Верховенство права в Интернете и в остальном цифровом мире

Основные положения доклада и рекомендации Комиссара

Тематический доклад

COMMISSIONER FOR HUMAN RIGHTS
COMMISSAIRE AUX DROITS DE L'HOMME

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Верховенство права в Интернете и в остальном цифровом мире

Тематический доклад, опубликованный Комиссаром Совета Европы по правам человека

Основные положения доклада и рекомендации Комиссара

Совет Европы

Полный текст доклада доступен на сайте www.commissioner.coe.int; Электронная версия также доступна на сайте http//www.coe.int/web/commissioner/publications

Фото на обложке: Shutterstock
Дизайн обложки и верстка: Департамент Совета Европы по подготовке документов и публикаций

Печать: издательство Совета Европы

Благодарности:

этот тематический доклад был подготовлен профессором Дуве Корффом, приглашенным научным сотрудником Йельского университета (Проект информационного общества), и сотрудником Оксфорд Мартин, Школа Оксфорд Мартин, Университет Оксфорда, Великобритания. Профессор Корфф совместно с Комиссаром благодарны Джо МакНами из организации «Европейские Цифровые права» за полезные комментарии и дополнения, которые он внес в черновую версию доклада, в особенности в часть посвященную контролю в частном секторе

Содержание

Резюме

Данный тематический доклад затрагивает актуальный вопрос: как обеспечить установление и поддержание верховенства права в Интернете и в большом цифровом мире? В первом разделе описываются виды деятельности «онлайн» и угрозы этой среде; во втором разделе обсуждаются возникающие принципы «управления Интернетом», отмечается особый контроль, осуществляемый над цифровым миром со стороны США (и Соединенного Королевства, если говорить о Европе), а также говорится об угрозе фрагментации Интернета, в качестве ответной реакции. В третьем разделе излагаются международные стандарты верховенства права и некоторые проблемы применения законодательства в этой новой среде. В четвертом разделе более детально анализируются основные вопросы, затронутые в предыдущих разделах: свобода выражения мнения, приватизация правоохранительной деятельности, защита данных, киберпреступность и национальная безопасность, и достижение необходимого тонкого равновесия.

Комиссар Совета Европы по правам человека предложил ряд рекомендаций на основе вопросов, поднимаемых в данном тематическом докладе; они излагаются в конце данного резюме.

Новая среда человеческой деятельности

Мы живем в глобальной цифровой среде, которая обеспечила возникновение новых средств деятельности в местных, региональных и всемирных масштабах, в том числе новых типов политической активности, культурных обменов и реализации прав человека. Вся эта деятельность не является фактической, то есть она «не является по настоящему реальной». Тем не менее, она стала важнейшей частью реальной жизни современного человека. Ограничения доступа к Интернету и цифровым СМИ, а также попытки осуществлять мониторинг «онлайн» деятельности и электронных коммуникаций являются вмешательством в основные права на свободу выражения мнения и информацию, свободу объединений, личную и частную жизнь (и, возможно, в другие права, такие как свобода совести и религии, а также право на справедливое судебное разбирательство).

Разумеется, новая глобальная цифровая среда создает и новое пространство для противоправного поведения: для разжигания ненависти, распространения детской порнографии, призывов к насилию, для нарушения авторского права («пиратство»), мошенничества, кражи личных данных, отмывания денег и атак на саму структуру электронных коммуникаций через вредоносные программы (такие как «трояны» и «черви») или же атак отказа в обслуживании. Киберпреступность и кибербезопасность стали вопросами чрезвычайной важности.

Эти угрозы приобретают транснациональный характер. Достигнутый широкий международный консенсус в отношении необходимости борьбы с киберпреступностью, обеспечения кибербезопасности и противодействия терроризму нивелируется отсутствием согласия в отношении деталей: нет единства даже в понимании, что представляет собой угрозу.

Четыре вопроса заслуживают особого внимания. Во-первых, действия государств по борьбе с киберпреступностью, угрозами кибер- и национальной безопасности становятся все более взаимосвязанными; границы между этими направлениями деятельности размываются, а органы и учреждения, занимающиеся ими, взаимодействуют все более тесно. Во-вторых, в настоящее время государства координируют свою деятельность по всем этим направлениям. В-третьих, работа органов национальной безопасности и разведки все больше зависит от мониторинга деятельности отдельных лиц и групп в цифровой среде. В-четвертых, вместо вмешательства правоохранительных органов постфактум, упор сегодня делается на разведку и предупреждение, при этом правоохранительные органы используют методы и технологии, которые ранее использовались только секретными службами.

Природа цифровой среды

Опасные данные

В эпоху «Больших Данных» (когда данные о наших действиях обмениваются и/или используются в агрегированной форме) и «Интернета Вещей» (когда все больше физических объектов – вещей – передаются через Интернет) достаточно трудно обеспечить подлинную анонимность: чем больше имеется данных, тем легче идентифицировать человека. Более того, анализ «Больших Данных» усовершенствованными способами приводят к созданию профилей. И хотя эти профили используются достаточно редко (например, для нахождения террориста в большом объеме данных, таких как регистрация пассажиров авиалиний), они не являются надежными и могут непреднамеренно привести к дискриминации по признаку расовой принадлежности, пола, религии или гражданства. Эти профили создаются в таких сложных формах, что решения, принимаемые на их основе, практически невозможно обжаловать: даже лица, реализующие такие решения, не в полной мере осознают те аргументы, которые лежат в основе этих решений.

Цифровая среда может в силу самой своей природы размывать основы частной жизни и фундаментальных прав, тем самым подрывая ответственное принятие решений. Здесь кроется потенциальная возможность подрыва верховенства права путем ослабления или разрушения права на частную жизнь, ограничения свободы коммуникаций или свободы объединений, а также произвольного вмешательства.

Глобальное и частное, но не в небесах

Учитывая открытый характер Интернета (что является его главной сильной стороной), из любой конечной точки в сети можно осуществлять коммуникацию с практически любой другой конечной точкой, причем следуя наиболее эффективному маршруту. Информация передается через разного рода коммутаторы, роутеры и кабели – физическую инфраструктуру Интернета.

Система электронных коммуникаций является транснациональной и, по сути, действительно глобальной; и при этом инфраструктура является физической и располагается в реальных местах, несмотря на разговоры об «Облаке». В настоящий момент многие из этих физических компонентов находятся в США, при этом многие из них управляются и контролируются частными компаниями, а не государственными органами.

