08.06.2022

1 группа вопросов

1–3. Поскольку речь идет о предписывающей юрисдикции (jurisdiction to prescribe), которая, как правило, относится к области материального права (substantive law), положения о ней целесообразно поместить в общих положениях или в разделе о криминализации, нежели в процессуальных положениях.

Положения о юрисдикции должны:

включать в себя императивные и дискреционные основания ее установления странами;

выделять территориальную юрисдикцию (в частности, по месту физического нахождения преступника или жертвы при совершении преступления либо их терминальных (end-point) ИКТ-устройств, использовавшихся при совершении преступления) и экстратерриториальную юрисдикцию на основе классических принципов – активного персонального, пассивного персонального, универсального, защитного, aut dedere aut judicare. При этом в составе защитного принципа (предполагает направленность деяния против интересов государства) по образцу других универсальных конвенций следует специально выделить направленность правонарушения против дипломатического представительства, консульского учреждения и иных правительственных объектов за рубежом, традиционно относящихся к наиболее уязвимым, в т.ч. для преступных посягательств в сфере ИКТ;

содержать указание на порядок урегулирования позитивных юрисдикционных конфликтов путем консультаций.

С другой стороны, среди процессуальных положений будут содержаться также нормы, указывающие на основания осуществления правоприменительной юрисдикции (jurisdiction to enforce).

Так, 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 состоянии рассредоточены по разным юрисдикциям или имеют в них свои многочисленные зеркальные копии.

В связи с этим процессуальная юрисдикция государства в отношении потоков данных основывается на локализации провайдера или его профессиональной деятельности. Для целей Конвенции эта юрисдикция определяется применительно к государству – адресату соответствующих запросов: 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 государства.

4. На этот вопрос мы ответили вчера под номером 6.

5. Соответствующие полномочия и процедуры, связанные с применением т.н. принудительных мер (coercive or compulsory measures), затрагивающих основные (конституционные) права человека, таких как тайна частной жизни или связи, к примеру получение сведений о трафике и контенте коммуникаций, в числе иного традиционно сопряжены с необходимостью судебного или приравненного к судебному санкционирования или последующей судебной валидации, а в отношении действий по сбору электронных доказательств в режиме реального времени – с необходимостью установления их предельных сроков с возможностью продления. Кроме того, должны быть обязательно оговорены случаи недопустимости или отложения уведомления (default notification) провайдером пользователя о действиях по сбору его данных в правоохранительных целях.

6. Считаем допустимой ссылку в проектируемой универсальной Конвенции только на универсальные инструменты о правах человека. Ссылку на не имеющие своего нормативного закрепления в таких договорах принципы необходимости и соразмерности не считаем приемлемой.

2 группа вопросов

1. Сохранение данных; предоставление данных об абоненте (подписчике), включая используемое им оборудование, его переписку со службой технической поддержки провайдера; получение информации о состоявшихся соединениях между абонентами и (или) абонентскими устройствами (хранящемся трафике, включая геолокацию); получение хранящихся данных о содержании сообщений (контенте); получение (перехват) трафика и контента в режиме реального времени; обыск и выемка информации, хранимой или обрабатываемой в электронной форме.

2–3. Мы уже дали ответы по этим пунктам в 1 группе вопросов под номером 5.

4. Должно быть обеспечено хранение информации в течение необходимого периода времени, не превышающего срока, установленного внутренним законодательством государства, а также должна быть предусмотрена возможность продления такого срока.

5. Целесообразно обсудить предполагаемые различия между этими терминами в ходе проработки раздела дефиниций.

6. Определение информации об абоненте обязательно. Все дефиниции целесообразно излагать в едином разделе, не фрагментируя их по всему тексту Конвенции.

7. Поскольку Конвенция должна быть применима не только к реактивным, но и проактивным расследованиям, подозрение о совершении соответствующих преступлений должно также служить основанием для проведения этих следственных действий (принудительных мер).

8. Предоставление возможности заявлений и оговорок в отношении процессуальных положений является оправданным.

3 группа вопросов

1. Уровень детализации положений, касающихся возврата активов, должен быть достаточным с учетом объекта и цели Конвенции и охватывать все стадии данного процесса.

2–3. Не возражаем против воспроизведения в Конвенции соответствующих норм КТОП.

4 группа вопросов

1. Установление стандартов сбора и допустимости цифровых доказательств по общему правилу является прерогативой национального законодателя.

Вместе с тем имеется существенная потребность в закреплении в Конвенции следующих несамоисполнимых (non-self-executing) норм, касающихся юридической силы, удостоверения подлинности и аутентификации (certification and authentication) собираемых на ее основе электронных доказательств:

- о функциях учреждаемой Конвенцией сети 24/7 по сохранению электронных доказательств, передаче запросов о правовой помощи и самих электронных доказательств;

- о рассмотрении государствами-участниками возможности создания платформ и каналов для передачи юридически значимых запросов о

правовой помощи в предоставлении электронных доказательств и самих электронных доказательств исключительно в безбумажной форме, основанных в том числе на взаимном признании цифровых подписей и штампов и других средств идентификации и аутентификации межгосударственного электронного документооборота, с возможной интеграцией таких платформ и каналов в сеть 24/7.

2–4. Поддерживаем воспроизведение названных положений КТОП в Конвенции, за исключением т.н. международного рецидива (ст. 22 КТОП).