Татьяна Тропина, старший научный сотрудник Института зарубежного и международного уголовного права им. Макса Планка

Споры вокруг директивы ЕС о сетевой и информационной безопасности отражают в целом более фундаментальную проблему выбора в сфере обеспечения информационной безопасности между добровольным сотрудничеством с индустрией или регулированием в форме прямого государственного вмешательства с наложением обязательств и последующими санкциями, а также гармонизации этих подходов на глобальном уровне.

Проект Директивы Европейского союза о сетевой и информационной безопасности: попытка гармонизации или путь к фрагментации?

Дебаты о подходах к сотрудничеству государства и бизнеса в сфере обеспечения информационной безопасности в Европейском союзе (ЕС) и о возможности гармонизации этих подходов ведутся на протяжении нескольких лет. Однако никогда эта тема не обсуждалась на уровне ЕС так остро, как весной и летом 2015 года. На протяжении последних месяцев дебаты сфокусировались на одном из ключевых вопросов, на который пока не найдено компромиссного ответа: необходимость регулирования компаний, представляющих индустрию интернет-услуг, в целях обеспечения информационной безопасности. Острота споров вокруг возможности регулирования обусловлена тем, что в течение десятилетий во многих государствах, включая государства–члены ЕС, подход к участию бизнеса в обеспечении информационной безопасности был основан на идеях о развитии добровольного сотрудничества в области обмена информацией о кибератаках и разработке совместных комплексных механизмов по предотвращению угроз.

Поводом для этих дебатов, исход которых может на следующее десятилетие определить вектор сотрудничества государства и бизнеса в сфере информационной безопасности, является проект **Директивы ЕС по сетевой и информационной безопасности**, который с 2013 года находится в стадии обсуждения в различных структурах ЕС. Именно сейчас, на финальной стадии переговоров по этому проекту, решается дальнейшая судьба возможной гармонизации подходов к этому сотрудничеству — и, более того, сама возможность такого сотрудничества в целом.

Проект директивы ЕС по сетевой и информационной безопасности: стадии и дебаты

Проект директивы по сетевой и информационной безопасности был представлен Европейской комиссией еще в феврале 2013 года. Основной целью директивы была гармонизация подходов к информационной безопасности в государствах–членах ЕС. Одно из самых значимых нововведений, вызвавшее жаркие дебаты и в итоге усложнившее достижение компромисса по поводу директивы и, как следствие, задержавшее ее принятие до сегодняшнего дня, — это предложение Европейской комиссии по наложению обязательств по сообщению об инцидентах в области информационной безопасности на частные компании. Размах этих обязательств покрывает широкий спектр компаний, оперирующих в области информационных технологий: и операторов критической инфраструктуры (в области энергетики, транспорта, финансовой отрасли, здравоохранения) и — что и стало камнем преткновения относительно различных подходов к обеспечению информационной безопасности — различные компании, представляющие интернет-индустрию. Количество субъектов, на которые предлагается наложить обязательство по сообщению об инцидентах в области информационной безопасности, превзошло по охвату все существующие подходы как в ЕС, так и вне его границ. Никогда прежде регулирование не распространялось на настолько широкий круг предприятий, оперирующих в области информационно-коммуникационных технологий. По сути, компании, оперирующие в области услуг сети Интернет, в проекте директивы применительно к обязательству по обмену информацией были приравнены по значимости — и, соответственно, по объему обязательств и ответственности, — к операторам объектов критической инфраструктуры. Так, приложение 2 к проекту директивы предлагало включить в круг регулируемых субъектов кроме операторов объектов критической инфраструктуры следующие организации, деятельность которых в ЕС определяется термином «услуги информационного общества»:

- *платформы электронной коммерции;*
- *компании, обеспечивающие доступ к системам интернет-платежей;*
- *социальные сети;*
- *поисковые системы;*
- *компании, работающие в сфере облачных вычислений;*
- *магазины программ-приложений.*

Включение операторов услуг информационного общества в круг регулируемых субъектов в области информационной и сетевой безопасности вызвало дебаты в связи с неопределенностью круга регулируемых субъектов, недостаточной ясностью положений об обязанности отчитываться об инцидентах в области сетевой безопасности, а также беспрецедентностью изменения подходов к информационной безопасности, а именно — поворота от концепции добровольного сотрудничества к государственному регулированию. В результате этих дебатов Европейский парламент в марте 2014 года принял проект директивы, но исключил операторов услуг информационного общества из круга регулируемых субъектов. После решения Европейского парламента, несмотря то что представители Европейской комиссии и некоторые эксперты выражали недовольство в связи с исключением нововведений по регулированию[1], казалось, что вопрос о наложении беспрецедентных обязательств на никогда прежде не регулируемые субъекты снят с повестки дня.

Однако в октябре 2014 года, когда проект директивы находился на последней стадии утверждения, а именно на рассмотрении Совета ЕС, вопрос о регулировании услуг

[1] См.: EU: Parliament's version of NIS Directive 'makes no sense'. Data Guidance. http://www.dataguidance.com/dataguidance_privacy_this_week.asp?id=2255

информационного сообщества встал гораздо острее, чем раньше. Выяснилось, что члены ЕС не могут прийти к консенсусу не только по вопросу о том, кто должен стать субъектом обязательств по сообщению об инцидентах в области информационной безопасности, но и о том, нужно ли налагать такие обязательства вообще. В итоге в проект директивы были внесены два основных изменения, касающиеся регулирования операторов услуг информационного общества. Во-первых, в список регулируемых субъектов не только были вновь внесены все исключенные Европейским парламентом операторы услуг информационного общества, но и в дополнение к ним Европейский совет предложил расширить список субъектов регулирования и включить в него точки обмена интернет-трафиком, регистраторов доменных имен и компании, предоставляющие услуги веб-хостинга. Во-вторых, поскольку государства–члены ЕС так и не смогли достичь консенсуса по вопросу о круге регулируемых субъектов, Совет ЕС в статье 3 (8) проекта директивы предложил оставить вопрос о включении того или иного вида компаний в список регулируемых субъектов (определение охвата регулирования) на усмотрение государств—членов ЕС.

Проблема выбора между добровольным сотрудничеством и государственным регулированием

Споры вокруг директивы ЕС о сетевой и информационной безопасности отражают в целом более фундаментальную (и в теории, и на практике) проблему выбора в сфере обеспечения информационной безопасности между добровольным сотрудничеством с индустрией или регулированием в форме прямого государственного вмешательства с наложением обязательств и последующими санкциями, а также гармонизации этих подходов на глобальном уровне. Эта проблема имеет несколько аспектов.

Первый и наиболее дискуссионный из них — это сама концепция «сотрудничества» и «государственно-частного партнерства» и расхождения в ее проявлениях в теории и на практике. В американских и европейских научных и экспертных исследованиях на тему государственно-частных партнерств именно концепции добровольного сотрудничества отдавалось предпочтение на протяжении многих лет, однако существующие формы такого сотрудничества зарождались на практике скорее как ответ на какую-либо существующую проблему или угрозу, как, например, сотрудничество государства и бизнеса по решению проблемы Millennium Software Bug в 1999 году или государственно-частная рабочая группа по устранению последствий вируса Conficker в 2008-2009 гг. Некоторые из инициатив в области государственно-частного сотрудничества не привели к успеху, многие испытывали недостаток предварительных договоренностей о правилах и рамках такого сотрудничества, однако несмотря на все трудности, механизмы обмена информацией и иной помощи друг другу между государством и бизнесом существовали и развивались вопреки всем недостаткам и трудностям, многие из них превратились в долговременное сотрудничество, основанное на доверии между сторонами. В этих обстоятельствах государственное вмешательство в виде наложения определенных обязательств в той области, где сотрудничество уже начало налаживаться, с одной стороны означает силой закона и под страхом санкций создать или усилить механизмы сотрудничества и силой принуждения «заставить» их работать. С другой стороны, такой подход пренебрегает уже сложившимися формами сотрудничества и тем уровнем доверия, которое стороны успели выработать друг к другу. Вместо того, чтобы развивать уже существующие инициативы, государственное вмешательство в виде регулирования по сути разрушает нынешние связи, построенные на добровольных началах, и заменяет их механизмами принуждения.

Роль доверия в механизмах сотрудничества в области информационной безопасности является еще одним ключевым моментом в проблеме выбора между государственным

принуждением и добровольным взаимодействием. Информационная безопасность — это скорее концепция и процесс, а не результат, и доверие между сторонами, участвующими в этом процессе, — некая нематериальная ценность, которую невозможно навязать или установить принятием закона об обязательном обмене информацией под угрозой санкций. Более того, такой подход может не только разрушить уже существующие доверительные отношения, но и серьезно ограничить возможности их построения в будущем. Именно доверие является основным спорным пунктом в дебатах вокруг директивы, которые в настоящее время проходят в Совете ЕС. Как говорится в одном из резюме этих дебатов,

«…Некоторые из делегаций особо подчеркивают, что эффективный опыт был набран на основе добровольного сотрудничества, и утверждают, что доверие не может быть навязано <законом>, в то время как другие <делегации> выражают уверенность в том, что результатом принятия Директивы станут зафиксированные обязательства <бизнеса>, которые со временем помогут построить доверие <между государством и бизнесом>…»[2]

Споры о причинно-следственных связях между доверием и обязательствами похожи на логический парадокс курицы и яйца. Позиция делегаций стран—членов ЕС по поводу того, что же все-таки первично — построение доверия между государством и бизнесом или принятие обязательств, зависит от состояния государственно-частного сотрудничества на национальном уровне и, конечно, от роли, которую доверие играет в уже существующих механизмах. К примеру, вряд ли можно ожидать сходных позиций от Великобритании и Германии.

Так, в Великобритании государство является одним из самых ярых сторонников концепции государственно-частного сотрудничества в сфере информационной безопасности. В Германии же в июле 2015 года был принят один из самых первых в ЕС законов об обязательствах бизнеса сообщать об инцидентах в сфере информационной безопасности[3] — закон, который, как и проект директивы ЕС, вызвал жаркие дебаты и был принят в форме компромисса, не устроившего в итоге ни сторонников, ни противников государственного регулирования. Этот закон уже и после его принятия вызывает шквал критики с обеих сторон по поводу содержащихся в нем недоработок и неопределенности как прописанных в нем обязательств, так и механизма их исполнения[4]. Позицию государств–сторонников прямого вмешательства — можно понять: на них давит необходимость предпринять усилия по обеспечению информационной безопасности, и государственное регулирование — это самый доступный и известный государственной власти способ решения проблем. Вопрос доверительных отношений в этом случае вторичен, потому что создание таких механизмов требует времени и больших усилий с обеих сторон — как государства, так и бизнеса. Однако опасность такого подхода в том, что, во-первых, доверие как элемент партнерства исключается из концепции регулирования, а во-вторых, обязательства налагаются во многих случаях на те компании, которые уже тем или иным образом предпринимают усилия в области обеспечения безопасности и сотрудничества с государством, фактически разрушая и слабые ростки этого доверия, и существующие механизмы сотрудничества.

---

[2] Council of the European Union (2014) Note from presidency to delegations. Proposal for a directive of the European parliament and of the council concerning measures to ensure a high common level of network and information security across the union. Preparations for the 1st informal exploratory trialogue. Brussels, 3 October 2014. Interinstitutional File: 2013/0027 (COD), 13848/14. http://www.statewatch.org/news/2014/oct/eucouncil-NIS-prep-trilogue-13848-14.pdf

[3] Gabel, D. & Schuba, M. Germany rolls out IT Security Act. http://www.whitecase.com/publications/article/germany-rolls-out-it-security-act

[4] Gaycken, S. Germany's Cybersecurity Law: Mostly Harmless, But Heavily Contested. http://blogs.cfr.org/cyber/2015/08/18/germanys-cybersecurity-law-mostly-harmless-but-heavily-contested/

Регулирование как индивидуальный выбор государств: гармонизация без гармонизации?

Во всех этих дебатах и попытках решить проблему выбора между сотрудничеством и регулированием, похоже, была забыта основная цель директивы ЕС: гармонизация подходов к обеспечению информационной безопасности. Из всех документов, отражающих процесс переговоров по директиве между делегациями в Совете ЕС, можно сделать вывод, что вряд ли возможен консенсус о том, какие компании необходимо регулировать, учитывая различие в подходах к механизмам государственно-частного сотрудничества на национальном уровне. Предложенное Советом ЕС «компромиссное решение» — а именно, введение в директиву статьи 3 (8) о том, что включение того или иного вида компаний в список остается на усмотрение государств—членов Европейского союза, на первый взгляд представляется логичным. Если государства не могут договориться о том, кого можно и нужно регулировать, то почему бы не принять общее рамочное соглашение об обязательствах бизнеса и оставить решение вопроса о наложении подобных обязательств на национальном уровне? Однако возникает вопрос: какие последствия такой подход может иметь для «гармонизации» подходов в государствах—членах Европейского союза? Уже на стадии обсуждения директивы стало ясно, что подходы к этой проблеме значительно отличаются. Последствием этих различий и поиска компромисса может стать принятие документа, который не только создает противоречия в решении важнейшего вопроса о государственно-частном сотрудничестве, но и оставит решение этой проблемы на усмотрение государств. Итогом такого компромисса может быть все что угодно, но не гармонизация подходов и не создание общеевропейской концепции регулирования и стратегий в области информационной безопасности. Скорее всего, результатом принятия и последующей имплементации директивы будет дальнейшая фрагментация подходов. Не совсем понятно, как такая фрагментация согласовывается с прилагаемыми в настоящее время усилиями по созданию единого европейского цифрового рынка: например, для панъевропейских компаний, ведущих деятельность в нескольких странах Европы, разница в обязательствах в области информационной безопасности в разных странах может создать большие неудобства. Более того, ЕС как часть глобального информационного сообщества этой директивой создаст дальнейшую фрагментацию и на общемировом уровне и, возможно,столкнется с проблемами регулирования компаний, зарегистрированных вне территории ЕС, но оперирующих, в том числе, и в странах ЕС.

Дальнейшие перспективы: принятие и имплементация

В настоящее время единственное, что можно предсказать о судьбе Директивы ЕС — это то, что скорее всего она будет принята. Безусловно, надежды Италии и Латвии, которые председательствовали в Совете ЕС во время переговоров по директиве, на ее принятие во время своего председательства не оправдались, несмотря на все приложенные к достижению консенсуса усилия. В настоящее время дебаты продолжаются уже под председательством в Совете ЕС Люксембурга. Однако и Европейская комиссия, и Совет ЕС неоднократно выражали твердое намерение сделать все возможное для принятия этой директивы в наиболее быстрые сроки. Возможно, именно эта непреклонность в достижении результата под названием «принятие директивы» и является причиной ее недоработок и компромиссов, последствия которых не проанализированы с достаточной осторожностью.

В какой редакции будет принята директива? Если говорить о спорных вопросах, то делать предсказания довольно сложно, так как малейшее изменение текста последнего предложенного варианта директивы может изменить очень многое. По последним сообщениям Reuters, компании-провайдеры услуг информационного общества все-таки останутся в списке регулируемых субъектов, однако рассматривается возможность

наложения на них меньшего количества обязательств, чем на операторов объектов критических инфраструктур.[5] Государства–члены ЕС в настоящий момент так и не достигли окончательного соглашения по вопросу о том, должен обмен информацией об инцидентах в области информационной безопасности осуществляться на добровольных началах или в обязательном порядке. Государства должны в очередной раз предоставить свое мнение по этому поводу в сентябре 2015 года, после чего планируется начать разработку окончательной версии текста директивы.

Учитывая то, что переговоры неоднократно заходили в тупик, скорее всего директива будет принята в редакции, содержащей наибольшее количество компромиссов и возможностей не имплементировать спорные положения на национальном уровне, что в итоге будет трудно назвать гармонизацией. Но самый важный вопрос — это даже не принятие директивы, а то, как и в какой форме она будет имплементирована государствами–членами ЕС. Все это означает, что в ближайшие несколько лет нас как минимум ожидает продолжение споров — уже не теоретических, а с практическими последствиями — о роли доверия в государственно-частных партнерствах, о выборе между обязательствами и добровольным сотрудничеством и о роли государственного принуждения в области обеспечения информационной безопасности. Возможно, в некой обозримой перспективе имплементация директивы ЕС все-таки сможет предоставить доказательства того, какие из этих моделей — регулирование или сотрудничество — лучше работают на практике. К сожалению, ценой получения таких доказательств может быть фрагментация подходов и разрушение уже существующих механизмов сотрудничества государства и частного сектора в области информационной безопасности.

[5] Reuters. Internet firms to be subject to new cybersecurity rules in EU. 06/08/2015. http://www.reuters.com/article/2015/08/06/us-eu-cybersecurity-idUSKCN0QB1ZD20150806