Основная инфраструктура Интернета состоит из оптоволоконных кабелей высокой емкости, которые проходят по дну морей и океанов и подсоединены к наземным кабелям и роутерам. Наиболее важные кабели для Европы – это те, которые проходят от континентальной Европы к Соединенному Королевству, а также по дну Атлантического океана в США. Учитывая доминирование в Интернете и в облачном хранилище данных американских компаний, эти кабели передают значительную часть всего Интернет-трафика и Интернет-коммуникации, включая почти все входящие и исходящие данные Европы.

Кто контролирует?

Управление Интернетом

Важные принципы управления Интернетом, предложенные Советом Европы и другими организациями, подчеркивают необходимость применения публичного международного права и международного права в области прав человека, как в «онлайн», так и «офлайн», при соблюдении принципа верховенства права и демократии в Интернете. Эти принципы признаются и продвигаются многочисленными заинтересованными в управлении Интернетом лицами. Они призывают все публичные и частные структуры соблюдать права человека во время всех операций в сети Интернет, а также при разработке новых технологий, услуг и приложений. Государства призываются уважать суверенитет других наций и воздерживаться от действий, которые могут нанести ущерб лицам или образованиям вне их территориальной юрисдикции.

Тем не менее, эти принципы остаются во многом декларативными: по-прежнему существует дефицит в таких договоренностях об управлении Интернетом, которые могли бы реально служить опорой применения установленных принципов на практике.

Управление Интернетом должно учитывать также и то, что – частично из-за корпоративного доминирования, частично из-за исторических обстоятельств – США имеют больший контроль над Интернетом, чем любое другое государство (или даже все другие государства вместе). Совместно со своим ближайшим партнером – Соединенным Королевством – США имеют доступ к большей части инфраструктуры Интернета.

Бывший сотрудник Агентства национальной безопасности США Эдвард Сноуден рассказал о том, что США и Соединенное Королевство используют этот контроль и доступ для осуществления массовой слежки в Интернете, глобальных системах электронных коммуникаций и социальных сетях. Есть опасения, что государства могут ответить на откровения Сноудена путем фрагментации Интернета, когда страны или регионы будут настаивать на передаче их данных исключительно через местные роутеры и кабели и хранении в местных облачных хранилищах

данных. Это создаст угрозу разрушения Интернета в том виде, в каком мы его знаем, поскольку приведет к воздвижению национальных барьеров в глобальной сети. Если США не примут меры по улучшению ситуации с соблюдением международных стандартов в области прав человека, то это нанесет ущерб сети Интернет и глобальным системам коммуникаций, в результате чего продвижение к усеченному Интернету будет трудно остановить.

Контроль в частном секторе

Значительная часть инфраструктуры Интернета и остальной цифровой среды находится в руках частных компаний, многие из которых – американские корпорации. Это создает проблемы, поскольку компании непосредственно не связаны нормами международного права в области прав человека. Оно напрямую применимо лишь к государствам и правительствам – и поэтому от частных компаний намного труднее добиться возмещения ущерба. Кроме того, деятельность частных компаний регулируется законодательством тех стран, на территории которых они созданы или действуют. К сожалению, национальные законы не всегда соответствуют международному праву или международным стандартам в сфере прав человека. Не исключены ограничения, нарушающие права человека на деятельность в Интернете (как правило, в отношении свободы выражения мнения), возможны чрезмерно широкие пределы вмешательства в охраняемые правами человека сферы. Примерами такого вмешательства могут служить слежение за деятельностью в Интернете или за электронными коммуникациями. К тому же эти действия могут осуществляться на экстерриториальной основе, тем самым нарушая суверенитет других государств.

Применение национального законодательства к деятельности частных компаний, контролирующих цифровой мир (или его значительные сегменты) – вещь чрезвычайно сложная и деликатная. Разумеется, государства имеют право, более того – они обязаны противодействовать преступной деятельности с использованием Интернета и систем электронных коммуникаций. И в этом они естественным образом опираются на помощь соответствующих частных структур. Ответственные компании также будут стремиться к тому, чтобы их продукция и услуги не использовались в преступных целях. Тем не менее, в таких ситуациях и государства должны соблюдать свои международные обязательства в области прав человека и уважать суверенитет других государств. В частности, государства не должны игнорировать свои конституционные и международные обязательства, поощряя ограничения прав человека через «добровольные» действия посредников; а компании, в свою очередь, должны соблюдать права отдельных граждан.

Правовое государство в цифровой среде

Верховенство права

Верховенство права – это принцип управления, на основании которого все лица, учреждения и образования, государственные и частные, в том числе и само государство, подчиняются законам, которые публично принимаются, равным образом исполняются, подлежат независимому судебному контролю и

соответствуют международным нормам и стандартам в области прав человека. Принцип верховенства права предусматривает верховенство закона, равенство перед законом, подотчетность закону, справедливость при применении закона, разделение властей, участие в процессе принятия решений, правовую определенность, необходимость избегать произвола, а также обеспечение процедурной и правовой прозрачности.

Основные тесты на соблюдение «верховенства права», разработанные Европейским судом по правам человека

Европейский суд по правам человека в своей прецедентной практике разработал подробные тесты на определение «верховенства права», и эти тесты применяются остальными международными органами по защите прав человека. Чтобы пройти такой тест, ограничения основных прав должны быть основаны на ясных, точных, доступных и прогнозируемых правовых нормах и при этом служить четко определенным законным целям; они должны быть «необходимыми» и «соразмерными» соответствующей законной цели (при определенных «пределах усмотрения»); и при этом должно иметься «эффективное [предпочтительно судебное] средство правовой защиты» в отношении предполагаемых нарушений этих требований.

«Каждый», без дискриминации

Одной из отличительных черт международного права в области прав человека с 1945 года и одним из его величайших достижений является то, что права человека должны быть обеспечены «каждому», то есть всем людям: это – права человека, а не просто права граждан.

Таким образом, за крайним исключением, все законы, затрагивающие права человека или предусматривающие вмешательство в них, должны применяться к «каждому» без «какой бы то ни было» дискриминации, включая дискриминацию по признаку места проживания или гражданства.

