва.

В 2016 году был разработан новый Генеральный план АСЕАН - AIM 2020. Основной акцент в нем сделан на обеспечении перехода к цифровой экономике и развитии человеческого потенциала, а также на создании безопасной и надежной цифровой среды. Подчеркивается, что современные онлайн-технологии должны использоваться для поддержки цифровой интеграции и социального равенства там, где маргинализированные и уязвимые общины имеют возможность для вовлечения и вхождения в цифровую экономику. В документе анализируются те направления, которые имеют непосредственное отношение к вопросу цифровых прав человека.

В 2021 году Ассоциация приняла решение о разработке Генерального плана более короткой продолжительности (от 2 до 3 лет). Такое решение было принято из-за последствий эпидемии COVID-19 в глобальном масштабе и в странах Азии в частности. **Короткий документ планируется сосредоточить на мерах в области ИКТ/цифровых технологий, которые могли бы помочь в восстановлении после COVID-19 и установлении *“новой нормы”*.**

В частности, в Генеральном плане поднимается вопрос неравного доступа к Интернету среди членов Ассоциации государств Юго-Восточной Азии. **Государствам-членам предлагается сосредоточиться на повышении спроса, качества и доступности широкополосного доступа в Интернет,** а именно:

- Определить и идентифицировать *“изолированные от Интернета и недостаточно обслуживаемые сообщества”*;
- Разработать рекомендации по расширению широкополосного доступа в регионе, в том числе повысить ценовую доступность услуг провайдеров;
- Определить основные цифровые услуги, которые должны быть доступны гражданам АСЕАН;
- Провести тематические исследования, освещающие вопросы проведения высокоскоростного Интернета в таких секторах, как здравоохранение, образование, энергетика.

Повышение доступности Интернета в регионе напрямую зависит от выявления и последующего сокращения диспропорций в сфере ИКТ. **Для этого государствам Юго-Восточной Азии необходимо картировать приоритетные места (города, провинции), требующие развертывания высокоскоростного Интернета, и сотрудничать с бизнесом в разработке и развертывании широкополосной связи. Внедрение новой версии интернет-протокола IPv6 также повысит доступность Интернета для жителей региона.**

Еще одним направлением в сфере расширения цифровых возможностей является разработка универсальных услуг следующего поколения (Next-Generation USO 2.0). Обновленная программа USO 2.0 подчеркивает важность равного доступа к онлайн-услугам и их использовании. Таким образом **акцент смещается с формальной процедуры подключения к Интернету на равный доступ для всех граждан к данной процедуре**. Государства Ассоциации намерены продолжить сотрудничество с другими странами в области USO 2.0 (например, с США).

Важнейшим направлением соблюдения цифровых прав человека является информационная безопасность. Члены АСЕАН содействуют защите данных путем разработки региональных руководящих принципов. Так, в Генеральном плане организации было закреплено намерение проведения анализа систем защиты конфиденциальности персональных данных пользователей и разработки общего руководства АСЕАН для защиты персональных данных, для информационной и сетевой безопасности. Также государства заинтересованы в укреплении сотрудничества в области реагирования на чрезвычайные ситуации в киберпространстве. Для этого реализуются следующие мероприятия:

- Разрабатываются системы отчетности об инцидентах, а также шаблоны, стандартизирующие реакцию на заранее определенные угрозы;
- Осуществляется содействие регулярному сотрудничеству в области кибербезопасности и диалогу между правительствами, бизнесом и гражданами посредством совместных информационно-просветительских кампаний.

EUROPEAN DIGITAL RIGHTS

Основной организацией по защите прав человека в цифровом пространстве ЕС является Международная общественная организация по защите прав человека в интернете “Европейские цифровые права” (EDRi). Она была создана в 2002 году, штаб-квартира расположена в Брюсселе. Целью организации является продвижение, защита и поддержка прав человека в Интернете и в сфере инфокоммуникаций и технологий. EDRi занимается такими вопросами, как защита персональных данных, цифровые права, конфиденциальность и анонимность в интернете, а также авторское право и свобода слова. EDRi объединяет 44 европейских НКО со схожими целями.

Последний крупный общеевропейский проект EDRi, “Reclame Your Face”, был направлен против технологии массового распознавания лиц. Представители организации заявляли, что *“ЕС стал убежищем для незаконных биометрических экспериментов и слежки”*. Петицию о запрете таких технологий подписали свыше 32 тыс. человек. В настоящий момент Бельгия является единственным государством-членом, которое заявило, что распознавание лиц нарушает национальное законодательство, также правительство Люксембурга подчеркнуло, что выступает против распознавания лиц.

IACHR

В 2017 году Межамериканская комиссия по правам человека (IACHR) одобрила Стандарт свободного, открытого и инклюзивного Интернета. В первом разделе Стандарта определяются руководящие принципы, которые должны лежать в основе работы государства в сфере цифровой политики:

1. **Принцип свободного и открытого Интернета**, понимаемый как с точки зрения функциональной открытости (интероперабельности), так и с точки зрения экономической (сетевой нейтральности);
2. **Принцип доступного Интернета**. Стандарт определяет право на доступ к Интернету как условие для эффективного осуществления базовых прав человека и призывает государства региона содействовать достижению всеобщего доступа к Интернет, как в отношении обеспечения аппаратного доступа, так и в отношении развития цифровой грамотности;
3. **Гарантия качества Интернет-услуг**. Стандарт фиксирует обязательство государств гарантировать качество интернет-услуг, защищая их от произвольных блокировок, помех, перерывов или замедлений;
4. **Принципы равенства и недискриминации**. Стандарт подчеркивает обязательство государств удовлетворять конкретные потребности в доступе к Интернету, возникающие у особо уязвимых групп (например, расовых и гендерных меньшинств).

Кроме того, **в Стандарте подчеркивается важность Интернета как посредника в осуществлении свободы слова.** В нем говорится, что любые ограничения работы веб-сайтов, блогов, приложений, поисковых систем или любых других систем распространения информации в Интернете возможны лишь в условиях, четко определенных законом. При этом необходима *“прозрачность в отношении контента, удаление которого было предписано, а также необходимости и обоснованности этих мер”.*

Также **Стандарт призывает создавать эффективные системы мониторинга и подачи жалоб с целью выявления фактического или потенциального ущерба правам человека, причиняемого деятельностью частных компаний.** При этом подчеркивается, что **возложение строгой ответственности на компании-посредники несовместимо с Американской конвенцией о правах человека.** Соответственно, они не должны *“нести ответственность за контент, созданный другими лицами, который распространяется с использованием их услуг, до тех пор, пока они специально не влияют на этот контент или не отказываются подчиняться судебному постановлению об удалении этого контента при наличии возможности”.*

ПРАВО НА ДОСТУП К ИНТЕРНЕТУ

В дигитальную эпоху доступ к Интернету (как в смысле буквального, физического доступа к Сети, так и в смысле наличия базовых компетенций, необходимых для ориентирования в ней, т.н. цифровой грамотности) становится необходимым условием для полноценного осуществления самых разных прав человека, включая право на свободу слова, образование, свободу мирных собраний и ассоциаций, участие в процессе принятия социально-политических решений, а также право на труд и отдых. Неотъемлемая связь с вышеперечисленными правами позволяет считать право на доступ к Интернету первостепенным правом человека.

В данной главе описываются практики иностранных государств, связанные с правом на доступ к Интернету. Расширение доступа граждан к Интернету является одним из приоритетов большинства государств, вне зависимости от их политической системы. Проблема увеличения доступности Интернета комплексная, имеющая разные аспекты: предоставление гражданам фактического подключения к Всемирной Сети - с этим, в частности, связаны регулирование цен на услуги провайдеров (реализуется в Австралии и Японии) и устройств (реализуется в Сингапуре); предоставление гражданам равного доступа к разным формам сетевого контента (к данному аспекту относится дискуссионный принцип сетевого нейтралитета, внедряемый в Японии, Канаде и Калифорнии); увеличение уровня цифровой грамотности граждан (разнообразные программы по ее повышению действуют в Сингапуре, Японии, Австралии); расширение доступа к Всемирной Сети для людей с ОВЗ (так, в настоящее время в Канаде и США преобладает подход, рассматривающий несоответствие той или иной Интернет-услуги стандартам инклюзивности как форму дискриминации).

ЯПОНИЯ

Япония - страна с очень высокой доступностью Интернета. **Япония имеет высокоразвитую онлайн-инфраструктуру с большой долей Интернет-пользователей (около 117 млн пользователей).** Использование Интернета на бытовом уровне сопоставимо с развитыми европейскими государствами и США. Доступность Интернета в Японии объясняется мощной инфраструктурой местного онлайн-пространства. **В 2020 году Япония заняла 17 место в мире по качеству и широте доступной Интернет-инфраструктуры.** Стоимость интернет-услуг является пропорциональной доходам и уровню конкуренции на интернет-рынке, что делает их доступными для всего японского населения.

В Японии наблюдается самый высокий в мире уровень цифровой грамотности, которого удалось достичь благодаря профильным учебным курсам для всех возрастов. В образовательные программы была внедрена система цифрового повествования - Digital Storytelling (DST). Она предлагает пользователям практические занятия, которые позволяют учащимся создавать короткие видео с использованием персональных компьютерных файлов (изображений, видео, аудио). Таким образом дети и взрослые могут изучать исторические и социальные вопросы и получать навыки работы в цифровом пространстве. Также в Японии действовала исследовательская платформа Media Exprimo.

Суть платформы заключалась в разработке новых культурных программ и технологических систем, позволяющих людям, в том числе школьникам и студентам, участвовать в общественных коммуникациях в Интернете.

Еще одним инструментом, направленным на развитие цифровой грамотности в Японии, являются перенесенные в онлайн-среду традиционные образовательные японские игры (например, карточная игра Comikaruta и игра слов A-I-U-E-O Gabun). Образовательный онлайн-контент ориентирован как на школьников, так и на пенсионеров. Подобные программы повышения цифровой грамотности продвигаются в университетах и школах, среди местных муниципальных органов, на традиционных фестивалях и через кабельные телевизионные станции.

Свободный доступ японских граждан к Интернету обусловлен политикой сетевого нейтралитета. Министерство внутренних дел и коммуникации Японии совместно с телекоммуникационными провайдерами разработало отраслевые руководящие принципы сетевого нейтралитета. К ключевым аспектам цифрового нейтралитета относятся следующие принципы: интернет-провайдеры должны бороться с резкими скачками трафика путем увеличения пропускной способности сети; изменение скорости интернет-трафика должно допускаться только в исключительных ситуациях и быть оправдано объективными критериями.

СИНГАПУР

В Сингапуре доля пользователей Интернета составляет 90% от населения, что является одним из самых высоких показателей в мире. Для достижения наивысших показателей доступности Интернета в стране уделяется особое внимание вопросам цифрового образования и детским цифровым правам. **В настоящее время власти Сингапура активно работают над так называемой цифровой готовностью (digital readiness).** Цифровая готовность в сингапурском контексте определяется как сфера, подразумевающая а) наличие доступа к цифровым технологиям; б) цифровую грамотность для их использования; в) способность участвовать и использовать цифровые технологии для дальнейшего развития. В обобщенном смысле, цифровая готовность включает в себя доступ к онлайн-среде, цифровую грамотность и участие.

Для достижения высоких показателей цифровой готовности в марте 2020 года была принята Национальная программа цифровой грамотности, направленная на детей школьного возраста. Программа представляет собой 10-часовые курсы для учеников начальной и средней школы. На сегодняшний день программа успешно реализуется во многих школах Сингапура. В 2021 году власти Сингапура запустили аналогичную программу для пожилых людей. Например, желающих учат, как скачивать и использовать электронные книги.

Суть сингапурской программы повышения цифровой грамотности заключается в освоении следующих принципов:

1. **Поиск информации:** пользователи должны уметь собирать и оценивать информацию в Интернете, а также использовать цифровые ресурсы безопасным и ответственным образом;
2. **Работа с электронными данными:** умение интерпретировать и анализировать данные из Интернета;
3. **Использование электронных устройств:** развитие навыков работы на электронных устройствах с использованием разных программных обеспечений;
4. **Производство электронного контента:** навыки производства контента посредством электронных устройств.

Другим компонентом цифровой готовности является наличие средств доступа к онлайн-информации, сетям и сообществам. Для реализации этого принципа Правительство Сингапура предоставляет компьютеры и планшеты по льготным ставкам семьям с низкими доходами. Также совершенствование цифровой готовности включает обеспечение всех граждан широкополосным доступом в Интернет, развитие безопасного способа совершения денежных транзакций и аутентификации цифровой личности.

КНР

В Белой книге Интернета, ключевом документе, определяющем политику КНР в Интернет-пространстве, подчеркивается, что **роль Интернета в удовлетворении права на информацию становится все более заметной. Государственные учреждения должны проявлять инициативу по раскрытию государственной информации для китайских граждан.** Центральное правительство требует от региональных правительств создания соответствующих механизмов и оперативного разъяснения вопросов, представляющих общественный интерес. Правительства на всех уровнях должны оперативно через все ресурсы, включая Интернет, распространять информацию об осуществлении политики, а также о мерах реагирования на стихийные бедствия, чрезвычайные ситуации в области здравоохранения и социального обеспечения.

Китайские власти поощряют использование Интернета в целях содействия экономическому и социальному прогрессу, улучшения государственных услуг и облегчения труда и жизни людей. Также осуществляется политика по созданию структурированного и сбалансированного использования Интернета и улучшению его развития и применения.

> *Китайское государство будет энергично содействовать развитию веб-сайтов, посвященных электронной торговле и образованию, придаст импульс созданию электронного правительства, будет выступать за развитие новых средств массовой информации, таких как онлайн-радио и онлайн-телевидение, и будет призывать к предоставлению разнообразных и богатых информационных услуг в Интернете для удовлетворения потребностей в информации.*

США

Одним из важнейших вопросов, связанных с Интернетом и регулярно обсуждающихся в США как на федеральном, так и на региональном уровне, является принцип сетевого нейтралитета, согласно которому операторы связи не должны отдавать предпочтения одному виду трафика перед другим (например, желая монетизировать доступ пользователей к собственным мессенджерам или иным онлайн-платформам).

Дискуссия о необходимости следования принципам сетевого нейтралитета началась еще в начале 2000-х годов и продолжается в наше время. В феврале 2015 году Федеральная комиссия по коммуникациям (FCC) закрепила принцип "сетевого нейтралитета". С приходом администрации Дональда Трампа ситуация изменилась: новый глава комиссии Аджит Паи заявил о необходимости отмены принципов сетевого нейтралитета, отметив, что он является "*репрессивным*" и в значительной степени противоречит принципам развития Интернета. Документ, разработанный комиссией получил название акта о "Восстановление свободы в Интернете" и фактически отменял принцип сетевой нейтральности, еще до голосования по нему акт вызвал значительное обсуждение, в том числе, крайнее недовольство правозащитных организаций и Интернет-гигантов. 12 июня 2017 года было объявлено "Днем действия для защиты сетевого нейтралитета", который был назван самым активным протестом в области Интернета в истории. **14 декабря 2017 года Федеральная комиссия по вопросам регулирования связи США с перевесом в один голос проголосовала за отмену принципа сетевого нейтралитета, закрепленного в 2015 году**.

18 июня закон о "Восстановлении свободы в Интернете" вступил в силу и принципы сетевого нейтралитета в Соединенных Штатах были ликвидированы.

Данное решение FCC вызвало не только недовольство профильных компаний и правозащитных организаций, но и некоторых американских штатов. 30 сентября 2018 года власти штата Калифорния приняли закон о защите принципов сетевого нейтралитета, сразу вслед за этим администрация Дональда Трампа подала против правительства штата иск, отметив в нем, что постановления, принятые властями штата, "*противоречат подходу федерального правительства к вопросу развития Интернета*". К иску также присоединились крупнейшие Интернет-провайдеры. Кроме Калифорнии, схожий закон был принят также в штате Мэн.

