ПРОБЛЕМЫ ЮРИСДИКЦИИ ПРИ РАССЛЕДОВАНИИ ТРАНСГРАНИЧНЫХ КИБЕРПРЕСТУПЛЕНИЙ В МЕЖДУНАРОДНОМ ПУБЛИЧНОМ ПРАВЕ

Нажиматдинов Илхам Полат улы

Магистрант Университета Мировой Экономики и Дипломатии

najimatdinovilxam@gmail.com

Аннотация (Abstract)

Настоящая статья посвящена комплексному исследованию фундаментальной научной проблемы международного публичного права — юрисдикционной коллизии, возникающей при расследовании трансграничных киберпреступлений. Архитектура глобального киберпространства разрушает классическое понимание территориального суверенитета, порождая ситуации несовпадения места нахождения потерпевшего, сервера, облачной инфраструктуры, провайдера цифровых услуг, подозреваемого лица и органа расследования. В работе детально проанализированы основные юрисдикционные принципы (территориальный, активный и пассивный персональный, защитный) и доказана их недостаточная эффективность в условиях распределенных облачных вычислений. Особое внимание уделено конфликту между государственным суверенитетом, потребностью правоохранительных органов в оперативном доступе к электронным доказательствам и необходимостью защиты фундаментальных прав человека. Исследована эволюция международно-правовых механизмов: от традиционных договоров о взаимной правовой помощи (MLAT) и положений Будапештской конвенции (включая Второй дополнительный протокол) до современных моделей экстерриториального доступа, таких как американский закон CLOUD Act и вступающий в силу в 2026 году Пакет Европейского союза

по электронным доказательствам (e-Evidence Package). Отдельно проанализированы итоги разработки Конвенции ООН против киберпреступности. В результате исследования предложены концептуальные подходы к преодолению юрисдикционного вакуума путем внедрения гибридных моделей межгосударственного взаимодействия и гармонизации коллизионных привязок в цифровой среде. Практическая и теоретическая значимость работы заключается в формировании доктринальной основы для модернизации механизмов уголовного преследования в киберпространстве.

Abstract

This article is devoted to a comprehensive study of a fundamental scientific problem in public international law: the jurisdictional collision arising during the investigation of cross-border cybercrimes. The architecture of global cyberspace dismantles the classical understanding of territorial sovereignty, engendering situations where the locations of the victim, server, cloud infrastructure, digital service provider, suspect, and investigating authority do not coincide. The paper analyzes in detail the core jurisdictional principles (territorial, active and passive personal, protective) and demonstrates their inadequacy in the context of distributed cloud computing. Special attention is given to the conflict between state sovereignty, the imperative for law enforcement to secure rapid access to electronic evidence, and the necessity of protecting fundamental human rights. The evolution of international legal mechanisms is examined: from traditional Mutual Legal Assistance Treaties (MLAT) and the provisions of the Budapest Convention (including the Second Additional Protocol) to modern models of extraterritorial access, such as the U.S. CLOUD Act and the European Union's e-Evidence Package, which comes into full effect in 2026. The outcomes of the drafting process for the UN Convention against Cybercrime are also analyzed. As a result of the study, conceptual approaches are proposed to overcome the jurisdictional vacuum by

implementing hybrid models of interstate cooperation and harmonizing conflict-of-law rules in the digital environment. The practical and theoretical significance of this work lies in establishing a doctrinal foundation for the modernization of criminal prosecution mechanisms in cyberspace.

Ключевые слова (Keywords): международное публичное право, киберпреступность, юрисдикция, государственный суверенитет, электронные доказательства, трансграничный доступ, Будапештская конвенция, CLOUD Act, e-Evidence, Конвенция ООН.

Введение: Кризис классического понимания территории в эпоху киберпреступности

Историческое развитие институтов международного публичного права неразрывно связано с концепцией государственного суверенитета, фундамент которой был заложен Вестфальским мирным договором в 1648 году. В рамках данной классической парадигмы суверенитет всегда имел четкое, математически измеримое физическое измерение: юрисдикция суверенного государства безусловно распространяется на определенную географическую территорию, жестко ограниченную сухопутными, морскими и воздушными границами. Уголовное преступление, как социальное, историческое и правовое явление, традиционно имело ясную привязку к физическому пространству (locus delicti), в котором совершалось общественно опасное деяние, наступали его материальные последствия и физически находились орудия совершения преступления и доказательства. Однако стремительное формирование и развитие глобального киберпространства спровоцировало беспрецедентный догматический кризис этой устоявшейся правовой модели.[1]

Актуальность настоящего исследования продиктована тем, что киберпреступность по своей внутренней технической природе является экстерриториальной и радикально трансграничной. Глобальная архитектура

сети Интернет, базирующаяся на базовых протоколах маршрутизации TCP/IP, технологически игнорирует политические и государственные границы. В процессе передачи цифровая информация разбивается на пакеты, которые в автоматическом режиме могут проходить через десятки серверов в различных, порой конфликтующих юрисдикциях за миллисекунды, прежде чем достигнут своего конечного аппаратного адресата. В результате этого процесса классическое понимание правовой территории полностью разрушается. Возникает парадоксальная ситуация: преступное деяние может быть инициировано за клавиатурой компьютера в одном суверенном государстве, промежуточный сервер управления хакерской атакой (C&C server) может быть арендован во втором, эластичное облачное хранилище с похищенными персональными данными может быть распределено между дата-центрами в третьем и четвертом, а колоссальный финансовый и материальный ущерб может быть причинен миллионам граждан, корпорациям и правительственным структурам в десятках других стран мира.[1]

В международном праве под уголовной юрисдикцией традиционно понимается суверенное право, обязанность и легитимные полномочия государства применять свои национальные законы, осуществлять отправление правосудия, а также назначать и исполнять наказание за их нарушение.[2] Возникающая при расследовании высокотехнологичных киберпреступлений юрисдикционная коллизия представляет собой не просто академический казус, а глубокую научную и острую практическую проблему. Хроническое несовпадение места нахождения потерпевшего, распределенного сервера, облачной инфраструктуры, провайдера цифровых услуг, подозреваемого лица и органа расследования создает правовой тупик. В такой ситуации на рассмотрение одного и того же уголовного дела могут обоснованно претендовать сразу несколько государств, опираясь на различные принципы международного права. Либо, что на практике случается гораздо чаще, ни

одно из затронутых государств не может эффективно реализовать свои юрисдикционные полномочия из-за непреодолимого отсутствия физического доступа к ключевым электронным доказательствам, изолированным за рубежом.

Теоретическая и практическая значимость данной работы заключается в необходимости критического переосмысления догматики международного уголовного права. Для эффективного противодействия информационным угрозам требуется выработка новых концептуальных моделей, которые позволили бы правоохранительным органам действовать со скоростью, сопоставимой со скоростью цифровых транзакций, не разрушая при этом архитектуру государственного суверенитета и систему защиты прав человека.

Теоретическая база и концептуальные подходы к исследованию

Формирование научной мысли относительно правового статуса киберпространства прошло несколько этапов эволюции. В ранних академических трудах (Дэвид Р. Джонсон, Дэвид Пост, Фрэнк Истербрук, Джек Л. Голдсмит) активно дискутировался вопрос о том, является ли Интернет фундаментальной угрозой самому институту территориального суверенитета, и способна ли классическая юриспруденция адаптироваться к виртуальной среде.[4] Долгое время среди теоретиков превалировал кибер-либертарианский подход, предполагавший, что цифровое пространство должно оставаться вне юрисдикции национальных правительств.