Учитывая уникальную роль самих Соединенных Штатов, а также американских компаний в функционировании Интернета, конституционная и корпоративная нормативная база США имеет особое значение. Однако, в отличие от вышеуказанного принципа международного права в области прав человека, многие гарантии прав человека, содержащиеся в Конституции США и в различных законах США, связанных с цифровой средой, применяются лишь к американским гражданам или негражданам США, проживающим в этой стране («US persons»). И только на эту группу лиц – граждан США и лиц, там проживающих, - распространяются первая Поправка к Конституции, охватывающая свободу слова и свободу объединения; четвертая поправка, защищающая граждан США от «необоснованных обысков»; и большинство (ограниченных) видов защиты от чрезмерного наблюдения (защита, предусмотренная в основных законодательных актах о национальной безопасности и разведки) (Поправка к Акту о наблюдении за иностранной разведкой (FISA) и Патриотический акт).

«[На территории и] под юрисдикцией [договаривающегося государства]»

Обязанность государств исполнять обязательства на основании международного права в области прав человека, в том числе и при экстерриториальных действиях

Основные международные договоры в области прав человека, включая Международный пакт о гражданских и политических правах (МПГПП) и Европейскую конвенцию о правах человека (ЕКПЧ), обязывают государства «обеспечивать» или «гарантировать» права человека, закрепленные в этих договорах, «каждому, находящемуся под их юрисдикцией». Это требование все больше приобретает функциональное, а не территориальное значение – как это недавно было подтверждено Комитетом по правам человека и Европейским судом по правам человека. Иными словами, каждое государство должно обеспечивать или гарантировать эти права лицам, находящимся под их физическим контролем, или же лицам, чьи права были затронуты действиями государства (или его органов).

Таким образом, государства должны соблюдать свои международные обязательства в области прав человека при любых действиях, которые они предпринимают и которые могут затронуть права отдельных лиц – даже если эти действия являются экстерриториальными или имеют экстерриториальные последствия.

Это обязательство имеет конкретные последствия для информации – из которой и состоит цифровой мир – и особенно для персональных данных, как это признается европейским правом о защите данных. Эта отрасль права защищает лиц, чьи данные обрабатываются европейскими органами контроля, независимо от места проживания, гражданства или иного статуса. Однако США официально отвергают такое применение международного права в области прав человека. Учитывая доминирование США (и американских корпораций, подчиняющихся юрисдикции этой страны) в цифровой среде, это создает серьезную угрозу верховенству права.

Сложности, связанные с конкурирующими и конфликтующими законами, применимыми одновременно к деятельности «онлайн», с конкретной ссылкой на свободу выражения мнения

Проблема применения конкурирующих – и конфликтующих – национальных законов к Интернет-материалам и деятельности в Интернете – это именно тот вопрос, который необходимо срочно урегулировать для обеспечения верховенства права в Интернете.

Проблема заключается не в возможности правительств предпринимать действия, которые соответствовали бы международному праву и которые были бы необходимы и соразмерны в демократическом обществе. Учитывая эти ограничения, правительства должны иметь свободу усмотрения в рамках собственной юрисдикции. Проблема – в способности и в праве национальных правительств или судов устанавливать ограничения в третьих странах, где лица действуют на основании собственных законов страны проживания, и эти

законы, в отличие от иностранных, должны быть известны (или «доступны») и при этом прогнозируемы в применении.

В принципе, лица и компании, которые публикуют информацию из своей страны пребывания (проживания), должны соблюдать законы лишь этой страны. Можно ожидать соблюдения законов страны пребывания от лиц, имеющих доступ к материалам или скачивающих материалы с иностранных веб-сайтов, если они могли или должны были знать, что эти материалы являются незаконными в стране их проживания. Теоретически, государства должны распространять свою юрисдикцию в отношении лишь тех иностранных материалов, которые являются законными исходя из норм международного права, и только при наличии четкой и тесной связи между этими материалами или их распространителем и государством, осуществляющим соответствующие действия.

Права человека и частные компании

Международное право в области прав человека и Принципы Рагги, а также Совет Европы и другие рекомендации

Международное право в области прав человека применяется в основном в отношении государств и государственных органов. Однако появляются и новые международные стандарты, которые должны применяться компаниями. Наиболее важными являются Руководящие принципы предпринимательской деятельности в аспекте прав ООН (Принципы Рагги), подготовленные Специальным представителем Генерального секретаря ООН в области предпринимательства и прав человека профессором Джоном Рагги. При этом Принципы Рагги по-прежнему сосредоточены на обязанности государств противодействовать нарушениям прав человека со стороны компаний. Они не затрагивают подробно обратную ситуацию – когда государства принуждают компании к действиям, влекущим нарушения международного права в области прав человека.

Важно разработать дополнительные рекомендации со стороны Совета Европы и других органов об ответственности бизнеса, который сталкивается с требованиями правительств или иных частных структур поддержать меры, способные нарушить международное право в области прав человека (более подробно об этом говорится в разделе об исполнении положений частного права).

Фильтрация и блокирование со стороны Интернет- и электронно-коммуникационных компаний по указанию или при "поощрении" со стороны государств

Помимо наложения уголовного запрета на материалы в Интернете – что, при производстве материалов в другой стране, часто происходит после их публикации – учащаются попытки государств блокировать доступ к определенным материалам и информации «онлайн». Такое блокирование или фильтрация осуществляется программным обеспечением или аппаратными средствами, которые позволяют просматривать сообщения и принимать решения на основе заранее определенных критериев о необходимости блокировать направление материалов адресату – лицу, просматривающему страницу в Интернете.

Неудивительно, что репрессивные государства пытаются заблокировать доступ к оппозиционным веб-сайтам и что теократические режимы делают то же самое по отношению к веб-сайтами, которые они рассматривают как богохульные. Однако все больше государств, в которых, как принято считать, соблюдается верховенство права, включая государства члены Совета Европы, также либо предпринимают попытки блокировать доступ к так называемым неприемлемым материалам, либо в более скрытых и подконтрольных формах «поощряют» структуры, контролирующие доступ к Интернету (провайдеров Интернет-услуг и операторов мобильных сетей), делать это «добровольно», вне четких юридических рамок публичного права.