Поражение Дональда Трампа на выборах президента в 2020 году вновь поставило вопрос о судьбе закона о сетевом нейтралитете. Вскоре после инаугурации Джо Байдена в качестве президента США Министерство юстиции прекратило участие в иске против штата Калифорния, настаивающие на продолжении иска компании в итоге потерпели поражение, так как суд встал на сторону властей Калифорнии. **Несмотря на окончание судебного разбирательства в Калифорнии, вполне возможно, что в ближайшее время FCC поставит вопрос о возвращении к принципам сетевого нейтралитета**, так как исполняющая обязанности главы FCC Джессика Розенворсель (которая, вероятно, станет полноценной главой комиссии) известна своей поддержкой принципа сетевого нейтралитета.

На фоне последних событий, связанных с блокировкой Дональда Трампа в социальных сетях, конфликт между провайдерами и крупнейшими IT-компаниями продолжился. Несколько Интернет-провайдеров в ответ на блокировку аккаунтов Трампа заблокировали для своих пользователей доступ к таким социальным сетям, как Twitter и Facebook, в частности, на это пошла компания YourT1Wifi, которая работает в штатах Айдахо и Вашингтон.

При рассмотрении инициатив по защите прав Интернет-пользователей следует уделить особое внимание американским инициативам, направленным расширение инклюзивного доступа в Интернет для людей с различными видами инвалидности. Процесс активного осмысления данной проблематики и создания полноценных практик, направленных на защиту прав людей с ОВЗ при пользовании Интернетом, начался в период администрации президента Барака Обамы. В 2010 году был принят указ, согласно которому государство должно было в значительной степени содействовать развитию доступного Интернета для граждан с ОВЗ (например, важным элементом должно было стать расширение применения субтитров в видеоконтенте); также выделялся обязательный пункт о создании такой формы информирования о чрезвычайных ситуациях, которая была бы доступна для людей с инвалидностью. Указ касался не только государственных учреждений, но и всех поставщиков контента для федеральных или региональных властей.

В последующие годы право людей с инвалидностью на комфортное пользование Интернетом было укреплено в американском прецедентном праве. В октябре 2019 года Верховный суд США отклонил апелляцию Domino's Pizza и оставил в силе решение апелляционного суда 9-го округа США, согласно которому принятый еще в 1990 году “Закон об американцах с инвалидностью” должен защищать доступ людей с ОВЗ не только к посещению публичных мест, но также и к веб-сайтам. Первоначально суд начался после того, как слепой житель Лос-Анджелеса Гильермо Роблес пожаловался, что не смог заказать еду онлайн на сайте Domino’s Pizza из-за того, что сайт блокировал специальное программное обеспечение для слепых, которым пользовался Роблес. Представители Domino’s Pizza пытались оспорить решение на основании того, что в Соединенных Штатах отсутствует единый федеральный стандарт предоставления доступа для людей с ОВЗ, а потому вплоть до его введения компании не обязаны каким-либо образом менять свою веб-архитектуру. Стоит отметить, что сам “Закон об американцах с инвалидностью” на момент его принятия не содержал каких-либо упоминаний сети Интернет. Однако после принятия решения Верховного суда можно говорить о том, что в Соединенных Штатах был создан правовой прецедент, который разрешил людям с ОВЗ подавать в суд на частные компании в случае, если их веб-ресурсы не поддерживают принципы инклюзивности. При этом, несмотря на активную работу как со стороны государства, так и частных компаний, согласно исследованию, проведенному некоммерческим Фондом информационных технологий и инноваций, в 2019 году 92% наиболее популярных в Соединенных Штатах сайтов не соответствовали основным принципам инклюзивности для людей с ОВЗ.

КАНАДА

В Канаде, как и в США, активно обсуждается вопрос сетевого нейтралитета (в Канаде этот процесс начался еще в середине 2000-х годов). В 2005 году один из крупнейших провайдеров Канады Telus заблокировал доступ к сайту Voices for Change, который активно использовался сотрудниками профсоюза работников телекоммуникаций, проводившими в то время забастовку. Вместе с ним Telus заблокировал еще порядка 700 сайтов, никак не связанных с забастовкой, но находящихся на том же сервере. События привели к дискуссии, которая достаточно быстро получила общегосударственный резонанс. Несмотря на то, что первоначально идеи о постепенном внедрении принципов сетевого нейтралитета принадлежали Консервативной партии, со временем последняя начала подчеркивать важность сохранения баланса между защитой прав пользователей в цифровом пространстве и рыночными принципами. Две более левые партии - Либеральная и Новая демократическая - активно отстаивают принципы сетевого нейтралитета. В конечном итоге именно представители Консервативной партии в 2015 году вновь обратились к данному вопросу. Глава правительства страны Стивен Харпер раскритиковал политику провайдеров, заявив, что сам сталкивается с проблемами при использовании, например, такой социальной сети как Twitter. Однако в тот момент стороны ограничились общественной дискуссией о принципах сетевого нейтралитета. В 2017 году, когда пост премьер-министра страны занимал представитель Либеральной партии Джастин Трюдо, принцип сетевого нейтралитета был закреплен законодательно. Провайдерам было запрещено устанавливать ограничения в скорости доступа в зависимости от контента. Эта идея была поддержана самим премьер-министром, который раскритиковал американскую администрацию за отказ от политики сетевого нейтралитета и заявил о высоком значении охраны принципа в Канаде, отметив, что он крайне важен для развития, например, предприятий малого бизнеса.

В Канаде процесс, направленный на расширение инклюзивности Интернета, начался примерно тогда же, когда и в США. Поводом для активизации общественной дискуссии на эту тему также выступило судебное решение: в 2010 году, после рассматривавшегося в течение 5 лет судебного иска, суд обязал правительство Канады сделать доступными государственные сайты для людей с ОВЗ, указав, что невозможность пользоваться сайтами является элементом дискриминации со стороны правительства. Позднее был принят закон, защищающий право граждан с инвалидностью на пользование Интернетом. При этом требования законодательства не идут дальше необходимости предоставления правительством возможности людям с ОВЗ обязательного доступа на государственные сайты федерального значения. В различных канадских регионах обязанности местных правительств варьируются в зависимости от местного законодательства, а само правительство страны не обязывает, например, Интернет-провайдеров создавать отдельные версии своих веб-страниц с доступом для людей с ОВЗ.

БАЗОВЫЕ ПРАВА ЧЕЛОВЕКА

В данном разделе рассматриваются практики иностранных государств, связанные с обеспечением соблюдения в цифровой среде базовых прав человека: права на жизнь, свободу и личную неприкосновенность (ст. 3 Всеобщей декларации прав человека); права на достойное обращение (ст. 5 Декларации); права на защиту от дискриминации (ст. 7 Декларации).

Все рассмотренные государства взяли на себя обязательство защищать данные права в цифровой среде. В ряде стран (например, в Японии, Южной Корее и Австралии) существуют профильные государственные институты, занимающиеся контролем соблюдения прав человека как в онлайн-, так и в оффлайн-среде. В самых разных государствах как на федеральном, так и на региональном уровне (например, США, Япония, Австралия) принимаются законы, направленные на защиту пользователей Интернета от киберугроз. При этом в целом фиксируется тренд постоянного расширения перечня киберпреступлений, происходит кодификация новых форм онлайн-насилия: к традиционно запрещенным мошенничеству и распространению педофильского контента в последнее десятилетие добавились кибербуллинг (например, Австралия) и разжигание ненависти (например, Япония, Австралия, Германия). Наиболее дискуссионным базовым правом человека продолжает быть свобода слова: так, в отношении реализации данного права в цифровом пространстве имеются диаметрально противоположные подходы США и КНР. При этом фактическое осуществление регулирования распространения контента в разных странах различается: в одних странах (например, в Южной Корее и Австралии) власти сами занимаются удалением контента, определяемого ими в качестве незаконного, в других (например, в Германии) делегируют данную обязанность частным компаниям.

ЯПОНИЯ

В Японии базовые права человека (например, право на безопасность, свободу от дискриминации) в Интернете активно защищаются. Действует система онлайн-консультаций по правам человека. В структуре Министерства юстиции Японии функционирует Бюро по правам человека. Каждый человек, проживающий в Японии, вне зависимости от наличия японского гражданства, может обратиться в Бюро, например, в следующих случаях: арендатор квартиры отказывается сдавать жилье из-за национальности квартиросъемщика; нарушение конфиденциальности в Интернете; физическое насилие; жестокое обращение с пожилым человеком или ребенком; сексуальные домогательства; распространение порочащих личность сведений; некорректное поведение соседей (например, шум). Консультации предоставляются как на японском, так и на других языках: английском, корейском, испанском, китайском, филиппинском, португальском. **Подробная инструкция по процедуре обращения размещена на сайте Бюро. Чтобы воспользоваться услугами Консультационной службы по правам человека в Интернете, необходимо отправить электронное письмо с сообщением о нарушении прав человека.** После получения запроса на консультацию автоматически отправляется ответное письмо с текстом *“ваш запрос на консультацию по правам человека получен”* и URL-адресом для более подробного описания обращения. Как правило, рассмотрение запроса занимает несколько дней. В случае крайней необходимости пользователям рекомендуется воспользоваться “Горячей линией по правам человека”, в том числе горячей линией для иностранцев. Ответная реакция Бюро бывает трех типов в зависимости от характера проблемы: 1) электронное письмо; 2) телефонный звонок; 3) личный прием. Таким образом, любой желающий в режиме онлайн может сообщить о любых нарушениях прав человека, в том числе цифровых, и получить подробную консультацию.

Регулирование вопросов прав человека в Интернет-пространстве в Японии также осуществляется и на местном уровне. Так, в 2016 году законодательное собрание города Осака приняло Постановление о борьбе с разжиганием ненависти. Данная инициатива стала ответной реакцией на серию негативных онлайн-публикаций о корейских жителях в городе. В Постановлении поднимается вопрос о публичной идентификации групп, распространяющих ненавистнические высказывания по признаку расы или этнической принадлежности, в том числе в онлайн-среде. Для этого в Осаке был создан специальный комитет, который расследует обвинения в разжигании ненависти, поданные местными жителями. Если комитет решит, что та или иная группа занимается разжиганием ненависти, ее название размещается на сайте города. Однако наказания за такие действия по данному закону не предусмотрено. В первый день вступления закона в силу, корейские жители Осаки подали жалобу на ненавистнические высказывания в адрес этнических корейцев в Интернете.

ЮЖНАЯ КОРЕЯ

Вопросами прав человека в Южной Корее занимается Национальная Комиссия по правам человека к Корее (NHRCK). Комиссия представляет собой независимый политический институт, не принадлежащий ни к одной из ветвей власти. К целям Комиссии относятся установление демократического порядка; защита прав человека; обеспечение коммуникации, построенной на принципе взаимного уважения. Граждане, столкнувшиеся со случаями нарушения своих прав, в том числе в Интернете, могут пожаловаться в Комиссию и получить необходимую юридическую консультацию и помощь. На сайте содержится подробная инструкция о том, как человек может составить жалобу. Жалобы разнообразны: среди них встречаются случаи нарушения конфиденциальности онлайн-данных (например, соглашений, фотографий), запрета на использование электронных устройств. **Деятельность NHRCK не ограничивается конкретными нарушениями, а затрагивает абсолютно все случаи нарушения прав человека**.

Южная Корея уделяет большое внимание онлайн-коммуникациям в целом. **В стране действует Корейская комиссия по коммуникационным стандартам, созданная для *“обеспечения подотчетности общественности и обеспечения справедливости вещательного контента при одновременном продвижении культуры безопасной интернет-коммуникации”*. Основная цель Комиссии заключается в создании безопасной, пользующейся доверием общественности медиасреды.** Комиссия может регулировать содержание интернет-коммуникаций и защищать пользователей и их права.

В 2020 году Комиссия занималась онлайн-контентом, связанным с пандемией COVID-19: удалением фейков и высказываний, направленных на разжигание вражды (в частности, нацеленных на конкретные этнические группы); контролем за медиа, предоставляющими некорректную информацию о лечении COVID-19.

В 2019 году Комиссия приняла решение заблокировать ряд зарубежных веб-сайтов, которые содержали порнографию, пиратский контент или азартные игры, обязав провайдеров (ISP) следить за указанием имени сервера (SNI). После такого решения Комиссии распространилось мнение, что этот шаг может расцениваться как способ ограничения прав человека в цифровом пространстве. Однако, по мнению экспертов аналитического центра New America, южнокорейские власти не используют данную инициативу в качестве ограничительного инструмента, а занимаются блокировкой исключительно незаконных материалов.

КНР

В Китае история регулирования Интернета берет свое начало с конца 90-х годов XX века. **Китай известен своей строгой политикой в отношении онлайн-среды. В 1997 году был принят Уголовный Кодекс КНР, криминализующий киберпреступления.**

На сегодняшний день ключевым документом, определяющим политику КНР в цифровом пространстве, включая вопросы соблюдения прав человека, является Закон об Интернете или так называемая “Белая книга об Интернете” (далее - Белая книга). Наименование законодательных актов Белыми книгами - распространенная практика в Китае. **Белая книга стала первой попыткой Китая изложить свое видение роли Интернета в современной политической системе общества:** *“Китай рассматривает развитие Интернета как важную возможность для активизации своей политики реформ, открытости и модернизации”.* **В документе подтверждается важность Интернета для экономического развития, однако подчеркивается, что Интернет находится под суверенитетом Китая и вопросы национальной безопасности узаконивают регулирование его использования**.

Связь между Интернетом и правами человека стала актуальным для Китая вопросом после того, как Хилари Клинтон в 2010 году включила вопрос о свободе Интернета в международную политическую повестку. **Белая книга рассматривается профильными экспертами как “ответная реакция” на заявление бывшего госсекретаря о важности соблюдения цифровых прав человека. Документ выступает главным законодательным источником понимания цифровых прав человека в Китае**. Он состоит из 6 ключевых пунктов, где подробно расписаны направления развития политики в Сети, а также цифровые права человека. В документе рассматриваются пункты, имеющие непосредственное отношение к соблюдению прав человека в онлайн-пространстве.

Согласно Белой книге, **китайское правительство поощряет и поддерживает развитие информационных коммуникаций в Интернете, предоставляет общественности полный спектр новостей и в то же время гарантирует гражданам свободу слова в Интернете:** *“Граждане Китая в полной мере пользуются свободой слова в Интернете. С правом на свободу слова в Интернете граждане могут высказывать свое мнение различными способами в Интернете. Энергичный обмен идеями в Интернете является основной характеристикой развития Интернета в Китае. Количество постов BBS и статей в блогах намного превосходит таковое в любой другой стране. Деятельность китайских веб-сайтов заключается в предоставлении пользователям Сети услуг по выражению своего мнения”*.

В документе подчеркивается, что Интернет является новым каналом коммуникации между органами власти и гражданами. Интернет обеспечивает прямую реализацию гражданских прав *“знать, участвовать, быть услышанным, контролировать и играть важную роль в деятельности госорганов”*. В заключении данного пункта декларируется, что *“китайское правительство преисполнено решимости неуклонно защищать свободу слова в Интернете, которой пользуются китайские граждане в соответствии с законом”.*

Еще одним направлением политики Китая в Интернете является безопасность несовершеннолетних. Интернет играет все более важную роль в развитии несовершеннолетних, которые являются самой многочисленной группой онлайн-пользователей. Китайское правительство придает большое значение онлайн-безопасности несовершеннолетних и уделяет приоритетное внимание их защите в информационной безопасности Интернета. **Закон Китайской Народной Республики о защите несовершеннолетних предусматривает, что государство принимает меры для предотвращения чрезмерного использования несовершеннолетними Интернета**. В Законе подробно описан запрет производить, продавать, сдавать в аренду или предоставлять другими способами электронные публикации и интернет-информацию, вредную для несовершеннолетних. Китайские власти поощряют исследования и разработку инструментов, способствующих защите несовершеннолетних в онлайн-пространстве, а также интернет-продуктов и услуг, подходящих для несовершеннолетних. В документе подчеркивается, что социальные учреждения должны совместно работать над защитой несовершеннолетних в Интернете и созданием здоровой онлайн-среды для их развития. Китайское правительство активно развивает и продвигает “Программу образования матерей” для содействия родителям в цифровом воспитании детей.