Однако с ростом киберпреступности, которая, согласно международному праву, признается преступлением международного характера, посягающим как на внутригосударственный, так и на международный правопорядок [5], международное сообщество перешло к концепции интеграции киберпространства в рамки существующего правового поля. Значительный

вклад в систематизацию этих норм внесла Группа правительственных экспертов ООН (GGE) и разработка Таллиннского руководства 2.0 по международному праву, применимому к кибернетическим операциям, созданного под эгидой Центра передового опыта НАТО по совместной защите от киберугроз (CCDCOE).[4]

Международная группа экспертов, работавшая над Таллиннским руководством, пришла к консенсусу, что ни одно государство не может претендовать на суверенитет над киберпространством как таковым (per se), поскольку оно представляет собой глобальное общественное благо.[7] Тем не менее, государства обладают суверенной властью над физической кибернетической инфраструктурой, физическими и юридическими лицами, а также любой кибератвностью, которые локализованы в пределах их суверенной территории.[7] Суверенитет, согласно Правилам 2 и 3 Таллиннского руководства, имеет как внутренний, так и внешний элементы, что наделяет государство исключительной прерогативой устанавливать уголовную юрисдикцию и требовать невмешательства извне.[7] Однако применение этого правила на практике обнажает свою уязвимость: установление точного географического местоположения электронных данных (data location) зачастую технически невозможно или юридически бессмысленно в эпоху распределенных облачных вычислений, что диктует необходимость анализа применения классических юрисдикционных принципов к новым реалиям.

Основные юрисдикционные принципы в международном публичном праве и их цифровая адаптация

Процесс установления уголовной юрисдикции в международном праве базируется на нескольких фундаментальных принципах, каждый из которых по-разному реагирует на вызовы транснациональной киберпреступности. В результате глубокого анализа доктрины и международных актов становится

очевидным, что конкретное содержание этих принципов применительно к глобальной цифровой среде все еще находится в стадии турбулентного формирования.[1]

Территориальная юрисдикция: от физической почвы к цифровым последствиям

Принцип территориальности исторически остается главным, наиболее легитимным и универсальным принципом, на основании которого суверенные государства устанавливают свою юрисдикцию в том числе и в киберпространстве.[1] Данная концепция предполагает, что государство обладает исключительным и непререкаемым правом применять свое уголовное законодательство в отношении любых преступлений, совершенных на его суверенной территории, независимо от гражданской принадлежности как самого преступника, так и потерпевшего лица.[2]

В сложном контексте транснациональных киберпреступлений территориальный принцип неизбежно распадается на два самостоятельных доктринальных аспекта:

1. **Субъективная территориальная юрисдикция:** Этот принцип применяется в тех случаях, когда преступное деяние (например, компиляция и первоначальный запуск вредоносного программного обеспечения, фишинговая рассылка) было физически начато на территории данного государства, даже если все деструктивные последствия этого акта наступили далеко за рубежом.

2. **Объективная территориальная юрисдикция (доктрина последствий):** Данный подход применяется, когда преступное деяние было инициировано за пределами государства, однако его существенные вредные последствия наступили именно на территории этого государства.[1] Классическим примером является парализация работы

национальной банковской системы или кража персональных данных из национального реестра в результате распределенной DDoS-атаки, организованной с зарубежных IP-адресов.

Фундаментальная проблема в киберпространстве заключается в определении самого понятия «места совершения преступления».[2] Является ли автоматический транзит зашифрованных пакетов данных через магистральный маршрутизатор, случайно расположенный в стране, достаточным международно-правовым основанием для утверждения о том, что преступление было совершено на ее территории? Как правило, в условиях отсутствия единой конвенции, государства стремятся максимально расширительно толковать территориальный принцип. Они признают свою абсолютную юрисдикцию в тех ситуациях, когда хотя бы малейшая часть объективной стороны преступного деяния (включая использование промежуточной цифровой инфраструктуры, регистрацию домена или хостинг временного файла) имела место в их правовом поле.[9] Это неизбежно порождает дублирование компетенций и международные правовые споры.

Активная персональная юрисдикция (Принцип национальности)

Принцип активной персональной юрисдикции (или активного гражданства) наделяет суверенное государство неотъемлемым правом преследовать в уголовном порядке своих собственных граждан за преступления, совершенные ими за пределами национальных границ.[2] В условиях глобализованной киберпреступности этот принцип приобретает колоссальное практическое значение. Злоумышленники часто выстраивают свою деятельность из стран, которые в силу политических или правовых причин не имеют договоров об экстрадиции с государствами, чьи интересы были затронуты атакой. В таких случаях государство гражданства киберпреступника может использовать принцип активной национальности

для привлечения лица к уголовной ответственности в собственных национальных судах.

Так, законодательство подавляющего большинства стран, в соответствии с рекомендациями УНП ООН, прямо предусматривает уголовную юрисдикцию в отношении киберпреступлений, если они совершены гражданином страны, даже если этот субъект постоянно проживает за ее пределами. Единственным существенным ограничением является соблюдение принципа двойной криминальности — деяние должно признаваться преступлением как по законам страны гражданства, так и по законам страны места фактического совершения деяния.[9] Главная уязвимость данного принципа заключается в практической плоскости: государство гражданства хакера часто не имеет ни политической мотивации, ни следственных ресурсов, ни технических возможностей для полноценного расследования неочевидного преступления, жертвы которого находятся на другом континенте, а серверные логи хранятся в третьей стране.

Пассивная персональная юрисдикция

Принцип пассивной индивидуальности (также известный как принцип пассивного гражданства) представляет собой зеркальное отражение предыдущей концепции. Он наделяет государство суверенным правом осуществлять экстерриториальную юрисдикцию в отношении уголовных преступлений, совершенных иностранными гражданами далеко за пределами его территории, если потерпевшим от этого преступления является гражданин данного государства.[2] В сфере глобального противодействия киберпреступности основание пассивной национальности влечет за собой существенные выгоды для государства-жертвы. Оно легитимизирует государственные усилия по защите своих физических и юридических лиц от дистанционных целевых кибератак, транснационального финансового

мошенничества, вымогательства (ransomware) и массовой кражи персональных данных.[10]

Тем не менее, практическая реализация принципа пассивной национальности на международной арене крайне затруднена и часто вызывает дипломатические трения. Государство физического нахождения подозреваемого крайне редко признает юрисдикцию государства гражданства потерпевшего в качестве достаточного и легитимного основания для ареста и последующей экстрадиции своего резидента, особенно если преступное деяние не было направлено непосредственно против государственных интересов или безопасности. Возникает глубокий правовой вакуум: государство потерпевшего имеет полное материально-правовое основание для возбуждения уголовного дела, однако оно не обладает реальной исполнительной властью ни над подозреваемым лицом, ни над цифровыми доказательствами, что делает правосудие невозможным.

