Сравнительно-правовой анализ
законодательства Республики Никарагуа и Российской Федерации
в части обеспечения правового регулирования информационно-
коммуникационного пространства в целях противодействия преступности

Интеграция информационно-коммуникационных технологий (далее – ИКТ) в экономику и социальную сферу создает новые возможности для развития, но одновременно рождает новые угрозы: киберпреступность, незаконный контент, вмешательство в критическую инфраструктуру. Правовые системы различных государств реагируют на вызов по-разному. Российская Федерация обладает разветвлённой системой нормативных актов, эволюционировавшей с начала 2000-х годов. Республика Никарагуа сформировала «молодую», но комплексную регуляторную модель, приняв в 2020-х годах несколько «сквозных» законов, ориентированных сразу на всю цифровую повестку. Настоящая работа ставит целью выявить общие и специфические черты правового регулирования ИКП в двух странах и оценить их реальную результативность в противодействии преступности.

Исследование основано на комплексном анализе:

– нормативных правовых актов Российской Федерации (Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ, Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ, Федеральный закон «О связи» от 07.07.2003 № 126-ФЗ, Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ, а также Уголовного кодекса и Уголовно-процессуального кодекса Российской Федерации);

– законодательства Республики Никарагуа («Закон о конвергентных телекоммуникациях от 06.11.2024» Ley General de Telecomunicaciones Convergentes № 1223/2024, «Специальный закон о киберпреступлениях от 27.10.2020» Ley Especial de Ciberdelitos № 1042/2020 и др.);

– официальной статистики МВД России и Национальной Полиции Республики Никарагуа;

– докладов регуляторов (Роскомнадзор[1], ФСТЭК[2], TELCOR[3]);

---

[1] Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор, сокращённо РКН) – российский федеральный орган исполнительной власти, задачами и функциями которого являются: контроль за соблюдением законов и нормативных актов в сфере информационных технологий и связи; обеспечение безопасности детей в информационном пространстве; защита информационной безопасности государства; обеспечение рационального использования радиочастотного спектра; контроль качества оказываемых связи услуг; лицензирование операторов связи и регулирование тарифов.

[2] Федеральная служба по техническому и экспортному контролю (ФСТЭК) – федеральный орган исполнительной власти России, созданный в 2004 году. Ведомство регулирует

– научной литературы и материалов СМИ.

Детерминированная выборка нормативных актов позволила провести качественный контент-анализ и построить сравнительную таблицу компетенций регуляторов, процессуальных возможностей следствия, а также динамики раскрываемости киберпреступлений.

Нормативная база Российской Федерации, используемая в сравнительно-правовом анализе:

1. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ закрепляет принципы свободы информации при одновременном введении режимов её ограничения, определяет обязанности владельцев информационных систем содействовать правоохранительным органам, создает механизм блокировки интернет-ресурсов по реестру запрещённой информации;

2. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ вводит понятие критической информационной инфраструктуры (КИИ) и систему её категорирования; предписывает операторам КИИ применять сертифицированные средства защиты;

3. Федеральный закон «О связи» № 126-ФЗ от 07.07.2003 г. регулирует лицензирование операторов, устанавливает обязанности по хранению трафика, внедрению технических средств оперативно-розыскных мероприятий;

4. Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ формирует режим обработки персональных данных, включая трансграничную передачу и локализацию.

Уголовный кодекс РФ выделяет специальные составы за неправомерный доступ к компьютерной информации (ст. 272), создание и распространение вредоносных программ (ст. 273), нарушение правил эксплуатации КИИ (ст. 274, 274.1). Уголовно-процессуальный кодекс регламентирует порядок изъятия электронных носителей, применения перехвата данных и оперативно-розыскных мероприятий (ст. 183, 186, 194–198).

информационную безопасность, защиту государственной тайны и экспортный контроль. В IT-сфере ФСТЭК разрабатывает стандарты, чтобы предотвратить утечки данных и кибератаки, обеспечивая надёжность систем. Задачами ФСТЭК являются: сертификация программ и оборудования для защиты информации; разработка нормативов по информационной безопасности; лицензирование работы с конфиденциальными данными; проверка соблюдения требований.

[3] TELCOR (Instituto Nicaragüense de Telecomunicaciones y Correos) – государственное учреждение Никарагуа, регулирующее сферу телекоммуникаций и почтовых услуг. TELCOR выполняет следующие функции: регулирует, планирует и контролирует соблюдение законов и норм, которые регулируют установку, подключение, работу и предоставление услуг телекоммуникаций и почты; управляет и регулирует спектр радиочастот; выдаёт лицензии, разрешения или сертификаты регистрации компаниям, которые предоставляют услуги телекоммуникаций и почты или используют радиочастотный спектр.

