УПРАВЛЕНИЕ, ГРАНИЦЫ И ЮРИСДИКЦИЯ В СЕТИ ИНТЕРНЕТ В КОНТЕКСТЕ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ

Дарья Владимировна ЗАВЬЯЛОВА,
аспирант кафедры криминалистики Университета имени О.Е. Кутафина (МГЮА)
dariazav@mail.ru
125993, Россия, г. Москва, ул. Садовая-Кудринская, д. 9

Аннотация. *Статья посвящена анализу технических особенностей функционирования сети Интернет, порождающих правовые и криминалистические последствия при расследовании кибепреступлений. Децентрализованная природа Интернета и специфика управления им, обусловленные его технической архитектурой, приводят к сложностям при определении юрисдикций в ходе расследований киберпреступлений. В статье автор также исследует особенности преступлений, совершенных с помощью информационных технологий, осложняющие их расследование; современные представления о возможностях «проведения границ» в Сети, последствия таких мер в контексте криминалистических задач, а также способы определения юрисдикций при расследовании киберпреступлений.*

Кроме того, рассматриваются система управления в Интернете, организации, осуществляющие его, их иерархия и подотчетность. Исследованы технический механизм функционирования Сети, факторы, угрожающие такому функционированию. По итогам исследования предлагаются методы повышения эффективности международного сотрудничества в сфере расследования компьютерных преступлений, решения вопросов юрисдикции. Отмечается необходимость повышения информационной и технологической осведомленности на всех уровнях, а также межведомственного сотрудничества.

Ключевые слова: *киберпреступления, компьютерные преступления, преступления в сфере информационных технологий, информационные технологии, локализация данных, юрисдикция, границы, международное сотрудничество.*

DOI: 10.17803/2311-5998.2021.78.2.155-161

D. V. ZAVIALOVA,
postgraduate student of the Criminalistics Department of the Kutafin Moscow State Law University (MSAL)
dariazav@mail.ru
125993, Russia, Moscow, ul. Sadovaya-Kudrinskaya, 9

INTERNET GOVERNANCE, BORDERS AND JURISDICTION IN THE CONTEXT OF CRIME INVESTIGATION

Abstract. *The article focuses on the technical features of Internet operation, causing legal and forensic consequences when investigating cybercrimes. Decentralized nature and the specificity of Internet governance resulting from its technical architecture lead to difficulties in identifying the jurisdiction during*

cybercrime investigations. In the article, the author also analyses IT crimes' particular features, which make them difficult to investigate, as well as some contemporary ideas on the possibility of delineating borders on the Net, the consequences of such measures, and the ways to identify jurisdiction when looking into cybercrimes. Apart from that, the article examines the Internet governance system, managing organizations as well as their hierarchy, and accountability. The technical mechanism of Internet operation is analyzed. Some factors threatening the operation are reviewed. Following the research results, the author proposes some methods to enhance international cooperation regarding cybercrime investigations and resolving jurisdictional issues. The need to increase informational and technical knowledge at all levels and to support interdepartmental cooperation is noted.
Keywords: *cybercrime, computer crime, IT crime, IT, cyberattack, IT, data localization, jurisdiction, borders, international cooperation.*

В 1997 г.на конференции в Сан-Франциско генеральный директор Google Эрик Шмит сказал: «Интернет — это первая вещь, созданная человечеством, которую оно само не может понять, величайший анархический эксперимент в истории»[1]. Сегодня, спустя больше 20 лет, понимаем ли мы Интернет хоть немного лучше и по-прежнему ли он так анархичен?

С того момента, как Сеть стала представлять интерес для кого-то, кроме узкого круга профессионалов и любителей, обладавших специальными знаниями в области технологий, Интернет воспринимался как пространство свободной коммуникации. Однако появление персонального компьютера, применение его в бизнесе, выход на потребительский рынок стали прорывом не только в контексте новых, непревзойденных возможностей для работы, творчества, управления и прочих видов созидательной деятельности. Персональные компьютеры и их сети стали условиями зарождения кибепреступности. Это явление заставило государства задаться вопросами об управлении и контроле в Интернете, о возможности установления границ и определения юрисдикций, введения новых составов преступлений, разработки криминалистических методик их расследования.