Защитный принцип (Принцип безопасности) и универсальная юрисдикция

Защитный (или покровительственный) принцип предоставляет государствам исключительное право осуществлять экстерриториальную уголовную юрисдикцию в целях превентивной и реактивной самозащиты. Это происходит в тех ситуациях, когда правонарушения, совершенные иностранными гражданами за границей, направлены непосредственно против жизненно важных интересов национальной безопасности страны, угрожают ее территориальной целостности, политической независимости или подрывают выполнение ключевых правительственных функций.[2]

В отличие от принципа пассивной национальности, фокус которого смещен на защиту частных гражданских интересов, защитный принцип оберегает государственность как таковую.[10] В эпоху тотальной цифровизации

и кибервойн этот принцип приобретает критическую, экзистенциальную актуальность. Масштабные кибератаки на объекты критической информационной инфраструктуры (КИИ) — национальные электросети, системы водоснабжения, серверы центральных избирательных комиссий, закрытые правительственные базы данных и оборонные комплексы — безоговорочно квалифицируются как прямая угроза национальной безопасности. Бескомпромиссное применение защитного принципа оправдывает возбуждение уголовных дел спецслужбами и санкционирование наиболее агрессивных следственных действий (включая негласный трансграничный доступ к данным, разведывательные кибероперации и перехват трафика) абсолютно независимо от гражданства и местонахождения злоумышленников или промежуточных серверов.[1]

Эволюционное развитие международного права также демонстрирует робкие попытки применения принципа универсальной юрисдикции к отдельным видам киберпреступлений, тесно связанным с международным терроризмом и отмыванием денег.[2] Однако критика универсальной юрисдикции в данной сфере остается суровой: исследователи указывают на ее недостаточное и избирательное использование, отмечая, что государства, действуя исключительно на основе национального эгоизма и политического интереса, часто оказываются не в состоянии добросовестно осуществить правосудие по преступлениям, которые не наносят им прямого ущерба.[10]

Киберпреступление как трансграничное деяние: Проблема сервера, облака, провайдера и потерпевшего

Уникальная анатомия современного киберпреступления порождает беспрецедентный феномен дефрагментации уголовно-правового события. В парадигме традиционного уголовного права орудие совершения преступления, материальные следы, сам потерпевший и преступник, как

правило, находятся в едином физическом локусе (locus delicti) в момент совершения общественно опасного деяния. Следственно-оперативная группа, прибыв на место происшествия, может одномоментно локализовать и зафиксировать всю доказательственную базу. В киберпространстве же эти фундаментальные элементы катастрофически разнесены в пространстве и времени, что делает любое расследование заложником многоуровневого, бюрократизированного международного сотрудничества.

Техническая децентрализация и правовая фикция локации

Рассмотрим типичный высокотехнологичный сценарий транснационального киберпреступления, который иллюстрирует полный крах традиционной территориальности: подозреваемый лидер преступной группировки, физически находящийся в государстве «A», использует предварительно скомпрометированные серверы (ботнет), географически расположенные в государствах «B», «C» и «D». Через эту запутанную сеть он осуществляет целевую фишинговую атаку на критическую информационную систему транснациональной корпорации (выступающей в роли потерпевшего), чья штаб-квартира зарегистрирована в государстве «E». При этом вся корпоративная переписка и базы данных потерпевшего физически не находятся в государстве «E»; они размещены в эластичном облачном хранилище глобального IT-гиганта (провайдера), дата-центры которого в реальном времени распределяют нагрузку между государствами «F» и «G», а юридическая штаб-квартира самого провайдера находится в государстве «H».

Для наглядности масштаба юрисдикционной коллизии, целесообразно структурировать данную проблему.

Элемент преступления	Физическое/Техническое воплощение	Легитимные юрисдикционные притязания	Ключевая юридическая проблематика
Субъект (Подозреваемый)	Физическое лицо, инициирующее скрипты за компьютером в Государстве А.	Территориальная субъективная (А), Активная персональная (А).	Требуется сложная процедура экстрадиции; конституции многих стран (Государство А) прямо запрещают выдачу собственных граждан иностранным судам.
Орудие (Маршрутизация/Ботнет)	Скомпрометированные прокси-серверы и IoT-устройства в Государствах B, C, D.	Территориальная объективная (B, C, D).	Исключительно временный характер цифровых следов (данные хранятся в RAM-памяти и перезаписывают

			ся); транзитные государства не понесли ущерба и не имеют мотивации расходовать ресурсы на расследование.
Следы (Электронные доказательства)	Электронная почта, логи авторизации провайдера (дата-центры в F, G; юрлицо в H).	Территориальная (F, G), Корпоративная юрисдикция провайдера (H).	Провайдер строго подчиняется законам о защите данных страны H, которые могут под угрозой штрафов запрещать выдачу приватных данных по прямому запросу следователей страны E. Глубокий

			конфликт законов.
Объект (Потерпевший/ Ущерб)	Экономические интересы юридического лица в Государстве Е.	Территориальная доктрина последствий (Е), Пассивная персональная (Е), Защитный принцип (Е).	Орган дознания страны Е, инициирующий расследование, не имеет абсолютно никакой процессуальной власти над иностранными провайдерами и зарубежными облачными доказательствами.

Данная матрица наглядно и безапелляционно демонстрирует, почему традиционные механизмы Договоров о взаимной правовой помощи по уголовным делам (Mutual Legal Assistance Treaties, MLATs) в современных условиях терпят полный крах. Процедура MLAT создавалась и оттачивалась для физического мира: она требует направления международных следственных поручений по дипломатическим каналам, длительных переводов, проверки соответствия принципу двойной криминальности и, наконец, обязательного судебного санкционирования в запрашиваемом

государстве. Как показывает статистика и аналитика, этот тяжеловесный процесс в среднем занимает от 6 до 10 месяцев.[11] В то же время жизненный цикл критически важных электронных доказательств (логов динамических IP-адресов, данных о сетевых сессиях, метаданных VoIP-трафика) часто исчисляется днями, а в условиях применения злоумышленниками систем автоматического стирания — часами или минутами.

Особую, непреодолимую сложность в рамках классического права представляет концепция «облачных вычислений» (cloud computing).[12] В современной облачной инфраструктуре пользовательские данные больше не привязаны к конкретному физическому магнитному диску или серверной стойке. Глобальные провайдеры (такие как AWS, Microsoft, Google) посредством сложных алгоритмов динамически дефрагментируют и перемещают массивы зашифрованных данных между серверами в разных суверенных странах в режиме реального времени для оптимизации балансировки нагрузки, снижения задержек и обеспечения отказоустойчивого резервного копирования.[13] В результате, к моменту получения следователем официального международного ордера на выемку данных с конкретного аппаратного сервера в государстве «F», искомая информация может быть уже автоматически перемещена инфраструктурным алгоритмом провайдера в государство «G». Это делает строгий территориальный подход к определению юрисдикции местонахождения электронных доказательств безнадежно устаревшим и формирует фундаментальный юридический конфликт мирового масштаба.

Проблема конфликта между государственным суверенитетом, эффективностью расследования и защитой прав человека

Квинтэссенцией современного кризиса международного права в сфере противодействия киберпреступности является глубокое, концептуально трудноразрешимое противоречие между тремя основополагающими ценностями современного демократического общества: незыблемостью государственного суверенитета, императивом эффективности правоохранительной деятельности и неукоснительным соблюдением фундаментальных прав человека.

1. **Государственный суверенитет.** Согласно положениям Таллиннского руководства 2.0 (в частности, Правилу 4), государство не должно проводить кибероперации, которые нарушают суверенитет другого государства.[7] Несанкционированный односторонний доступ правоохранительных органов и специальных служб одного государства к базам данных и серверам, физически расположенным на территории другого суверенного государства, традиционно рассматривается международным сообществом как грубое нарушение суверенитета последнего.[7] Классическое международное право исходит из незыблемой презумпции: любые принудительные следственные действия, обыски и выемки на чужой территории могут проводиться исключительно с ясно выраженного согласия местного суверена.