Изначально в демократических странах меры блокирования или фильтрации, по крайней мере официально, были по преимуществу направлены на очевидно законные цели: борьбу с разжиганием ненависти на почве расовой или религиозной розни и противодействие детской порнографии. Однако данные подходы имеют серьезные недостатки в том виде, в котором они существуют:

- блокирование само по себе может (непреднамеренно) привести к неправильным «позитивным результатам» (блокирование веб-сайтов, не содержащих запрещенных материалов) и неправильным «негативным результатам» (когда веб-сайт с запрещенными материалами проскальзывает сквозь фильтр);
- критерии выбора сайтов для блокирования, и списки заблокированных веб-сайтов часто являются неконкретными, а в худшем случае – секретными;
- процесс обжалования может быть дорогостоящим, малоизвестным или вообще отсутствовать, особенно в тех случаях, когда решение о блокировании намеренно возлагается на частные структуры;
- меры по блокированию легко обойти даже не очень технически грамотным людям;
- и, что крайне важно особенно в отношении детской порнографии, блокирование полностью игнорирует реальную проблему: надругательства над этими детьми.

Вышеизложенные проблемы усугубляются тем фактом, что внедрив блокирование в отношении наиболее серьезных случаев, таких как детская порнография и разжигание ненависти, государства стали распространять эти процедуры на остальные, не угодные им, темы. В глобальном плане, в том числе в Европе, со стороны государств наблюдаются попытки заблокировать веб-сайты, содержащие не только призывы к ненависти и поддержку терроризма, но и, например, политические дискуссии или информацию о сексуальных правах или правах меньшинств.

Полезно проводить различие между двумя разными ситуациями: блокирование контента, основанное на законе, и блокирование, не основанное на законе. Нет сомнений в том, что определенный контент может быть законным объектом блокирования (блокирование незаконного контента на правовой основе). Однако цель блокирования и используемые для этого технические средства попрежнему имеют принципиально важное значение для определения, является ли мера соразмерной и, исходя из этого, законной. Например, если уровень

случайного доступа к данному контенту незначителен или если намеренный доступ к контенту относительно легок даже после принятия меры по блокированию, соразмерность блокирования остается сомнительной.

Ситуация усложняется, если решение о том, какие веб-сайты подлежат блокированию, передается на усмотрение частных структур, «поощряемых» государствами, которые при этом заявляют, что они не несут ответственности за блокирование (блокирование контента, не основанное на законе). Некоторые страны, такие как Соединенное Королевство и Швеция, внедрили системы блокирования, основанные на добровольных договоренностях с Интернет провайдерами. Тогда как вопросы об эффективности и соразмерности, остаются актуальными и для этого типа блокирования, возникает более общий и глубокий вопрос, на который необходимо ответить: в какой степени данные меры по блокированию являются добровольными и/или влекут ли они за собой ответственность государства? Тот факт, что в статье 10 ЕКПЧ говорится только о вмешательстве в это право «со стороны публичных властей», не означает, что государство не несет ответственности за меры, принимаемые частными структурами, тем более, если государство активно поощряет такие меры. Можно говорить об ответственности государства за отсутствие у этой системы взаимодействия законодательной базы, поскольку без такой основы ограничения не опираются на «закон».

В своей недавней прецедентной практике Европейский суд по правам человека четко заявил об опасности неразборчивого блокирования. В своем постановлении по делу *«Йильдирим (Yildirim) против Турции»* Суд отметил, что блокирование доступа из Турции ко всем веб-сайтам Google было произволом и цель блокировки, а именно отсутствие доступа к конкретному веб-сайту, который рассматривался как неуважительный по отношению к Кемалю Ататюрку, не была очевидна в виду масштабов блокирования. Более того, процедуры судебного обжалования блокирования веб-сайтов в Интернете были оценены как несоответствующие критерию отсутствия злоупотреблений, поскольку национальное законодательство не содержало гарантий того, чтобы указание о блокировании конкретного веб-сайта не использовалось в качестве средства блокирования доступа в целом. Исходя из этого, Суд установил нарушение статьи 10 ЕКПЧ.

Неразборчивое использование Глубокой Инспекции Пакетов (DPI) компаниями на основании судебных постановлений, принятых по запросу других компаний для соблюдения авторского права

Владельцы интеллектуальной собственности все чаще просят установить фильтры или блокирование, аналогичные тем, которые описаны выше, для сайтов, которые, предположительно способствуют обмену пиратским содержанием. Также все чаще звучат просьбы обеспечить правообладателям доступ к координатам Интернет-пользователей, скачивающих пиратский контент, в том числе посредством обязательного использования DPI со стороны Интернет-провайдеров, для выявления вероятных (или возможных) нарушителей прав.

Глубокая инспекция пакетов требует от «инспектора» изучить не только широкие метаданные, связанные с происхождением и предназначением «пакета», но и содержание этих коммуникаций. «Пакеты» выбираются исходя из шаблона или

алгоритма, связанного с конкретным контентом. Для владельцев интеллектуальной собственности это будут особые маркеры для конкретного видео или фотографий, защищаемых авторским правом. Однако эта технология позволяет вести поиск практически чего угодно: определенных политических высказываний, революционной песни или профсоюзного лозунга. Подобные меры крайне навязчивы, потому что предполагают наблюдение Интернет провайдера (или мобильной телефонной сети) за всеми пользователями с целью выявления тех немногих пользователей, которые, предположительно нарушают авторское право, и таким образом вновь возникают серьезные сомнения насчет соответствия таких мер критериям необходимости и соразмерности.

Как Европейский суд по правам человека, так и Суд Европейского Союза вынесли важные судебные постановления, в которых настойчиво подчеркивается, что проводимая Интернет-провайдером (или оператором мобильных сетей) неразборчивая фильтрация всех коммуникаций – то есть общий мониторинг или слежение – за всеми невиновными пользователями с целью выявления возможных нарушителей, противоречит нормам прав человека.

Экстерриториальная юрисдикция государств

Государство осуществляет экстерриториальную юрисдикцию в отношении другого государства, когда использует свои законодательные и исполнительные полномочия для установления и осуществления контроля в отношении данных, которые находятся за пределами его физической территории и на территории другого государства. Как правило, для извлечения данных с серверов в другом государстве используется физическая инфраструктура Интернета и глобальные системы коммуникаций. Возможно также принуждение частных структур, которые имеют доступ к данным за границей, извлекать эти данные с заграничных серверов или устройств и передавать их государству.