Таким образом, китайские власти активно исследуют каналы и методы эффективного управления Интернетом на законодательном уровне.

АВСТРАЛИЯ

На сегодняшний день Австралия выступает одним из ключевых акторов в определении, соблюдении и продвижении прав человека в Интернете. Интернет-среда в Австралии характеризуется как свободная; инфраструктура информационно-коммуникационных технологий - развитая. Цены на подключение к Интернету - низкие, что обеспечивает доступ значительной части населения к онлайн-среде. Вопросы прав человека в онлайн-пространстве регулируются как государственными органами, так и частными организациями. В Австралии действует группа государственных агентств, занимающихся вопросами прав человека и онлайн-безопасности.

Австралийская комиссия по правам человека является национальным институтом, образованным и финансируемым Правительством Австралии. **Основным источником, затрагивающим цифровые права человека, является Документ по вопросам прав человека и технологий от 2018 года.** В документе анализируются права, которые связаны с Интернетом, искусственным интеллектом и онлайн-средой в целом. Подчеркивается, что защита прав в онлайн-среде (например, свободы слова, собраний в Интернете, конфиденциальности и защиты данных) является трудным процессом по следующим причинам: быстрые темпы изменений в этой области; новые технологии в основном разрабатываются частным сектором и, как следствие, не могут автоматически регулироваться государством; онлайн-среда может исключать определенные группы.

Отдельное внимание уделяется влиянию Интернета и его роли в современной жизни на свободу слова. **Утверждается, что право на свободу выражения мнений включает в себя право доступа к Интернету.** Учитывая огромное влияние, которое научные достижения и технологии оказывают на повседневную жизнь людей, цифровые права предлагается рассматривать наравне с другими гражданскими, политическими, экономическими и социальными правами, включая свободу выражения мнений и право на участие в государственных делах в Интернете. **Права человека в Интернете должны формулироваться и реализовываться с учетом общепринятых правозащитных подходов, в данном случае принципов PANEL: участие, ответственность, отсутствие дискриминации, расширение прав и возможностей, законность.**

Комиссариат по безопасности в Интернете (eSafety Commisioner) - национальное независимое регулирующее агентство безопасности в Интернете Австралии. eSafety был создан в 2015 году с целью координации и руководства политикой по обеспечению безопасности в Интернете со стороны органов государственной власти, бизнеса и некоммерческих организаций. Основная миссия eSafety заключается в *“спасении австралийцев от онлайн-угроз”*. Комиссар по безопасности - Дж.Инман Грант - стремится предоставить всем австралийцам возможность иметь более безопасный и позитивный опыт в Интернете. **eSafety позиционируется как первый и единственный в мире регулирующий орган, стремящийся обеспечить безопасность граждан в Интернете.**

eSafety предоставляет широкий спектр онлайн-программ и ресурсов по обеспечению безопасности для разных групп: детей, родителей, молодых и пожилых людей, женщин, учителей и меньшинств. Одна из основных функций eSafety заключается в борьбе с кибербуллингом и оскорбительным и незаконным контентом. Агентство выступает *“страховочной организацией”* для людей, особенно детей, которые не смогли пресечь онлайн-оскорбления с помощью предоставляемых в социальных сетях инструментов. eSafety активно сотрудничает со службами социальных сетей, помогая противодействовать интернет-травле.

Комиссия определяет формы кибербуллинга, которые могут быть удалены: оскорбительные комментарии; публикация интимных изображений для унижения кого-либо или шантажа; угрозы насильственных действий; случаи злоупотребления чужим аккаунтом в социальных сетях; создание поддельных аккаунтов для преследования и запугивания других; обмен расстраивающими изображениями и видео; установление нежелательных и постоянных контактов с кем-либо в Интернете (например, преследование). **Отдельное внимание уделяется борьбе с вредоносным онлайн-контентом и распространением интимных изображений.** eSafety обладает регулирующими полномочиями для принудительного удаления противоправного контента в Интернете. Каждый гражданин Австралии может пожаловаться на такой онлайн-материал, а также воспользоваться психологической помощью, оказываемая жертвам таких преступлений.

Многие формы кибератак и распространение вредоносного контента могут считаться незаконными в соответствии с законодательством отдельных штатов Австралии или федеральным законодательством. В австралийском Уголовном кодексе 1995 года преступлением является угроза, преследование или причинение вреда, в том числе с использованием дополнительных средств. Это значит, что случаи угрожающего и оскорбительного поведения, осуществляемого с использованием стационарных телефонов, мобильных телефонов (в том числе через MMS, SMS), Интернета, электронной почты и социальных сетей, могут быть признаны незаконными. **Виды травли и ответственность за такие преступления определяется и на региональном уровне.** Например, в штате Виктория действует Закон Броуди, применимый ко всем формам серьезного запугивания, включая кибербуллинг. По Закону случаи травли признаются серьезным преступлением, наказуемым тюремным заключением сроком до 10 лет.

eSafety также занимается другими онлайн-сферами, где пользователи могут потенциально стать жертвами. Каждое направление содержит подробную информацию о том, как безопасно вести себя в той или иной онлайн-среде, а также о действиях в случаях нарушения прав человека. К основным аспектам деятельности eSafety относятся: безопасность электронных устройств; вопросы цифровой репутации; действия против сексуальных домогательств; борьба с онлайн-мошенничеством и кражей персональных данных; пресечение нежелательных онлайн-контактов; защита персональных данных; грамотное поведение в социальных сетях.

Агентство руководствуется Стратегией eSafety 2019-2020. Для реализации основной миссии eSafety фокусируется на 6 областях, каждая из которых подкреплена стратегической целью и реализуется с помощью ряда проверенных тактик и мероприятий:

1. **Профилактика:** профилактика онлайн-нарушений посредством информирования граждан о том, как быть в безопасности в Интернете и куда обратиться за помощью в случаях киберпреступлений;
2. **Сотрудничество:** прочные партнерские отношения с профильными акторами (органы госвласти, частные и некоммерческие организации, академическое сообщество, эксперты, адвокаты);
3. **Продвижение:** медиа-и маркетинговые кампании для повышения осведомленности о проблемах безопасности в Интернете, продвижение тематического контента в социальных сетях, почтовая рассылка, взаимодействие со СМИ;
4. **Программы:** адаптированные программы развития цифровой грамотности для социально уязвимых групп (женщины, подвергающиеся насилию в семье, пожилые);
5. **Защита:** eSafety защищает австралийцев с помощью систем отчетности, расследований и уведомлений. eSafety проводит расследования, собирает разведданные и работает с партнерами для ликвидации незаконного онлайн-контента. eSafety защищает тех, кто страдает от кибербуллинга, борется с оскорбительным и экстремистским контентом, который бросает вызов общественным нормам, стандартам и ценностям и отстаивает права человека в Интернете;
6. **Активные изменения:** осуществление системных изменений с учетом новых технологий для совершенствования онлайн-среды.

В 2020 году из-за перехода многих аспектов социальной жизни в онлайн-пространство количество случаев нарушения онлайн-безопасности увеличилось на 340%. Особое распространение получил онлайн-шантаж с использованием интимных материалов (sextortion). eSafety блокировал такой контент: в среднем, за неделю удалялось в среднем 1000 сообщений. Комиссариат распоряжается об удалении “вредоносного” контента в течение 24 часов. Таким образом, Комиссар по безопасности в Интернете играет ключевую роль в реализации соблюдения прав человека в онлайн-пространстве Австралии.

Австралийский Центр Кибербезопасности (ACSC, далее - Центр) возглавляет усилия австралийского Правительства по повышению кибербезопасности. Основная цель Центра сосредоточена на превращении Австралии в *“самое безопасное место для подключения к Интернету”*. Центр предоставляет консультации, помощь и оперативные меры реагирования органам государственной власти, бизнесу и частным лицам для предотвращения, обнаружения и устранения угроз кибербезопасности как в Австралии, так и за ее пределами. Также в Австралии действует Объединенный Центр Кибербезопасности, который включает в себя более 200 институтов: Центр, частные компании, представителей академического сообщества. ACSC активно сотрудничает с правоохранительными органами в борьбе с киберпреступностью.

Центр проводит различные просветительские кампании для повышения безопасности граждан и организаций в онлайн-пространстве. Например, с 2006 года реализуется программа “Оставайтесь умными онлайн”. Программа предоставляет актуальную и своевременную информацию о том, как пользователи Интернета и малые предприятия могут защитить себя от киберугроз, таких как уязвимость программного обеспечения, онлайн-мошенничество, вредоносные действия в Интернете. На сегодняшний день программа насчитывает почти 100 тыс. активных участников. В целом, политика Центра направлена как на просветительскую деятельность о правилах поведения в цифровом пространстве, так и на мероприятия по устранению киберугроз. Любой желающий может сообщить о киберпреступлении (например, краже личных данных, онлайн-мошенничество, предполагаемом взломе электронного устройства). В настоящее время Центр занимается ликвидацией и пресечением последующих масштабных атак на частные компании Австралии. Кибератаки были вызваны ошибкой Microsoft, которая позволила предполагаемой китайской государственной хакерской группе получить доступ к тысячам корпоративных электронных писем со всего мира.

Австралийская Комиссия по конкуренции и защите прав потребителей (ACCC) отвечает за обеспечение соблюдения Австралийского Закона о конкуренции и защите прав потребителей 2010 года. **Для борьбы со всеми видами мошенничества, в том числе в Интернете, Комиссией была создана платформа Scamwatch. Она предоставляет потребителям и малому бизнесу подробные сведения о том, как распознать мошенничество, избежать его и сообщить о нем.** Согласно статистическим данным Scamwatch за 2020 год, большая доля мошенничеств совершается онлайн: 22% преступлений совершаются с помощью электронной почты, 6,3% - в Интернете, 4,5% - в социальных сетях.

Scamwatch предоставляет информацию о распространенных видах мошенничеств и о том, как распознать и избежать их. К электронным способам совершения подобных преступлений относятся сайты и приложения для онлайн-знакомств и свиданий; интернет-магазины; вредоносные компьютерные программы и программы-вымогатели. Платформа приводит примеры онлайн-мошенничества, а также дает подробные инструкции, как пользователи могут защитить себя. В случае уже произошедшего преступления, пользователь может сообщить об этом и получить соответствующую юридическую помощь. Примером деятельности Scamwatch является действующая кампания против мошенничества с электронной почтой. Австралийцы получают письма, в которых розничный торговец Х.Норман сообщает о выигрыше конкурса и просит предоставить пользовательские данные для получения приза. Scamwatch распространяет копию мошеннического письма и призывает получателей удалить его и сообщать о случаях получения подобных писем.

ЕС

Нормативно-правовая база ЕС по модерации контента в Интернете постепенно становится все более сложной. Директива об электронной коммерции 2000 года содержит базовые принципы, применимые ко всем категориям Интернет-платформ и всем типам контента:

1. **принцип «страны происхождения»** - поставщики онлайн-услуг подчиняются законам государства-члена, в котором они учреждены, а не законодательствам государств-членов, в которых услуга предоставляется;
2. **освобождение от ответственности хостинговых платформ, которые остаются нейтральными и удаляют незаконный контент в Интернете, как только им становится известно о нем**;
3. **поощрение саморегулирования и совместного регулирования контента Интернет-платформами, а также альтернативных механизмов разрешения споров**.

Этот базовый нормативный режим был дополнен в 2018 году пересмотренной **Директивой по аудиовизуальным медиауслугам, которая налагает больше обязательств на видео-хостинговые платформы.** Им следует самостоятельно принимать меры, предпочтительно посредством совместного регулирования, для защиты широкой общественности (и, в первую очередь, несовершеннолетних) от незаконного контента (например, террористический контент, материалы о сексуальном насилии над детьми, риторика ненависти и вражды).

Эти правила усиливаются более строгим законодательством в случае трех типов контента, незаконность которых была зафиксирована на уровне ЕС:

1. **Экстремистский контент.** Директива 2017/541 о борьбе с терроризмом дает определение публичной провокации с целью совершения террористического преступления и требует, чтобы государства-члены принимали меры по удалению и блокировке веб-сайтов, содержащих или распространяющих контент, пропагандирующий терроризм.

   Европейская комиссия стремится пойти дальше - **в настоящий момент обсуждается проект Регламента, который потребовал бы от провайдеров хостинговых услуг проактивно принимать меры по удалению экстремистского контента. Требования Регламента были значительно смягчены в результате двухлетней работы правозащитных организаций.** К примеру, в законе появился пункт, который исключает материалы, распространяемые в образовательных, журналистских, художественных или исследовательских целях, из сферы действия Регламента. Кроме того, обсуждение предотвращения терроризма или борьбы с ним не будет считаться экстремистским контентом. Наконец, в Регламент были внесены смягчающие обстоятельства, позволяющие хостингам избежать ответственности за неудаление террористического контента в течение часа после получения распоряжения.

2. **Детская порнография.** Директива 2011/93 о сексуальном насилии над детьми дает определение детской порнографии и требует государства-члены принимать меры по блокировке и удалению сайтов, содержащих или распространяющих материалы, демонстрирующих сексуальное насилие над детьми.

3. **Риторика ненависти и вражды.** Рамочное решение 2008/913 о борьбе с отдельными формами и проявлениями расизма и ксенофобии посредством уголовного права предусматривает, что государства-члены ЕС должны обеспечить наказание за расистские и ксенофобские высказывания, разжигающие ненависть, но при этом не налагает подробных обязательств, связанных с практикой модерации онлайн-контента.

В ЕС активно ведется дискуссия по поводу способов регулирования контента в социальных сетях, позволяющих соблюдать свободу слова и избегать цензуры; к этому призвали депутаты Европарламента 10 февраля 2021 года. В настоящий момент в ЕС ведется работа над Законом о цифровых услугах (DSA) и Законом о цифровых рынках (DMA) - двумя документами, которые характеризуются как “новая конституция Интернета”. Они будут включать правила для интернет-платформ, а также решения по борьбе с вредоносным или незаконным контентом в Интернете, например дезинформацией.

Заявленная цель DSA заключается в обновлении правовой базы Европейского Союза в отношении незаконного контента, регулирования рекламы и дезинформации. Гражданское общество ранее призывало власти ЕС обеспечить введение четких определений вредоносного контента, чтобы решить проблемы онлайн-насилия, например, “доксинг” (от англ. слова dox, сокр. от documents - систематический сбор публичных и приватных данных какого-либо лица с целью их последующей публикации в Интернете в открытом доступе без разрешения этого лица; эти данные могут быть получены как из общедоступных поисковых систем, таких как Google, и социальных сетей, так и из аккаунтов, взломанных путем фишинга) и гендерное насилие в Интернете, с которыми сталкиваются пользователи в социальных сетях. **DSA введет новые обязательства для платформ по раскрытию регулирующим органам того, как работают их алгоритмы, как принимаются решения об удалении контента и как рекламодатели таргетируют пользователей.** Многие из его положений применимы только к платформам, у которых более 45 миллионов пользователей в Европейском Союзе. Платформы Facebook, YouTube, Twitter и TikTok будут подпадать под новое законодательство. Компании, которые не соблюдают обязательства, рискуют получить штраф в размере до 6% от их годового оборота.