Надзор и контроль распределены между Роскомнадзором (контент и персональные данные), Минцифры (политика в сфере связи), ФСТЭК (КИИ) и ФСБ России (оперативно-розыскная деятельность). Такая полицентрическая модель обеспечивает многоуровневую фильтрацию рисков, но иногда снижает оперативность принятия решений.

Нормативная база Республики Никарагуа, используемая в сравнительно-правовом анализе:

1. Ley General de Telecomunicaciones Convergentes № 1223/2024 (Закон о конвергентных телекоммуникациях № 1223/2024 от 06.11.2024).

Закон объединяет ранее разрозненные нормы о связи, радиочастотах и интернет-услугах, вводит универсальную лицензию сроком 10 лет, обязывает операторов хранить журналы соединений не менее 12 месяцев и предоставлять их следственным органам по постановлению суда. TELCOR, получивший статус «единого окна», сочетает функции надзора, лицензирования и управления спектром, что позволяет оперативно блокировать ресурсы, распространяющие противоправный контент;

2. Ley Especial de Ciberdelitos № 1042/2020 (Специальный закон о киберпреступлениях № 1042/2020 от 27.10.2020).

Акт типологизирует 19 видов киберпреступлений: от неправомерного доступа до цифрового отмывания средств. Он вводит возможность «отложенного уведомления» о проведении обыска в сетевой среде и предоставляет Национальной Полиции Республики Никарагуа право использовать сетевые «ловушки» для идентификации злоумышленников;

3. Дополнительные нормативные акты

– Ley de Defensa de los Derechos del Pueblo a la Independencia, la Soberanía y Autodeterminación para la Paz № 1055/2021 (О защите прав народа на независимость № 1055/2021 от 21.12.2020) – аналог российских антиэкстремистских норм, применимый к цифровому контенту.

– Decreto 70-2010 (Исполнительный декрет 70-2010) регулирует борьбу с финансированием преступных организаций через электронные каналы.

– Reglamento TELCOR 2023 (регламент деятельности TELCOR) устанавливает кроме прочего технические требования к хранению геолокационных данных мобильных устройств.

Созданная система, несмотря на сравнительно недавнее принятие, уже включает все основные элементы: уголовную типологию, процессуальные инструменты и регуляторный контроль.

Сравнительный анализ ключевых законов

Критерий	Российская Федерация Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ	Никарагуа Ley General de Telecomunicaciones Convergentes № 1223/2024 (Закон о конвергентных телекоммуникациях № 1223/2024 от 06.11.2024)
Модель регулирования	Смешанная: принцип свободного обращения + секторальные ограничения, адресный реестр запрещённого контента	Конвергентная: «единое окно» лицензирования, контент-триггерная модель блокировки
Полномочия регулятора	Роскомнадзор: ведет реестр, выдаёт предписания, взаимодействует с операторами связи	TELCOR: объединяет надзор, лицензирование и следственные функции (метаданные, QoS)
Содействие следствию	Операторы обязаны устанавливать специальное оборудование; выдача данных по судебному решению	Операторы хранят логи ⩾ 12 мес.; TELCOR может предоставить доступ по постановлению спецсуда по киберпреступлениям

В целом конвергентная модель Республики Никарагуа демонстрирует более высокую оперативность в сборе доказательств. Российская схема обеспечивает более сильные процессуальные фильтры, но иногда затягивает раскрытие преступлений.

Практическая эффективность: эмпирические данные:

Показатели (2024 г.)	Российская Федерация	Республика Никарагуа
Доля раскрываемости киберпреступлений	36 %	41 %
Средний срок получения данных у операторов[1]	7–30 суток	3–10 суток
Уровень судебной нагрузки (дел на100 000 населения)	12,3 %	4,7 %

[1] Данные опросов сотрудников полиции России и Республики Никарагуа.

Централизованная структура TELCOR и небольшое число крупных провайдеров (Claro, Tigo, Yota de Nicaragua) упрощают процесс запроса данных в Республике Никарагуа. В России фрагментация рынка связи (более 8 крупных операторов и более 6 000 малых) и сложная процедура санкционирования приводят к большему среднему сроку получения данных. Тем не менее, российская модель обеспечивает высокий уровень защиты персональных данных и процессуальных прав граждан.