В соответствии с международным публичным правом, для обеспечения законности и в отсутствие договоров по предоставлению иностранным органам полномочий экстерриториально распространять свою юрисдикцию на территорию другого государства необходимо согласие этого государства.

Проблемы и установление баланса

Проблемы

Установление верховенства права в Интернете и в остальном цифровом мире потребует уточнения норм, затрагивающих свободу выражения мнения, деятельность частных структур (особенно корпораций), а также права человека, защиту данных и киберпреступность; при этом возникает необходимость ответить на вопрос: как найти необходимое равновесие между названными аспектами в этой новой среде?

Свобода выражения мнения

Национальные законы, связанные с деятельностью в Интернете и в остальной цифровой среде, особенно законы затрагивающие свободу выражения мнения,

часто противоречат друг другу. В соответствии с законодательством большинства государств, лица, делающие заявления «онлайн» или посредством электронных коммуникаций в/из одной страны, могут быть привлечены к ответственности в соответствии с законодательством другой страны, если эти заявления нарушают законы данной страны, невзирая на правомерность таких заявлений в стране, где/откуда они были сделаны. Все это создает серьезнейшую угрозу верховенству права в Интернете и в соответствующей среде. Пока эти аспекты не были освещены в полной мере в прецедентной практике Европейского суда по правам человека.

Как отмечалось выше, единственный способ решения данной проблемы состоит в том, чтобы государства и национальные суды демонстрировали последовательное противодействие навязыванию национальных юридических стандартов в отношении того, как выражены мнения и подана информация, распространяемая в сети Интернет из-за границы. Исключения составляют случаи, когда эти действия незаконны на основании международного права или имеются очевидные основания для осуществления юрисдикции данного государства.

Еще один важный вопрос – ответственность отдельных лиц и компаний, управляющих веб-сайтом, или даже Интернет-провайдеров за контент, размещенный на веб-сайте. Здесь прецедентная практика на европейском уровне на сегодняшний день также ограничена. В настоящий момент, как представляется, частные компании оказались между четкими обязательствами (удалять контент или быть наказанными) и неясными обязательствами (гарантировать пользователям доступ к законному контенту). В результате, частные компании могут переусердствовать и воспрепятствовать всем пользователям в доступе к совершенно законным материалам. Чтобы защитить себя от возможных жалоб со стороны пользователей, испытывающих негативные последствия таких решений, им навязываются неясные и двусмысленные условия договоров. Это – ключевые проблемы, которые необходимо урегулировать.

Исполнение законов частными лицами

Тот факт, что Интернет и остальное цифровое пространство во многом контролируются частными структурами (по преимуществу корпорациями США), угрожает верховенству права. Частные компании могут навязывать ограничения (или же «поощряться» за это) в отношении доступа к информации, при этом не подвергаясь ограничениям на основании конституционного и международного права, поскольку последние распространяются исключительно на государства. Эти частные компании могут также получать указания от национальных судов, действующих по просьбе других частных компаний, осуществлять весьма интрузивный анализ данных для выявления реальных (или вероятных) нарушений прав частной собственности, а зачастую и прав интеллектуальной собственности. Могут быть даны указания «изъять» данные, в том числе правительственные, коммерческие и личные, из серверов в других странах для целей соблюдения закона или для обеспечения национальной безопасности. Это может происходить в отсутствие согласия другой страны, компании или иных субъектов этих данных, в нарушение суверенитета стран, коммерческой тайны, а также в нарушение прав человека в отношении лиц, информация о которых подвергается воздействию.

В принятых ООН Принципах Рагги подчеркивается важность и необходимость решения этих вопросов, однако не содержится ответов на них. С учетом вышеизложенного, необходимы новые подходы и руководящие принципы. Совет Европы внес важный вклад в эти обсуждения, предложив государствам нести ответственность в том случае, если они не обеспечивают соблюдение прав человека частными компаниями, и обязать государства обеспечивать признание недействительности тех условий частноправовых договоров, которые не соответствуют международным стандартам в области прав человека.

Защита данных

Европейское право в сфере защиты данных основывается на ряде принципов (справедливая обработка; четкое определение ограничение целей; минимизация данных; качество данных; и защита данных), а также на ряде прав (прав субъекта данных) и средствах правовой защиты (надзор со стороны независимого органа защиты данных) – это является конкретным выражением общих принципов «верховенства права», разработанных Европейским судом по правам человека. Конвенция Совета Европы о защите частных лиц в отношении автоматизированной обработки данных (Конвенция № 108) и нормы ЕС в данной области уточняют, как необходимо обеспечивать исполнение прав человека в контексте обработки личных данных. Европейская модель защиты данных все шире используется за пределами Совета Европы: Конвенция № 108 (которая сейчас находится в процессе модернизации) становится глобальным «золотым» стандартом обеспечения международного верховенства права в данной сфере. Это имеет важнейшее значение и для Интернета, и для остального цифрового мира.

Европейская защита данных была дополнительно укреплена постановлением Суда Европейского Союза, который отклонил обязательное, не основанное на подозрениях, и нецелевое сохранение данных. В связи с дискуссиями о деятельности разведывательных служб и служб безопасности, вызванными откровениями Эдварда Сноудена, становится понятно, что программы тайного, массового и неразборчивого слежения не соответствуют европейским нормам в области прав человека и не могут быть оправданы борьбой с терроризмом или иными угрозами национальной безопасности. Такое вмешательство может быть обосновано исключительно в случае острой необходимости и соразмерности законной цели.

Защита данных в рамках европейских стандартов представляет собой первый и краеугольный камень установления верховенства права в Интернете и в остальной цифровой среде. Следовательно, принципиально важным представляется, чтобы проходящий ныне пересмотр (модернизация) Конвенции № 108 не привел к снижению этих стандартов. Присоединение США к Конвенции № 108 было бы особо ценным, не только для граждан США, но и как шаг в направлении всеобъемлющего глобального подхода к соблюдению основных прав на защиту данных и связанных с ними прав.