DSA должен улучшить модерацию контента на платформах социальных сетей, придерживаясь правила, что компании, размещающие чужие данные, не несут ответственности за контент, если они действительно не знают, что он нарушает закон. Однако существует значительное исключение из этого правила: как только кто-либо в Интернете отмечает любой контент как потенциально незаконный, требуется, чтобы хостинговая компания “в срочном порядке” удалила или отключила доступ к этому контенту. Таким образом, удаление или отключение помеченного контента становится наиболее коммерчески разумным действием для компаний во избежание риска юридической ответственности. **Как отмечает правозащитная организация EDRi, такой подход может привести к созданию системы контроля контента с произвольными правилами, выходящими за рамки судебного и демократического регулирования.** EDRi подчеркнула, что DSA следует принципу “сначала удаляй, а потом думай”.

ФРАНЦИЯ

С ноября 2020 года представители гражданского общества во Франции регулярно протестуют против принятия Закона о глобальной безопасности. Накануне парламентского голосования по закону в Париже прошли массовые протесты. Тем не менее, 20 ноября 2020 года депутаты двухпалатного Национального собрания проголосовали за принятие документа.

Особенно сильной критике подверглась 24-ая статья законопроекта, предполагающая штрафы за фото- и видеосъемку отдельных полицейских, если распространение этих кадров "*угрожает физической или психической неприкосновенности сотрудников полиции*"; за это правонарушение грозит год тюрьмы или штраф в 45 тыс. евро. Эта статья была включена в текст законопроекта под давлением полицейских профсоюзов, жалующихся на рост насилия в отношении полицейских. Однако журналистские объединения и правозащитники опасаются *"несоразмерного нападения на свободу слова"*. **Резкую критику вызвало еще одно положение законопроекта, согласно которому журналисты должны предварительно зарегистрироваться для освещения демонстрации с места событий.** Еврокомиссия уже высказала свое мнение по поводу новых предписаний, предупредив, что СМИ и "впредь должны свободно выполнять свою работу". **Эксперты ООН призвали Францию полностью пересмотреть предлагаемый новый закон о безопасности, посчитав его "несовместимым" с международным правом и правами человека.**

Голосование верхней палаты парламента, Сената, прошло в марте 2021 года. В результате Закон был принят со значительными изменениями. В частности, была значительно скорректирована 24-ая статья законопроекта, которая касалась проведения фото- и видео-съемки действий полицейских в ходе манифестаций. Новая редакция статьи предполагает создание нового состава преступления: "провокация по установлению личности" с очевидной целью подрыва физической или психической неприкосновенности сотрудника правоохранительных органов. Это изменение было направлено на то, чтобы устранить неопределенность, возникающую в предыдущей редакции статьи относительно свободы информирования.
В дальнейшем обе палаты Национального собрания должны будут согласовать единый текст законопроекта. Если этого сделать не получится, будет организовано новое чтение.

ГЕРМАНИЯ

С 1 января 2018 года вступил в действие немецкий закон “О мерах в отношении социальных сетей” (NetzDG), обязывающий социальные сети удалять контент, подпадающий под определенную характеристику. Закон обязывает крупные сетевые платформы, такие как Facebook, Instagram, Twitter и YouTube, оперативно удалять «незаконный контент», признаваемый таковым по 22 разделам уголовного кодекса. Речь идет о широком круге высказываний: от оскорбления представителей власти до прямых призывов к насилию.

Отмечается, что закон, по сути перекладывающий функции цензоров на администраторов соцсетей, создает опасный прецедент для других государств, которые стремятся ограничить свободу выражения мнений в интернете. По мнению Human Rights Watch, данный закон, обязывающий социальные сети удалять риторику ненависти и вражды и другой незаконный контент, чреват бесконтрольной и неоправданно широкой цензурой и должен быть как можно скорее отменен.

Закон обязывает компании, имеющие в Германии более 2 млн зарегистрированных пользователей, создавать эффективный и прозрачный механизм приема и рассмотрения обращений о незаконном контенте. В течение 24 часов после поступления такого обращения они должны блокировать доступ или удалять «явно незаконный контент», в неоднозначных случаях на решение вопроса дается до недели или даже больше времени. Для самых сложных ситуаций предусмотрена возможность передачи вопроса отраслевому органу, который финансируется компаниями, но при этом утверждается правительством. Этот орган затем должен принять решение в течение семи дней. Предъявляемые к такому органу требования правительством до сих пор не приняты, а в будущем могут в любой момент быть изменены по усмотрению властей.

Компании обязаны информировать пользователей обо всех принимаемых по их обращениям решениях – с мотивировкой, однако **закон не предусматривает реального судебного контроля или обжалования для тех пользователей, которые хотели бы оспорить решение компании или отраслевого органа о блокировке или удалении того или иного поста**.

Закон предоставляет федеральному министерству юстиции и защиты потребителей право штрафовать ответственных лиц на сумму до 5 млн евро, а компании – до 50 млн евро за необеспечение механизма его реализации или за непубликацию дважды в год отчета о его исполнении. Теоретически, размер штрафа зависит от тяжести нарушения и объема пользовательской аудитории, однако соответствующая шкала министерством еще не обнародована.

Правозащитная организация отмечает, что два ключевых аспекта закона нарушают обязательства Германии в области соблюдения свободы слова. Во-первых, **бремя ответственности за квалификацию высказываний третьих сторон возлагается на администраторов той или иной соцсети, причем последняя поставлена в условия, когда ей проще и выгоднее удалить сомнительный контент, чем разбираться с ним**.

Однозначно квалифицировать те или иные высказывания не всегда способен даже суд, поскольку это требует учета нюансов контекста, культуры и права. Компаниям же в условиях жестких временных рамок, которые даются на вынесение решения, и риска подвергнуться крупному штрафу нет большого резона в пограничных ситуациях трактовать сомнения в пользу свободы слова. Во-вторых, **закон не предусматривает ни судебного контроля, ни судебной защиты на тот случай, если администрация соцсети, перестраховавшись, нарушит право человека на свободу слова или на доступ к информации**. Такая ситуация чревата превращением крупных сетевых платформ в «неподконтрольные зоны», где правительство может чужими руками осуществлять цензуру без надзора со стороны судебной власти. В числе пользователей, чьи высказывания были подвергнуты цензуре на основании закона или пользовательского соглашения, оказались один из лидеров правой партии «Альтернатива для Германии», сатирический журнал и уличная художница политической направленности.

Против закона выступили левые, которые голосовали против его принятия, Свободные демократы и "Альтернатива для Германии", которые не были представлены в парламенте на момент его принятия и “Зеленые”, которые воздержались при голосовании. Высокопоставленный член Христианско-социального союза, входящего на момент разработки законопроекта в правящую коалицию, также высказался против закона. **Принятие закона стало причиной создания "Альянса за свободу слова", куда вошли представители промышленных объединений, ассоциации журналистов, сетевые активисты и правозащитники**. Со временем из-за широкой общественной кампании против закона он был частично смягчен. Например, были отменены первоначально запланированные фильтры содержимого и выгрузки.

Однако, по мнению экспертов, сформулированному в комплексном докладе о состоянии прав человека в Германии Grundrechte-Report 2018, косметические изменения не решают фундаментальных проблем, связанных с данным законом.

Важной составляющей противодействия нарушению прав человека в Германии является информационная работа. Так, при поддержке немецкого правительства функционирует сайт HateAid.org, предоставляющий информационную поддержку лицам, пострадавшим от разнообразного насилия в интернете. На ресурсе размещаются материалы о связанных с дигитализацией специфических угрозах для прав человека. Как наиболее уязвимые отмечаются право на свободу личности (12 статья Всеобщей декларации прав человека), право на свободу от дискриминации (2 статья); право на свободу мирных собраний и ассоциаций (20 статья), принцип равенства (1 статья).

На ресурсе размещаются тематические материалы о тех или иных типах дигитальных угроз. В частности, отдельно рассматриваются оскорбления/травля; клевета и такое явление как доксинг. Так, в 2019 году доксинг затронул многих общественных деятелей в Германии. Личные адреса, номера телефонов и адреса электронной почты целого ряда немецких знаменитостей оказались в открытом доступе. В некоторых случаях доксинг сочетается с деаномизацией, из-за чего опасность возрастает. Советы, которые HateAid приводит для борьбы с доксингом традиционны и не отличаются от типовых советов сетевой гигиены: регулярная смена паролей, ограничение объема личных данных, размещаемых в открытом доступе. Также эксперты портала призывают пользователей, столкнувшись с доксингом, отправлять соответствующие жалобы администрации социальных сетей. На портале имеется форма обратной связи, позволяющая пользователям, пострадавшим от доксинга, получить бесплатную консультацию от экспертов. Пользователи, пострадавшие от травли или клеветы, также могут получить консультацию на сайте.

США

Соединенные Штаты принимают активное участие в работе различных международных организаций, чья деятельность направлена на защиту прав и свобод в Интернете, в том числе Freedom Online Coalition. **В отличие от многих других стран в США нет единого определенного закона о защите свободы слова в цифровом пространстве: свобода слова, в том числе в Интернете, там защищается первой поправкой к Конституции**. При этом оценки уровня свободы в американском Интернет-пространстве расходятся: так, правозащитная организация Freedom House неоднократно характеризовала Интернет в стране как “свободный”, а организация “Репортеры без границ” в 2014 году добавила США в список “врагов Интернета”, в котором, среди прочего, находятся такие государства, как КНДР и Исламская Республика Иран.

В Соединенных Штатах еще с середины 1990-х периодически появляются различные законодательные инициативы, направленные на регулирование Интернета. Первыми такими законами, действующими и в настоящее время, стали Закон о борьбе с распространением детской порнографии и Закон о борьбе с мошенничеством в Интернете (он же Computer Fraud and Abuse Act - CFAA), устанавливающий ответственность за компьютерный шпионаж; несанкционированный доступ к информации; компьютерное мошенничество; умышленное или неумышленное повреждение защищенных компьютеров; угрозы, вымогательство, шантаж, совершаемые с использованием компьютерных технологий.

Тем не менее, большое количество законопроектов, которые были направлены на защиту прав пользователей, так и не получили развития и не были приняты. Так, в 2006 году активно обсуждался, но не был принят акт “Об удалении онлайн-хищников”. Целью законопроекта была защита детей от педофилов и угрожающей психике информации, он предполагал введение строгих ограничений для школ и библиотек, в частности, практически полностью блокировался доступ к любым социальным сетям и мессенджерам. Данный законопроект вызвал опасения со стороны общественности, что в результате его принятия будут значительно ограничены не только “небезопасные сайты”, но и большая часть Интернет-пространства, в том числе ресурсы, предоставляющие важную образовательную информацию. В частности, отмечалась чрезвычайная абстрактность формулировок законопроекта, оставляющая пространство для широкого произвольного толкования.

КАНАДА

Согласно исследованию Freedom House, в рейтинге свободы Канада опережает США (87 баллов против 76).

При обзоре канадского опыта необходимо затронуть аспект работы с экстремистским контентом в Интернете. Данный вопрос начал активно обсуждаться в Канаде после теракта в мечети Крайстчерча в Новой Зеландии, результате которого погиб 51 человек. Вскоре после теракта, министр общественной безопасности и чрезвычайных ситуаций Канады Ральф Гудэйл заявил о том, что правительство будет требовать от социальных медиа удаления экстремистского контента, разжигающего ненависть. Несмотря на то, что Гудэйл заявил о необходимости разработки полноценного набора инструментов, которые позволили бы пресечь распространения подобного контента еще до его публикации, никаких реальных мер предпринято не было. Как отмечают в том числе противники удаления подобного контента, **власти Канады мало вмешиваются в работу социальных сетей, которые по большей части сами занимаются удалением контента, который опознают как не соответствующий правилам**. Тем не менее, согласно данным одного из канадских VPN-сервисов, который провел опрос относительно свободы в Интернете, 23% участников опроса заявило о том, что они так или иначе лично сталкивались с Интернет-цензурой, еще 30% считают, что у правительства существуют способы ограничения свободы слова в Интернет-пространстве.

Специфическим является канадское законодательство в отношении распространения клеветы в Интернете. Еще в 2011 Верховный суд Канады постановил, что **за размещение ссылки на материал, в котором содержится дискриминирующая кого-либо информация, пользователь не может быть привлечен к ответственности**.

ПРАВО НА НЕПРИКОСНОВЕННОСТЬ ЧАСТНОЙ ЖИЗНИ

В данном разделе рассматриваются практики иностранных государств, связанные с обеспечением в цифровом пространстве права на неприкосновенность частной жизни (ст. 12. Всеобщей декларации прав человека).

В первую очередь в цифровом пространстве данное право связано с проблемой конфиденциальности/анонимности. Широко конфиденциальные данные можно определить как любую относящуюся к субъекту данных информацию, которую можно использовать прямо или косвенно для его определения (широкие трактовки данного понятия используются, например, в ЕС и США). Преобладает подход, рассматривающий защиту конфиденциальности как одно из средств повышения у пользователей ощущения безопасности и уверенности при использовании Интернета. Дискуссионным вопросом, связанным с проблемой конфиденциальности, является т.н. “право на забвение”. В частности, отмечается, что данное право может быть использовано для сокрытия нарушений других прав человека.

Расширение политики защиты конфиденциальных данных пользователей влечет за собой значительные издержки, как экономические, так и связанные с национальной безопасностью, что продемонстрировало, например, введение в ЕС Общего регламента защиты персональных данных (GPDR).

КНР

В Белой книге Интернета рассматриваются вопросы конфиденциальности и неприкосновенности частной переписки. Свобода граждан в онлайн-среде охраняется законодательно, при этом закреплено, что она ограничена интересами государства: при осуществлении свобод, гражданам не разрешается посягать на государственные, общественные и коллективные интересы или законные свободы и права других граждан. Это также распространяется на отдельные институты: ни одна организация или юридическое лицо не вправе использовать Интернет для осуществления деятельности, угрожающей государственной безопасности, общественным интересам или законным правам человека.

Защита конфиденциальности в Интернете тесно связана с чувством безопасности и уверенности людей в Интернете. Китайские власти занимаются совершенствованием соответствующего законодательства и правил корпоративного обслуживания в Интернете для постоянного развития системы защиты конфиденциальности в Интернете. Решением Постоянной комиссии Всекитайского Собрания народных представителей по охране интернет-безопасности предусмотрено, что незаконный перехват, подделка или удаление чужой электронной почты или иных данных, а также посягательство на свободу и неприкосновенность частной переписки граждан, составляющее преступление, подлежат уголовной ответственности.

ЮЖНАЯ КОРЕЯ

Право на неприкосновенность частной жизни тесно связано с проблемой сетевой анонимности.

Южная Корея стала первым государством, внедрившим сетевую систему реального имени. Такая система подразумевает, что пользователь может зарегистрировать учетную онлайн-запись (например, в социальной сети, на веб-сайте), используя свое официальное имя. Интернет-система реальных имен предусматривала, что онлайн-платформы со 100 тыс. ежедневных посетителей должны регистрировать только достоверные сведения о пользователях. В качестве верификации использовались регистрационные номера пользователей. Идея заключалась в том, что данные пользователей могут быть раскрыты, если жертвы вредоносных сообщений захотят подать в суд за клевету и/или нарушение конфиденциальности. Предполагалось, что количество негативной информации, публикуемой в Интернете, будет минимизировано, а пользователи будут осознавать ответственность за поведение в онлайн-среде. Разработка и внедрение такой системы стала ответной реакцией южнокорейского правительства на увеличившиеся случаи кибербуллинга и резкого роста числа самоубийств на этом фоне.