2. **Эффективность расследования.** Статистические исследования, проведенные Европейской комиссией, неопровержимо доказывают, что электронные доказательства (e-evidence) в той или иной форме сегодня являются критически релевантными примерно в 85% всех проводимых уголовных расследований.[11] И в двух третях этих случаев искомые цифровые данные физически хранятся в другой стране, преимущественно находясь под прямым корпоративным контролем транснациональных IT-гигантов.[11] Следователям в условиях цифрового цейтнота необходима беспрецедентная скорость. Строгое, педантичное

соблюдение принципа территориального суверенитета (многомесячное ожидание ответов по каналам MLAT) неизбежно приводит к безвозвратной утрате улик и формированию чувства абсолютной безнаказанности у киберпреступников. Правоохранительные органы справедливо требуют внедрения принципиально новых, экстерриториальных инструментов для прямого и незамедлительного кросс-бордерного доступа к данным.[15]

3. **Защита прав человека.** С другой стороны баррикад выступают институты гражданского общества. Прямой, неконтролируемый доступ иностранных силовых структур к персональным данным абонентов, их переписке и финансовой истории создает колоссальные, системные риски для фундаментального права на приватность, свободы выражения мнений и права на справедливое судебное разбирательство.[17] Правозащитные организации (такие как EFF) и профильные надзорные органы (например, Европейский совет по защите данных — EDPB) обоснованно бьют тревогу, указывая на то, что радикальное упрощение процедур трансграничного доступа позволяет исполнительной власти легко обходить национальные суды.[17] Если иностранный полицейский следователь получает законодательное право напрямую потребовать конфиденциальные данные у частного интернет-провайдера, из цепочки правосудия исключается критически важный фильтр в виде независимого судебного контроля запрашиваемого государства. Именно этот фильтр исторически призван оценивать законность, обоснованность и соразмерность запроса, а также предотвращать политически мотивированные или репрессивные преследования диссидентов и журналистов.[17]

Разрешение этого сложнейшего треугольника противоречий стало главной стратегической задачей всего международного сообщества в XXI

веке. Это предсказуемо привело к фрагментации правовых подходов и появлению различных, порой жестко конкурирующих, региональных и национальных моделей трансграничного доступа к электронным доказательствам.

Подходы Будапештской конвенции и Второго дополнительного протокола к модернизации юрисдикции

Конвенция Совета Европы о киберпреступности (широко известная как Будапештская конвенция), открытая для подписания в 2001 году, стала первым в истории человечества международным договором, предпринявшим попытку масштабно гармонизировать материальное и процессуальное уголовное право в цифровой сфере.[19] Долгое время она оставалась золотым стандартом, открытым для присоединения государств, не являющихся членами Совета Европы.[19]

Однако отношение к архитектуре Конвенции в международном публичном праве весьма неоднозначно. Главным камнем преткновения и предметом ожесточенных научных и политических дискуссий стала **Статья 32** («Трансграничный доступ к хранящимся компьютерным данным с согласия или при наличии открытого доступа»). Данная революционная статья прямо позволяет правоохранительным органам государства-участника без предварительного разрешения (официальной авторизации) другого суверенного государства осуществлять две вещи: во-первых, получать неограниченный доступ к публично доступным данным (open source) независимо от их географического положения; во-вторых, получать удаленный доступ через компьютерную систему на своей территории к хранящимся на территории другой стороны компьютерным данным, если получено законное и абсолютно добровольное согласие лица, имеющего правовые полномочия раскрывать эти данные.[12]

С точки зрения повышения оперативной эффективности, Статья 32 легитимизировала устоявшуюся полицейскую практику получения информации (OSINT) и добровольного взаимодействия с лояльными зарубежными провайдерами.[12] Однако ряд крупных государств усмотрел в этой формулировке прямую угрозу и подрыв государственного суверенитета. В частности, Российская Федерация категорически и принципиально отказалась от участия в Будапештской конвенции именно из-за Статьи 32. Доктринальная позиция России сводится к тому, что данная статья фактически легализует возможность для иностранных спецслужб проводить несанкционированные следственные кибероперации и сбор данных на суверенной чужой территории в обход национальных компетентных органов, что является грубым нарушением императивного принципа невмешательства во внутренние дела государств.[23]

Возникает также сложнейшая цивилистическая проблема квалификации самого понятия «законного добровольного согласия». Провайдеры информационных услуг, физически владеющие серверами, за редким исключением не являются собственниками (owners) данных своих пользователей; они выступают лишь в роли хранителей (holders).[25] Это ставит под серьезное сомнение их легитимное право давать «добровольное согласие» на выдачу конфиденциальной пользовательской информации иностранным силовикам без судебного ордера.[25]

Второй дополнительный протокол: Радикальная легализация прямого сотрудничества

Остро осознавая растущую неадекватность традиционных механизмов MLAT и явную ограниченность Статьи 32 перед лицом глобальных облачных технологий, Совет Европы предпринял попытку модернизации режима. В мае 2022 года был принят **Второй дополнительный протокол к Конвенции о**

киберпреступности, направленный на усиление сотрудничества и ускоренное раскрытие электронных доказательств.[26] По состоянию на последние годы, этот протокол активно подписывается десятками стран (включая Великобританию, Словению, Хорватию и др.), стремящимися получить современный инструментарий борьбы с транснациональной преступностью.[23]

Второй протокол совершил настоящую концептуальную революцию в международном уголовном процессе, жестко закрепив правовые механизмы прямого трансграничного взаимодействия. Наиболее значимыми и дискуссионными являются следующие новеллы:

- **Статья 6 (Прямые запросы информации о регистрации доменных имен):** Данная норма позволяет компетентным органам одного государства напрямую, без дипломатических проволочек, обращаться к субъектам (например, регистраторам в системе ICANN) в других юрисдикциях для получения специфической информации (WHOIS данных), идентифицирующей владельцев интернет-доменов.[29]
- **Статья 7 (Прямое сотрудничество с поставщиками услуг для получения информации об абонентах):** Эта статья вызывает наибольший резонанс. Она наделяет правоохранительные органы правом направлять обязательные для исполнения приказы о выдаче абонентской информации (subscriber information) напрямую сервис-провайдерам, находящимся на территории других суверенных государств-участников, полностью минуя правительства этих государств.[20]

Таким образом, Второй протокол де-юре санкционировал частичный, но весьма существенный отказ суверенных государств от своей исторической монополии на юрисдикционный контроль над частными компаниями в пользу глобальной скорости и эффективности уголовных расследований. Для балансировки этой радикальной уступки предусмотрены определенные

гарантии: государства имеют право заявить оговорки и требовать обязательного одновременного уведомления (notification mechanism) о таких прямых запросах на своей территории, а также могут настаивать на том, чтобы подобные иностранные приказы издавались исключительно под строгим судебным контролем прокурора или судьи запрашивающего государства.[20] Тем не менее, международные правозащитники подвергают Статью 7 жесткой критике за то, что она недопустимо опускает планку гарантий неприкосновенности частной жизни, фактически оставляя сложную правовую оценку правомерности уголовного запроса на откуп частным IT-корпорациям, юристы которых не обладают ни компетенцией, ни полномочиями для анализа уголовно-правовых нюансов иностранного законодательства.[17] Европейский совет по защите данных (EDPB) также подчеркивает, что обязательства по международным соглашениям не могут превалировать над конституционными принципами защиты фундаментальных прав в ЕС.[18]

Национальные и региональные модели экстерриториального доступа к данным: CLOUD Act и Пакет e-Evidence ЕС

Параллельно с многосторонними, но медленными усилиями Совета Европы, ключевые геополитические и экономические игроки — Соединенные Штаты Америки и Европейский Союз — сформировали собственные мощные односторонние и региональные правовые механизмы, которые сегодня кардинально меняют весь ландшафт международного публичного права.

Американская экстерриториальность: Закон CLOUD Act

В 2018 году Конгресс США принял резонансный **CLOUD Act** (Clarifying Lawful Overseas Use of Data Act — Закон об уточняющем правомерном использовании данных, хранящихся за рубежом). Философия этого акта

базируется на принципе корпоративного контроля над данными, полностью игнорируя принцип их физического местоположения.[13]

Согласно императивным нормам CLOUD Act, американские правоохранительные органы, получив соответствующий судебный ордер, могут принудить любую технологическую компанию, подпадающую под широкую юрисдикцию США (имеющую хотя бы «минимальные контакты» с американской экономикой, что охватывает почти весь глобальный IT-рынок), выдать электронные данные ее пользователей, абсолютно независимо от того, в какой стране мира эти данные физически расположены или зашифрованы.[13] Этот закон одномоментно устранил для американских следователей все преграды, связанные с государственными границами и местонахождением серверов, однако он же породил беспрецедентный международный конфликт юрисдикций (conflict of laws).[32]

Когда федеральный судья США обязывает транснациональную корпорацию (например, Microsoft или AWS) выдать деловую или личную переписку, хранящуюся в дата-центре в Швейцарии или Германии, корпорация оказывается в правовой ловушке. С одной стороны, неисполнение ордера США грозит ей колоссальными штрафами и санкциями за неуважение к суду. С другой стороны, прямая передача персональных данных граждан Евросоюза по требованию иностранного (неевропейского) органа исполнительной власти прямо и недвусмысленно запрещена статьей 48 Общего регламента по защите данных (GDPR) ЕС, которая признает законными только те трансграничные запросы, которые прошли валидацию через официальный механизм MLAT.[33] Аналогичные острейшие коллизии возникают в связи с новым Актом ЕС о данных (EU Data Act), который также императивно блокирует экстерриториальные запросы иностранных правительств на получение неперсональных промышленных данных.[34]

Законодатели США попытались смягчить этот удар, предусмотрев в CLOUD Act механизм защиты: провайдер получил процессуальное право оспорить ордер в американском суде, если сможет доказать, что целевой пользователь не является гражданином или резидентом США, и что выдача данных создаст существенный риск нарушения законов иностранного государства. Однако этот механизм работает только в том случае, если с этим государством у США заключено специальное двустороннее исполнительное соглашение.[35] На практике бремя доказывания коллизии целиком ложится на плечи частной компании, судебная процедура не приостанавливает действие ордера, а реальная защита «европейского суверенитета» данных остается иллюзорной.[34] В рамках этой парадигмы США начали активно выстраивать закрытую сеть двусторонних соглашений с наиболее доверенными партнерами (например, с Великобританией), создавая эксклюзивные блоки обмена разведданными в обход классических и универсальных международных структур.[13]

Пакет Европейского Союза по электронным доказательствам (e-Evidence Package 2026)

В ответ на агрессивную американскую правовую экспансию и осознавая нарастающую критическую неэффективность режима MLAT, Европейский Союз разработал и утвердил собственный масштабный, технологичный правовой механизм — Пакет по электронным доказательствам (e-Evidence Package). Этот пакет концептуально состоит из Регламента (ЕС) 2023/1543 и гармонизирующей Директивы (ЕС) 2023/1544.[26] Данный комплекс актов формирует жесткую, унифицированную и обязательную правовую рамку, которая, после завершения трехлетнего переходного периода, вступает в полную юридическую силу во всех без исключения государствах-членах ЕС **18 августа 2026 года**.[15]

Пакет e-Evidence закрепляет беспрецедентный в истории Европы уровень глубокой интеграции следственных и судебных органов. Он вводит в процессуальный оборот два принципиально новых наднациональных инструмента:

1. **Европейский ордер на предоставление информации (EPOC — European Production Order Certificate):** Этот сертификат позволяет компетентным судебным или следственным органам одного государства-члена ЕС напрямую, минуя министерства юстиции, затребовать электронные доказательства (абонентские данные, метаданные транзакций, и даже сам контент переписки) у провайдера цифровых услуг. Ключевое условие юрисдикции — провайдер должен просто «предлагать услуги» (offering services) на территории ЕС (например, иметь пользователей в ЕС или таргетировать на них рекламу), независимо от того, где физически находится его штаб-квартира (даже если в третьей стране) или где физически расположены жесткие диски с данными.[16]

2. **Европейский ордер на сохранение информации (EPOC-PR — European Preservation Order Certificate):** Этот инструмент предписывает провайдеру немедленно «заморозить» искомые данные на срок не менее 60 дней до момента получения полноценного ордера EPOC на их изъятие. Это эффективно предотвращает умышленное удаление улик киберпреступниками.[16]

Сравнительный анализ наглядно демонстрирует радикальный сдвиг парадигмы:

Характеристика процессуального режима	**Классический режим MLAT**	**Новый режим e-Evidence ЕС (вступает в силу с августа 2026 года)**
Субъекты правового взаимодействия	Государство ↔ Суверенное Государство	Государство ↔ Частный Провайдер цифровых услуг (напрямую)
Основание для установления юрисдикции	Физическое нахождение данных (сервер)	Экономическая связь (предложение цифровых услуг на рынке ЕС) [16]
Нормативные сроки исполнения запроса	От 6 до 10 месяцев (не регламентировано жестко)	**10 дней** в обычном порядке, всего **8 часов** в экстренных случаях (угроза жизни) [16]
Механизм официального представительства	Межправительственная работа через центральные органы (Министерства юстиции)	Провайдеры обязаны назначить официальных юридических представителей (addressees) на территории ЕС [16]

Карательные санкции за неисполнение	Дипломатические протесты, политическое давление	Прямые финансовые штрафы до **2% от глобального годового оборота** корпорации [16]

Инновационным и наиболее спорным элементом Регламента 2026 года является полный перенос тяжести бремени реагирования и комплаенса на частный коммерческий бизнес. Любая IT-компания (социальные сети, мессенджеры, платформы облачного гейминга, хостинги), обслуживающая граждан ЕС, категорически обязана назначить контактное лицо и за свой счет интегрироваться в децентрализованную, криптографически защищенную IT-инфраструктуру (система e-CODEX, строящаяся на базе строгих технических спецификаций ETSI) для получения официальных ордеров от властей ЕС.[16] Например, в Германии, согласно закону о внедрении e-Evidence (EBewMG), контроль за этим процессом возложен на Федеральное ведомство юстиции (BfJ), а за нарушение сроков провайдер и его представитель несут солидарную юридическую ответственность.[16]

Однако внедрение e-Evidence также порождает серьезные внутриевропейские коллизии. В целях защиты остатков национального суверенитета, орган-исполнитель (то есть власти государства, в котором физически находится представитель провайдера) уведомляется о запросе только в наиболее чувствительных случаях — при запросе данных о трафике и самом контенте коммуникаций. У этого государства есть право заявить официальные основания для отказа (grounds for refusal), такие как иммунитеты, профессиональные привилегии (например, адвокатская тайна), свобода прессы, очевидные нарушения фундаментальных прав или принцип ne bis in idem.[16] Если такие основания заявляются, ордер отзывается. Этот механизм призван стать щитом цифрового суверенитета государств внутри

ЕС.[16] Тем не менее, гражданские институты и парламентарии выражают глубокие опасения, что из-за сверхжестких сроков (всего 10 дней) государства-исполнители физически не смогут провести качественную и всестороннюю правовую экспертизу каждого поступающего запроса, что превратит судебный контроль в простую формальность.[16] Данный законодательный пакет ЕС уже стал мощнейшим катализатором для начала интенсивных двусторонних переговоров между Брюсселем и Вашингтоном (в контексте преодоления противоречий с CLOUD Act) с целью создания единого трансатлантического соглашения, способного гармонизировать эти мощные, но конкурирующие юрисдикционные подходы.[11]

Глобальная доктринальная коллизия: Конвенция ООН против киберпреступности (2024–2026)

В то время как Западный мир в лице США и ЕС выстраивает региональные механизмы, основанные на концепции прямой экстерриториальной власти над данными и взаимодействии с корпорациями, на глобальном уровне развернулась масштабная геополитическая битва под эгидой ООН. Кульминацией этих многолетних усилий стало принятие Генеральной Ассамблеей ООН в конце 2024 года Конвенции Организации Объединенных Наций против киберпреступности (UNCC).[42] Этот всеобъемлющий договор, открытый для подписания всеми суверенными государствами мира, ознаменовал собой амбициозную попытку создать глобальный альтернативный контур правового регулирования, в отличие от Будапештской конвенции, которая воспринималась многими странами как сугубо европейский проект.[42] Ожидается, что процесс масштабной ратификации договора и имплементации его норм в национальные законодательства развернется в период 2025–2026 годов, после церемонии подписания.[42]

В ходе длительной разработки Конвенции (в рамках работы Специального межправительственного комитета с 2021 по 2024 год) в штаб-квартирах в Нью-Йорке и Вене столкнулись диаметрально противоположные концепции понимания юрисдикции и суверенитета в цифровую эпоху.[43]

Одна мощная коалиция государств, концептуально возглавляемая Российской Федерацией, последовательно и жестко настаивала на абсолютном, непререкаемом приоритете государственного суверенитета и территориальной неприкосновенности информационных систем. В рамках этой консервативной доктрины (которая была полно отражена еще в первоначальном российском проекте конвенции 2017 года) предлагался категорический запрет на любой трансграничный доступ правоохранителей к компьютерной информации без официального взаимодействия с соответствующими компетентными органами государства, на суверенной территории которого расположена инфраструктура.[45] Этот подход абсолютно отвергает легитимность прямых запросов к транснациональным провайдерам (в стиле e-Evidence или Статьи 7 Второго протокола), признавая единственно законным исключительно межгосударственное взаимодействие в рамках классических, хотя и ускоренных процедур правовой помощи (MLAT).[45] Кроме того, сторонники этой модели ратовали за более широкое понимание субъекта и объекта преступления, предлагая использовать термины «ИКТ-преступность» (преступность с использованием информационно-коммуникационных технологий), акцентируя внимание на монопольном контроле государства над информационной инфраструктурой и криминализации более широкого спектра деяний.[46]

С другой стороны дипломатического стола, делегации США (включая экспертов Министерства юстиции, таких как Томас Барроуз), стран Европейского Союза и их союзники пытались интегрировать в текст

Конвенции ООН либеральные концепции, методологически схожие со Статьей 32 Будапештской конвенции и принципами e-Evidence.[43] Они резонно настаивали на том, что без внедрения механизмов быстрого, децентрализованного трансграничного получения доказательств любая глобальная конвенция будет мертворожденной, поскольку не сможет угнаться за технологическим прогрессом.[43]

Итоговый принятый текст Конвенции ООН представляет собой чрезвычайно сложный, многовекторный политико-правовой компромисс.[43] С одной стороны, он существенно расширяет сферу охвата, устанавливая 11 базовых составов преступлений и распространяя механизмы взаимной правовой помощи на сбор электронных доказательств по любым «серьезным преступлениям» (наказываемым лишением свободы на срок от четырех лет), чем выгодно отличается от Будапештской конвенции, которая фокусировалась преимущественно на узких компьютерных деликтах.[42] Конвенция ООН упрощает процедуры экстрадиции, базируясь на стандартизированном принципе двойной криминальности, и создает прочную правовую основу для сотрудничества государств Глобального Юга, не охваченных региональными пактами.[43] С другой стороны, Конвенция оставляет государствам-участникам чрезвычайно широкие рамки для национального толкования юрисдикционных связей (статьи о юрисдикции и процессуальных мерах) и, по сути, не решает окончательно фундаментальную проблему одностороннего прямого доступа к облачным хранилищам. Она деликатно оставляет острейшую правовую коллизию между «суверенным» (территориальным) и «экстерриториальным» (корпоративным) подходами неразрешенной на универсальном уровне, перенося тяжесть ее разрешения на стадию двусторонних договоренностей и национального правоприменения.[42]

Результаты и выводы

Синтезируя результаты проведенного всестороннего догматического и сравнительно-правового исследования проблем юрисдикции при расследовании трансграничных киберпреступлений, можно с полной научной уверенностью констатировать, что классическая вестфальская система международного публичного права, базирующаяся на географическом локусе, потерпела глубокий институциональный крах при столкновении с цифровой средой. Цифровые данные лишены физического измерения; их местоположение в облачной инфраструктуре изменчиво, технологически условно и зачастую юридически случайно. Привязка следственных действий к месту расположения сервера больше не отвечает критериям правовой логики и оперативной эффективности.

Прямым следствием этого технологического сдвига является перманентный и обостряющийся конфликт юрисдикций. Одно транснациональное киберпреступление сегодня объективно и одновременно затрагивает правопорядок государства активной национальности (местонахождение хакера), государства объективной территориальности (инфраструктура маршрутизации), государства корпоративной юрисдикции провайдера (место регистрации IT-гиганта) и государства потерпевшего (реализация доктрины последствий или принципа пассивной национальности).

Анализ новейшей международной практики ярко демонстрирует опасную дивергенцию правовых режимов, ведущую к фрагментации мирового правопорядка. Если страны Совета Европы (в рамках Второго дополнительного протокола к Будапештской конвенции) и институты Европейского Союза (в рамках революционного Пакета e-Evidence 2026) взяли решительный курс на легализацию прямого государственно-частного взаимодействия, фактически размывая историческую монополию

территориального государства на отправление правосудия, то Конвенция ООН и подходы суверенитет-ориентированных стран (таких как Российская Федерация) отчаянно пытаются спасти межгосударственный механизм взаимодействия, модернизируя и ускоряя традиционные институты дипломатической правовой помощи. Параллельно с этим, американская правовая доктрина (выраженная в CLOUD Act) агрессивно навязывает глобальную экстерриториальную юрисдикцию по принципу экономического контроля над корпорациями, систематически провоцируя непреодолимые конфликты с европейским законодательством о защите данных (GDPR и Data Act).

Для преодоления прогрессирующего правового нигилизма в киберпространстве, разрешения указанных коллизий и выработки эффективной международной стратегии, предлагаются следующие концептуальные шаги и реформы международного права:

1. **Доктринальный отказ от исключительности территориального критерия местонахождения данных.** В международном публичном праве, на уровне обычных норм и будущих протоколов к конвенциям, должен быть официально закреплен принципиально новый коллизионный принцип — критерий «центра тяжести» (center of gravity) или «эффективной связи» (genuine link). При определении приоритетной и легитимной юрисдикции для истребования электронных доказательств правоохранительные органы и суды должны опираться не на случайное физическое местоположение серверов, а на место обычного проживания (habitual residence) субъекта данных или потерпевшего.[50] Это позволит устранить корпоративный арбитраж и защитить права граждан по законам их собственной страны.

2. **Институционализация гибридного механизма «уведомления с**

правом вето». В качестве сбалансированного компромисса между прямым доступом (модель e-Evidence/Второй протокол) и традиционным, но медленным MLAT, необходимо под эгидой структур ООН разработать глобальную защищенную платформу электронного документооборота. При направлении следственного запроса транснациональному цифровому провайдеру, компетентный орган страны базирования провайдера должен автоматически и мгновенно уведомляться через защищенный криптографический шлюз. Ему должен предоставляться сжатый, но реалистичный срок (например, 72 часа) для наложения суверенного вето на передачу данных. При этом право вето должно реализовываться исключительно на основе закрытого, исчерпывающего перечня критериев (явное нарушение фундаментальных прав человека, угроза национальной безопасности, политическое преследование). Отсутствие вето в установленный срок (режим молчаливого согласия) будет означать автоматическую правовую валидацию запроса.

3. **Строгое разграничение уровней доступа по степени вмешательства.** Юрисдикционные правила и процедуры авторизации должны жестко дифференцироваться в зависимости от характера запрашиваемых данных. Прямой трансграничный доступ правоохранителей (с последующим уведомлением) должен быть легализован исключительно для получения базовой технической и абонентской информации, а также регистрационных данных доменов (на что справедливо направлена Статья 6 Второго протокола). В то же время, экстерриториальный доступ к чувствительному контенту сообщений (содержимое почты, облачные диски) и глубокому поведенческому анализу трафика должен осуществляться исключительно через процедуру обязательного судебного санкционирования с полным

вовлечением компетентных властей запрашиваемого государства для недопущения произвольного нарушения конституционного права на тайну переписки.

4. **Технологическая унификация стандартов доказательственного права.** Для обеспечения реализации процессуальных прав, международному сообществу необходимо разработать единый технический протокол хеширования и криптографической защиты изымаемых цифровых следов (по аналогии с успешными спецификациями ETSI для европейской системы e-CODEX [16]). Это необходимо для того, чтобы электронные доказательства, собранные напрямую от иностранного провайдера, обладали презумпцией целостности и автоматически признавались допустимыми в уголовном процессе любой страны-участницы, исключая возможность их манипуляции в процессе передачи.

Только путем кропотливого формирования компромиссной, сбалансированной международно-правовой парадигмы, которая, с одной стороны, безусловно признает суверенные права государств на обеспечение правопорядка и защиту своих граждан, а с другой — объективно учитывает экстерриториальную природу цифровых потоков и императив защиты фундаментальных прав человека, возможно создать реальный и эффективный заслон транснациональной киберпреступности. Без концептуальной гармонизации этих базовых принципов глобальная сеть продолжит оставаться территорией правового хаоса, где технологическая изощренность злоумышленников всегда будет превосходить архаичные юрисдикционные возможности государств.

Источники

1. Международно-правовые принципы установления юрисдикции ..., дата последнего обращения: июня 12, 2026,

https://aprp.msal.ru/jour/article/download/4185/2340

2. 12.00.08 (5.1.4.) Уголовное право, криминология - Удмуртский государственный университет, дата последнего обращения: июня 12, 2026, https://udsu.ru/files/priyomnaya-komissiya/006394-12.00.08%20(5.1.4.)%20%D0%A3%D0%B3%D0%BE%D0%BB%D0%BE%D0%B2%D0%BD%D0%BE%D0%B5%20%D0%BF%D1%80%D0%B0%D0%B2%D0%BE,%20%D0%BA%D1%80%D0%B8%D0%BC%D0%B8%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D1%8F.docx

3. The Role of Cybercrime Law - United Nations Office on Drugs and Crime, дата последнего обращения: июня 12, 2026, https://www.unodc.org/cld/ru/education/tertiary/cybercrime/module-3/key-issues/the-role-of-cybercrime-law.html

4. Territorial Sovereignty in Cyberspace after Tallinn Manual 2.0 - Melbourne Law School, дата последнего обращения: июня 12, 2026, https://law.unimelb.edu.au/__data/assets/pdf_file/0010/3567439/Circop.pdf

5. Международно-правовое регулирование борьбы с киберпреступлениями - DOI, дата последнего обращения: июня 12, 2026, https://doi.org/10.37399/issn2072-909x.2023.4.24-30

6. The Tallinn Manual 2.0: Highlights and Insights - Georgetown Law, дата последнего обращения: июня 12, 2026, https://www.law.georgetown.edu/international-law-journal/wp-content/uploads/sites/21/2018/05/48-3-The-Tallinn-Manual-2.0.pdf

7. Sovereignty (Chapter 1) - Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations - Cambridge University Press & Assessment, дата последнего обращения: июня 12, 2026, https://www.cambridge.org/core/books/tallinn-manual-20-on-the-international-law-applicable-to-cyber-operations/sovereignty/6BA0C5B9829FD15D997B8C973C395E16

8. 1 States and cyberspace - Institute for Security Policy and Law, дата последнего обращения: июня 12, 2026, https://securitypolicylaw.syr.edu/wp-content/uploads/2015/06/Tallinn-Manual-Sovereignty.pdf

9. Cybercrime Module 7 Key Issues: Sovereignty and Jurisdiction - UNODC, дата последнего обращения: июня 12, 2026, https://www.unodc.org/cld/ru/education/tertiary/cybercrime/module-7/key-issues/sovereignty-and-jurisdiction.html

10. ТАДЖИКСКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ На правах рукописи УДК: 341+341.4+32та - ИНСТИТУТИ ФАЛСАФА, СИЁСАТШИНОСӢ ВА ҲУҚУҚИ БА НОМИ А.БАҲОВАДДИНОВ, дата последнего обращения: июня 12, 2026, https://ifppanrt.tj/dissertatsii_hukuk/OdinazodaNH/Dissertatsiya.pdf

11. Navigating Toward an EU-U.S. Agreement on Electronic Evidence - Lawfare, дата последнего обращения: июня 12, 2026, https://www.lawfaremedia.org/article/navigating-toward-an-eu-u.s.-agreement-on-electronic-evidence

12. Art. 32 CCC (Convention on Cybercrime) - Onlinekommentar, дата последнего обращения: июня 12, 2026, https://onlinekommentar.ch/en/kommentare/ccc32

13. Microsoft признала, что не может гарантировать суверенитет данных в Европе, дата последнего обращения: июня 12, 2026, https://servernews.ru/1126645

14. How Microsoft is addressing digital sovereignty in Switzerland - Source EMEA, дата последнего обращения: июня 12, 2026, https://news.microsoft.com/source/emea/2026/02/how-microsoft-is-addressing-digital-sovereignty-in-switzerland/

15. дата последнего обращения: июня 12, 2026, https://www.bakermckenzie.com/en/insight/publications/2026/03/european-union-

european-criminal-law-enforcement-is-stepping-up#:~:text=The%20European%20Union's%20Regulation%20(EU,evidence%20held%20by%20service%20providers.

16. European Union: European Criminal Law Enforcement is Stepping ..., дата последнего обращения: июня 12, 2026, https://www.bakermckenzie.com/en/insight/publications/2026/03/european-union-european-criminal-law-enforcement-is-stepping-up

17. Global Law Enforcement Convention Weakens Privacy & Human Rights, дата последнего обращения: июня 12, 2026, https://www.eff.org/deeplinks/2021/06/global-law-enforcement-convention-weakens-privacy-human-rights

18. EDPB contribution to the consultation on a draft second additional protocol to the Council of Europe Convention on Cybercrime (B, дата последнего обращения: июня 12, 2026, https://www.edpb.europa.eu/sites/default/files/files/file1/edpbcontributionbudapestconvention_en.pdf

19. ПРАКТИКОВ В ОБЛАСТИ УГОЛОВНОГО ПРАВОСУДИЯ - Обеспечение Соблюдения Прав Человека при Расследовании Киберпреступлений - OSCE Projects, дата последнего обращения: июня 12, 2026, https://projects.osce.org/sites/default/files/f/documents/d/f/573995_1.pdf

20. Battling Cybercrime Through the New Additional Protocol to the Budapest Convention, дата последнего обращения: июня 12, 2026, https://ccdcoe.org/library/publications/battling-cybercrime-through-the-new-additional-protocol-to-the-budapest-convention/

21. When is Cyber Defense a Crime? Evaluating Active Cyber Defense Measures Under the Budapest Convention | Chicago Journal of International Law, дата последнего обращения: июня 12, 2026, https://cjil.uchicago.edu/print-archive/when-cyber-defense-crime-evaluating-active-cyber-defense-measures-

under-budapest

22. T-CY Guidance Note # 3 Transborder access to data (Article 32) - CCDCOE, дата последнего обращения: июня 12, 2026, https://www.ccdcoe.org/uploads/2019/09/CoE-141203-Guidance-Note-on-Transbprder-access-to-data.pdf

