

Ноябрь 2024



МЕЖДУНАРОДНАЯ СИЛА В ЕДИНСТВЕ ЖИЗНЬ

*Проблемы
внешней политики,
дипломатии,
национальной
безопасности*



В номере:

Татьяна Москалькова, уполномоченный по правам человека в России. Интеграция на правозащитном треке

Петр Литвишко, заместитель начальника Главного управления международно-правового сотрудничества Генеральной прокуратуры России. Первый глобальный договор против киберпреступности

Филипп Трунов, ведущий научный сотрудник ИНИОН РАН. Россия как провайдер безопасности для Запада

Анатолий Бажан, руководитель отдела экономических исследований Института Европы РАН

Энварбик Фазельянов, ведущий научный сотрудник Института Европы РАН. Мировые рынки нефти и Европа



Петр Литвишко

Заместитель начальника Главного управления международно-правового сотрудничества Генеральной прокуратуры Российской Федерации - начальник управления правовой помощи и правоохранительного содействия, старший помощник Генерального прокурора Российской Федерации, кандидат юридических наук

petrlitvishko@yandex.ru

Ключевые слова: Конвенция ООН против киберпреступности, правовая помощь и правоохранительное содействие по уголовным делам, согласование языковых версий.

ПЕРВЫЙ ГЛОБАЛЬНЫЙ ДОГОВОР ПРОТИВ КИБЕРПРЕСТУПНОСТИ: ОТ ГЕОПОЛИТИЧЕСКОЙ КОНФРОНТАЦИИ К ПРОФЕССИОНАЛЬНОМУ КОМПРОМИССУ

В августе 2024 года Специальный комитет по разработке всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях (далее - Спецкомитет), учрежденный резолюцией Генеральной Ассамблеи ООН 74/247 от 27.12.2019, одобрил и представил для принятия Генеральной Ассамблее проект Конвенции ООН против киберпреступности; укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационно-коммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьезным преступлениям (далее - Конвенция, Конвенция ООН¹). Работа над договором велась в течение четырех лет, сессии Спецкомитета и консультации в межсессионные периоды проводились в штаб-квартирах ООН в Нью-Йорке и Вене².

ПЕРВЫЙ ГЛОБАЛЬНЫЙ ДОГОВОР ПРОТИВ КИБЕРПРЕСТУПНОСТИ:
ОТ ГЕОПОЛИТИЧЕСКОЙ КОНФРОНТАЦИИ К ПРОФЕССИОНАЛЬНОМУ...**Внешнеполитические аспекты Конвенции**

Существо и облик преступности и органов правопорядка современности высокотехнологичны и уже мало что общего имеют с противостоянием персонажей чапековских «карманных» рассказов относительно недавнего XX века. Излишне повторять здесь вездесущую статистику об экспоненциальном росте киберпреступлений у себя дома и за рубежом для простой констатации, что этот глобальный международный договор - более чем своевременное, долгожданное и знаковое событие для мирового сообщества.

Как бы то ни было, переговорный процесс по разработке Конвенции, запущенный по инициативе нашей страны, на всем своем протяжении был обременен крайне неблагоприятным геополитическим контекстом пика международной напряженности и неоднократно балансировал на грани срыва. В нем, как в нехорошей миниатюре, ожидаемо отразилось цивилизационное противостояние неолиберального коллективного Запада с его сателлитами и значительной частью мирового большинства, в особенности исламским миром, что ярко высветило инициированное Ираном голосование по проекту Конвенции.

Начальные этапы разработки договора протекали на фоне антироссийских заявлений дипломатических агентов оппонентов, выказывавших недоговороспособность к взаимоуважительному или по крайней мере сугубо прагматичному взаимодействию, провоцируя на ответные меры. Ближе к завершению работы над документом практиковались «дипломатический» шантаж и создание искусственного цейтнота. Столь агрессивная отработка политической повестки во многом заглушала профессиональный межгосударственный диалог экспертов от правоохраны, юстиции и цифровизации, усугубляла дефицит взаимного доверия и деструктивную обстановку, в которой приемлемость либо отторжение тех или иных предложений делегатов-практиков по тексту Конвенции порой зависели не столько от их существа, сколько от государства-автора.

Свою дестабилизирующую партию отыгрывали вклады ангажированных мультистейкхолдеров - НПО и западных ИТ-корпораций, а также несовместимые со статусом страны пребывания ООН визовые бесчинства. В таких спорах под воздействием подобного рода посторонних факторов истина иногда не рождается вовсе, а, родившись, погибает во младенчестве, да и сам спор перерождается в лишенный конструктивности конфликт.

Делегации были вынуждены растрачивать ресурсы на взаимный поиск разного рода вредоносных закладок³, логических бомб и пасхалок в тексте проекта Конвенции, словом, на выявление уязвимостей и признаков недобросовестности со стороны контрагентов, способных заложить эти уязвимости при верстке документа.

Выработке и продвижению российских подходов в Спецкомитете, их закреплению в виде конкретных норм в Конвенции способствовала слаженная совместная работа в рамках межведомственной рабочей группы (МРГ) и в ходе сессий Спецкомитета, организованные МИД России многочисленные переговоры с единомышленниками

Петр ЛИТВИШКО

и конструктивно настроенными делегациями, информационно-пропагандистская работа, проведенные на полях сессии презентации монографии (размещена в базе данных УНП ООН SHERLOC и на сайте Спецкомитета) и доклада⁴.

Прокуратура РФ наряду с МИДом России играет ведущую роль в определении глобальных правил игры на международно-правовом виртуальном поле, функции этих ведомств по координации деятельности правоохранительных органов по борьбе с преступностью, с одной стороны, координации проведения единой внешнеполитической линии государства в этой сфере и координации деятельности федеральных органов исполнительной власти по реализации государственной политики в области международной информационной безопасности, с другой стороны, являются взаимодополняющими.

Приказом Генерального прокурора РФ от 06.07.2020 №352 создана МРГ по противодействию информационной преступности под эгидой Генеральной прокуратуры РФ в целях обеспечения участия в работе Спецкомитета, выработки консолидированной российской позиции по проекту Конвенции, а также проработки вопросов, касающихся повышения эффективности работы правоохранительных органов в борьбе с киберпреступностью. В состав группы, возглавляемой заместителем Генерального прокурора РФ, входят представители Генеральной прокуратуры РФ, МИД России, аппарата Совета безопасности РФ, СК России, МВД России, ФСБ России, СВР России, Минцифры России и Минюста России.

В связи с исполнением мандата МРГ в части разработки Конвенции ее дальнейшая работа будет направлена в том числе на обеспечение выполнения внутригосударственных процедур для ее вступления в силу для России (формулирование заявлений и оговорок, внесение изменений в действующее законодательство РФ к выходу на ратификацию), а также разработку дополнительного протокола к Конвенции (предполагается, что он будет содержать только материальную часть - дополнительные составы подлежащих криминализации деяний).

Так, в настоящее время межведомственное согласование проходит разработанный Генеральной прокуратурой РФ проект федерального закона, направленного на урегулирование порядка обеспечения сохранности электронных данных по запросам как иностранных, так и российских органов и одновременно на предотвращение исполнения российскими провайдерами иностранных запросов о сохранении или предоставлении данных, поступивших к ним напрямую из-за рубежа.

Повлияют ли вступление в силу и действие Конвенции ООН на процесс новых присоединений к Конвенции Совета Европы о киберпреступности 2001 года (Будапештской конвенции) в сторону их уменьшения, предсказать сложно.

С одной стороны, основные нормы Будапештской конвенции воспроизведены или улучшены, хотя и не до конца актуализированы, в принятой спустя без малого четверть века Конвенции ООН. С другой стороны, материнская Конвенция 2001 года сохраняет свою конкурентоспособность постольку, поскольку была существенно модернизирована в 2022 году за счет принятия Второго дополнительного протокола к ней о расширенном сотрудничестве и раскрытии электронных доказательств, содержащего вос-

ПЕРВЫЙ ГЛОБАЛЬНЫЙ ДОГОВОР ПРОТИВ КИБЕРПРЕСТУПНОСТИ:
ОТ ГЕОПОЛИТИЧЕСКОЙ КОНФРОНТАЦИИ К ПРОФЕССИОНАЛЬНОМУ...

требуемые упрощенные экстра TERRИТОРИАЛЬНЫЕ механизмы, которые приближены к основанным на взаимном признании ордерным инструментам Европейского союза и которые в Конвенцию ООН не вошли и априори войти не могли, а именно: прямого раскрытия регистраторами доменных имен и поставщиками ИКТ-услуг, расположенными на территории страны - участницы Протокола, находящейся в их владении или под их контролем информации о регистрантах доменов, об абонентах (подписчиках) соответственно по запросам и ордерам правоохранительных и судебных органов другой страны-участницы (хотя во многих аспектах, в силу оговорок, режимов уведомления и консультаций с государством поставщика услуг, это положение может сводиться к межгосударственному взаимодействию); приведения в исполнение ордеров другой стороны об ускоренном предоставлении данных об абоненте и трафике; ускоренного раскрытия сохраненных компьютерных данных через контактные пункты сети 24/7 без запроса о правовой помощи, оказания взаимной правовой помощи в чрезвычайных обстоятельствах. Государство не может участвовать в Протоколе с этим облегченным режимом, не участвуя в материнской Конвенции.

При применении нового глобального договора следует принимать во внимание также риски его возможной недобросовестной инструментализации в военно-политических целях, например, исходящие от интенсивно наращиваемого потенциала и планов Украины и ее союзников по массовому сбору электронных доказательств, включая разведку по открытым источникам, против Российской Федерации. Для этого уже создан ряд межгосударственных проектов, под которые выделены существенные финансовые средства⁵. Такие электронные доказательства могут добываться в рамках Конвенции опосредованно, через разного рода прокси и под прикрытием сторонних производств об общеуголовных преступлениях.

Для предотвращения реализации подобных и иных сценариев угроз национальной безопасности разработан и сейчас проходит процедуру утверждения Регламент межведомственного взаимодействия при получении запросов компетентных органов иностранных государств, связанных с преступлениями и иными правонарушениями, совершаемыми с использованием (применением) информационно-телекоммуникационных технологий, компьютерными атаками и компьютерными инцидентами.

Основное содержание Конвенции можно разделить на материальную (криминализация деяний) и процессуальную, а также внутригосударственную и межгосударственную части. В фокусе настоящей публикации - преимущественно процессуальная и межгосударственная части, инвентаризация их соответствующих

Повлияют ли вступление в силу и действие Конвенции ООН на процесс новых присоединений к Конвенции Совета Европы о киберпреступности 2001 года (Будапештской конвенции) в сторону их уменьшения, предсказать сложно.

Петр ЛИТВИШКО

преимуществ и недостатков, авторская фиксация некоторых подготовительных материалов (*travaux préparatoires*) для освещения намерений разработчиков как одного из средств толкования договора.

Охват Конвенции

Россия последовательно отстаивала необходимость всеобъемлющего охвата Конвенции в соответствии с установленным мандатом Спецкомитета в ее как материальной, так и процессуальной частях, низких порогов для возможности антикриминальной кооперации, в то время как противоположный лагерь ратовал за максимальное сужение и высокие пороги для активации обязательств; призывал «не засорять эфир» менее важными запросами, не допускать контрпродуктивную перегрузку ими ограниченных ресурсов стран, не говоря уже о тех, которые не отвечают требованию двойной криминализации, по делам об административных правонарушениях, *de minimis*, что среди прочего не учитывало бы кумулятивный эффект менее тяжких уголовных правонарушений и отрицательно сказывалось бы на предупреждении преступности.

Все же в итоге возможность исполнения таких запросов вошла в Конвенцию на правах исключения из правила об отказе - по свободному усмотрению запрашиваемой стороны, по аналогии с Конвенцией ООН против транснациональной организованной преступности 2000 года (Палермской конвенцией) и некоторыми другими конвенциями. При несоблюдении условия двойной криминализации запрашиваемая сторона может отказать также в обеспечении сохранности данных.

Обязательства же сторон Конвенции по международному сотрудничеству в обмене электронными доказательствами (в отличие от внутригосударственного режима) и в рамках сети 24/7 ограничены, помимо установленных ею составов преступлений, только кругом серьезных преступлений, как они определены в Конвенции, в то время как, например, по Будапештской конвенции такое ограничение может налагаться государствами-участниками только на перехват содержания сообщений и данных о трафике.

Вместе с тем охват международного сотрудничества заужен преимущественно путем установления Конвенцией его основных форм исключительно в отношении преступлений, признанных таковыми в соответствии с ней (установленных в главе о криминализации), в частности, это касается экстрадиции, передачи на время содержащегося под стражей лица, передачи уголовного производства, совместных расследований, принятия любых обеспечительных и конфискационных мер в отношении активов и даже блока правоохранительного содействия (ст. 47).

Ряд положений Конвенции (в их числе ст. 38 о передаче осужденных) сформулированы как дискреционные, а не императивные (запрашиваемая Страна может, но не обязана оказывать помощь или содействие - *may vs. shall*), что, хотя и имеет место в договорной практике, во многом лишает эти нормы добавленной стоимости, поскольку для такого «может» государства не нуждаются в заключении между собой

ПЕРВЫЙ ГЛОБАЛЬНЫЙ ДОГОВОР ПРОТИВ КИБЕРПРЕСТУПНОСТИ:
ОТ ГЕОПОЛИТИЧЕСКОЙ КОНФРОНТАЦИИ К ПРОФЕССИОНАЛЬНОМУ...

международного договора, всегда направленного на создание их взаимных обязательств, а могут и сами по себе свободно предоставлять соответствующую помощь по собственному усмотрению, в том числе на основе принципов взаимности или международной вежливости. Поэтому в качестве компромиссной развязки по отдельным ключевым положениям Конвенции, не снискавшим консенсуса, применены формулировки «стремится» и «принимает (эффективные) меры».

Так, принципиально важные нормы о международном взаимодействии в перехвате в режиме реального времени данных о трафике и контенте коммуникаций по аналогии с Будапештской конвенцией (хотя и закладывающей прямое обязательство по такому взаимодействию, а не лишь по стремлению к нему, как в Конвенции ООН) имеют бланкетный характер за счет отсылки к иным договорам и (или) национальному законодательству сторон и применяются только во взаимосвязи с таковыми. Отдельные делегации не принимали императивность этих норм по мотивам отсутствия или недостатка ресурсов в их странах для данного вида сотрудничества. Перехват содержания по общему правилу не может оказываться Соединенными Штатами⁶.

Конвенция, как и ряд других конвенций ООН, для целей своего внутри- и межгосударственного применения, оперирует триадой стадийности уголовного процесса «расследование, уголовное преследование или судебное разбирательство⁷» (*investigation, prosecution or judicial proceeding*).

В отличие от отечественного уголовного процесса, под (уголовным) расследованием в универсальном международно-правовом лексиконе понимаются, помимо собственно процедур предварительного следствия или дознания, также доследственные проверки и оперативно-розыскные мероприятия (ОРМ), равно как и финансовые расследования по линии подразделений финансовой разведки⁸.

В международной литературе выделяются расследование совершенного преступления (*reactive investigation*) и упреждающее расследование (*proactive investigation*, обычно связанное с применением контролируемой поставки, оперативным внедрением и т. д.), иногда также подрывное расследование (*disruptive investigation*), которые в принципе корреспондируют с нашими понятиями собственно расследования и уголовного преследования, выявления и пресечения преступлений соответственно⁹.

Наднациональные ордерные инструменты Европейского союза для возможности задействования трансграничного обмена доказательствами, в том числе электронными¹⁰, внутри ЕС используют формулу «наличие разумных оснований полагать, что правонарушение совершено, совершается или, вероятно, будет совершено».

Удалось во многом преодолеть, аккуратно обойдя, нежелание оппонентов распространять закрепляемые Конвенцией механизмы сотрудничества (правовой помощи и правоохранительного содействия, за исключением мер профилактического характера, ограниченного обмена информацией и технической помощи), в особенности требующие судебного решения принудительные интрузивные меры, на стадии выявления, предупреждения и пресечения преступлений, как во внутреннем, так и международном контексте применения этого глобального договора.

Петр ЛИТВИШКО

Так, помимо используемой сквозным образом в Конвенции пары «предупреждение и борьба» и ст. 47 (Сотрудничество между правоохранительными органами) Конвенции, это главным образом достигнуто за счет проведения нужного нам определения термина «уголовное расследование» в Примечания для толкования по конкретным статьям Конвенции, по сути составляющие неотъемлемое приложение к Конвенции, в том числе через ст. 19 Конвенции о приготовлении к преступлениям и покушении на них (неоконченные преступления - *inchoate offences*). В этом же контексте особо важен функционал сети 24/7 (ст. 41).

В соответствии с п. 4 Примечаний для толкования (по ст. 23 и 35 Конвенции) под «уголовными расследованиями» понимаются ситуации, когда фактические обстоя-

тельства дают разумные основания полагать, что совершено или совершается уголовное правонарушение (включая правонарушение, предусмотренное в статье 19 Конвенции), в том числе когда расследование направлено на то, чтобы остановить соответствующее преступление или воспрепятствовать его совершению.

Тем самым «расследование» в его международно-правовой универсальной интерпретации, для внутренней и международной составляющих Конвенции по всему ее тексту, может охва-

Россия последовательно отстаивала необходимость всеобъемлющего охвата Конвенции в соответствии с установленным мандатом Спецкомитета в ее как материальной, так и процессуальной частях.

тывать как следственные действия, так и проактивные негласные ОРМ в их понимании в российском праве - на стадиях выявления, предупреждения и пресечения уголовно наказуемых деяний¹¹.

Исключительно важно констатировать, что в этом плане удалось превзойти Будапештскую конвенцию, которая в ее буквальном толковании не содержит каких-либо намеков на применимость ее механизмов к стадиям предотвращения преступлений.

Многие делегации твердо придерживались позиции о необходимости высокого порога для активации соответствующих норм Конвенции - только в случае уже совершенного преступления, в дальнейшем заявляя о необязательном характере Примечаний для толкования¹².

Помимо подобных заявлений, которые, по всей видимости, будут делаться к Конвенции отдельными государствами-участниками, для Российской Федерации будет затруднительным и по другой причине использовать положения Конвенции о международном сотрудничестве в получении электронных доказательств, в частности ст. 44 (обыск и аналогичный доступ к хранимым электронным данным, их изъятие и раскрытие), 45 (сбор в режиме реального времени данных о трафике) и 46 (перехват данных о содержании), не для производства следственных¹³ или судебных действий, а для испрашивания и проведения ОРМ¹⁴ по делам оперативного учета при отсут-

ПЕРВЫЙ ГЛОБАЛЬНЫЙ ДОГОВОР ПРОТИВ КИБЕРПРЕСТУПНОСТИ:
ОТ ГЕОПОЛИТИЧЕСКОЙ КОНФРОНТАЦИИ К ПРОФЕССИОНАЛЬНОМУ...

ствии материалов доследственной проверки или возбужденного уголовного дела. Дело в том, что Конвенция предписывает для этих действий необходимость соблюдения процедуры взаимной правовой (судебной) помощи (*legal (judicial) assistance*) в области уголовной юстиции, которая по российскому закону (ст. 453-457 УПК РФ) возможна лишь в рамках уголовного судопроизводства (предварительного расследования или по крайней мере проверки сообщения о преступлении, а также судебного разбирательства) и направлена на получение допустимых доказательств по делу, в то время как ОРМ по общему правилу проводятся в режиме международного правоохранительного (полицейского) содействия (*law enforcement (police-to-police) assistance*), нацеленного на добывание ориентирующей, оперативно значимой информации. Будапештская конвенция во всех соответствующих случаях оперирует более выгодным широким понятием «взаимная помощь» (ст. 31, 33-34), которое может охватывать как правовую помощь, так и правоохранительное содействие.

Достигнутая формула позволила в некоторой степени компенсировать и совершенно абсурдное, с точки зрения неотъемлемого арсенала средств и методов борьбы с киберпреступностью, исчезновение из Конвенции, по вине пассивной позиции большинства, классической нормы о негласных специальных методах расследования, имеющейся в Палермской конвенции и других универсальных инструментах.

По большому счету, из-за недопонимания отдельными делегациями существа вопроса в Конвенцию не вошел и традиционный институт консульской правовой помощи по уголовным делам¹⁵, дополненный положениями об использовании систем видеоконференцсвязи или телефонной конференции, из российского проекта Конвенции 2021 г. (ст. 54). К слову, из этого первоначального проекта мало что осталось в Конвенции¹⁶. Никак не упоминается в Конвенции и современная проблематика электронных иммунитетов, в том числе международно-правовых, в уголовном производстве¹⁷.

В Конвенции государствам-участникам не предложено, несмотря на чрезвычайную востребованность этого, в целях эффективного обеспечения допустимости и юридической силы доказательств, собираемых в соответствии с ней, рассмотреть возможность создания между ними защищенных платформ и каналов связи, обеспечивающих аутентификацию и удостоверение запросов о правовой помощи и доказательств, передаваемых исключительно в электронно-цифровой (безбумажной) форме, и, при необходимости, взаимное признание электронных подписей, печатей или штампов, проставляемых на таких запросах и доказательствах, где это уместно, включая указанные платформы и каналы в состав контактных пунктов 24/7. Лишь отдаленно напоминающая подобное положение расплывчатая норма представлена в п. 14 ст. 40 (правовая помощь) Конвенции.

Сопrotивление оппонентов по охвату имело и другое очевидное объяснение. Участие в Будапештской конвенции, хотя и претендующей на статус универсальной, нежели региональной, и ее протоколах для стран - не участниц Совета Европы фактически увязывается с членством в закрытом клубе «развитых демократий», дверь в который приоткрывается только по приглашению Комитета министров Совета

Петр ЛИТВИШКО

Европы, в то время как Конвенция ООН настежь открыта для присоединения любого государства. Развитые демократии не желают сотрудничать с теми, кто в их ранжире числится в государствах-изгоях, попирающих права человека и хулиганящих в информационном пространстве, в том же объеме и по тем же правилам, что и между собой, внутри «порядочного» общества. Финальный же продукт общих усилий свидетельствует о том, что это нежелание так или иначе во многом удалось преодолеть.

Права человека

Прозападный лагерь постарался насытить Конвенцию положениями, которые препятствовали бы ее применению как во внутригосударственном контексте, так и для международного сотрудничества по широким мотивам угроз правам человека. Подчеркивались беспрецедентность разрабатываемого международного договора по степени вторжения его предписаний в основные права и свободы человека, в частности касающиеся тайны связи, общей неприкосновенности частной жизни и личной тайны, и необходимость установления корреспондирующих гарантий их соблюдения.

Как известно, кто хочет сотрудничать - ищет возможности, кто не хочет - причины. В случае с Конвенцией искать допустимые причины для отказа в запрашиваемых помощи или содействии не нужно - их палитра на все случаи жизни представлена, в частности, в п. 21 ст. 40, причем две из них, в силу существующей правоприменительной практики, могут рассматриваться в качестве всеобъемлющих, покрывающих ряд других - возможное нанесение ущерба публичному порядку и противоречие требованиям правовой системы запрашиваемого государства. Поэтому, наряду с приводимыми ниже возможностями политических злоупотреблений ими, при прочих равных условиях и с сугубо практической точки зрения работы центральных и иных компетентных правоохранительных и судебных органов стран по вопросам правовой помощи и правоохранительного содействия борьбу с правочеловеческими «закладками» в Конвенции оправданно воспринимать как сражение с ветряными мельницами.

Речь идет о повседневных сценариях двусторонних сношений запрашивающего и запрашиваемого государств - участников Конвенции по оказанию друг другу предусмотренной ею правовой помощи либо отказу в таковой по очерченным ею основаниям. И ничто не препятствует, например, Конференции Сторон Палермской конвенции, не содержащей широких правочеловеческих «предохранителей», или любым иным механизмам обзора конвенций рассматривать вопросы нарушения прав человека при их применении.

Положения п. 2 ст. 6 (Соблюдение прав человека) Конвенции (небезупречные даже грамматически, впрочем как и название Конвенции, как следствие нежелания вскрывать компромисс) стали одними из самых неконсенсусных в переговорном процессе, но при голосовании устояли. В ст. 24 Конвенции закреплены широкие условия и гарантии обеспечения прав человека, включая принцип соразмерности,

ПЕРВЫЙ ГЛОБАЛЬНЫЙ ДОГОВОР ПРОТИВ КИБЕРПРЕСТУПНОСТИ:
ОТ ГЕОПОЛИТИЧЕСКОЙ КОНФРОНТАЦИИ К ПРОФЕССИОНАЛЬНОМУ...

а в ст. 36 среди правил защиты персональных данных фактически содержится дополнительное основание для отказа в сотрудничестве со ссылкой на внутреннее законодательство в сфере защиты персональных данных. Кроме того, классическая правочеловеческая формула отказа в экстрадиции по мотивам дискриминации экстраполирована также на основания отказа в правовой помощи, чего нет в действующих секторальных конвенциях.

На первый взгляд, закономерен вопрос, кто из нас, выполняя добровольно взятые на себя обязательства по международным договорам в области прав человека и прописав аналогичные ценности и их гарантии в Основном законе своей страны, разделяя и исповедуя их, может быть против этих правильных формулировок Конвенции? Их неприятие многими странами объясняется в первую очередь не имеющим аналогов в прошлом и создающим нежелательный прецедент «разбавлением» положений антикриминальной конвенции не свойственным ее целям правочеловеческим языком, а также опасностью их политической инструментализации в ущерб сотрудничеству сторон Конвенции между собой в двустороннем формате.

Такая опасность может исходить от любой третьей стороны Конвенции или группы таковых, желающих непосредственно или опосредованно через Конференцию Сторон примерить на себя роль оценщика соблюдения требований Конвенции в этой части и ставить их реальные или мнимые нарушения на вид как запросившему помощь, так и прежде всего оказавшему ее государству, осуществлять мониторинг по спискам штрафников, вводить против них санкции, что будет оказывать сдерживающий эффект на двустороннее сотрудничество по Конвенции.

В рамках правочеловеческой повестки эксплуатировались и оруэлловские теории заговора. Процесс разработки и принятия Конвенции на всех этапах сопровождался - так же, как прогнозируемо будет сопровождаться ее применение - некомпетентным шумом и умышленной дезинформацией вокруг нее как якобы инструмента органов национальной безопасности - «массовой слежки» (*mass surveillance (interception) of bulk communications*), особенно в руках недемократических режимов.

При этом Конвенция сама по себе не имеет никакого отношения к разведывательной, контрразведывательной деятельности спецслужб для целей госбезопасности (*national security intelligence, counterintelligence*), а находится исключительно в домене уголовного правосудия (юстиции), направлена на получение допустимых доказательств, подлежащих судебному контролю (в то время как разведсообщество допустимость доказательств мало заботит), и может также служить для «разведывательной» оперативной правоохранительной деятельности (*law enforcement intelligence, criminal intelligence*).

Именно для снятия каких-либо озабоченностей по этому поводу в текст включено, по аналогии с Будапештской конвенцией и по мнению многих излишне в силу очевидности, слово «конкретный» (*specific, specified*) для обозначения отдельных, определенных уголовных расследований, преследования или судебного разбирательства и получаемых в их рамках данных и сообщений - в противоположность общему, проактивному, сплошному сбору и хранению данных. В свое время, в особенности

Петр ЛИТВИШКО

в свете разоблачений Э.Сноудена, Комитет Конвенции о киберпреступности, представляющий государства - участников Будапештской конвенции, был вынужден отбиваться от аналогичных нападков со стороны Евросоюза в связи с разработкой прототипа Второго дополнительного протокола к ней и в контексте ее ст. 32 (b)¹⁸.

Не просматривались перспективы договориться по смежному вопросу об установлении обязанностей поставщиков ИКТ-услуг по хранению (*retention*) данных (в отличие от их сохранения (обеспечения сохранности) - *preservation*), в том числе из-за позиций о недопустимости возложения в Конвенции подобных обязанностей на частный сектор, которые еще влекли бы для него колоссальные, а для многих его представителей неподъемные, финансовые расходы. Аналогичная ситуация была и при принятии Будапештской конвенции¹⁹.

Экстратерриториальные «закладки»

Российская Федерация выступала категорически против экспансии экстратерриториальных элементов в тексте договора, прежде всего внедрения в него какого бы то ни было аналога п. «b» ст. 32 Будапештской конвенции. При этом учитывая, что центральный слой киберпространства образует логический (виртуальный) уровень, не имеющий материальных, географических границ, закрепленные в ст. 5 Конвенции гарантии защиты именно территориального суверенитета с легкостью превращаются в эфемерные, подверженные вольному толкованию заинтересованного, чья точка зрения, по известному выражению, зависит от «места сидения» в физическом пространстве конкретной страны.

Как уже было упомянуто, Спецкомитет упустил уникальный шанс урегулирования предотвращения односторонних трансграничных тайных киберопераций государств-участников, нацеленных на обход двусторонней координации, создающих риск «дружественного огня» в отношении взаимной агентурной деятельности и противоречащих международному праву с точки зрения как суверенитета государств, так и защиты прав человека²⁰.

Со стороны развитых кибердержав коллективного Запада, заинтересованных сохранять в правовой серой зоне свои односторонние проактивные экстратерриториальные кибероперации правительственного хакинга, подобные попытки установить минимальные универсальные правила их проведения вызвали ожесточенное сопротивление. Опять же под благовидным предлогом нежелательности вмешательства негласных мероприятий, помимо закрепленных в Конвенции (электронное наблюдение в форме негласного получения (перехвата) данных трафика и контента), в права человека, степень которого особо высока²¹.

В свою очередь, в целях противодействия принятию иностранными и международными органами односторонних мер по нелегитимному самостоятельному сбору доказательств, включая электронные, и иных сведений в Российской Федерации, в том числе посредством дистанционных трансграничных контактов из-за рубежа с физическими и юридическими лицами, находящимися на территории Российской

ПЕРВЫЙ ГЛОБАЛЬНЫЙ ДОГОВОР ПРОТИВ КИБЕРПРЕСТУПНОСТИ:
ОТ ГЕОПОЛИТИЧЕСКОЙ КОНФРОНТАЦИИ К ПРОФЕССИОНАЛЬНОМУ...

Федерации, проведению мероприятий по выманиванию таким путем российских граждан за рубеж в целях их задержания разработан проект «блокирующего» федерального закона, в настоящее время рассматриваемый в Государственной Думе Федерального Собрания РФ²².

Государство, в той или иной форме соглашаясь на размещение у себя серверов, сетей и иного оборудования зарубежного провайдера, в основном дает определенное выраженное или подразумеваемое согласие на использование и иную обработку, в том числе и для экстратерриториальных правоохранительных целей, хранящихся или передаваемых в них данных этим провайдером, во владении или под контролем которого они находятся, если размещающее государство не устанавливает строгие правила локализации у себя таких данных, не оговаривает иные условия их обработки, например, по критерию гражданства субъектов обрабатываемых персональных данных. И наоборот, государство, чей провайдер предоставляет свои услуги за рубежом, размещает там свою техническую инфраструктуру, а тем более юридически локализуется («приземляется») страной пребывания, по общему правилу тем самым соглашается на взаимодействие своего провайдера с властями таких стран, в том числе в правоохранительной сфере и вне зависимости от гражданства субъектов обрабатываемых персональных данных.

Тем самым объективно на практике имеет место позитивный конфликт юрисдикций ряда государств в отношении данных по месту нахождения: ИКТ-провайдера; хранения или передачи данных и (или) устройства (оборудования) для хранения и передачи данных; абонента (пользователя). К ним может быть также добавлено при определенных условиях государство гражданства абонента (пользователя).

Существенным экстратерриториальным потенциалом обладает ст. 27 Конвенции, хоть она и расположена, в отличие от ст. 32 Будапештской конвенции, во внутригосударственной, а не международной части договора. Следует учесть, что «внутригосударственные» статьи требуют от государства-участника установления для своих органов полномочий, которые Конвенция рассматривает только в качестве минимальных, полностью оставляя за государством-участником пределы расширения их объема (ст. 59).

В соответствии со ст. 27 Конвенции, аналогичной ст. 18 Будапештской конвенции, каждое государство-участник принимает такие законодательные и иные меры, какие могут потребоваться для наделения его компетентных органов полномочиями давать распоряжения: а) лицу на своей территории предоставить конкретные электронные

Конвенция, как и ряд других конвенций ООН, для целей своего внутри- и межгосударственного применения, оперирует триадой стадийности уголовного процесса «расследование, уголовное преследование или судебное разбирательство».

Петр ЛИТВИШКО

данные, находящиеся во владении или под контролем этого лица, которые хранятся в информационно-коммуникационной системе или на носителе электронных данных; и б) поставщику услуг, предлагающему свои услуги на территории государства-участника, предоставить абонентские данные, имеющие отношение к этим услугам и находящиеся во владении или под контролем этого поставщика услуг.

Тем самым положения п. «а» ст. 27 Конвенции не исключают возможного их применения для одностороннего трансграничного доступа властей одного государства к данным, хранящимся на территории другого государства, без задействования процедуры международной правовой помощи или правоохранительного содействия, посредством обращения, при необходимости с применением мер принуждения, к лицу, в чьем распоряжении находятся эти данные, чьи характер, принадлежность и правомерность нахождения у данного лица ничем не ограничены.

Таким лицом может быть любое физическое или юридическое лицо, имеющее незаконный экстратерриториальный доступ к серверам и другим устройствам в другом государстве и хранящимся в них данным, которые, в свою очередь, могут оказаться в его распоряжении в результате совершения охватываемого Конвенцией преступления и тем самым легализуются этой нормой Конвенции для целей уголовного судопроизводства; им может быть секретноноситель-перебежчик и т. д. Наконец, несмотря на наличие специальной экстратерриториальной нормы о поставщике услуг в следующем пункте «б» этой же статьи, в материалах толкования к идентичной ст. 18 Будапештской конвенции справедливо указывается, что п. «а» также охватывает поставщиков услуг²³. Причем в отличие от строго лимитированного характера данных в п. «б» их категории в п. «а» в статьях обеих Конвенций ничем не ограничены. В распоряжении же поставщиков, в первую очередь иностранных, могут находиться какие угодно данные с зарубежных серверов и иных устройств²⁴.

В п. «б» ст. 27 Конвенции ООН заложен целевой юрисдикционный критерий: ее положения предусматривают возможность прямого истребования государством, на территории которого поставщик оказывает услуги в сфере ИКТ, информации об абонентах, относящейся к таким услугам и находящейся во владении или под контролем поставщика. Тем самым, учитывая непостоянство местонахождения данных в облаке, имеют значение только место предоставления услуги и факт нахождения интересующих данных во владении или под контролем провайдера, но не месторасположение (в том числе за рубежом) провайдера, самих данных (серверов).

Директивная записка Комитета Будапештской конвенции определяет понятия предоставления услуг на территории государства, а также реальной и существенной связи поставщика услуг с этим государством. «Стороны могут считать, что поставщик услуг «предоставляет свои услуги на территории Стороны», когда: поставщик услуг предоставляет возможность лицам на территории Стороны подписываться на его услуги (и, например, не блокирует доступ к таким услугам) и (*кумулятивное условие*) поставщик услуг установил реальную и существенную связь со Стороной. Относимые факторы включают в себя объем, в котором поставщик услуг ориенти-

ПЕРВЫЙ ГЛОБАЛЬНЫЙ ДОГОВОР ПРОТИВ КИБЕРПРЕСТУПНОСТИ:
ОТ ГЕОПОЛИТИЧЕСКОЙ КОНФРОНТАЦИИ К ПРОФЕССИОНАЛЬНОМУ...

рует свою деятельность в отношении таких подписчиков (например, путем осуществления местной рекламы или рекламы на языке территории Стороны), использует информацию о подписчиках (или связанные данные трафика) в ходе своей деятельности, взаимодействует с подписчиками в Стороне либо другим образом может считаться установленным на территории Стороны. Тот только факт, что поставщик услуг использует доменное имя или адрес электронной почты, связанные с конкретной страной, не создает презумпции, что его место ведения дел находится в этой стране. Поэтому требование о том, что подлежащая предоставлению информация о подписчиках должна относиться к услугам поставщика, предоставляемым на территории Стороны, может считаться выполненным, даже если эти услуги предоставляются посредством национального доменного имени верхнего уровня, относящегося к другой юрисдикции».

В записке также отмечается, что «правовые режимы все больше признают, что как в сфере уголовной юстиции, так и в сфере защиты частной жизни и данных, местонахождение данных не является определяющим фактором для установления юрисдикции».

В Конвенцию не вошла норма (к слову, ее никто особо и не продавливал), подобная спорному для России п. «b» ст. 32 Будапештской конвенции, - о праве на односторонний трансграничный доступ к хранящимся в другом государстве - участнике этой конвенции компьютерным данным, не находящимся в открытом доступе, с согласия лица, имеющего законное полномочие по их раскрытию иностранной стороне, и без обязательного уведомления этого другого государства. В качестве примера применения нормы обычно приводится осмотр устройства (сотрудничающего) подозреваемого с открытым ящиком его электронной почты на иностранном домене (с данными, хранимыми на зарубежном сервере) при согласии этого лица.

При этом возможны и прочие ничем не ограниченные сценарии, где бы и когда бы такое лицо ни находилось. В своем официальном толковании, придаваемом директивной запиской Комитета Будапештской конвенции, норма практически не применима к испрашиванию из-за рубежа у поставщиков услуг в сфере ИКТ данных их пользователей, поскольку якобы маловероятно, что поставщики, обычно будучи только держателями этих данных, не контролируя их и не обладая ими (тем самым не имея законного полномочия по их раскрытию), могут давать законное и добровольное согласие на раскрытие пользовательских данных²⁵. (Причем это разъяснение противоречит названной директивной записке Комитета к ст. 18 Будапештской конвенции (подп. «a» п. 1 ст. 18), в которой указано на включение поставщиков услуг в круг подобных уполномоченных лиц²⁶.)

Сопоставление положений Конвенции ООН и Будапештской конвенции в разбираемых частях позволяет заключить, что при нахождении предоставляющего согласие по п. «b» ст. 32 Будапештской конвенции лица не за рубежом²⁷, а на территории государства, чей орган получает доступ к находящимся за границей данным (основной сценарий ст. 32 (b)), положения п. «b» ст. 32 Будапештской конвенции во многом будут совпадать с положениями ее же подп. «a» и «b» п. 1 ст. 18 и ст. 27 Конвенции

Петр ЛИТВИШКО

ООН. Смежный характер в плане возможности экстратерриториального сохранения и доступа к данным имеют соответственно также ст. 16-17 Будапештской конвенции и ст. 25-26 Конвенции ООН, поскольку в них не ограничивается круг адресатов требований, предъявляемых к ним компетентными органами, не называются иные территориальные признаки их применения.

Итак, основные различия между ст. 27 Конвенции ООН и п. «б» ст. 32 Будапештской конвенции в своей совокупности свидетельствуют о более широком экстратерриториальном потенциале ст. 27 Конвенции ООН по сравнению со ст. 32 Будапештской конвенции в случаях названного сценария и сводятся к следующему:

В первой сами конкретные данные предоставляет лицо, во второй - доступ к конкретным данным или их получение осуществляются органами самостоятельно или через кого-то посредством расположенной на территории их государства компьютерной системы. Интересующий конечный результат - получение из-за рубежа самих данных - один и тот же; хотя в случае своего непосредственного доступа органы могут добыть выходящий за рамки согласия лица объем данных, однако такая несанкционированная порция данных может быть признана недопустимым доказательством.

В первой действия органов являются принудительными, на лице лежит обязанность им подчиниться, во второй - действия органов по самостоятельному или опосредованному доступу могут осуществляться только по законному и добровольному согласию лица.

В первой требование правомерности распоряжения лицом требуемыми данными не выдвигается, во второй - лицо должно обладать законным полномочием по раскрытию данных органам через упомянутую компьютерную систему.

В свете указанных положений обоих пунктов ст. 27 Конвенции ООН на практике может оказаться проблематичной реализация вносимой с 2022 года в заключаемые двусторонние межправительственные соглашения о сотрудничестве в области обеспечения международной информационной безопасности специальной «анти-экстратерриториальной» нормы. Например, в соответствии с Соглашением между Правительством Российской Федерации и Правительством Азербайджанской Республики о сотрудничестве в области обеспечения международной информационной безопасности от 24.06.2022 (ст. 2) «не допускается трансграничный доступ к компьютерной информации, хранящейся в информационной системе одного из государств Сторон, без официального взаимодействия с соответствующими компетентными органами государств Сторон; такое взаимодействие может осуществляться, в частности, в рамках двусторонних и многосторонних международных договоров, в том числе о правовой помощи по уголовным делам, а также в рамках международного сотрудничества правоохранительных органов»²⁸.

Как видно, договорный запрет налагается на трансграничный доступ к самой компьютерной информации, без каких-либо изъятий случаев такого доступа органов к ней как напрямую, так и посредством любого лица или поставщика ИКТ-услуг. Более того, этот запрет не имеет ограничений по характеру информации, которая в

ПЕРВЫЙ ГЛОБАЛЬНЫЙ ДОГОВОР ПРОТИВ КИБЕРПРЕСТУПНОСТИ:
ОТ ГЕОПОЛИТИЧЕСКОЙ КОНФРОНТАЦИИ К ПРОФЕССИОНАЛЬНОМУ...

действительности может быть и публично доступной (открытые источники). Поэтому названная стандартная формулировка требует совершенствования.

По причине использования населением зарубежных мессенджеров, электронной почты, криптобирж²⁹ и других интернет-сервисов следует признать очевидное, что отраженные в этих нормах Конвенции ООН действия правоохранителей, в том числе в отношении неправомерного держателя данных, равно как упомянутый пример задействия демонизированного п. «b» ст. 32 Будапештской конвенции, - повседневная, рутинная профессиональная практика, в связи с чем ограничивать местонахождение упоминаемых в ст. 27 ИКТ-системы и носителя данных пределами территории государства, чьи органы реализуют полномочия по даче соответствующих распоряжений, не соответствовало бы реалиям «на земле»³⁰. Напротив, пространственный предел действия норм об обыске и изъятии данных (ст. 28) строго ограничен территорией государства дающих распоряжения органов, где располагаются хранящие электронные данные информационно-коммуникационная система или ее часть либо носитель данных, а норм о перехвате данных о трафике или содержании (ст. 29-30) - территорией государства, где применяются соответствующие технические средства, либо где с помощью информационно-коммуникационной системы передаются искомые сообщения.

Статьи 42, 44-45 Конвенции в качестве адресата запросов об обеспечении сохранности или о предоставлении электронных данных называют государство, на территории которого расположена информационно-коммуникационная система, в которой они хранятся, а при перехвате данных о трафике - на территории которого передаются сообщения с помощью информационно-коммуникационной системы (при этом при перехвате контента в ст. 46 государство-адресат, чья территория затрагивается, не конкретизируется). Сами по себе эти формулировки в современных условиях могут расцениваться как вводящие в заблуждение, «на деревню дедушке»: следовательно, составляющий запрос о правовой помощи, не знает и не может точно знать и указать в своем запросе, где конкретно, в какой информационной системе, в какой стране и в какой момент времени провайдер хранит и обрабатывает интересующие следователя данные или передает сообщения.

При использовании облачных вычислений и анонимайзеров существуют проблемы локализации данных: потери сведений об их местонахождении, включая отсутствие этих сведений у самого провайдера; ситуации, когда образующие единое целое (информационный ресурс) данные во фрагментированном и (или) в динамическом (мигрирующем) состоянии рассредоточены по разным юрисдикциям или имеют

Прозападный лагерь постарался насытить Конвенцию положениями, которые препятствовали бы ее применению как во внутригосударственном контексте, так и для международного сотрудничества по широким мотивам угроз правам человека.

Петр ЛИТВИШКО

в них свои многочисленные зеркальные копии. Актуальна и проблема неконтролируемого выхода внутригосударственного трафика за пределы национальной информационной инфраструктуры, в частности в результате эксплуатации негеостационарных (низкоорбитальных) спутниковых систем связи и широкополосного доступа в Интернет типа «Старлинк».

По этим причинам в текущей правоприменительной практике по общему правилу адресатами запросов о сохранении и получении данных являются государства «национальности» поставщиков ИКТ-услуг и иных кастодианов. Процессуальная юрисдикция государства в отношении информационных систем, сетей и данных, основанная на локализации провайдера или его профессиональной деятельности, показательно определена применительно к государству - адресату соответствующих запросов в Модельном законе УНП ООН о взаимной правовой помощи по уголовным делам: таковым является государство, в котором провайдер, владеющий данными или их контролирующий, расположен, учрежден либо - путем деятельности по хранению, передаче или иной обработке данных - иным образом действует из этого государства³¹.

По настоянию российской делегации в Спецкомитете в Конвенцию включены соответствующие развязки, отражающие реальное положение дел. Так, в ст. 41 (Сеть 24/7) среди задач контактного центра определено предоставление информации о местонахождении поставщика услуг, если оно известно запрашиваемому государству-участнику, для оказания содействия запрашивающему государству-участнику в составлении запроса. В ст. 42 (Международное сотрудничество в целях оперативного обеспечения сохранности хранимых электронных данных) закреплено, что запрашивающее государство-участник может воспользоваться предусмотренной в ст. 41 Конвенции сетью 24/7 для получения информации о местонахождении электронных данных, хранящихся с помощью информационно-коммуникационной системы, и при необходимости информации о местонахождении поставщика услуг. Перечисленные положения этих двух статей служат и применению ст. 43-46 Конвенции³². Кроме того, в качестве альтернативных сведений в запросах должны указываться: любая имеющаяся информация, идентифицирующая либо хранителя хранимых электронных данных, либо местонахождение информационно-коммуникационной системы (запросы о сохранении данных); любые имеющиеся данные, идентифицирующие либо владельца или пользователя данных, либо местоположение информационно-коммуникационной системы (запросы о перехвате данных о трафике).

В Будапештской конвенции же в качестве критерия определения запрашиваемого государства-адресата в международном сотрудничестве отражена лишь территория местонахождения соответствующих данных (перехватываемых сообщений, компьютерных систем), что не отвечает современным реалиям облачных вычислений, является недостаточным и устаревшим критерием. Во Втором дополнительном протоколе 2022 года к Будапештской конвенции названный критерий оправданно заменен на месторасположение физического присутствия поставщика услуг в соответствующем государстве³³.

ПЕРВЫЙ ГЛОБАЛЬНЫЙ ДОГОВОР ПРОТИВ КИБЕРПРЕСТУПНОСТИ: ОТ ГЕОПОЛИТИЧЕСКОЙ КОНФРОНТАЦИИ К ПРОФЕССИОНАЛЬНОМУ...

Исключением являются прослушивание переговоров и иной перехват сообщений и других данных в режиме реального времени, которые могут запрашиваться не только у государства провайдера услуги, но и во многих случаях, если не в их большинстве, у государств по месту расположения:

- абонента (пользователя) и (или) принадлежащего ему или используемого им окончного устройства;
- терминального или транзитного оборудования либо сетей провайдера, через которые осуществляется пропуск данных.

Язык Конвенции

Для обеспечения согласованности равно аутентичных текстов Конвенции на шести официальных языках ООН была создана Группа по согласованию языковых версий Спецкомитета, объединившая в себе шесть репрезентативных языковых подгрупп (в свою очередь, каждая из них состояла из представителей разных стран, в которых соответствующий язык является государственным или официальным), регулярно консультировавшихся друг с другом в тесной координации с переводчиками секций перевода Отделения ООН в Вене.

Эксперты Группы решили не рассматривать тексты Палермской и других конвенций ООН в качестве неприкосновенных и не составлять специальные глоссарии терминов по образцу глоссария к Палермской конвенции, а, наоборот, исправить в новой Конвенции многие неточности и несоответствия между языковыми версиями, выявленные почти за четверть века применения Палермской конвенции и Конвенции ООН против коррупции 2003 года (Меридской конвенции). В рамках Группы русский текст тщательно сличался с английским (который являлся «первым среди равных», так как разработка Конвенции велась преимущественно на нем) и испанским (затем в учреждениях ООН с остальными языками) при активном участии членов российской делегации - представителей правоохранительных органов, Минцифры и дипломатов. Этот межведомственный формат позволил во взаимодействии с венскими переводчиками выработать качественный с лингвистической и правовой точек зрения русскоязычный текст и одновременно устранить обнаруженные недочеты в английском и испанском, обеспечить тождественность разноязычных юридических терминов между собой в их современном значении.

Изначально разработчики по аналогии с Будапештской конвенцией условились использовать в договоре только технологически нейтральный язык для обеспечения применимости Конвенции в бесконечном будущем вне зависимости от возникновения новых технологий; в ней отсутствует даже дефиниция электронного доказательства, и вместо этого термина используется «доказательство в электронной форме», которое может трактоваться и как более широкое, и как более узкое по сравнению с электронным доказательством, поскольку составлять электронное доказательство иногда могут и определенные сведения на бумажном носителе³⁴.

Петр ЛИТВИШКО

В качестве стадий противодействия преступности или борьбы с ней выделяются выявление, предупреждение, пресечение и раскрытие преступлений. К ним иногда относят и профилактику, а предупреждение и пресечение входят в объем понятия «предотвращение». Стояла задача обеспечить включенность всех этих стадий во внутригосударственную и международную части Конвенции. В отличие от мандата Спецкомитета в Конвенции предпочли использовать «борьбу» вместо «противодействия». Определенные сложности вызывал подбор английского эквивалента узкоспециального «пресечения», поскольку наиболее близкие к нему *«disruption»* и *«frustration»*, обозначающие срыв какого-либо начатого и неоконченного действия, используются в зарубежном законодательстве, но не в конвенциях в этом узкоспециальном значении.

В то же время используемое в них *«suppression»* вариативно передается и как пресечение, и как в целом борьба и имеет более широкое значение подавления, блокирования какой-либо деятельности, нежели строго ее пресечения, так же как широким охватом обладает *«deterrence»* (воспрепятствование, недопущение). Носители английского языка склонны рассматривать пресечение как составляющую предупреждения - *prevention*, не выделяя его в самостоятельный элемент внутри предотвращения. Первоначальная одобренная многими идея передачи одного понятия двумя (*prevention* - предупреждение и пресечение), хотя и практикуется (например, *integrity* - честность и неподкупность), представлялась нежелательной, в том числе ввиду главы VI (Меры по предупреждению) Конвенции, чье содержание фактически составляет только профилактика. В результате был выбран более удачный вариант включения стадии пресечения преступления в понятие расследования, а точнее, в одну из его целей (остановить преступление или воспрепятствовать его совершению - *stopping or impeding the commission of the offence*) в примечаниях для толкования Конвенции.

Необходимо учитывать, что ввиду различий в правовых системах стран мира (например, конвергенции предварительного (досудебного) расследования и оперативно-разыскной деятельности, вариативности содержания понятия «уголовное дело») и универсальности языка международных документов наименования процессуальных (следственных, судебных) действий в иностранном и международном праве зачастую не совпадают с используемыми российским правом, а отечественные (негласные) ОРМ в большинстве случаев отнесены к следственным (*investigative measure*), разведывательным (*criminal (law enforcement) intelligence operation*) либо охватываются зонтичным международно-правовым понятием *«special investigative technique»*, поэтому сами по себе терминологические обозначения условны и не должны быть определяющими при выборе конкретного вида правовой помощи или правоохранительного содействия.

Под судебными органами, органами (уголовной) юстиции (*judicial authorities*) для целей международных договоров в российском правовом порядке традиционно понимаются органы предварительного расследования (дознания и предварительного следствия), прокуратуры и суды³⁵; соответственно под «судебными документами» - документы, изданные ими или иным образом исходящие от них.

ПЕРВЫЙ ГЛОБАЛЬНЫЙ ДОГОВОР ПРОТИВ КИБЕРПРЕСТУПНОСТИ: ОТ ГЕОПОЛИТИЧЕСКОЙ КОНФРОНТАЦИИ К ПРОФЕССИОНАЛЬНОМУ...

В качестве других особенностей перевода стоит обратить внимание также на следующие.

Двойственный перевод «*offence*» как «правонарушение» и «преступление» в зависимости от контекста: первое - преимущественно в сочетании «уголовное правонарушение» (оно во многих правовых системах подразделяется по тяжести на преступления и уголовные проступки) при криминализации устанавливаемых Конвенцией деяний, второе - в остальных контекстах, в которых очевидно его значение именно как уже признанного или охватываемого Конвенцией преступления. То же и в отношении «*seizure*»: контекст определяет, что это либо узкоспециальный процессуальный термин «выемка» для обозначения только одного следственного действия, особенно требующего судебного решения, либо широкое «изъятие», охватывающее как выемку, так и осмотр и любые другие следственные действия и ОРМ, в ходе которых могут изыматься объекты.

Термин «*grooming*» в ст. 15 Конвенции не имеет однословного эквивалента в русском языке для обозначения требуемого явления, который можно было бы считать общеупотребительным иностранным заимствованием, пригодным для использования в правовых актах данного уровня. Этимология слова так или иначе связана с ухаживанием, обхаживанием. Транслитерированное понятие «груминг» в русском языке употребляется преимущественно в своих иных значениях из областей зоологии и процедур ухода за домашними питомцами. Поэтому однословный английский термин передан русскоязычной дефиницией, отражающей суть явления - создания доверительных отношений (с целью совершения сексуального преступления в отношении ребенка).

Заключение

Всякий международный договор, прежде всего многосторонний, - в той или иной мере продукт компромисса. В случае с Конвенцией это были хрупкий баланс и компромисс в квадрате, априори не способные на генерацию чего-то очень прорывного. Но вопреки всему удалось выработать качественный и востребованный практикой текст, вобравший в себя сочетание лучших элементов Палермской и Будапештской конвенций. И применительно ко всякому международному договору (не только к двустороннему, в этом смысле более естественному), а к Конвенции вдвойне, уместна аллегория с ребенком. Этот долгожданный первенец вынашивался в токсичной среде, имеющей мало общего с духом Объединенных Наций, и родился в муках таким, как есть, вопреки замыслам и запросным позициям заведомо малосовместимых родителей. Как бы то ни было, Конвенция - наше собственное детище, здоровое развитие и успешность которого - в том числе в наших собственных руках.

Нам всем предстоит продолжение и совершенствование профессиональной, напряженной и кропотливой работы по противодействию информационной преступности в условиях многополярной архитектуры современного миропорядка, включая блок «недружественных» государств³⁶, теперь уже с новым универсальным инстру-

Петр ЛИТВИШКО

ментом в нашем распоряжении, эффективность применения которого будет зависеть прежде всего от нас самих, и с новым праздником, который планируется объявить в честь принятия Конвенции, - Международным днем борьбы с киберпреступностью. Какие конкретно успехи будем отмечать в этот день - тоже будет зависеть от нас.

¹В настоящее время в качестве возможного места открытия Конвенции для подписания предварительно рассматривается столица Вьетнама, так что в дальнейшем по традиции она может получить название Ханойской.

²Автор являлся членом делегации Российской Федерации в Специальном комитете по разработке всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях (2021-2024 гг.), членом Группы по согласованию языковых версий Спецкомитета от Российской Федерации. Содержание публикации отражает авторские правовые оценки и не представляет собой официального мнения ведомства.

³Расхожее в среде международной информационной безопасности и за ее пределами в качестве сленгового понятие «закладка» применительно к договорной практике привнесения нежелательных положений в разрабатываемый документ («правочеловеческие закладки» и т. д.) не всегда употребляется корректно, поскольку не учитывает этимологию и значение в киберлексиконе термина «программная (аппаратная) закладка» (*backdoor*), от которого оно производно. Так, он предполагает прежде всего тайный или по крайней мере неявный характер внедрения и эксплуатации определенного скрытого или обладающего недеklarированными возможностями функционала (см. термины и определения ГОСТ Р 51275-2006). При самоочевидности договорных положений и их задуманного эффекта (как в случае «правочеловеческих закладок») вести речь о них как о закладочных средствах неверно.

⁴National legal frameworks and approaches to challenges in gathering electronic evidence across borders in light of the new global Convention provisions: Russian Federation's perspective: Side event at the Concluding session of the UN Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes; United Nations HQ, New York, Jan. 30, 2024. Здесь и далее материалы с официального интернет-сайта Спецкомитета // URL: https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home (дата обращения: 14.10.2024).

⁵CyberUA: Strengthening capacities on electronic evidence of war crimes and gross human rights violations in Ukraine // Сайт Совета Европы // URL: <https://www.coe.int/en/web/kyiv/cyberua> (дата обращения: 14.10.2024); Eurojust and the war in Ukraine; Core International Crimes Evidence Database (CICED) // Сайт Евроюста // URL: <https://www.eurojust.europa.eu/eurojust-and-the-war-in-ukraine> (дата обращения: 14.10.2024); Hill S. International Efforts to Collect Evidence Related to Russia's Aggression Against Ukraine // Saint Louis University Law Journal. 2024. Vol. 68. №2. P. 243-255; Quilling Ch. The Future of Digital Evidence Authentication at the International Criminal Court // Journal of Public & International Affairs. 2022. P. 7; Назарко А.А. Електронні докази в українському кримінальному судочинстві: Дослідження правових реалій та теоретичних перспектив // Науковий вісник Ужгородського Національного Університету. Серія Право. 2023. Вип. 80. Ч. 2. С. 183-188; Литвишко П.А.

ПЕРВЫЙ ГЛОБАЛЬНЫЙ ДОГОВОР ПРОТИВ КИБЕРПРЕСТУПНОСТИ:
ОТ ГЕОПОЛИТИЧЕСКОЙ КОНФРОНТАЦИИ К ПРОФЕССИОНАЛЬНОМУ...

Уголовно-процессуальные аспекты решения Международного Суда ООН по делу «Украина против Российской Федерации» от 31 января 2024 года // Вестник Университета прокуратуры Российской Федерации. 2024. №4 (102). С. 108-123.

⁶Practical Guide for Requesting Electronic Evidence across Borders. Vienna: United Nations, 2021. P. 39.

⁷Согласно источникам официального толкования ряда универсальных конвенций употребляемый в них термин «судебное разбирательство» (*judicial proceedings*) может в отдельных странах включать в себя и досудебное уголовное производство, а термин «производство (разбирательство)» (*a proceeding*) «призван охватить все этапы официального государственного производства (разбирательства), которое может включать этап досудебного разбирательства по делу». Сам по себе термин «*proceedings*» в зависимости от контекста может обозначать как производство по делу в целом (уголовное (суд)производство, которое по Уголовно-процессуальному кодексу РФ (УПК РФ) и в других континентальных правовых порядках начинается с момента приема сообщения о преступлении), нежели более узкое «судебное разбирательство», так и отдельное процессуальное действие (*procedural action*). См.: Legislative guides for the implementation of the United Nations Convention against Transnational Organized Crime and the Protocols thereto. New York: United Nations, 2004. P. 217, 220. Paras. 453, 465; Legislative guide for the implementation of the United Nations Convention against Corruption. New York: United Nations, 2012. P. 168. Para. 597; Technical guide to the United Nations Convention against Corruption. New York: United Nations, 2009. P. 163; Legislative Guide to the Universal Legal Regime against Terrorism. New York: United Nations, 2008. P. 39-40; Подготовительные материалы, касающиеся переговоров о разработке

Конвенции Организации Объединенных Наций против транснациональной организованной преступности и протоколов к ней. Нью-Йорк: Организация Объединенных Наций, 2006. С. 223-224; UNODC Revised Manual on the Model Treaty on Mutual Assistance in Criminal Matters. P. 67-68, 70. Paras. 5-7, 12; Mutual Legal Assistance Manual. Belgrade: Council of Europe Office in Belgrade, 2013. P. 75.

⁸См. подробнее: *Кальцов Д.В.* Негласные оперативно-розыскные мероприятия как форма реализации специальных методов расследования в российском законодательстве // Труды Академии управления МВД России. 2022. №4(64). С. 147-158.

⁹Сборник методических пособий по вопросам борьбы с торговлей людьми. Нью-Йорк: ООН, 2008. Пособие 5.2-5.5. С. 177-186; Toolkit to Combat Trafficking in Persons. New York: UN, 2008. Tools 5.2-5.5. P. 177-186; *Литвишко П.А.* Международное сотрудничество в области борьбы с преступностью: избранные вопросы // Сборник материалов по международному сотрудничеству Следственного комитета Российской Федерации. М., 2015. С. 213-233.

¹⁰Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings; Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings.

¹¹Explanatory notes on the Updated draft text of the convention and the revised draft General Assembly resolution, 15 July 2024. P. 14; Выступления на возобновленной заключительной сессии Спецкомитета (Нью-Йорк, 29 июля -

Петр ЛИТВИШКО

- 9 августа 2024 г.): Толкование термина «расследование»; Statement by the delegation of the Russian Federation at the resumed final session of the UN Ad Hoc Committee (New York, July 29 - August 9, 2024): Interpretation of the term «investigation».
- ¹²См., например: Posición del Ecuador respecto al texto aprobado. P. 1.
- ¹³Получение информации о состоявшихся соединениях между абонентами и (или) абонентскими устройствами (ст. 186¹ УПК РФ), осмотр и выемка электронных сообщений или иных передаваемых по сетям электросвязи сообщений (ч. 7 ст. 185 УПК РФ), контроль и запись переговоров и иных сообщений, а также получение информации о соединениях между абонентами и (или) абонентскими устройствами в режиме реального времени (ст. 186-186¹ УПК РФ).
- ¹⁴Контроль сообщений, прослушивание переговоров, снятие информации с технических каналов связи, получение компьютерной информации (ст. 6 Федерального закона от 12.08.1995 №144-ФЗ «Об оперативно-розыскной деятельности»).
- ¹⁵Пояснительная записка к проекту Федерального закона №280226-8 «О внесении изменений в статьи 453 и 456 Уголовно-процессуального кодекса Российской Федерации» (по вопросу о консульской функции по выполнению отдельных процессуальных действий по уголовным делам по запросам компетентных органов представляемого государства); Уголовный процесс России и стран Европы: сравнительно-правовое исследование: монография / под общ. и науч. ред. С.П.Щербы. М.: Проспект, 2023. С. 174-205.
- ¹⁶См. также: Заявление делегации Российской Федерации на пятой сессии Спецкомитета по разработке всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях (Вена, 11-21 апреля 2023 г.).
- ¹⁷См. подробнее: Collecting Electronic Evidence in Criminal Cases in Russia and Foreign Countries: Experiences and Problems: Monograph / editors S.P.Shcherba (Russian ed.) and P.A.Litvishko (English ed.). Moscow: Publishing House «Gorodets», 2024. P. 158-195.
- ¹⁸Transborder access to data and jurisdiction: Options for further action by the T-CY: Report prepared by the Ad-hoc Subgroup on Transborder Access and Jurisdiction adopted by the 12th Plenary of the T-CY (2-3 Dec. 2014) (T-CY (2014)16 of 3 Dec. 2014). P. 5, 10-11. Paras. 2.2.1, 2.4; Criminal justice access to data in the cloud: challenges: Discussion paper prepared by the T-CY Cloud Evidence Group (T-CY (2015)10 of 26 May 2015). P. 6. Para. 2.2. Здесь и далее материалы с официального интернет-сайта Комитета Конвенции о киберпреступности (Будапештской конвенции) // URL: <https://www.coe.int/en/web/cybercrime/the-budapest-convention> (дата обращения: 14.10.2024).
- ¹⁹Explanatory Report to the Convention on Cybercrime. Budapest, 23.XI.2001. P. 21. Para. 135.
- ²⁰См.: Заявление делегации Российской Федерации на пятой сессии Спецкомитета по разработке всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях (Вена, 11-21 апреля 2023 г.).
- ²¹См. подробнее: Collecting Electronic Evidence... P. 81-157.
- ²²Законопроект №462337-8 «О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации» (в части установления ответственности за незаконное осуществление следственных, иных процессуальных действий и оперативно-розыскных мероприятий на территории Российской Федерации). Пояснительная записка к нему.
- ²³T-CY Guidance Note №10: Production orders for subscriber information (Article 18 Budapest

ПЕРВЫЙ ГЛОБАЛЬНЫЙ ДОГОВОР ПРОТИВ КИБЕРПРЕСТУПНОСТИ:
ОТ ГЕОПОЛИТИЧЕСКОЙ КОНФРОНТАЦИИ К ПРОФЕССИОНАЛЬНОМУ...

Convention) adopted by the T-CY following the 16th Plenary by written procedure (28 Feb. 2017) (T-CY(2015)16 of 1 Mar. 2017). Para. 3.1.

²⁴Выступление Российской Федерации в Спецкомитете по разработке всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях по всему тексту Конвенции (30 июля 2024 г.).

²⁵T-CY Guidance Note №3: Transborder access to data (Article 32) adopted by the 12th Plenary of the T-CY (2-3 Dec. 2014) (T-CY (2013)7 E of 3 Dec. 2014). P. 4-5, 7-8. Paras. 3, 3.6, 3.8.

²⁶T-CY Guidance Note №10. Para. 3.1.

²⁷В директивной записке указывается, что «следует учитывать, что многие Стороны [Конвенции] возражали бы - а некоторые даже считают это уголовным правонарушением, - если к лицу, которое физически находится на их территории, напрямую обращаются иностранные правоохранительные органы за его сотрудничеством».

²⁸См. также: Соглашение между Правительством Российской Федерации и Правительством Республики Таджикистан о сотрудничестве в области обеспечения международной информационной безопасности от 19.06.2023 (ст. 7); Соглашение между Правительством Российской Федерации и Правительством Республики Союз Мьянма о сотрудничестве в области обеспечения международной информационной безопасности от 05.12.2023 (ст. 3).

²⁹См. подробнее: Collecting Electronic Evidence... P. 195-209.

³⁰Ibid. P. 81-126.

³¹Model Law on Mutual Assistance in Criminal Matters (2007), as amended with provisions on electronic evidence and the use of special investigative techniques (2022) (UN Doc. E/CN.15/2022/CRP.6 of 11 May 2022).

³²Explanatory notes on the Updated draft text of the convention and the revised draft General Assembly resolution, 15 July 2024. P. 16.

³³Explanatory Report to the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence. Strasbourg, 12.05.2022. Paras. 99, 128.

³⁴См. подробнее: Collecting Electronic Evidence... P. 58-59, 210-221.

³⁵Так, в соответствии с заявлением Российской Федерации к ст. 24 Европейской конвенции о взаимной правовой помощи по уголовным делам 1959 г. в редакции ст. 6 Второго дополнительного протокола к ней 2001 г. в качестве судебных органов в Российской Федерации рассматриваются суды, органы прокуратуры, дознания и предварительного следствия (Федеральный закон от 06.06.2019 №120-ФЗ «О ратификации Второго дополнительного протокола к Европейской конвенции о взаимной правовой помощи по уголовным делам»).

³⁶Литвишко П. Антикриминальное взаимодействие Российской Федерации с иностранными государствами и территориями, совершающими недружественные действия в отношении Российской Федерации, ее юридических и физических лиц // Законность. 2024. №5(1075). С. 26-35.