Однако инициатива вызвала широкое общественное осуждение. Система реальных имен подверглась критике со стороны пользователей сети, правозащитных организаций и Национальной комиссии по правам человека Кореи. Данная система также привела к конфликту с глобальными IT-компаниями. В 2009 году видеохостинг YouTube отказался выполнять предписанные южнокорейскими властями требования.

В 2012 году Конституционный суд Кореи единогласно постановил, что система реальных имен является неконституционной и нарушает свободу слова в Интернете. Интернет-система реальных имен была полностью отменена. **Конституционный суд заключил, что система не принесла пользы обществу, так как количество негативных сообщений в Интернете не уменьшилось.** Вместо этого пользователи перешли на иностранные сайты, а система стала носить дискриминационный характер по отношению к онлайн-пользователям. Система также мешала иностранцам, у которых не было регистрационного номера резидента, выражать свое мнение на корейских интернет-платформах.

АВСТРАЛИЯ

Управление Комиссара по информации (OAIC) является австралийским независимым национальным регулирующим органом, занимающимся вопросами конфиденциальности. К основным областям Управления относятся конфиденциальность, свобода информации и государственная информационная политика. Сфера деятельности OAIC включает в себя: расследование жалоб на нарушение конфиденциальности и свободы информации; принятие нормативных мер против нарушений конфиденциальности; предоставление консультаций и рекомендаций организациям и сообществу по вопросам защиты личных данных. Управление Комиссара по информации осуществляет контроль за соблюдением Закона о конфиденциальности 1988 года, Закона о свободе информации 1982 года и других законодательных актов при обработке личной информации австралийскими правительственными учреждениями и частными организации с годовым оборотом более $3 млн.

Комиссар по информации, как и другие упомянутые государственные институты, занимается просветительской деятельностью. Управление предоставляет подробную информацию о возможных действиях по защите конфиденциальности информации для пользователей социальных сетей, детей, а также всех жителей Австралии. В 2020 году OAIC инициировало первое гражданское взыскание за вмешательство в частную жизнь и открыло 11 инициированных Комиссаром расследований случаев нарушения свободы информации. Также Комиссариат рассмотрел 2,5 тыс. частных жалоб на нарушение конфиденциальности в Интернете.

УРУГВАЙ

С правом на приватность (неприкосновенность частной жизни) тесно связано т.н. право на забвение.

22 января 2020 года Национальная партия Уругвая опубликовала на своем сайте проект “срочного закона”. Конституция Уругвая позволяет президенту предлагать срочные законы, которые автоматически принимаются, если они не отклоняются или не заменяются после кратких дебатов (не более 90 дней) в законодательных органах.

Среди сотен положений проекта находится “право на забвение”, которое позволит людям, которые находят в Интернете информацию о себе, которую они считают *“неадекватной, неточной, устаревшей или чрезмерной”*, просить поисковые системы удалить ее в соответствующих результатах поиска. В законопроекте говорится, что характер информации и общественный интерес будут приниматься во внимание, но не уточняется, как это будет работать или кто будет предотвращать возможные правонарушения.

Этот проект вызвал беспокойство в гражданском обществе и среди журналистов. В частности, международная НКО Комитет защиты журналистов (Committee to Protect Journalists, CPJ) заявила, что возможность удаления личной информации из Интернета может ослабить “*один из самых мощных исследовательских инструментов журналистики*” и “*наносит вред журналистам, позволяя цензуру ссылок на их работу*”.

ЧИЛИ

В Чили широко известным делом, в ходе которого было подтверждено право граждан на забвение, стал процесс Surgeon v. Court of Appeals of Santiago от 2019 года. В 2009 году чилийский хирург был приговорен к 61 суткам тюремного заключения и выплате компенсации за смерть пациента в результате врачебной халатности. Несколько СМИ опубликовали информацию об этом деле на своих цифровых порталах. Врач отбыл наказание и выплатил соответствующую компенсацию, а в 2018 году потребовал удалить статьи из интернет-СМИ. Просьба была отклонена СМИ, а впоследствии и судом первой инстанции. Верховный суд, рассмотрев дело, счел, что опубликованная в СМИ информация представляет общественный интерес. **Чтобы достичь баланса между правом на информацию и правом на забвение, Верховный суд Чили обязал СМИ обновить публикации, указав, что хирург понес наказание согласно приговорам и выплатил необходимые компенсации.**

АРГЕНТИНА

16 июня 2020 года Федеральная уголовно-исправительная палата (Cámara Criminal y Correccional Federal) Аргентины отменила постановление мирового судьи, предписывающее Google не индексировать определенные URL-адреса, связанные с прошлым истца - Энрике Сантоса. Данное дело является прецедентным и имеет силу источника права.

Иск был подан Энрике Сантосом Каррио из-за серии статей, в которых утверждалось, что он был арестован в Мексике за хранение оружия и наркотиков, а также за предполагаемую связь с наркокартелями. Он также является сыном Элизы Каррио, важной политической фигуры в Аргентине. Статьями поделились более 24000 раз на Facebook.

14 марта 2019 года мировой судья предписал Google удалить из индексации URL-адреса, связанные с арестом Энрике Сантоса на том основании, что они являются ложными. Однако **в апелляции компания Google ответила, что постановление суда затрагивает информацию, доступную также в других странах, и, следовательно, нарушает принцип государственного суверенитета.** Федеральная уголовно-исправительная палата согласилась с аргументами Google и подтвердила, что предыдущий вердикт суда повлиял на домены и услуги, подпадающие под действие иностранного права. **Тем самым он не только нарушает национальные законы других стран, но также заявляет, что аргентинский суд имеет право определять контент, который находят и читают в Интернете люди по всему миру.** Следовательно, такое постановление - серьезное вмешательство в свободу слова и право искать, получать и распространять информацию свободно.

БРАЗИЛИЯ

Другим резонансным решением, связанным с правом на неприкосновенность частной жизни, стало решение Верховного суда Бразилии от 7 мая 2020 года, которое приостановило **выполнение президентской Временной меры No. 954/2020, согласно которой телефонные операторы были обязаны предоставлять все данные о своих абонентах бразильской государственной службе статистики.** В 2020 году национальная перепись населения Бразилии была прервана пандемией COVID-19, и личные опросы были приостановлены. Бразильский статистический институт (Instituto Brasileiro de Geografia e Estatística, IBGE) решил перейти на телефонные интервью. По его запросу президент Жаиру Болсонару принял Временную меру No. 954/2020, обязывающую телефонных операторов предоставлять IBGE все данные абонентов (включая имена, номера телефонов и адреса) в течение семи дней после запроса. Однако Бразильская ассоциация адвокатов оспорила эту меру, заявив, что она нарушает конституционные гарантии - право на неприкосновенность частной жизни, конфиденциальность сообщений и частной жизни. **Суд постановил, что в законодательном акте не были прописаны достаточные меры по защите данных и прозрачности их использования.**

ЕС

В Евросоюзе преобладает универсальный подход к защите персональных данных во всех сферах, предполагающий унификацию норм права ЕС для государств-членов.

Право на защиту персональных данных закреплено, в частности, в ст. 8 Хартии Европейского Союза об основных правах (от 2000 г.):

1. Каждый человек имеет право на защиту относящихся к нему данных личного характера;
2. Обработка подобных данных должна производиться в четко определенных целях, с согласия заинтересованного лица либо при наличии других правомерных оснований, предусмотренных законом. Каждый человек имеет право на получение доступа к собранным в отношении него данным, и право на устранение в них ошибок;
3. Соблюдение этих правил подлежит контролю со стороны независимого органа.

Также о праве на защиту персональных данных физических лиц говорится в ст. 16 Договора о функционировании Европейского союза. При осуществлении любого рода деятельности институты ЕС, а также государства – члены Союза обязаны заботиться о защите персональных данных как в аналоговом, так и в цифровом виде.

В 2016 году Европейский парламент и Совет Европы приняли Общий регламент защиты персональных данных (GDPR). Сам Регламент GDPR представляет собой документ объемом 88 страниц (в официальном издании на английском языке) и состоит из вводной части и 99 статей, распределенных по 11 главам. Статья 1 Регламента отражает главный принцип, которым руководствуется ЕС в проведении политики защиты персональных данных: ***“для обеспечения согласованного и высокого уровня защиты физических лиц и устранения препятствий для движения потоков персональных данных в рамках Союза, уровень защиты прав и свобод физических лиц в отношении обработки таких данных должен быть одинаковым во всех государствах-членах”***.

Под действие Регламента подпадают все “субъекты персональных данных” в ЕС, находящиеся на территории ЕС, например, граждане стран союза, их резиденты, субъекты, пребывающие в ЕС на основании виз, беженцы. **GDPR имеет экстерриториальное действие - правила распространяются и на зарубежные компании, работающие с данными резидентов ЕС**.

С момента принятия GDPR законодательство ЕС по защите персональных данных является наиболее полным и строгим в мире. Его особенностью является **широкое трактование понятия персональных данных как любой информации, относящейся к физическому лицу или "субъекту данных", которая может быть использована прямо или косвенно для его определения.** Примерами являются данные об отпечатках пальцев, генетические и биометрические данные, информация о расовой принадлежности, семье, религиозных взглядах, философских воззрениях, о доме и работе, сексуальной ориентации и личной жизни, о здоровье, поведенческих моделях и используемых устройствах.

GDPR значительно расширяет права субъектов по контролю за их персональными данными. Европейские пользователи имеют право запрашивать подтверждение факта обработки их данных, место и цель обработки, категории обрабатываемых персональных данных, каким третьим лицам персональные данные раскрываются, период, в течение которого данные будут обрабатываться, а также уточнять источник получения организацией персональных данных и требовать их исправления. Более того, пользователь имеет право требовать прекращения обработки и переноса своих данных. Последнее право заключается в том, что компании обязаны бесплатно предоставлять электронную копию персональных данных другой компании по требованию самого субъекта персональных данных.

Процесс внедрения GDPR европейскими компаниями оказался крайне долгим и сложным: спустя полтора года после вступления Регламента в силу лишь около трети представителей опрошенных компаний утверждали, что соблюдают его. Особенно проблематичным соблюдение Регламента оказалось для малого бизнеса. **Среди 716 опрошенных в мае 2019 года (спустя год после вступления GDPR в силу) руководителей малого бизнеса в ЕС около половины не были полностью уверены, что соблюдают положения Регламента. При этом малые предприятия вынуждены вкладывать значительные средства в соблюдение GDPR**: более половины опрошенных сообщили о расходах от 1000 до 50.000 евро.

Исключения из GDPR относятся, в основном, к сфере национальной и общественной безопасности, защите независимости судебной власти, а также обеспечению соблюдения норм гражданского права. Отмечается, что исключения должны уважать право граждан на защиту данных и быть необходимой и соразмерной мерой.

Европейский суд даровал европейцам "право на забвение" в решении 2014 года, которое касалось иска гражданина Испании Гонсалеса в отношении материалов о нем в поисковике Google. Согласно этому решению, поисковики должны удалять "неадекватную, не соответствующую или больше не соответствующую действительности" информацию, если любой гражданин обратится к ним с такой просьбой. К сентябрю 2019 года компания Google получила 845501 запрос на удаление и удалила 45% от 3,3 млн ссылок, которые пользователи просили удалить.

Кроме того, GDPR с 2018 года дает каждому жителю ЕС право требовать, чтобы **не только поисковые машины, но и любые другие компании не выдавали ссылки с касающейся его "*устаревшей информации личного характера, если она не имеет общественной значимости*"**. Чтобы добиться удаления из интернета какой-либо информации о себе, жителям ЕС необходимо письменно или устно обратиться в компанию, ответственную за распространение информации. У той есть месяц на изучение проблемы. В настоящее время эта норма действует также в Швейцарии, Лихтенштейне, Норвегии и Исландии. Причинами для отказа в удалении информации могут стать, например, законные обязательства по обнародованию информации, соблюдение права на свободу слова или важность информации для научных исследований. Несогласие с отказом удалить информацию заявитель может оспорить в суде.

GDPR Великобритании дополнительно выделяет обстоятельства, при которых право на удаление не будет применяться:

1. если обработка необходима в целях общественного здравоохранения;
2. если обработка необходима в целях профилактической или профессиональной медицины; для трудоспособности работника; для медицинской диагностики; для оказания медицинской или социальной помощи; или для управления системами или услугами здравоохранения или социальной помощи. Это относится только к тем случаям, когда данные обрабатываются или находятся под ответственностью специалиста, на которого распространяется юридическое обязательство сохранять профессиональную тайну (например, медицинского работника).

Вопрос соблюдения свободы слова в Интернете в рамках европейского данного законодательства остается сложным. "*В подобных случаях важно соблюдать равновесие между общественным интересом и правом на защиту личных данных*", - отметил глава представительства организации "Репортеры без границ" в Германии К. Мир. Он также подчеркнул, что "*обращения граждан с требованием удалить ссылки на ту или иную информацию о них рассматривает не суд, а специально созданная в каждом отдельном государстве комиссия экспертов при концерне Google*".

Представители компании Google в 2019 году заявили, что правом на забвение могут злоупотреблять авторитарные правительства, пытающиеся скрыть нарушения прав человека.

Также продолжается дискуссия, вызванная тем, что право на забвение, обеспечивая удаление персональных данных, собранных частными компаниями, работающими в сфере социальных сетей, телекоммуникаций, медицины, финансов и науки, усложняет работу спецслужб. Ранее эти данные были доступны государственным учреждениям без ограничений или при наличии ордера, судебной повестки или постановления суда. Осложняется также работа европейских спецслужб, в основном использующих методы разведки с открытым исходным кодом (OSINT) (например, Европола и Разведывательного и ситуационного центра Европейского союза (EU INTCEN)). **Скрывая цифровой след персональных данных, законодательство о праве на забвение может оказать помощь террористам в деле уклонения от спецслужб**.

США

Учитывая особенности государственного устройства США, инициативы по защите данных Интернет-пользователей принимаются чаще всего на региональном уровне. Самым ярким примером стал принятый штатом Калифорния в 2018 году закон California Consumer Privacy Act (CCPA) о защите персональных данных интернет-пользователей, который активно обсуждался в медиапространстве и был охарактеризован в СМИ как один из самых "*жестких*" подобных законодательных актов в стране. Причина, по которой подобный закон появился в Калифорнии, понятна: в этом штате расположены штаб-квартиры крупнейших технологических гигантов Google и Apple. Профильные НКО, которые занимаются защитой прав граждан в Интернете, положительно восприняли новость о принятии подобного законодательства. Джеймс Стейр, основатель некоммерческой правозащитной организации в области медиа и технологий Common Sense Media, отметил: "*Наконец-то у нас появился настоящий закон. Это победа для каждого гражданина Соединенных Штатов*". Представительница другой некоммерческой организации CALPRIG Эмили Раш отметила, что принятие подобного закона улучшает положение потребителей не только в одном из американских штатов, но и во всем мире. Профильное издание ExchangeWire и вовсе назвало новый закон "*первым шагом к абсолютно новому пониманию безопасности информации в Америке*" и "*концом дикого Запада в сфере данных*".

Сам закон достаточно широко трактует понятие персональных данных, определяя их как любую информацию, которая идентифицирует (относится, описывает, характеризует прямо или косвенно) конкретного потребителя, а именно:

- Реальные имена или псевдонимы;
- Почтовые адреса;
- Имена аккаунтов;
- Номера карточек социального обеспечения, водительских прав и паспортов;
- Списки покупок товаров или услуг;
- Биометрические данные (рост, вес, отпечатки пальцев);
- Геолокация;
- Профессиональная информация (история трудоустройства);
- Информация об образовании, которая не является общедоступной.