Киберпреступность

Конвенция о киберпреступности требует от Государств-Сторон уголовного преследования на основании национального законодательства таких действий,

как незаконный доступ к компьютерным системам (хакерство), незаконный перехват электронных коммуникаций, распространение вирусов, нарушение авторских прав и производство или распространение детской порнографии. Дополнительный протокол к Конвенции требует от Государств-Сторон преследовать в уголовном порядке распространение расистских и ксенофобских материалов («разжигание ненависти»). В Конвенции содержится подробное положение о международном сотрудничестве в борьбе с подобными преступлениями, включая оказание правовой помощи в расследовании и сохранении улик, экстрадицию и аналогичные вопросы. Данная Конвенция открыта для неевропейских государств и была ратифицирована пятью из них, в том числе США.

Несмотря на то, что необходимость соглашения о борьбе с преступностью в глобальной цифровой среде несомненна – и можно выразить признательность Совету Европы за инициирование этого процесса – данная Конвенция не может в полной мере обеспечить соблюдение принципов верховенства права.

Одной из причин является отсутствие в Конвенции ясного и детального положения о правах человека, и поэтому она не обеспечивает достаточную защиту в государствах, материальное право которых использует необоснованно широкие формулировки составов уголовных правонарушений или же не предусматривает обстоятельства, исключающие или смягчающие ответственность (например, гарантии гражданам, которые сообщают о правонарушениях). Конвенция не защищает также от повторного привлечения к уголовной ответственности и не предоставляет гарантий (ни официальных, ни неофициальных) помощи государствам-сторонам в случае, когда это может нарушить права человека.

Еще одной причиной является то, что Конвенция не связана с иными важными документами, разработанными Советом Европы для поддержания верховенства права в цифровом и/или транснациональном контексте. Такая связь представляется тем более необходимой, учитывая, что Конвенция открыта для государств, не являющихся сторонами ЕКПЧ или не в полной мере принявших соответствующие требования Международного пакта о гражданских и политических правах (например, США в отношении экстерриториальной деятельности или в отношении прав лиц, которые не являются гражданами США и не имеют вида на жительство или политического убежища в США). Для обеспечения верховенства права в Европе, присоединение к Конвенции о киберпреступности должно требовать полного принятия государствами их обязательств на основании ЕКПЧ и/или МПГПП и ратификации Конвенции о защите данных, Европейской конвенции о выдаче и Европейской конвенции о взаимной помощи по уголовным делам.

Наконец, статьи 26 и 32 Конвенции, как представляется, содействуют тенденции правоохранительных органов прибегать к «неофициальным» средствам по сбору информации, в том числе и заграницей, не предусматривая при этом четких гарантий (например, что такие неофициальные меры не должны использоваться для интрузивного сбора информации, для которого в правовом государстве потребовалось бы судебное постановление). Кроме того, представляется, что эти две статьи, подкрепляют тенденцию государственных органов «изымать» данные напрямую с серверов в других странах либо требовать, чтобы компании, находящиеся под их юрисдикцией – прежде всего основные

гиганты Интернета – делали бы это за них, не прибегая при этом к официальным межгосударственным договоренностям о взаимной правовой помощи и явно нарушая суверенитет тех государств, где находятся эти данные.

Принцип - установленный в статье 16 Конвенции № 108 в отношении взаимной помощи между органами, занимающимися защитой данных - согласно которому существуют ограничения обстоятельств, когда личные данные можно собирать и/или передавать в рамках транснациональных действий, должен быть более четко сформулирован в Конвенции о киберпреступности. В ряде рекомендаций и деклараций Комитета министров Совета Европы предоставляются полезные ориентиры для установления равновесия между принципами сохранения защиты данных и применения соответствующих правоохранительных мер. Требуется усиливать соблюдение этих документов со стороны государств-членов, которые являются также и сторонами Конвенции о киберпреступности.

Подготовка предлагаемого нового Дополнительного протокола к Конвенции о киберпреступности дает возможность решить, по крайней мере, некоторые из этих вопросов. Благодаря таким улучшениям Конвенция о киберпреступности могла бы стать вторым краеугольным камнем в установлении верховенства права в Интернете и в остальном цифровом мире.

Национальная безопасность

Как Европейская конвенция о защите прав человека, так и Конвенция Совета Европы о защите данных в принципе применимы в отношении любых действий государств - участников этих конвенций. Несмотря на отсутствие прямого упоминания деятельности в сфере национальной безопасности в тексте названных конвенций, эта сфера напрямую не исключается из области их применения. В этом смысле полномочия Совета Европы и сфера действия его инструментов отличаются от законодательства ЕС, которое непосредственно исключает национальную безопасность из компетенции и юрисдикции Союза. Это означает, что, когда речь заходит о международном правовом регулировании деятельности национальных органов безопасности и разведки, Совет Европы должен играть лидирующую роль, если не в масштабах всего мира, то, по крайней мере, в Европе.

Необходимость обеспечить верховенство права в деятельности органов национальной безопасности и разведки возникла в связи с откровениями Эдварда Сноудена о глобальных операциях по слежению со стороны Агентства национальной безопасности США (АНБ), Центра правительственной связи Соединенного Королевства (GCHQ) и, в частности, их партнеров по группе 5EYES (Австралия, Канада и Новая Зеландия). Благодаря этим откровениям стало известно, что названные агентства рутинно прослушивают оптоволоконные кабели высокой емкости, которые образуют основную структуру Интернета, а также перехватывают мобильные и другие переговоры по всему миру и в огромных масштабах, например, осуществляя перехват радиокоммуникаций, используя «черные ходы», созданные ими в основных системах коммуникаций, и эксплуатируя несовершенности в защите этих систем.

Ни в европейском, ни в международном праве в области прав человека национальная безопасность не является аргументом, который способен перевесить

остальные соображения. Действительно, сам объем понятия «национальной безопасности» относится к сфере судебного усмотрения: именно суды должны определять, с учетом международного права в области прав человека, что охватывается данным термином. Полезные рекомендации в этой связи изложены в Йоханнесбургских принципах национальной безопасности, свободы выражения мнения и доступа к информации, которые были подготовлены НПО «Статья 19» и поддержаны рядом международных форумов, включая Специального докладчика ООН по свободе слова и выражения мнений. Названные принципы свидетельствуют о том, что государства могут ссылаться на национальную безопасность как на основание для вмешательства в права человека в связи с угрозами самому устройству государства и его основным институтам. Иногда угроза терроризма может достигать названного уровня серьезности, однако в большинстве случаев этим должны заниматься правоохранительные органы, причем не в рамках парадигмы национальной безопасности. То же относится и к действиям государств в сфере Интернета и электронных коммуникаций.