23. Ещё 6 стран подписали Второй дополнительный протокол к Конвенции о киберпреступности - ЗАЩИТА ИНФОРМАЦИИ - Портал органов власти Чувашской Республики, дата последнего обращения: июня 12, 2026, https://it-zaschita.med.cap.ru/press/2022/12/1/eschyo-6-stran-podpisali-vtoroj-dopolniteljnij-pro

24. Ещё 6 стран подписали Второй дополнительный протокол к Конвенции о киберпреступности | Digital Russia, дата последнего обращения: июня 12, 2026, https://d-russia.ru/eshhjo-6-stran-podpisali-vtoroj-dopolnitelnyj-protokol-k-konvencii-o-kiberprestupnosti.html

25. CYBERCRIME CONVENTION COMMITTEE (T-CY), дата последнего обращения: июня 12, 2026, https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_draft_transborderart32_/7_draft_transborderart32_en.pdf

26. E-evidence - cross-border access to electronic evidence - European Commission, дата последнего обращения: июня 12, 2026, https://commission.europa.eu/law/cross-border-cases/judicial-cooperation/types-judicial-cooperation/e-evidence-cross-border-access-electronic-evidence_en

27. Second Additional Protocol to Cybercrime Convention - eucrim, дата последнего обращения: июня 12, 2026, https://eucrim.eu/news/second-additional-protocol-to-cybercrime-convention/

28. Борьба с киберпреступностью в Молдове: кабмин ратифицировал международный протокол, а покупателей SIM-карт обяжут предъявлять удостоверение личности - NewsMaker, дата последнего обращения: июня 12,

2026, https://newsmaker.md/ru/borba-s-kiberprestupnostyu-v-moldove-kabmin-ratificziroval-mejdunarodnyi-protokol-a-pokupatelei-sim-kart-obyajut-predyavlyat-udostoverenie-lichnosti

29. Future of the Convention - Cybercrime - The Council of Europe, дата последнего обращения: июня 12, 2026, https://www.coe.int/en/web/cybercrime/future-of-the-convention

30. Requests for Domain Name Registration Information under Article 6 of the Second Additional Protocol to the Convention on Cybercr - Eurojust, дата последнего обращения: июня 12, 2026, https://www.eurojust.europa.eu/sites/default/files/assets/requests-for-domain-name-registration-information-under-article-6-of-the-second-additional-protocol-to-the-convention-on-cybercrime-23-01-2024.pdf

31. ЭЛЕКТРОННЫЙ СБОРНИК - ТРУДОВ МОЛОДЫХ СПЕЦИАЛИСТОВ ПОЛОЦКОГО ГОСУДАРСТВЕННОГО УНИВЕРСИТЕТА Выпуск 32 (102) ЮРИДИЧЕСКИЕ НАУКИ, дата последнего обращения: июня 12, 2026, https://elib.psu.by/bitstream/123456789/25896/1/2020_%D0%A2%D0%9C%D0%A1_%D0%AE%D1%80%D0%B8%D0%B4%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D0%B5%20%D0%BD%D0%B0%D1%83%D0%BA%D0%B8.pdf

32. The CLOUD Act - Microsoft, дата последнего обращения: июня 12, 2026, https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/CLOUD-Act-What-it-is-and-is-not.pdf

33. CLOUD Act vs. GDPR: The Conflict About Data Access Explained - Exoscale, дата последнего обращения: июня 12, 2026, https://www.exoscale.com/blog/cloudact-vs-gdpr/

34. EU Data Act vs. U.S. CLOUD Act: Data Sovereignty Conflict - Kiteworks,

дата последнего обращения: июня 12, 2026, https://www.kiteworks.com/gdpr-compliance/eu-data-act-gdpr-cloud-conflict/

35. Clarifying Lawful Overseas Use of Data (CLOUD) Act - Amazon Web Services, дата последнего обращения: июня 12, 2026, https://aws.amazon.com/compliance/cloud-act/

36. US CLOUD Act vs European/UK Data Sovereignty Explained - CMS.law, дата последнего обращения: июня 12, 2026, https://cms.law/en/deu/legal-updates/white-paper-demystifying-the-debate-on-the-us-cloud-act-vs-european-uk-data-sovereignty-in-the-context-of-cloud-services

37. EU e-Evidence Package - Bird & Bird, дата последнего обращения: июня 12, 2026, https://www.twobirds.com/en/trending-topics/eu-e-evidence-package

38. The e-Evidence Package: A new regime for cross-border law enforcement requests, дата последнего обращения: июня 12, 2026, https://www.arthurcox.com/knowledge/the-e-evidence-package-a-new-regime-for-cross-border-law/

39. About the e-Evidence Package, дата последнего обращения: июня 12, 2026, https://www.gov.ie/en/department-of-justice-home-affairs-and-migration/organisation-information/about-the-e-evidence-package/

40. Digital sovereignty: Europe's declaration of independence? - Atlantic Council, дата последнего обращения: июня 12, 2026, https://www.atlanticcouncil.org/in-depth-research-reports/report/digital-sovereignty-europes-declaration-of-independence/

41. E-Evidence Regulation Takes Effect in August, Enabling Direct Cross-Border Data Requests, дата последнего обращения: июня 12, 2026, https://acompli.ie/news/e-evidence-regulation-august-2026/

42. Preparing for the UN Cybercrime Convention and Its Impact on Technology Service Providers - Debevoise Data Blog, дата последнего обращения: июня 12, 2026, https://www.debevoisedatablog.com/2025/11/25/preparing-for-the-un-

cybercrime-convention-and-its-impact-on-technology-service-providers/

43. Panel Shares Insights on Drafting New U.N. Cybercrime Treaty | Yale Law School, дата последнего обращения: июня 12, 2026, https://law.yale.edu/yls-today/news/panel-shares-insights-drafting-new-un-cybercrime-treaty

44. Ad Hoc Committee on Cybercrime | Digital Watch Observatory, дата последнего обращения: июня 12, 2026, https://dig.watch/processes/cybercrime-ad-hoc-committee

45. Первый глобальный договор против киберпреступности: от геополитической конфронтации к профессиональному компромиссу - Посольство, дата последнего обращения: июня 12, 2026, https://russianembassyza.mid.ru/ru/press-centre/news/pervyy_globalnyy_dogovor_protiv_kiberprestupnosti_ot_geopoliticheskoy_konfrontatsii_k_professionalno/

46. Международный диалог по проблеме высокотехнологичной преступности Текст научной статьи по специальности «Право - КиберЛенинка, дата последнего обращения: июня 12, 2026, https://cyberleninka.ru/article/n/mezhdunarodnyy-dialog-po-probleme-vysokotehnologichnoy-prestupnosti

47. What Is the New UN Cybercrime Treaty? - Epicenter.works, дата последнего обращения: июня 12, 2026, https://epicenter.works/en/content/un-cybercrime-treaty

48. UN Cybercrime Convention Budapest Convention (“BC”) and Second Additional Protocol (“Second Protocol”), дата последнего обращения: июня 12, 2026, https://www.crossborderdataforum.org/wp-content/uploads/2025/05/Chart-UN-Cybercrime-Convention-Budapest-Convention-and-Second-Additional-Protocol.pdf

49. UN Cybercrime Convention - Full Text - UNODC, дата последнего обращения: июня 12, 2026,

https://www.unodc.org/unodc/en/cybercrime/convention/text/convention-full-text.html

50. Международный научный журнал АКАДЕМИК № 1 (299) 2026 г., дата последнего обращения: июня 12, 2026, https://journal-academic.com/f/mezhdunarodnyi_nauchnyi_zhurnal_akademik_3003_chast_1.pdf