В соответствии с законом, вступившим в силу с 1 января 2020 года, пользователи получают право знать, какую именно и зачем персональную информацию собирают компании, а также как они намереваются использовать полученные данные. Важным аспектом является также вопрос, кому продаются или передаются данные пользователей. Закон обязывает Интернет-ресурсы позволять пользователю формально запрещать компаниям продажу своих данных, указав этот запрет в пользовательском соглашении. Пользователь младше 16 лет должен отдельно согласиться на продажу своих данных. При этом необходимо отметить, что термин "*продажа*" в законе не обозначает непосредственно передачу какой-либо информации за деньги. Он подразумевает еще и обмен какой-либо конфиденциальной информацией в обмен на предоставление каких-либо других услуг (например, обмен конфиденциальными данными пользователей между различными Интернет-компаниями или сервисами). Пользователи также получили право обращаться к компаниям с запросами, откуда они получили те или иные данные, причем закон подразумевает, что компании должны создать рабочие инструменты, с помощью которых пользователи могут запросить подобную информацию (например, специализированные веб-страницы и бесплатные телефонные номера). Через эти сервисы пользователи должны иметь возможность запрашивать у компаний удаление полученной ранее персональной информации. Наконец, **важным аспектом является прямой запрет на какую-либо дискриминацию пользователей на основании полученных данных**. На основании этих данных компании не могут отказывать в каких-либо товарах или услугах, назначать разные цены или предоставлять другим потребителям товары или услуги иного качества. **Компании не могут дискриминировать пользователей, отказавшихся предоставить свои персональные данные, но при этом закон допускает возможность введения системы поощрений для тех, кто согласился это сделать**.

В случае нарушения какого-либо положения закона потребители имеют право предъявить иск к Интернет-компании. Как отмечается в СМИ, после того как закон вступил в силу, в Калифорнии началось несколько крупных судебных разбирательств, подобные иски были преимущественно коллективными. При этом нельзя сказать, что итог подобных разбирательств предрешен. Например, одно из самых известных разбирательств "Каллен против Zoom", начавшееся в марте 2020 года, продолжается и в данный момент, а иск "Рахтман против Marriott International", предметом разбирательства в рамках которого стала претензия истца, что злоумышленники в результате утечки получили доступ к базам данных гостей отелей, был отклонен. Калифорнийский суд отказал истцу в удовлетворении иска, отметив, что в результате утечки данных важные данные гостей сети (такие как номера карт социального страхования, информация о кредитных картах или пароли) не были скомпрометированы.

После принятия закона в Калифорнии началось активное обсуждение схожих законодательных актов в других американских штатах. Еще до того, как CCPA вступил в силу, компания Microsoft заявила, что поддерживает распространение CCPA на территорию всех Соединенных Штатов, компания Mozilla и вовсе объявила, что основные положения калифорнийского закона будут распространяться на всех пользователей их продукции, и клиенты, например, смогут потребовать удаления той или иной информации, полученной через продукты компании. На данный момент нет инициатив по созданию подобного законодательства на федеральном уровне, однако такие штаты, как Вашингтон, Иллинойс, Нью-Йорк, Небраска, Вирджиния и Флорида, занимаются разработкой законов, схожих с CCPA. Большинство из данных инициатив могли быть приняты еще в 2020 году, но из-за пандемии коронавирусной инфекции сроки их принятия сдвинулись.

В 2018 году в США был принят так называемый CLOUD Act (Clarifying Lawful Overseas Use of Data Act), который значительно расширил возможности правоохранительных органов Соединенных Штатов в отношении доступа к частной информации в Интернете. После принятия данного закона правоохранительные органы впервые получили право запрашивать у IT-компаний доступ к данным, вне зависимости от того, где эта информация хранится, включая, в том числе и другие страны. Кроме того, положения закона дают государству возможность вступать с другими странами в особые соглашения, связанные с обменом данными. В рамках этих соглашений третьи страны могут запрашивать данные пользователей у американских IT-компаний, при условии, что они не являются гражданами США и не проживают на их территории.

Несмотря на то, что крупнейшие IT-компании (среди которых Microsoft, Google, Facebook, Apple) заявили о полной поддержке закона и даже выпустили совместное письмо, в котором назвали принятие акта “*заметным прогрессом в сфере защиты прав потребителей*”, множество правозащитных организаций раскритиковали закон. В частности, критики указывают на то, что при выдаче Соединенными Штатами переписок гражданина другого государства США фактически раскрывают сообщения всех задействованных в переписке лиц, а не только тех, информация о которых была запрошена. Кроме того, критики данного закона отмечают, что согласно его положениям правоохранительные органы США получают право без каких-либо дополнительных согласований, ордеров или судебных предписаний получать доступ к частной переписке граждан, в чем критики закона усматривают нарушение четвертой поправки к Конституции, запрещающей проведение произвольных обысков и арестов.

Еще в 2008 году в “Закон о наблюдении за иностранной разведкой” была внесена важная новация, которая дала право американским спецслужбам без санкции суда прослушивать телефонные разговоры и просматривать электронную переписку между иностранными гражданами, находящимися за пределами США, но использующими американские спутниковые каналы, узлы связи или Интернет-серверы. В 2018 году действие этого положения было продлено Конгрессом сроком еще на 6 лет. Как отмечают критики закона, он не только предоставляет американскому государству право читать переписку иностранных граждан, но также позволяет читать переписку собственных граждан, если они контактируют с иностранцами, которые находятся в поле зрения разведки. Еще на стадии принятия данный законопроект рассматривался как акт вмешательства в личную жизнь миллионов человек по всей планете, в частности, известный предприниматель Тимоти Феррис сравнил принятые поправки с расширением прав специальных служб США “*до уровня Штази*”. Иск, который против данного закона подала правозащитная организация Amnesty International, в конечном итоге дошел до Верховного суда, судьи которого в 2013 году поддержали правительство США, заявив, что предположения истцов, что переписка любого гражданина США может быть прочитана спецслужбами, является беспочвенной и основанной “*на домыслах*”. Продление действия закона в 2018 году вновь вызвало негативную реакцию со стороны правозащитных организаций. Совсем недавно, после назначения на пост нового генерального прокурора (в администрации Джо Байдена) Меррика Гарланда Американский союз защиты гражданских свобод призвал его приложить усилия к отмене действующей поправки.

ПРАВО НА СВОБОДНЫЙ ДОСТУП К ИНФОРМАЦИИ И ЕЕ РАСПРОСТРАНЕНИЕ

В данном разделе рассматриваются практики иностранных государств, связанные с правом на свободу искать, получать и распространять информацию (ст. 19 Всеобщей декларации прав человека). В первую очередь это право связано с ограничениями распространения той или иной информации в Интернете, осуществляемым как государствами, так и IT-гигантами.

Хартия прав человека и принципов в Интернете от 2011 года, подготовленная Коалицией по правам и принципам в Интернете, в качестве ориентира провозглашает принцип сетевого равенства в отношении информации: каждый человек должен иметь открытый доступ к контенту Интернета, свободный от дискриминационного определения приоритетов, фильтрации или контроля трафика по коммерческим, политическим или иным основаниям. Можно констатировать, что в действительности этот принцип соблюдается не всегда. В большинстве стран так или иначе имеется разной степени жёсткости система регулирования распространения информации.

В последние годы одним из наиболее популярных обоснований функционирования подобных систем является необходимость противодействия распространению дезинформации (фейков). При этом трактовка понятия “фейк” отличается значительной произвольностью: так, в некоторых странах (например, в Сингапуре или Таиланде) под фейком помимо прочего понимается информация, которая может навредить имиджу государственных институтов.

Помимо государств в качестве угрозы праву на свободный доступ к информации выступают крупные IT-компании. Кейс конфликта австралийского правительства с Facebook продемонстрировал, что IT-гиганты, преследуя свои коммерческие интересы, готовы идти на прямую конфронтацию с национальными правительствами, в качестве инструмента давления используя блокировку доступа рядовых пользователей к тому или иному виду контента.

СИНГАПУР

Принятый в 2019 году Закон о защите от онлайн-лжи и манипуляций (Protection from Online Falsehoods and Manipulation - POFMA) значительно расширил степень государственного контроля над распространением онлайн-контента. Закон направлен на предотвращение распространения в интернет-пространстве Сингапура ложных заявлений о фактах; защиту от использования онлайн-аккаунтов для распространения ложных сообщений и манипулирования информацией; принятие мер по повышению прозрачности политической рекламы в Интернете. **Целями Закона POFMA являются:**

- предотвращение сообщений с ложными утверждениями о фактах и обеспечение возможности принятия мер по противодействию распространения таких сообщений;
- пресечение финансирования, продвижения и иной поддержки онлайн-сайтов, распространяющих ложные сообщения;
- обеспечение возможности реализации деятельности по выявлению, контролю и защите от злоупотреблений онлайн-аккаунтами и ботами;
- принятие необходимых мер для расширения раскрытия информации, касающейся платного контента, направленного на достижение политических целей.

В документе вводятся разные понятия, связанные с темой распространения онлайн-лжи. Так, утверждение считается ложным, если оно *“ложно или вводит в заблуждение, полностью или частично, само по себе или в контексте, в котором оно фигурирует”*. Под неаутентичным онлайн-аккаунтом понимается *“аккаунт, который контролируется лицом, отличным от лица, представленного (профиль пользователя, уникальный идентификатор или другая информация) в качестве его владельца; такая подмена сделана с целью введения в заблуждение пользователей относительно личности владельца”*. Бот в документе представляется как *“компьютерная программа, созданная или измененная с целью выполнения автоматизированных задач”*. **Вся деятельность в рамках Закона осуществляется “в интересах общества”** (например, в интересах безопасности Сингапура; в интересах дружественных отношений Сингапура с другими странами; с целью не допустить разжигания чувства вражды, ненависти между различными группами лиц).

Закон определяет противоправные действия, связанные с распространением ложных сведений, а также наказания за их распространение. К недостоверным фактам и онлайн-лжи относится:

- информация, которая наносит ущерб безопасности Сингапура, общественному здоровью, спокойствию, государственным финансам, а также дружественным отношениям Сингапура с другими странами;
- сведения, влияющие на результаты выборов Президента, всеобщих выборов членов парламента, дополнительных выборов члена парламента или референдума;
- сообщения, возбуждающие чувства вражды, ненависти между различными группами лиц;
- контент, направленный уменьшение доверия общества к исполнению государственными органами власти своих обязанностей.

Также к противоправным действиям относится создание и использование ботов для распространения ложных утверждений. В случаях, если человек, вне зависимости от местонахождения, запрашивает, получает или соглашается получить материальную выгоду за предоставление и распространение ложных сведений, то он/она считается виновным в совершении преступления.

Наказание за распространение ложных сведений дифференцированно в зависимости от реализующего противоправные действия лица: для физического лица предусмотрен штраф в размере не более $50-60 тыс. сингапурских долларов, или лишение свободы на срок не более 5-10 лет, или оба наказания (в зависимости от масштабов распространения и сути фейков). **Закон POFMA требует, чтобы онлайн-платформы, включая социальные сети, поисковые системы и службы агрегирования новостей, исправляли или удаляли контент, который Правительство считает ложным.** Компаниям, которые не соблюдают эти требования, грозит штраф в размере до $1 млн сингапурских долларов.

В 2020 году вспышка COVID-19 в Сингапуре была использована для оправдания факта принятия Закона, который не получил широкой общественной поддержки. Правительство Сингапура активно применяет новый Закон в борьбе с дезинформацией о COVID-19. Авторы ложных сообщений были обязаны опубликовать информацию о том, что их сообщения содержат ложные заявления, и предоставить ссылку на правительственный сайт с официальными разъяснениями. Примерами сообщений, которые были признаны недостоверными, являются: утверждения о том, что человек умер от COVID-19 в конце января 2020 года (в то время смертей в городе-государстве не было, первая смерть была зафиксирована в марте), информация о том, что станция МРТ была закрыта из-за вируса (в тот момент она все еще функционировала).

Многие правозащитные организации и IT-гиганты (Facebook, Google) высказывают обеспокоенность законодательным решением Сингапура. Компания Google заявила, что эта мера *“может остановить инновации, качество, которое город-государство хочет развивать в рамках планов расширения своей технологической индустрии”*. Facebook также выразил обеспокоенность тем, что закон может *“предоставить широкие полномочия исполнительной власти Сингапура”*. Организация “Репортеры без границ” указала на *“тоталитарный аспект”* нового сингапурского Закона о защите от онлайн-лжи и манипуляций. Во Всемирном докладе Human Rights Watch за 2020 год также говорится о том, что власти используют жесткие и чрезмерно широкие законы для преследования критикующих госорганы высказываний или произвольно называют их “ложными” или “вводящими в заблуждение”, а также приказывают онлайн-платформам блокировать или исправлять контент.

КНР

В 1998 году был разработан проект “Великий китайский файрвол” (The Great Firewall of China, 防火长城). Проект представляет собой совокупность законодательных и технологических систем, которые регулируют Интернет в КНР. Основной целью Проекта является мониторинг и регулирование распространения информации в китайском сегменте Интернета. Проект по сей день продолжает совершенствоваться в методах ограничения Интернета. **Эксперты отмечают, что Китай имеет *“самый сложный в мире режим фильтрации контента в Интернете”*.** Китайский файрвол не распространяется на специальные административные районы Китая: Гонконг и Макао.

Одними из первых были заблокированы сайты, которые не разделяли позицию Коммунистической партии Китая, в частности, иностранные СМИ (например, New York Times, The Guardian). В дальнейшем были заблокированы практически все иностранные платформы. **На сегодняшний день в КНР заблокированными являются: поисковые системы Google, Yahoo, социальные сети Facebook, Twitter, Instagram, Printerest, мессенджеры WhatsApp, Slack, хостинги YouTube, Vevo и другие популярные платформы.** Также в Китае заблокированы сайты многих зарубежных университетов, среди которых Колумбийский, Аризонский, Виргинский университеты. Китайские власти закрывают иностранные технологические компании и блокируют веб-сайты, не соответствующие государственным стандартам.

Суть китайского файрвола заключается в фильтрации поступающих из-за рубежа данных, которые цензурируются Министерством общественной безопасности КНР. **Проект реализует множество различных типов регулирования распространения и фильтрации контента для контроля китайского интернет-трафика.** Двумя наиболее известными являются 1) IP-блокировка, при которой маршрутизаторы отбрасывают трафик, направляемый к IP-адресу из черного списка, и 2) подделка DNS, при которой DNS-серверы отвечают на запрос фальсифицированным DNS-адресом, тем самым приводя к ложному домену. Из-за большого списка запрещенных онлайн-платформ также используются другие способы блокировки контента в Интернете (например, фильтрация на основе QoS). Таким образом, онлайн-платформы, разработанные вне Китая, просто не работают на территории государства.

Ограничения также касаются онлайн-контента, генерируемого внутри КНР. Так, китайские IT-гиганты Tencent, владелец WeChat, и ByteDance, владеющая TikTok, играют значительную роль в ограничении прав человека в цифровом пространстве. **Внутри социальных сетей (WeChat), новостных агрегаторов (например, Toutiao), поисковых систем (Toutiao Search) фильтрации подвергается вся информация, относящаяся к *“политически чувствительному”* контенту.** Так, статьи, в которых упоминаются члены высшего эшелона власти в негативном ключе, или видео, загруженные уйгурами, автоматически удаляются.

Отдельного внимания в контексте прав человека в цифровом пространстве заслуживают китайские социальные сети, а именно WeChat или WeiXin - китайское супер-приложение, *“которое изменило способ использования людьми своих телефонов и разрушило индустрию социальных сетей”*. WeChat с 1,2 млрд ежемесячных активных пользователей сочетает в себе функции социальной сети, мессенджера, систему мобильных платежей, доставки и онлайн-ритейла. Многофункциональность системы сделала WeChat одним из самых *“заметных и мощных приложений”* в мире, существование без которого практически невозможно для проживающих в Китае.

WeChat превратился в полноценную цифровую экосистему, вмещающую в себя всю онлайн-жизнь людей и полностью подконтрольную государству. В ней отслеживаются действия пользователей на предмет противоправной деятельности и антигосударственной риторики. Информация передается соответствующим государственным органам (например, Министерству государственной безопасности КНР). Также WeChat осуществляет автоматический мониторинг изображений в реальном времени на основе текста, содержащегося в изображениях, и их визуального сходства с изображениями из так называемого черного списка уже заблокированного контента. Так, в 2020 году блокировался контент, связанный с коронавирусом. За первые месяцы в черный список попало свыше 500 разных слов и словосочетаний: “неизвестная уханьская пневмония”, “вспышка атипичной пневмонии в Ухане” и “местные власти + эпидемия + центральное (правительство) + сокрытие”. Также блокировались ссылки на доктора Л.Вэньлян, который был среди группы врачей в Ухане и выпустил первые предупреждения о вирусе в конце декабря.

ТАИЛАНД

Последние значительные изменения в области прав человека в цифровом пространстве в Таиланде были связаны с созданием Анти-фейкового Новостного Центра в 2019 году. Центр является частью Министерства цифровой экономики и общества (DES). Анти-фейковый Центр работает в сотрудничестве со специальной полицейской кибергруппой, а также с частными компаниями/лицами для борьбы с распространением дезинформации в Интернете. При этом понятие “фейк” трактуется исключительно широко. Критериями блокировки фейковых новостей являются:

- недостоверные новости о темах, которые непосредственно влияют на жизнь и имущество людей (эпидемии, катастрофы, вопросы экологии и экономики);
- новости, направленные на создание социальных разногласий;
- информация, формирующая ложные убеждения в обществе;
- фейковые новости, разрушающие имидж страны.

Бывший Министр цифровых технологий в экономике и обществе Буддхипонгсэ Пуннаканта определил фейковые новости значительно шире: *“любой вирусный онлайн-контент, который вводит людей в заблуждение или наносит ущерб имиджу страны”*. Различие между ненамеренной ложной информацией и преднамеренной дезинформацией не делается.

За первый месяц Центр опубликовал сведения о 14 заблокированных статьях. **Преимущественно блокируется контент, который относится к вопросам национальной безопасности, правительству, экономической ситуации, стихийным бедствиям и наркотикам. На сегодняшний день на сайте размещается в среднем 3-4 фейковые новости.** Информация о заблокированном контенте размещается по усмотрению сотрудников Центра. Особенность работы Центра заключается в том, что любой желающий может сообщить о факте распространения фейковых новостей. Для этого необходимо указать ссылку на недостоверный контент, прикрепить изображение, а также предоставить контактную информацию. Результатом деятельности является не только борьба с дезинформацией, но и с контентом, который не соответствует политическим интересам властей Таиланда.

АВСТРАЛИЯ

Отдельного внимания заслуживает конфликт между австралийским правительством и международными IT-гигантами (Google и Facebook). 17 февраля 2021 года компания Facebook выпустила заявление, согласно которому социальная сеть ограничивает издателей и пользователей в Австралии от обмена или просмотра австралийского и международного новостного контента. Утверждается, что такие меры стали *“ответной реакцией”* на австралийский Кодекс ведения переговоров со СМИ и цифровыми платформами.

Первопричиной создания Кодекса стали многолетние жалобы СМИ на то, что социальные сети забирают себе большую часть прибыли от работы журналистов и медийных организаций. По мнению министра финансов Австралии Джоша Фриденберга, *“на каждые $100 расходов на рекламу в Интернете $53 идут в Google, $28 в Facebook и $19 долларов - другим участникам”*. Кодекс, по мнению австралийских властей, необходим для устранения *“фундаментальных дисбалансов переговорной силы между австралийскими компаниями средств массовой информации и крупными цифровыми платформами”*. **Основная идея законопроекта заключается в том, что заинтересованные стороны, а именно СМИ и цифровые платформы, должны достигать согласия о стоимости распространяемого платформами новостного контента. В случаях, если подобные соглашения не могут быть достигнуты, технологические компании и средства массовой информации должны обращаться в арбитраж, чтобы определить планы распределения доходов.**

Проект Кодекса был встречен возмущением со стороны Google и Facebook. Во время обсуждений законопроекта обе организации публично выступали против планов Австралии. **Так, социальная сеть Facebook утверждала, что издатели *“получают больше от Facebook, чем Facebook получает от новостного контента”*. Компания Google также утверждала, что издатели получают больше пользы от ресурсов Google, а не наоборот.** Обе компании публично осудили проект кодекса после того, как он был опубликован 31 июля. Компания Google разместила открытое письмо, в котором говорилось, что австралийцев ожидают *“значительно худшие”* услуги, если новые правила вступят в силу.

17 февраля 2021 года компания Facebook в ответ на принятие закона заблокировала весь новостной контент для своих австралийских пользователей и весь контент от австралийских изданий для пользователей по всему миру. Таким решением Facebook значительно ограничил права человека в Интернете, а именно свободу распространения информации. В заявлении компании говорилось о том, она была вынуждена пойти на этот шаг во избежание необходимости соблюдения нового Кодекса: *“Предлагаемый закон неправильно трактует отношения между нашей платформой и издателями, которые используют ее для обмена новостным контентом. Это поставило нас перед суровым выбором: попытаться соблюдать закон, игнорирующий реалии, или прекратить разрешать использование новостного контента в наших сервисах в Австралии. С тяжелым сердцем выбираем последнее”*.

Запрет вызвал немедленную негативную реакцию у пользователей социальной сети. Пользователи были крайне возмущены ограничением доступа к информации и страницам масс-медиа в социальных сетях. **Многие австралийцы разозлились из-за внезапной потери доступа к привычным надежным и авторитетным источникам.** Как следствие, пользователи запустили онлайн-движение "удалить Facebook", сопровождая посты тегом #DeleteFacebook. Хэштеги #deletefacebook, #FacebookWeNeedToTalk и #BoycottZuckerberg получили широкое распространение в социальной сети Twitter. Некоторые пользователи призывали удалять свои аккаунты в других сервисах компании — WhatsApp и Instagram. Однако число австралийцев, удаливших свои аккаунты, неизвестно. **С резкой критикой решения Facebook также выступили многие международные и австралийские СМИ:** The Sydney Morning Herald, The Guardian, The Australian, ABC News, The Washington Post, а также многие политические деятели.

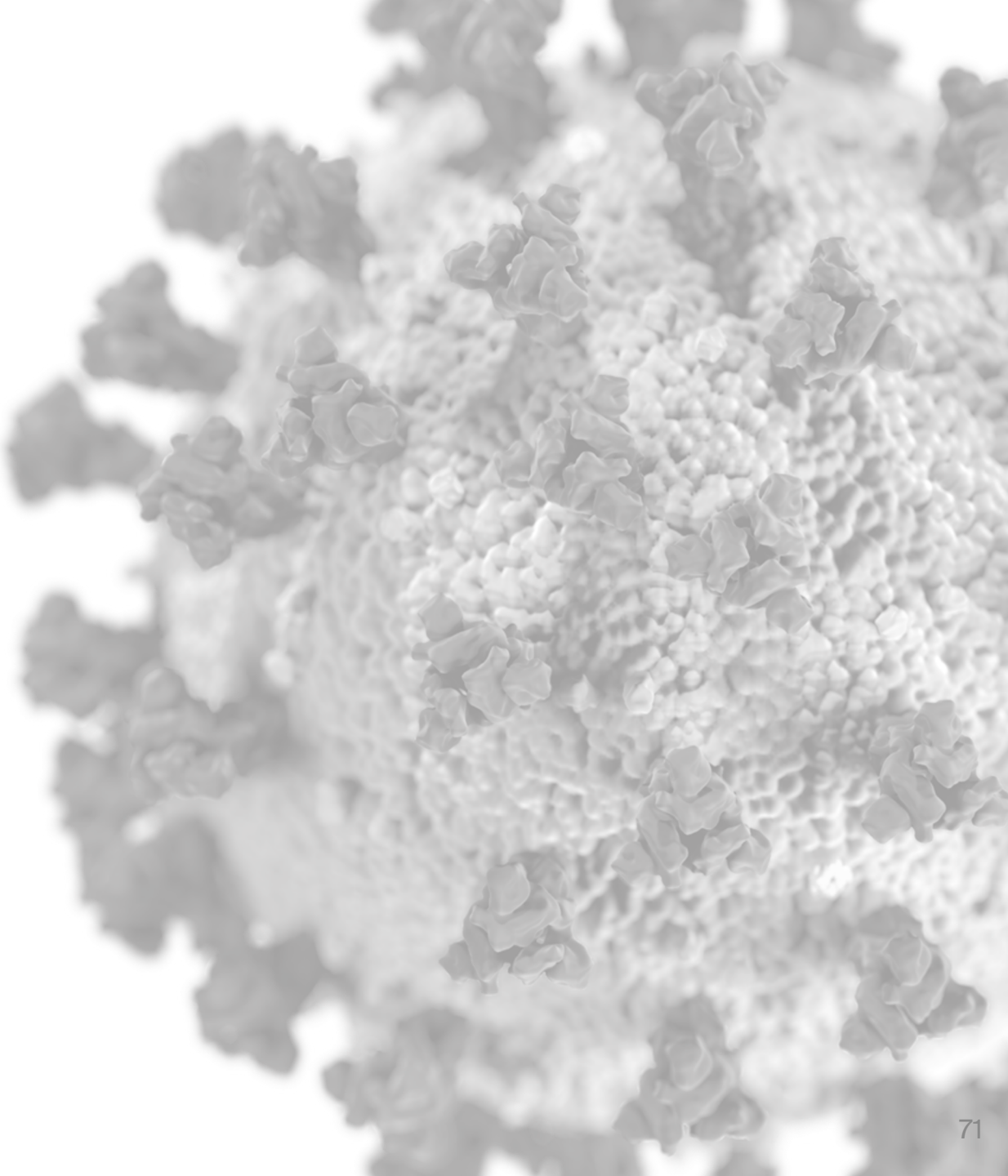
После действий Facebook Правительство Австралии подчеркнуло свою приверженность новой законодательной инициативе. Тем не менее, стороны (Facebook и власти Австралии) сразу приступили к "конструктивным дискуссиям". **Итогом переговоров стало заключение соглашения, которое позволило восстановить полноценную работу социальной сети в Австралии. Правительство Австралии согласилось внести поправки в законопроект, которые удовлетворили Facebook.**

Согласно нескольким поправкам к кодексу, Facebook получит больше времени для заключения сделок с издателями, чтобы не быть немедленно вынужденным совершать платежи, определенные медиа-компаниями. Поправки также предполагают, что если цифровые платформы добровольно внесут достаточно денег в австралийскую новостную индустрию, то компании смогут полностью избежать кодекса, по крайней мере на данный момент. Facebook заявил, что удовлетворен достигнутым соглашением: "*После дальнейших обсуждений мы удовлетворены тем, что австралийское правительство согласилось на ряд изменений и гарантий, которые решают наши основные проблемы, связанные с разрешением коммерческих сделок, признающих ценность нашей платформы для издателей по сравнению с ценностью, которую мы получаем от них*".

Данный прецедент свидетельствует о большом влиянии медиа-компаний на реализацию прав человека в онлайн-среде. **Действия Facebook продемонстрировали, что IT-гигант способен вести переговоры с национальными правительствами с позиции силы. Социальная сеть, преследуя свои политические и экономические цели, ограничила свободу информации в Интернете без учета мнения общественности.** Как следствие, Правительство Австралии для сохранения реализации прав человека в цифровом пространстве было вынуждено частично принять условия IT-компании. Такая ситуация свидетельствует о важности взаимодействия всех заинтересованных сторон в формировании цифровой политики, особенно с учетом новостей о планируемых аналогичных законодательных изменениях в других странах.

ЕС

Пандемия коронавируса выступила катализатором дискуссии об ответственности за распространение фейковой информации в Сети. Евросоюз впервые выразил тревогу по поводу дезинформации и фейковых новостей, связанных с пандемией коронавируса, в начале лета 2020 года. “*Пандемия COVID-19 сопровождалась беспрецедентной инфодемией*”, - заявила вице-президент Европейской комиссии Вера Джурава. Политика европейских стран в отношении распространения фейков различается. **Если в Румынии и в Боснии и Герцеговине отказались от законов о фейковых новостях после давления со стороны Европейского союза и ОБСЕ, то Венгрия в конце марта 2020 года приняла поправки, криминализирующие распространение дезинформации, которая подрывает борьбу властей с вирусом COVID-19.** Это наказывается штрафом и лишением свободы на срок до 5 лет. По официальным данным, с момента принятия закона в конце марта власти возбудили 86 уголовных дел. Этот закон вызвал беспокойство венгерских журналистов и представителей НКО; по их мнению, он создает опасность для свободы слова и может использоваться правительством для борьбы с оппозицией. Оппозиционная партия Momentum заявила, что один из ее сторонников был задержан после публикации в Facebook сообщения об антиправительственном протесте.



США

Дискуссию в американском обществе вызывает политика в отношении свобода слова, которая осуществляется крупными IT-компаниями, контролирующими социальные сети. Особенно активно данный вопрос стал подниматься в период президентства Дональда Трампа, при котором отношении между государством и крупнейшими социальными сетями в значительной степени ухудшились. Согласно опросу, проведенному летом 2018 года социологическим центром Pew Research Center, 72% участников опроса заявили, что социальные сети занимаются цензурой на основании политических взглядов. Согласно опросу того же социологического центра, проведенного через два года, 73% участников опроса заявили о цензуре со стороны социальных сетей. После того, как Twitter присвоил двум сообщениям Трампа маркировку с указанием, что твит может содержать недостоверную информацию, действовавший президент подписал указ о регулировании соцсетей. Указ Трампа отменил действие закона, определяющего нормы поведения, в том числе, в социальных сетях.

Это изменение освободило крупнейшие технологические компании от ответственности за содержание сообщений, размещенных на созданных ими платформах. Таким образом, например, компании Twitter и Facebook были защищены от возможных судебных исков по обвинениям в клевете и попрании чести и достоинства. Вскоре после публикации указа Трампа общественная организация Центр демократии и технологий подала иск с требованием признать указ президента незаконным и нарушающим первую поправку Конституции. **Уже после того, как Дональд Трамп покинул пост президента Соединенных Штатов, продолжается активное обсуждение различных инициатив, направленных на недопущение цензурирования граждан со стороны социальных медиа**. В частности, в марте 2021 года в Техасе при содействии губернатора и местных парламентариев был подготовлен законопроект, который позволит всем жителям Техаса, которые столкнулись с давлением администрации социальных медиа, подавать на них в суд. При этом под цензурой законопроект понимает не только непосредственное блокирование аккаунта, но и достаточно большой набор мер, включая отключение монетизации и сокрытие определенных сообщений.

КАНАДА

В целом канадское законодательство об Интернете предполагает гораздо больше ограничений, чем законодательство Соединенных Штатов, как на уровне отдельных регионов, так и страны в целом. С 2015 по 2018 годы шла активная дискуссия вокруг деятельности в провинции Квебек онлайн-казино, не получивших разрешения на работу от организации Loto-Québec, являющейся регулятором азартных игр в регионе. Loto-Québec выступала за блокировку подобных Интернет-ресурсов и в конечном итоге была поддержана правительством провинции в 2016 году. Однако в стране началась активная дискуссия по поводу допустимости подобных инициатив. Правозащитные организации заявляли о том, что в интересах региональной монополии были приняты первые законы о цензуре в канадском Интернете. Активно против данного законодательства выступали несколько общественных организаций, которые обратились в суд. Судебное разбирательство затянулось на два года и лишь в июле 2018 года суд провинции выступил против закона, отметив, что решение подобного вопроса лежит в сфере регулирования канадского правительства и не может быть решено правительством одной из провинций.

В рамках рассмотрения вопроса о защите прав человека в цифровом пространстве Канады необходимо упомянуть **возможность введения в Канаде законодательства, аналогичного австралийскому Кодексу ведения переговоров со СМИ и цифровыми платформами.** В рамках данного Кодекса СМИ и цифровые платформы должны достигать согласия о стоимости новостного контента, который распространяется на платформах Интернет-гигантов. Наиболее активно против данного решения выступили Facebook и Google. Конфликт обострился после того как компания Facebook ограничила для австралийских пользователей обмен и просмотр австралийского и международного новостного контента. **Канада решительно осудила действия социальной сети, встав на сторону Австралии**. Канадский министр культуры Стивен Гильбо заявил, что действия Facebook “*крайне безответственны*” и отметил, что Канада может внедрить схожие с Австралией правила для распространения новостного контента. Также Гильбо отметил, что Канада ведет переговоры о введении подобных мер и с другими государствами, в частности, с Францией, Германией и Финляндией. Глава представительства Facebook Кевин Чан призвал Оттаву воздержаться от подобных мер, отметив историю успешного сотрудничества социальной сети с Канадой в деле удаления запрещенного контента. Тем не менее, на данный момент Канада не предприняла каких-либо действий, схожих с теми, что осуществила Австралия. При этом Оттава также не заявила об отказе от намерения разработать схожее с австралийским законодательство.

ВЫВОДЫ
И РЕКОМЕНДАЦИИ

1.

В России озабоченность проблематикой влияния цифровизации на права человека и роли государства в защите прав человека в цифровом пространстве в последние года проявляется на самом высоком уровне. Так, 10 декабря 2020 года состоялась встреча членов Совета по развитию гражданского общества и правам человека при Президенте РФ с Президентом, где, помимо прочего, обсуждалась проблема обеспечения прав человека в цифровом пространстве. По итогу Правительству РФ совместно с СПЧ Президентом была поручена разработка проекта концепции обеспечения защиты прав и свобод человека и гражданина в цифровом пространстве Российской Федерации и проекта "дорожной карты" по ее реализации, которые должен включать в себя мероприятия по повышению цифровой грамотности граждан и обучению их навыкам информационной безопасности и "цифровой гигиены". Однако **определенная работа в данной сфере была начата значительно раньше**. Можно констатировать, что **к настоящему моменту Российская Федерация уже в той или иной степени следует многим мировым трендам в области обеспечения прав человека в цифровом пространстве**.

Право на доступ в Сеть в настоящий момент не зафиксировано в России на законодательном уровне, однако данная возможность последние годы обсуждалась (так, соответствующая инициатива была предложена Минкомсвязи еще в 2016 году). **Ведется работа по повышению цифровой грамотности граждан**: реализуются соответствующие проекты как регионального, так и федерального уровня.

Ведется активная деятельность по повышению доступности онлайн среды для лиц с ОВЗ по слуху и зрению. В 2020 году было проведено первое в России масштабное исследование доступности сайтов госорганов для людей с ОВЗ, выполненное АНО "Институт развития интернета" по заказу Министерства труда и социальной защиты РФ.

Несмотря на то, что Конституция РФ писалась и принималась в тот период времени, когда интернет находился еще на ранней стадии своего развития и распространения, статья 29 Основного закона, гарантирующая свободу слова ("*Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом*"**), позволяет в настоящее время относить к ней и интернет-среду.**

В регулировании распространения контента Россия также следует общемировым трендам. В начале нулевых годов были приняты такие законодательные акты в области информационного права, как: Федеральный закон от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации" и целый ряд связанных с ним других законодательных актов, регулирующих оборот информации, в том числе "О персональных данных", "Об обеспечении доступа к информации о деятельности судов в Российской Федерации", "О защите детей от информации, причиняющей вред их здоровью и развитию" и др. **Ведется постоянная работа по конкретизации фундаментальных прав человека в условиях цифровой эпохи (необходимость работы в данном направлении, в частности, отмечал председатель Конституционного суда РФ В.Зорькин)**. Так, еще в 2014 году была выдвинута идея создания Информационного кодекса РФ, в котором право граждан на информацию и формы его реализации должны быть зафиксированы более подробно. В 2018 году председатель Конституционного суда РФ вернулся к данной идее, заявив о необходимости создания такого документа. В настоящий момент в российской юридической среде по поводу концепции Информационного кодекса РФ ведутся дискуссии, предлагаются разные проекты кодекса.

Имеется профильное федеральное ведомство Роскомнадзор, занимающееся надзором в сфере связи, информационных технологий и СМИ. **В России постепенно определяются новые формы незаконного контента**. Так, в 2019 году Госдума приняла закон о наказании за распространение недостоверной общественно значимой информации. **На фоне зарубежных аналогов российский закон можно охарактеризовать как относительно мягкий**: он не запрещает высказывать критические мнения (в том числе и в отношении государственных служащих или институтов), суждения или точку зрения, отличную от официальной.

Отмечается взвешенный подход российского государства в отношении проблемы конфиденциальности: так, пользователям разрешено в частной переписке (не затрагивающей гостайну) использовать несертифицированные средства шифрования.

В целом, Россия последовательно придерживается политики выстраивания суверенного Интернет-пространства. В частности, в ходе вышеупомянутого заседания СПЧ Президентом была поставлена задача встраивания зарубежных IT-гигантов в российское правовое поле. Было отмечено, что иностранные IT-компании для легальной работы в России должны иметь российские юридические представительства. Это требование позволит контролировать сбор иностранными платформами персональных данных российских граждан и предпринимать ответные меры на попытки из-за рубежа незаконно повлиять на формирование российского информационного поля.

2.

В отношении концептуализации прав человека в Интернете имеется несколько противоречащих друг другу подходов. Преобладает тренд, рассматривающий цифровые права человека как продолжение естественных прав человека в цифровом пространстве (таким образом, Интернет-пространство выступает проекцией публичного пространства государства). Однако встречается и более радикальный **подход** (его придерживается, например, организация Human Rights Watch), **рассматривающий Интернет как принципиально новое общественное явление и предполагающий, что существующие национальные и наднациональные нормы** (в том числе и в отношении прав человека) **к нему неприменимы**;

3.

Различные международные организации, как наднациональные, так и общественные продвигают повестку прав человека в цифровом пространстве преимущественно декларативно. Практическое продвижение такими организациями конкретных прав человека встречается редко. Можно констатировать, что в настоящий момент деятельность международных организаций в сфере защиты прав человека в цифровом пространстве не является значимым фактором профильной политики: ключевые решения, затрагивающие данную сферу, почти всегда принимаются на национальном уровне исходя из интересов конкретных государств;

4.

Практически все государства так или иначе провозглашают защиту прав человека (в том числе и в Интернете) основой своей политики. Однако само понимание прав человека и области их действия значительно различается: в этом отношении показателен пример КНР, в которой свобода в Интернете охраняется на законодательном уровне, но при этом отмечается, что эта свобода ограничена не только свободой других граждан, но и государственными, общественными и коллективными интересами. Таким образом, **одна и та же риторика может использоваться при диаметрально противоположных практических политических подходах**;

5.

В настоящий момент множество государств и международных организаций рассматривают доступ к Интернету в качестве базового цифрового права человека. Преобладает позиция, что все люди, вне зависимости от социального статуса, гендера и расы, должны быть равны в цифровых правах. Развитые и развивающиеся государства активно способствуют увеличению числа Интернет-пользователей (так, в Сингапуре людям с низкими доходами предоставляются скидки на электронные устройства; в Австралии под давлением государства провайдеры снижают цены);

6.

Принцип сетевого нейтралитета является наиболее дискуссионной темой, связанной с темой права на доступ к Интернету. Согласно данному принципу, провайдеры телекоммуникационных услуг не должны отдавать предпочтения одному целевому предназначению перед другим или одним классам приложений перед другими.Таким образом, предполагается, что провайдер должен относиться нейтрально к сетевому трафику. По мнению сторонников данного подхода, крупные телекоммуникационные компании, пользуясь своей монопольной позицией, навязывают потребителю одни услуги в ущерб другим. В основном, принцип поддерживают крупнейшие поставщики Интернет-контента, группы защиты прав потребителей и лево-либеральные политические блоки. Противники принципа считают, что он является контрпродуктивным и ущемляющим интересы крупного бизнеса. Оппозиция к сетевому нейтралитету чаще всего исходит от крупных телекоммуникационных компаний, производителей сетевого оборудования и организаций защиты свободного рынка. В настоящий момент консенсусное решение по данному вопросу не принято: одни развитые страны (например, Канада) активно поддерживают данный принцип, другие (например, США, с 2017) - нет;

7.

С правом на доступ к Интернету тесно связана проблема доступа к Интернету людей с ОВЗ. В странах с высокой степенью развития Интернет-культуры (например, в США и Канаде) в последние годы **преобладает тренд, при котором несоответствие той или иной Интернет-услуги стандартам инклюзивности рассматривается как форма дискриминации**;

8.

Одним из наиболее популярных обоснований необходимости расширения Интернет-регулирования является необходимость противодействия распространению дезинформации (особенно в условиях катастрофы или пандемии). **Границы области, затрагиваемой этим регулированием, зависят от толкования определяющим политику актором понятия фейка, которое отличается значительной произвольностью** (так, показательны примеры Таиланда и Сингапура, в законодательных практиках которых под фейками, помимо прочего, подразумеваются сообщения, подрывающие имидж государственных институтов);

9.

Ужесточение оборота персональных данных связано с значительными экономическими издержками для включенных акторов. Это продемонстрировал, в частности, опыт введения общеевропейского регламента защиты персональных данных (GDPR), оказавшийся травматичным для малого бизнеса;

10.

В некоторых случаях государства, столкнувшиеся с необходимостью регулирования распространения онлайн-контента, фактически дистанцируются от ограничения свободы слова, перекладывая функцию регулятора на частные компании (например, кейс немецкого закона “О мерах в отношении социальных сетей” (NetzDG)). Таким образом **наблюдается ситуация, при которой размывается монополия государства на насилие** (в данном случае, в аспекте цензуры);

11.

Конфликт Facebook с австралийским правительством стал уникальным прецедентом прямой конфронтации между транснациональной корпорацией и государственной властью конкретного государства, при котором корпорация решилась на использование массовой блокировки контента в качестве инструмента шантажа. Хотя в данном случае конфликт был обусловлен коммерческим спором, **нельзя исключать, что в будущем Facebook, Google или другие подобные корпорации не будут использовать аналогичные инструменты давления в случае конфликтов, вызванных политическими или социальными противоречиями**. В этом отношении данный кейс требует от национальных государств проработки сценариев ответных действий на возможные выпады со стороны международных IT-корпораций.

С УЧЕТОМ ВСЕГО ВЫШЕИЗЛОЖЕННОГО ПРЕДСТАВЛЯЕТСЯ ВОЗМОЖНЫМ ВЫДЕЛИТЬ СЛЕДУЮЩИЕ РЕКОМЕНДАЦИИ:

- Расширению фактического доступа российских граждан в Интернет способствовало бы введение специальных программ поддержки для малоимущих россиян. В зарубежной практике встречаются разные формы такой поддержки: помощь в приобретении Интернет-устройств (подобная мера реализуется в Сингапуре, правительство которого предоставляет семьям с низким уровнем дохода компьютеры и планшеты по льготной ставке); помощь в оплате услуг провайдеров (так, программа снижения услуг провайдеров для малоимущих действует в Австралии);

- Обеспечение доступа россиян в Интернет предполагает не только предоставление им возможности фактического подключения к Сети, но и формирование у них необходимого уровня цифровых компетенций. В качестве ориентиров работы в данном направлении может служить опыт Японии, Сингапура и Австралии - стран с высоким уровнем цифровой грамотности. Особый интерес в этом отношении представляет японский подход: во-первых, программы, направленные на формирование у граждан цифровых компетенций, не выступают отдельным элементом, а интегрируются в образовательные курсы для самых разных возрастов (например, формат Digital Storytelling, при котором в ходе практических занятий учащиеся обучаются использованию разных типов файлов); во-вторых, активно используется геймифицированный образовательный контент (например, японские программы Comikaruta и A-I-U-E-O Gabun). Более “традиционным” является подход Сингапура, в котором имеется национальная программа цифровой грамотности для школьников, представляющая собой 10-часовые курсы. Разработка и интеграция подобной программы в российскую систему школьного образования (например, в рамки обязательного предмета “Информатика и ИКТ”) позволила бы в средней и долгой перспективе значительно повысить уровень цифровой грамотности россиян;

- Важным аспектом, связанным с предоставлением гражданам стабильного доступа к Интернет-контенту, является регулирование деятельности провайдеров. В этом отношении также примечателен японский опыт: министерство внутренних дел и коммуникации Японии разработало совместно с провайдерами обязательный отраслевой стандарт. Создание и внедрение подобного стандарта в России защитило бы граждан от произвольных действий со стороны провайдеров. Основанием для такого стандарта мог бы стать принцип сетевого нейтралитета, согласно которому провайдеры телекоммуникационных услуг не должны отдавать предпочтения одному виду сетевого трафика перед другим. Опыт стран, реализующих его (например, Канады и Японии) демонстрирует, что данный принцип не только делает работу пользователей в Интернете более комфортной, но и оказывает позитивное влияние на развитие малого бизнеса;

- В отношении граждан с ОВЗ России имеет смысл ориентироваться на зарубежные практики, обусловленные позицией, рассматривающей несоответствие веб-ресурсов стандартам инклюзивности рассматривается как форма дискриминации;

- Позитивное влияние на осведомленность российских граждан об имеющихся у них правах окажет создание платформ для онлайн-консультаций. По аналогии с японским Бюро по правам человека или южнокорейской Комиссией по правам человека в Российской Федерации такая платформа могла бы быть создана и функционировать при СПЧ;

- Интернет-насилию важно противодействовать не только на регуляторном, но и на информационном уровне: в частности, России имеет смысл заимствовать успешный опыт создания комплексных профильных порталов, на которых размещается информация для пострадавших от насилия в Интернете. Примером такого портала является немецкий сайт HateAid.org, на котором размещаются тематические материалы о тех или иных типах дигитальных угроз. Создание подобных порталов особенно актуально потому, что ввиду интенсивного развития Интернет-технологий постоянно появляются все новые типы киберугроз, требующие немедленного информационного реагирования со стороны государства. К числу таких угроз, в частности, относятся доксинг (систематический сбор публичных и приватных данных лица с целью их последующего размещения в открытом доступе), кибersталкинг (использование Интернета для преследования или домогательств); сваттинг (ложный вызов экстренных служб, обычно полиции со спецназом, на адрес стримера (ведущего онлайн-трансляции));

- После криминализации распространения фейковой информации (зафиксированной в законе, принятом в 2019 году) имеет смысл активизировать работу по криминализации иных формы Интернет-насилия, в первую очередь, кибербуллинга. В этом отношении примечателен опыт Австралии, в которой на уровне штатов введена уголовная ответственность за травлю (в том числе и в форме кибербуллинга);

- В случае, если решение о создании Информационного кодекса РФ все же будет принято, при подготовке данного документа имеет смысл ориентироваться на уже принятые (например, Общий регламент защиты персональных данных (GPDR) в ЕС) и в настоящий момент разрабатываемые комплексные зарубежные законопроекты в данной сфере (например, европейские Закон о цифровых услугах (DSA) и Закон о цифровых рынках (DMA), которые характеризуются некоторыми экспертами как “новая конституция Интернета”);

- В качестве ориентира для развития Роскомнадзора можно обозначить австралийский Комиссариат по безопасности в Интернете (eSafety), который не только выполняет функции регулятора распространения контента, занимается профильными исследованиями и образовательными программами, но и, в целом, выступает в качестве координатора политики по обеспечению безопасности граждан в Интернете.