На сегодняшний день отсутствуют четкие договорные правила, регулирующие действия органов национальной безопасности и разведки, а также отсутствует основа их деятельности и обмена данными. Во многих странах не достает четких опубликованных законов, регулирующих работу таких органов. В некоторых странах опубликованные нормы вообще отсутствуют. До тех пор пока не известны правила, на основании которых действуют эти органы и службы – на национальном, экстерриториальном уровне или во взаимодействии друг с другом – их деятельность не может рассматриваться как соответствующая верховенству права. Еще один вопрос, вызывающий серьезную обеспокоенность – это проявление неэффективности многих систем надзора.

Иными словами, в области национальной безопасности в настоящее время не существует реальной опоры для поддержания верховенства права, хотя и имеются по крайней мере базовые принципы, которые могли бы составить фундамент этой важнейшей части общей конструкции прав человека.

Учитывая укрепление партнерских связей между правоохранительными органами и органами разведки и безопасности, подобное отрицание верховенства права угрожает распространиться и далее – на сотрудников полиции и прокуроров. В этой связи отсутствие четких правовых рамок, как на национальном, так и на международном уровне, представляет собой дополнительную угрозу верховенству права в Интернете и в глобальной цифровой среде.

Рекомендации Комиссара

Исходя из данного тематического доклада, Комиссар предлагает следующие рекомендации, направленные на совершенствование соблюдения верховенства права в Интернете и в остальной цифровой среде.

I. Об универсальном характере прав человека и их равном соблюдении «онлайн» и «офлайн»

1. Основные требования верховенства права применяются и должны применяться на практике, равным образом как «онлайн», так и «офлайн». Это означает, в частности, что:

- Европейская конвенция о защите прав человека (ЕКПЧ) и правила Совета Европы в области защиты данных применяются ко всем действиям по обработке личных данных всеми органами всех государств-членов Совета Европы, включая органы национальной безопасности и разведки государств-членов;
- Государства не должны использовать договоренности с частными компаниями, которые контролируют Интернет и остальное цифровое пространство, чтобы обойти закрепленные в статье 8 (Право на уважение частной и семейной жизни) и статье 10 (Свобода выражения мнения) ЕКПЧ обязательства по обеспечению верховенства права;
- государства-члены Совета Европы должны стремиться обеспечивать аналогичное соблюдение неевропейскими государствами их международных обязательств в области прав человека во всех сферах их деятельности, где затрагиваются лица, использующие Интернет, или же иным образом действующие в остальном цифровом пространстве; и
- государства (и органы государства, включая правоохранительные органы и органы национальной безопасности и разведки), европейские или иные, не должны иметь доступ к данным, хранящимся в другой стране – или же передающимся по Интернет-кабелям и «магистральным» кабелям электронных коммуникаций между странами – без непосредственного согласия соответствующей страны. Исключение составляет наличие ясного и строго ограниченного основания такого доступа в международном праве, при условии, что такой доступ сообразуется с международной защитой данных и соответствует стандартам прав человека.

II. О защите данных

2. Государства-члены, которые еще не успели этого сделать, должны ратифицировать Конвенцию Совета Европы о защите физических лиц при автоматизированной обработке персональных данных (Конвенция № 108). Данная конвенция открыта также для государств-нечленов, и, если будет широко принята, сможет стать краеугольным камнем верховенства права в Интернете и в остальной цифровой среде.

3. Те государства-члены, которые уже ратифицировали названную конвенцию, должны обеспечивать ее полное соблюдение на национальном уровне.

4. Осуществляемый сейчас пересмотр Конвенции № 108 не должен привести к какому-либо снижению европейских и всемирных стандартов защиты данных. Наоборот, это должно привести к уточнению и более эффективному исполнению норм, прежде всего в отношении Интернета и остальной цифровой среды, а также в отношении применения мер слежения в интересах национальной безопасности и разведки.

5. В контексте осуществляемой реформы правил защиты данных ЕС, должны быть уточнены и приведены в соответствие с международными обязательствами в области прав человека уже существующие правила, которые могут подрывать верховенство права, например, связанные с согласием, профилированием или доступом иностранных правоохранительных органов к личным данным, включая те, что вытекают из Конвенции № 108, а также из соответствующих рекомендаций и руководящих принципов Совета Европы.

6. Массовое сохранение коммуникационных данных без наличия подозрений в основе своей противоречит верховенству права, несовместимо с основными принципами защиты данных и является неэффективным. Государства-члены не должны прибегать к этой мере и не должны устанавливать обязательное сохранение данных третьими лицами.

III. О киберпреступности

7. Государства-стороны Европейской конвенции о киберпреступности должны полностью выполнять свои международные обязательства в области прав человека, действуя (либо бездействуя), в рамках данной конвенции, как при определении соответствующих преступлений (их составов, связанных с ними обстоятельств, исключающих и смягчающих ответственность), так и при ведении уголовных расследований, исполнении наказаний, либо же при осуществлении взаимной правовой помощи и экстрадиции.

8. Если какое-либо государство-сторона предпринимает действия, которые затрагивают лиц вне его территории, оно не освобождается от обязательств в соответствии с Конвенцией о киберпреступности и международных договоров в области прав человека (в первую очередь ЕКПЧ и МПГПП). Напротив, эти обязательства точно также распространяются на подобные экстерриториальные акты.

9. Все государства-стороны Конвенции о киберпреступности должны ратифицировать и строго соблюдать Конвенцию о защите данных, Европейскую конвенцию о выдаче и Европейскую конвенцию о взаимной помощи по уголовным делам.

10. Государства-члены, включая их правоохранительные органы, должны выполнять Рекомендацию № R (1987) 15 Комитета министров Совета Европы о регулировании использования личных данных в сфере деятельности полиции, а также Рекомендацию Rec(2010)13 о защите лиц в отношении автоматической обработки личных данных в контексте профилирования и его Декларацию 2013 о рисках для основных прав, вытекающих из цифрового слежения или иных технологий для проведения слежения.