По данным за 2018 г., стоимость ущерба от кибепреступлений в развитых странах выросла в среднем на 22,7 %[2]. Число киберпреступлений в России, согласно данным Главного управления правовой статистики и информационных технологий Генеральной прокуратуры РФ, в 2019—2020 гг. также росло[3].

Не будет преувеличением сказать, что пандемия COVID-19 стала тем импульсом, который запустил реализацию давно назревавших технологических и социальных изменений. Коронавирус показал, как быстро могут сложиться новые онлайн-подходы к деятельности, когда меняется социальный контекст и

---

1 *Singer P. W., Friedman A.* Cybersecurity and Cyberwar: What Everyone Needs to Know. New York : Oxford University Press, 2014. P. 26.

2 *Broadhead S.* The contemporary cybercrime ecosystem: A multi-disciplinary overview of the state of affairs and developments // Computer Law & Security Abstract. 2018. Vol. 34. P. 1186.

3 URL: https://genproc.gov.ru/stat/data/ (дата обращения: 22.07.2020).

разрушается привычная рутина[4]. Эта новая реальность проявляет себя на всех уровнях: от введения электронного документооборота (в области трудового права, гражданского оборота, налоговых отношений, следствия и судопроизводства[5]) до цифровизации системы госзакупок[6].

Дистанционные форматы обучения и работы охватывают огромное количество людей, которые до этого момента избегали постоянного контакта с информационными технологиями, сводя такое взаимодействие к минимуму, воспринимая IT как развлечение или вспомогательный инструмент. Эти люди максимально уязвимы перед кибепреступностью, так как в большинстве своем они обладают низкой технической грамотностью, и их вынужденная вовлеченность в «сетевые» процессы и отношения ставит под удар в первую очередь их финансы и персональные данные.

Кроме того, уровень безопасности самих платформ и сетей может быть довольно низким, что также неизбежно привлекает киберпреступников.

Исходя из этого, можно предположить, что одним из последствий нового импульса для углубления и ускорения цифровизации станет рост компьютерной преступности.

Здесь важно отметить, что до сих пор отсутствует единое понятие этого явления, а как следствие — его однородная криминализация в мире. То, что в одном государстве является киберпреступлением, в другом таковым может не быть.

Это объясняется тем, что нормы уголовного права различных государств, в отличие, скажем, от норм гражданского права, традиционно носят более закрытый, внутренний характер. На протяжении большей части современной истории большинство деяний, подпадавших под регулирование нормами именно уголовного права, предполагали если не непосредственное взаимодействие жертвы и преступника, то как минимум тот факт, что они находятся на территории одного государства[7]. С наступлением эры информационного общества такое предположение больше нельзя назвать оправданным.

Часто Интернет воспринимается пользователями как некая хаотичная структура, не имеющая границ и не привязанная к физическим географическим точкам. Но это совсем не так.

Одна из ключевых характеристик Сети, на которой сделал акцент Эрик Шмит, это ее рукотворность. Система создана человеком и контролируется им. Несмотря на то, что Сеть глобальна, она не оторвана от концепции государственной принадлежности и не является в полной мере общим достоянием человечества, как мы привыкли о ней думать.

---

[4] *Ribaux O., Souvignet T. R.* “Hello are you available?” Dealing with online frauds and the role of forensic science // Forensic Science International: Digital Investigation. 2020. Vol. 33. P. 1.

[5] URL: http://www.consultant.ru/document/cons_doc_LAW_327513/ (дата обращения: 22.07.2020) ; URL: http://www.consultant.ru/document/cons_doc_LAW_355063/63125e835439d4ab1fa3e2dc27e7f4048813a02b/ (дата обращения: 22.07.2020).

[6] URL: https://rg.ru/2020/07/21/pandemiia-podstegnula-cifrovizaciiu-rossijskoj-sistemy-goszakupok.html (дата обращения: 22.07.2020).

[7] *Balkin J. M.* Cybercrime: Digital Cops in a Networked Environment. Information Society Project (Yale Law School). New York : NYU Press. 2007. P. 208.

Точно так же, как люди когда-то искусственно разделили поверхность Земли и провели государственные и национальные границы, возможно разделить и киберпространство[8]. Конечно, его «география» гораздо сложнее, так как это очень подвижная среда. Постоянно меняются и эволюционируют не только элементы системы, но и наши ожидания от нее.

Так, на ранних этапах Интернет воспринимался как технология, не связанная непосредственно с повседневной жизнью и решающая узкий круг задач. По мере развития Интернет интегрировался в самые разные сферы, его социальное и политическое значение постепенно росло. На данный момент сетевые технологии, IT являются неотъемлемой частью критической инфраструктуры. Они играют огромную роль в нормальном функционировании важнейших систем общества: финансовой, здравоохранения, энергоснабжения и др.

Вместе с ростом значимости росли и социальные ожидания от устойчивости и безопасности работы Интернета, требования к компаниям и лицам, обеспечивающим эту работу. На данный момент тот факт, что сетевые технологии являются частью критической инфраструктуры, а значит, могут выступать в том числе и политическим рычагом, а также стремительное развитие киберпреступности вызывают повышенный интерес к вопросам контроля в Интернете, инструментам установления его «границ» и определения юрисдикций.

Чтобы рассматривать вопросы юрисдикций и контроля, необходимо разъяснить механизм функционирования Сети.

При любом запросе в Сеть компьютер ищет путь к серверу с запрашиваемой информацией. Чтобы ее найти, он будет использовать IP-номер «пункта назначения». IP — это набор цифр (IPv4) или цифр и букв (IPv6), которые понятны компьютеру в двоичной системе, но неудобны для человека. Именно поэтому была создана система доменных имен (DNS — Domain Name System), которая «переводит» IP-адреса в удобные для человека имена в форме слов.

Архитектуру DNS можно представить в виде дерева. Основа этой системы — корневые домены. Над ними стоят домены верхнего уровня (это, например, кодовые домены стран, такие как .ru или .uk, а также домены типа .comи, .net).

Домены верхнего уровня контролируются ICANN (Internet Corporation for Assigned Names and Numbers). ICANN — частная некоммерческая организация, созданная в Калифорнии в 1998 г.[9] И здесь складывается уникальная ситуация, потому что частная компания контролирует ресурс, обеспечивающий бесперебойное функционирование системы, которая является частью критической инфраструктуры всех развитых стран мира. В целом система управления Интернетом весьма нетривиальна: она не централизована и строится на широком участии частных заинтересованных лиц и компаний, международных организаций[10].

Такое положение вещей при включении Интернета в критическую инфраструктуру устраивает государства все меньше. Предпринимаются попытки выстраивания централизованного контроля, о которых мы будем говорить ниже.

---

[8] *Singer P. W., Friedman A.* Op. cit. P. 14.

[9] *Žolnerčíková V.* ICANN: Transformation of Approach towards Internet Governance // Masaryk University Journal of Law and Technology. 2017. Vol. 11. P. 155—172.

[10] *Dr. De Nardis L.* Five Destabilizing Trends in Internet Governance // A Journal of Law and Policy for the Information Society. 2015. Vol. 12. P. 113—114.

Каждый запрос разбивается на отдельные пакеты, в каждом из которых есть выходные данные. Каждый из пакетов по отдельности направляется компьютером в локальную сеть, из которой они также по отдельности будут направлены в большую сеть. Разные пакеты одного и того же запроса могут идти разными маршрутами.

Выбор маршрута отдельного пакета обеспечивается роутером, который принимает решение, куда направить пакет, как доставить его быстрее, опираясь на данные, которыми роутеры обмениваются между собой. Если один из них будет случайно или намерено введен в заблуждение, это может стать причиной серьезного сбоя в работе всей системы в целом. Как это, например, произошло в феврале 2008 г., когда правительство Пакистана сделало попытку заблокировать доступ к YouTube для своих граждан. С этой целью «Пакистан Телеком» неверно проинформировал компьютеры своих клиентов, представив путь к YouTube через свой сервер как наикратчайший.

Это информация вышла за пределы локальной сети Пакистана и вскоре около 2/3 всех пользователей Интернета в мире были неверно направлены в «Пакистан Телеком» при попытке попасть на YouTube, что, конечно, обрушило сеть «Пакистан Телеком»[11]. Последствия этого инцидента были ликвидированы довольно быстро, но эта ситуация показывает, во-первых, критичную взаимозависимость и связь элементов, на которых строится работа Сети, и, во-вторых, важность понимания того, как эта система функционирует при попытках контролировать потоки информации.

Помимо технических попыток контроля, сейчас предпринимаются и законодательные попытки установления «государственных границ» в Интернете. Одна из них — концепция локализации данных. Такие модели различной степени закрытости выстраиваются по всему миру: в России[12], Китае, США, странах Евросоюза[13].

Вопрос, к каким последствиям технически, экономически и политически может привести такая модель «национальных интернетов», требует самостоятельного исследования. Что касается криминалистических последствий, то уже сейчас можно сделать вывод: представление о том, что локализация данных помогает защитить информацию, создать более безопасное пространство для нее, не совсем верно:

1) локализованные сервера не дают возможности распределять данные по разным серверам в разных точках мира. Такое аккумулирование потенциально уязвимой информации (конфиденциальных данных) в одном месте представляет собой идеальную мишень для злоумышленников;
2) отсутствие полноценной конкуренции среди провайдеров может привести к снижению уровня безопасности их инфраструктуры;
3) скопление большого количества важных данных на серверах одних и тех же провайдеров статистически повышает шансы на успех атак, так как в системе защиты становится меньше элементов, она становится более однородной,

[11] *Singer P. W., Friedman A.* Op. cit. P. 21.

[12] URL: http://www.consultant.ru/document/cons_doc_LAW_323815/ (дата обращения: 25.07.2020).

[13] *Taylor R. D.* “Data Localization”: The internet in the balance // Telecommunications Policy. Elsevier. 2020. Vol. 44. Is. 8.

а значит, менее устойчивой — злоумышленникам нужно априори прилагать меньше усилий для достижения своих целей.

Здесь необходимо вернуться к вопросам определения юрисдикции в Сети при расследовании последствий таких атак.

Под «юрисдикцией» понимаются полномочия конкретного государственного органа или его должностного лица; юрисдикционная деятельность — определенные действия по реализации данных полномочий конкретным субъектом в процессе рассмотрения и разрешения юридических конфликтов[14].

Полноценная реализация юрисдикции тем или иным государством включает в себя три аспекта:

— законодательную юрисдикцию, т.е. государство имеет законодательную власть над соответствующим деянием;
— судебную юрисдикцию, т.е. суды имеют право рассматривать данное дело;
— исполнительную юрисдикцию, т.е. государство обеспечивает соблюдение закона в данном деле[15].

Как подчеркивают зарубежные коллеги, у нас нет законов, механизмов, которые созданы специально для того, чтобы защищать граждан одного государства от того, чтобы они не стали жертвами граждан другой страны[16]. Таким образом, ситуацию с регулированием процесса расследования киберперступлений и юрисдикционных вопросов, связанных с ним, можно охарактеризовать как нормативный вакуум.

При создании действующих механизмов борьбы с киберперступностью очень большую роль играет положение на международной арене, репутация акторов.

У каждого государства есть два основных инструмента для заявления и отстаивания своей позиции в киберпространстве — это жесткая и мягкая сила. Мягкая сила предполагает непрямое влияние[17], позволяющее добиваться желаемого через добровольное участие, доверие, личную склонность, а не прямое принуждение, которое характерно для жесткой силы.

Так как IT и киберпространство очень нестабильны и подвижны, предсказывать их изменения и развитие, выносить долгосрочные директивные решения, характерные для жесткой силы, становится крайне сложно, хотя концепция локализации данных — это пример подхода именно с позиций жесткой силы, попытка формирования твердых границ и предписаний. Насколько эффективен такой подход, нам только предстоит оценить.

Однако нельзя полностью отказываться от идеи, что нормы, которые будут регулировать международные отношения по вопросам расследования киберпреступлений и юрисдикции, будут вытекать из двух вещей — сложившейся или складывающейся практики и гибких, открытых соглашений между государствами,

---

[14] Подробно см.: Уголовно-юрисдикционная деятельность в условиях цифровизации : монография / Н. А. Голованова , А. А. Гравина , О. А. Зайцев [и др.]. М. : Институт законодательства и сравнительного правоведения при Правительстве РФ ; Контракт, 2019.

[15] *Clough J.* Principles of Cybercrime. Cambridge, UK : Cambridge University Press, 2010. P. 404—405.

[16] *Balkin J. M.* Cybercrime: Digital Cops in a Networked Environment. Information Society Project (Yale Law School). New York : NYU Press. 2007. P. 209—210.

[17] *Ghappour A.* Searching Places Unknown : Law Enforcement Jurisdiction on the Dark Web // Stanford Law Abstract. April 2017. Vol. 69. P. 1112.

ведомствами, международными организациям и частным сектором, в основе которых будут лежать в первую очередь авторитет, экспертный уровень и доверие.

Исходя из вышеизложенного, на наш взгляд, в контексте борьбы с киберпреступностью и разрешения вопросов юрисдикции как на местах, так и на международном уровне необходимо осуществлять развитие по следующим направлениям:

1) дополнительной подготовки и переподготовки сотрудников правоохранительных органов, осуществляющих расследование киберпреступлений, на местах;
2) разработки научной и практической базы судебной компьютерно-технической экспертизы;
3) международной коммуникации и обмена в рамках обучения кадров и разработок практических методик проведения трансграничных следственных действий в ходе расследования киберпреступлений;
4) максимальной доступности информации об информационных технологиях и обучения работе с ними.

БИБЛИОГРАФИЯ

1. *Першин А. Н., Сидорова К. С.* Криминалистические основы установления пользователя информационно-телекоммуникационной сети Интернет // Вестник Университета имени О.Е. Кутафина (МГЮА). — 2019. — № 3 (55). — С. 82—94.
2. Уголовно-юрисдикционная деятельность в условиях цифровизации : монография / Н. А. Голованова , А. А. Гравина , О. А. Зайцев [и др.]. — М. : Институт законодательства и сравнительного правоведения при Правительстве РФ ; Контракт, 2019. — 212 с.
3. *Balkin J. M.* Cybercrime: Digital Cops in a Networked Environment. Information Society Project (Yale Law School). — New York : NYU Press, 2007. — 268 p.
4. *Broadhead S.* The contemporary cybercrime ecosystem: A multi-disciplinary overview of the state of affairs and developments // Computer Law & Security Abstract. — 2018. — Vol. 34. — P. 1180—1196.
5. *Clough J.* Principles of Cybercrime. — Cambridge, UK : Cambridge University Press, 2010. — 449 p.
6. *Dr. De Nardis L.* Five Destabilizing Trends in Internet Governance // A Journal of Law and Policy for the Information Society. — 2015. —Vol. 12. — P. 113—133.
7. *Ghappour A.* Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web // Stanford Law Abstract. — April 2017. — Vol. 69. — P. 1075—1136.
8. *Ribaux O., Souvignet T. R.* “Hello are you available?” Dealing with online frauds and the role of forensic science // Forensic Science International: Digital Investigation. — 2020. — Vol. 33. — P. 1—11.
9. *Singer P. W., Friedman A.* Cybersecurity and Cyberwar: What Everyone Needs to Know. — New York : Oxford University Press, 2014. — 312 p.
10. *Taylor R. D.* “Data Localization”: The internet in the balance // Telecommunications Policy. — Elsevier, 2020. —Vol. 44. Is. 8. — P. 1—15.
11. *Žolnerčíková V.* ICANN: Transformation of Approach towards Internet Governance // Masaryk University Journal of Law and Technology. — 2017. — Vol. 11. — P. 155—172.