11. Государства-члены должны обеспечивать, чтобы их правоохранительные органы не получали данных с серверов или инфраструктур в другой стране на основе неофициальных договоренностей. Вместо этого должны использоваться договоренности о взаимной помощи и специальные договоренности о срочном сохранении данных, как это предусмотрено Конвенцией о киберпреступности. Правоохранительные органы в одной стране не должны ссылаться на тот факт, что частные структуры – такие как провайдеры Интернет-услуг, социальные сети или операторы мобильных систем – в других странах получили разрешение на раскрытие данных своих клиентов на основании общих положений и условий, поскольку получение данных при этих обстоятельствах противоречит верховенству права и не должно иметь места.

IV. О юрисдикции

12. Должны быть установлены пределы экстерриториального осуществления национальной юрисдикции в отношении транснациональных киберпреступлений. Эти пределы должны исходить из определения состава соответствующего правонарушения, а также обстоятельств смягчающих или исключающих юридическую ответственность согласно национальному праву страны предполагаемого нарушителя (либо страны, в которой произошло предполагаемое правонарушение) в случае если право страны, которая имеет юрисдикцию в данном конкретном деле, определяет это преступление шире, либо не содержит таких же обстоятельств, смягчающих или исключающих ответственность.

13. В отношении права на свободу выражения мнения, отдельные лица и компании, которые распространяют информацию из своей страны проживания или пребывания, должны, в принципе, соблюдать лишь законы данной страны; если лица имеют доступ к материалам или скачивают их с иностранных веб-сайтов (в случаях, когда они могли или должны были бы знать, что эти материалы являются незаконными в их стране проживания), то от них должно ожидаться соблюдение законов своей страны. Помимо контента, который является незаконным на основании международного права, государства должны осуществлять юрисдикцию в отношении иностранных цифровых материалов лишь при ограниченных обстоятельствах, например, когда существует ясная и тесная связь между этими материалами и/или их распространителем с соответствующей страной.

V. О правах человека и частных компаниях

14. Государства-члены должны прекратить делегировать частным компаниям, которые контролируют Интернет и остальную цифровую среду, установление ограничений, нарушающих обязательства государства в области прав человека. Для этого необходимы дополнительные инструкции, при каких обстоятельствах действия или бездействие частных компаний, нарушающих права человека, влекут за собой ответственность государства. Сюда же можно включить рекомендации о необходимой доле участия государства в правонарушении для наложения на него ответственности, а также об обязательствах государства по приведению условий в частных компаниях в соответствие со стандартами в области прав человека. Ответственность государства в отношении мер, принимаемых частными сторонами по соображениям ведения бизнеса без прямого вовлечения государства, также должна быть рассмотрена.

15. Основываясь на Руководящих принципах ООН в сфере бизнеса и прав человека ООН (Принципах Рагги), необходимо разработать дальнейшие рекомендации об ответственности частных предприятий за их деятельность в Интернете или в остальной цифровой среде. В частности это необходимо для урегулирования ситуаций, при которых правительства предъявляют компаниям требования, идущие в разрез с международным правом в области прав человека.

VI. О блокировании и фильтрации

16. Государства-члены должны гарантировать, чтобы любые ограничения доступа к Интернет-контенту, которые затрагивают пользователей под их юрисдикцией, основывались на ясных и предсказуемых правовых нормах. Сфера действия любых ограничений также должна быть четко урегулирована. Для предупреждения возможных злоупотреблений большое значение имеет предоставление гарантий судебного контроля. Помимо этого, национальные суды должны установить, является ли мера по блокированию необходимой, эффективной и соразмерной, а также, носит ли она целевой характер, чтобы воздействовать лишь на конкретный контент, требующий блокирования.

17. Государства-члены не должны стимулировать частные структуры, контролирующие Интернет и остальное цифровое пространство, и поощрять блокирование за рамками, отвечающими вышеизложенным критериям.

VII. О деятельности в сфере национальной безопасности

18. Положения ЕКПЧ и Конвенции № 108 должны быть применимы в отношении любой деятельности государств, являющихся сторонами этих конвенций, в том числе в отношении деятельности органов национальной безопасности и разведки.

19. Конкретно говоря, для соблюдения верховенства права в Интернете и в остальной цифровой среде:

- государствам должно быть разрешено ссылаться на национальную безопасность в качестве обоснования вмешательства в права человека лишь в вопросах, которые угрожают устройству государства и его основным институтам;
- для осуществления вмешательства, мотивированного предполагаемой угрозой национальной безопасности, государства должны доказать неэффективность обычных средств уголовного права, которое соответствует международным стандартам уголовного права и процесса;
- вышесказанное применимо также к действиям государств в области Интернета и электронных коммуникаций.

20. Государства-члены должны установить правовые границы деятельности национальных органов безопасности и разведки. В отсутствие улучшения прозрачности правил, на основании которых действуют данные службы внутри страны, на экстерриториальной основе и/или в сотрудничестве друг с другом – их деятельность не может рассматриваться как соответствующая верховенству права.

21. Государства-члены должны также обеспечивать осуществление эффективного демократического надзора над службами национальной безопасности. Для того чтобы демократический надзор был эффективным, необходимо популяризировать культуру соблюдения прав человека и верховенства права, в особенности среди сотрудников служб безопасности.

Сегодня мы зачастую реализуем права человека через Интернет и при помощи остальной цифровой среды. Однако эти же средства могут быть использованы для нарушения наших прав.

Принято считать, что лица обладают равным объемом прав человека, как в реальной жизни, так и в сети - однако практика убеждает в обратном. В частности, на глобальном уровне Интернет и его физическая инфраструктура подвержены непропорциональному влиянию и контролю со стороны ряда государств и некоторых частных компаний.

В данном тематическом докладе рассматривается средства поддержания верховенства права в среде, характеризуемой вышеупомянутыми аспектами управления. Особое внимание уделяется таким важным с точки зрения защиты прав человека областям деятельности, как свобода слова, защита персональных данных, киберпреступность и национальная безопасность. В докладе также приводятся возможные пути обеспечения верховенства права в отношении деятельности в цифровой среде.

www.commissioner.coe.int

PREMS 176314 RUS

RUS

www.coe.int

Совет Европы является ведущей организацией на континенте в области прав человека. Он включает в себя 47 стран, 28 из которых являются членами Европейского Союза. Все страны-члены Совета Европы подписали Европейскую конвенцию о правах человека – международный договор, призванный защищать права человека, демократию и верховенство права. За применением Конвенции в государствах-членах следит Европейский суд по правам человека.

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE