

11. Текст Договору Рамбуїє [Електронний ресурс]. – Режим доступу: <http://www.un.org/russian/document/kosovo/99-648.pdf>
12. Текст “Конституційних рамок тимчасового самоуправління в Косово” [Електронний ресурс]. – Режим доступу: <http://www.unmikonline.org/constframework.htm>
13. Текст доповіді Спеціального посланника Генерального секретаря ООН по визначенню майбутнього статусу Косово [Електронний ресурс]. – Режим доступу: <http://www.unosek.org/docref/report-russian.pdf>
14. Borba za Kosovo se nastavlja. [Електронний ресурс]. – Режим доступу: – <http://www.kurir-info.rs/vesti/jeremic-borba-za-kosovo-se-nastavlja-43005.php>
15. Constitution of the Republic of Kosovo. [Електронний ресурс]. – Режим доступу: <http://www.kosovoconstitution.info/repository/docs/Constitution.of.the.Republic.of.Kosovo.pdf>
16. Ustav Republike Srbije. [Електронний ресурс]. – Режим доступу: http://www.sllistbeograd.rs/documents/ustav_republike_srbije_lat.pdf

УДК 32.019.5(477)

Г. Г. Четверик МІЖНАРОДНІ ВІДНОСИНИ ТА «ЕЛЕКТРОННИЙ СУВЕРЕНІТЕТ» УКРАЇНИ

Стаття присвячена дослідженню тенденцій використання мережі Інтернет та їх наслідків для державного суверенітету. Розкрито особливості врегульованості правових відносин в Інтернеті. Визначено основні проблеми які змушують шукати новий, кращий підхід до вироблення політики в сфері Інтернету та набір функцій і повноважень, який дозволяє державам здійснювати регулювання Інтернету.

Ключові слова: Інтернет, електронний суверенітет, мережеві спільноти, кіберпростір.

Статья посвящена исследованию тенденций использования сети Интернет и их последствий для государственного суверенитета. Раскрыты особенности урегулированности правовых отношений в Интернете. Определены основные проблемы, которые заставляют искать новый, лучший подход к выработке политики в сфере Интернета и набор функций и полномочий, который позволяет государствам осуществлять регулирование Интернета.

Ключевые слова: Интернет, электронный суверенитет, сетевые сообщества, киберпространство.

To research trends of the Internet and its implications for national sovereignty. The features of adjustment of law relationships online are describes. Define the main problems are forced to seek a new and better approach to policy-making in the field of Internet and set of functions and powers, which allows states to regulate the Internet.

Keywords: Internet, electronic sovereignty, network community, cyberspace.

Заява Президента Казахстану Нурсултана Назарбаєва 15 червня 2011 року про необхідність впровадження поняття «електронний суверенітет» була не тільки наслідком побоювань авторитарного лідера за свою владу в світлі подій на арабському Сході, але й наслідком тривалих дискусій фахівців на цю тему. Розмови про «інформаційний» чи «цифровий» суверенітет піднімаються давно і можна очікувати подальшої їх інтенсифікації, оскільки відкритим залишається питання про можливість й межі контролю в Інтернеті та його вплив на суверенітет держави.

Прагнення держав узяти Інтернет під свій контроль є цілком зрозумілим, оскільки між технічно безмежним Інтернетом і обмеженими націями виникла динамічна напруга, коли важливо не стільки відокремити свої території, скільки визначитися з природою та статусом загальних та все більш транскордонних взаємодій в середовищі Інтернет. Стикається з цим завданням і Україна, тому особливої актуальності набуває розгляд питання про статус «електронного суверенітету» України та його вплив на міжнародні відносини і зовнішню політику України. Тому метою даного дослідження є визначення зв'язку між «електронним суверенітетом» України та її діями в системі міжнародних відносин.

Основна частина. Інтернет залишається фактично поза сферою правового та політичного регулювання всередині націй-держав. У світовій політиці складається ситуація, коли майже всі

країни зацікавлені в розвитку інтернет-простору, однак при цьому хотіли б розповсюдити свою юрисдикцію на його територію. Правові відносини в Інтернеті зачіпають проблеми: юрисдикції відносин між користувачами; відповідальності контент-провайдерів; саморегулювання стандартів і протоколів. Загальносвітова практика правового регулювання Інтернету зводиться на сьогодні до низки суперечливих судових рішень, що визначають державну юрисдикцію. Це пов'язано з тим, що для нього відсутні так звані колізійні норми (наприклад, *lex patrie* - закон громадянства, *lex loci actus* - закон місця укладання угоди і т.д.). Шляхи врегулювання статусу Інтернету розташовані в сферах укладення багатосторонніх угод, прийняття міжнародних договорів і поступової уніфікації національних законодавств з даного питання. Такому процесу перешкоджають насамперед неоднакові політичні режими країн субконтиненту і, відповідно, відмінності в підходах до регулювання Інтернету. Режим контролю над провайдерами контенту і доступу в нього - в діапазоні від практично тотального (Саудівська Аравія, Північна Корея, Ірак, Лівія) до обмеженого втручання у відносини всередині мережі та надання імунітету провайдеру за дії своїх користувачів (США).

Розвиток кібер-простору дистанціює його мешканців від місцевого контролю та матеріальних атрибутів громадянства, суверенітету та державності. Це викликає потребу у регуляторних рішеннях, що виходять за межі старих парадигм, та популярність таких функцій як самоорганізація та соціальна взаємодія, аніж інституційна влада» [1, с.5].

Все це обумовлює необхідність осмислення сучасних глобальних інформаційно-комунікаційних відносин та вирішення актуальних питань їх регулювання за допомогою як правових, так і інших технічних, технологічних, організаційних, саморегулятивних інструментів тощо.

Наявний комплекс питань, викликаних появою та розвитком Інтернет, що потребує вирішення міжнародною спільнотою за допомогою міжнародно-правового регулювання, на нашу думку, можна умовно розділити на дві групи. До першої – належать політико-правові аспекти регулювання функціонування та розвитку інфраструктури Інтернету як глобальної інформаційно-комунікаційної мережі. До другої – спеціальні правові питання, що можна охарактеризувати як цивілізаційні «виклики», що привніс Інтернет по відношенню до вже традиційних комунікаційних та медіа засобів, таких як пошта, телефонний зв'язок і телебачення. Останнє пов'язано, насамперед, з дигіталізацією пристроїв та конвергенцією технологій, що викликає потребу перегляду вже існуючих міжнародно-правових актів з метою приведення їх у відповідність до вимог часу. Питаннях, що виникають у зв'язку із функціонуванням та розвитком інфраструктури Інтернету пов'язані, в першу чергу з організаційно-правовими засадами управління Інтернетом.

У чому полягає актуальність цієї теми, які проблеми в управлінні Інтернет на сьогоднішній день потребують вирішення за допомогою міжнародно-правових інструментів, які шляхи та моделі для цього можуть бути обрані?

Як національне регулювання, так і міжнародні процеси явно наштовхнулись на операційні та законодавчі обмеження у взаємопов'язаному та незалежному світі, із 190 країнами дуже різного розміру, впливу, рівнем демократизації та стабільності. До числа головних викликів які змушують шукати новий, кращий підхід до вироблення політики в сфері Інтернету належать:

1. Складні політичні проблеми. Декілька авторів продемонстрували помилковість ідеї, що Інтернет зможе взагалі уникнути будь-якої регуляції. Немає необхідності розробляти: численні національні закони, які прямо або опосередковано впливають на людську діяльність в Інтернеті, незалежно від того, подобається нам це чи ні. Більш того, більшість проблем державної політики, які стосуються Інтернету, не є новими, як, наприклад: свобода висловлення, захист конфіденційності та персональної інформації, протидія злочинності усіх видів, прийнятні правила для інтелектуальної творчості або навіть оподаткування, якщо обмежитись лише декількома.

Подібні до тих, з якими стикаються в національних врегулюваннях, ці проблеми можуть, тим не менш, враховуючи масштаб (по своїй сутності глобальної транскордонної мережі), швидкість (оскільки ми рухаємось в режимі реального часу) та кількість і різноманітність задіяних дійових осіб, все ж таки спричинити якісний зсув в складності вирішення проблем. Більш того, щільні взаємозв'язки викликають сильні нелінійні ефекти, які складно передбачити, не кажучи вже про усунення наслідків, традиційними засобами. Ініціатива «День спалювання Корану» поодинокого пастора із Флориди за лічені години викликала демонстрації в Пакистані, наслідком яких стало кілька смертей. Проблеми традиційної політики отримали несподіване завихрення через Інтернет.

2. Взаємозв'язок. Головна трансформація, запущена Інтернетом – це мультиплікація людських груп транснаціонального або навіть глобального масштабу. В економічному

просторі, Інтернет запусив та полеглив глобалізацію. В результаті виникли компанії з об'ємами більшими, ніж національні ВВП, із своїми транснаціональними мережами працівників, клієнтів та постачальників. Навіть наймолодші мережеві старт-апи негайно здобувають міжнародну аудиторію, а платформи соціальних медіа збирають сотні мільйонів користувачів. Більшість людських мереж також отримала можливість долати кордони: родини, асоціації, неурядові організації, діаспори зараз можуть бути глобально пов'язаними, більше і більше в режимі реального часу завдяки майже універсальному поширенню мобільних телефонів.

Такі мережі не заміщують традиційних дійових осіб, якими є держави. Вони просто зросли і досягли порівняних, або навіть більших, масштабів. Такий взаємозв'язок, можливо, досяг межі, роблячи з людства складне суспільство, а не просто зіставлення окремих національних суспільств з обмеженими взаємодіями. Це не означає, звичайно, що кожен може бути пов'язаний з кожним: тим не менш щільність зв'язків кардинально зросла. Як кажуть в теорії складних динамічних систем: збільшене є іншим. Глобальне суспільство є мішаниною численних суспільств, що перетинаються між собою, і прагнуть взяти участь в глобальній дискусії стосовно простору, який вони розділяють.

3. Різноманітність партнерських груп. Більшість державних дійових осіб розглядає появу транскордонних корпорацій або мереж громадянського суспільства як виклик їхній власній владі. Тим не менш громадяни, як користувачі, постачальники або клієнти, мають свій особистий інтерес в питаннях, яким їхні власні уряди не надають першочергового значення або взагалі опонують, і через це вони покладаються на недержавні організації, аби забезпечити, що їх погляди будуть враховані в ході міжнародних дискусій. До того ж, національні процеси ухвалення рішень, навіть найдемократичніші, мають природним результатом зведення різноманітності точок зору до єдиної позиції, що означає практичну неможливість підходу, який відстоює меншість, бути винесеним на міжнародне міжурядове обговорення.

Індивідууми все ще хочуть, аби їх уряди представляли їх інтереси як громадян національного суспільства. Але зараз вони мають інші більш диверсифіковані інтереси в еволюції Інтернету, його екосистеми та правил, які до нього застосовуються. Для все більшої кількості людей громадянство є однією серед кількох інших можливостей відстояти свої інтереси. Вони прагнуть, аби різноманітність їхніх інтересів та турбот була повністю взята до уваги в процесі визначення глобального інтересу, який не є лише агрегацією національних громадянських інтересів.

4. Конфлікти юрисдикцій. Національні законодавства залишаються ключовим інструментом розробки політики. Тим не менш, некоординоване накопичення потенційно несумісних національних норм – стосовно, наприклад, конфіденційності або свободи вираження – генерує конфлікти юрисдикцій. Для глобальних платформ дуже важко поважати цю різноманітність правил. Більше того, діяльність індивідуумів, яку вони здійснюють через Інтернет, часто має транскордонний характер, що привносить особливі складності стосовно правозастосування. Нарешті, національні рішення однієї держави можуть мати прямий або опосередкований ефект на території іншої. Якщо суверенітет – це здатність здійснювати вищу владу на території, то Інтернет є прямим викликом територіальності законодавства, яка є одним з ключових компонентів вестфальської моделі.

5. «Фракталізація» суверенітету. Ще більш важливо, що виникнення великих платформ соціальних медіа дає несподіваний ефект їхнім користувачам, беззастережно до їх фізичної локалізації, а саме можливість підпадати під дію «Умов користування» (ToS - Terms of Service), які встановлюють юрисдикцію країни інкорпорації компанії, або, в найкращому випадку, локалізації її дата-центру. Цей феномен веде до «фракталізації» суверенітету, коли юрисдикція та правові засади країни стають де-факто застосованими до громадян іншої країни, розширюючи межі першої та звужуючи, по відношенню до суверенних повноважень, межі останньої.

6. Цифрові території. В популярній пресі є поширеним софізм, що, якби Facebook був би країною, він посів би третє місце в світі за розміром. Порівняння неприйнятне: для того, аби стати країною, треба набагато більше, аніж просто колективність користувачів, навіть дуже велика. Тим не менш, до тих пір, поки вони залишаються в цій мережі, більш ніж 600 мільйонів користувачів Facebook передусім підкоряються «Умовам користування» стосовно, наприклад, свободи вираження або захисту конфіденційності. Така структура відображає загальну тенденцію, за якою все більша кількість людей все більше часу проводить у транскордонних взаємодіях.

Не надто далеко заходячи в своїх міркуваннях, ми можемо стати свідками виникнення «цифрових територій», що є ознакою розвитку нової географії кіберпростору, потенційно побудованої навколо спільнот платформ соціальних медіа. Такі платформи, в намаганнях знайти спільні правила співіснування мільйонів своїх користувачів, грають де-факто роль розробників політики. Втім, ця роль, яка виконується під суворим корпоративним керівництвом, повністю

поважає демократичний принцип, який вимагає залучення тих, ким вона керує. Конфлікт між цією новою віртуальною географією та фізичними кордонами, які потребували століть для свого установа, в найближчі роки буде, схоже, тільки наростати.

7. Конкуренція з міжнародними інституціями. Якщо національні законодавства зустрічаються з головними викликами в транскордонному Інтернеті, то, можливо, міжнародні угоди дадуть належне рішення? Теоретично, так. Декілька корисних інструментів були розроблені в намаганнях вирішити основні проблеми. Добрим прикладом є Будапештська конвенція з кіберзлочинності, завдяки якій вдалося значно підвищити усвідомлення необхідності більш тісної кооперації, та ініціювати деяку гармонізацію між національними законодавствами, а також встановити чіткі правила для правозастосування. Тим не менш, справа не тільки в тому, що створення таких інструментів триває надзвичайно довго, а ще й в тому, що вони дуже рідко є універсальними, адже зазвичай ініціюються спеціалізованими або регіональними агенціями. І, оскільки Інтернет зростає, все більше і більше організацій починають конкурувати між собою за лідерство, у відповідності до своїх власних мандатів, відтворюючи на глобальному рівні неузгодженість і потенційну несумісність, яка існує між різними національними законами.

Поширення Інтернету, через 30 років після його створення, тепер істотно впливає на сферу, де він був утворений. Принципи мережевої організації, пірінгових взаємодій, абсолютизація ролі інформації в інфраструктурі держави - всі ці фактори призвели до початку справжньої революції у міжнародних відносинах. У відповідних концепціях держав з'являється поняття інформаційної війни, різні визначення інформаційної зброї. Єдиної, або скільки-загальнозвживаної, класифікації інформаційної зброї не існує. Важливо розуміти, що об'єктом впливу в інформаційній війні, і взагалі у війні нового типу, є не тільки військова інфраструктура супротивника, але і його загальна інфраструктура управління країною, її населення. Чим більше розвинена країна, тим вразливіші її інфраструктура. Загрози для неї здатні виходити звідусіль, у т.ч. від індивідів, терористичних угруповань і т.д. Якщо військові системи управління зазвичай досить добре захищені і не мають гейтів, що зв'язують їх з Інтернетом, то системи управління рухом, енергетичні та комунальні структури очевидно підлягають таким загрозам.

Однак в останні роки більшість країн сприймають і реагують на виклик Інтернету на державному рівні. Можна виділити наступні типи реакцій на появу глобального інформаційного середовища: відторгнення, прийняття, ухвалення з обмеженнями, використання, ставка на розвиток. Основне завдання, що стоїть перед розвиненими націями-державами, які беруть активну участь у світовій політичній системі і роблять ставку на розвиток Інтернету, - адекватний перехід на інтернет-якість державних і громадських структур, конвергенція держави і суспільства на основі інформаційних технологій. Вектор вербалізований інтелектуалами, просувається бізнесом і верифікований урядами. «Клас» (поки в лапках) інтернет-користувачів вимагає нововведень і наближення стандартів офлайн до можливостей онлайн. Цей «клас» - основна рушійна сила, імовірно, нового революційного процесу, а так як його представники апріорі є багатшими, мобільнішими і впливовішими тих, хто працює в офлайні, то вони з великим успіхом впливають на процеси прийняття рішень, що стосуються створення інтернет-держав і т.д. Чим більше впливу, тим більше людей включаються в їх «клас» і стають носієм його ідеології, тим більше їх сукупний вплив на світ.

Дослідження зазначеної проблематики оптимальним чином може бути вирішене за допомогою порівняльного методу, який дозволить визначити особливості позицій кожної з зацікавлених сторін і на цій основі виявити позицію оптимальну для України, з врахуванням її національних інтересів.

При реалізації низки сценаріїв світового політичного розвитку Інтернет здатний розпастися на безліч національних та інших зон, вхід і вихід з яких буде контролюватися урядами та іншими суб'єктами світової політики. Уже сьогодні тут функціонує кілька альтернативних зон, підтримуваних великими інтернет-провайдером. Крім того, в Інтернеті є багато так званих темних і «сутінкових» чи «присмеркових» зон [2, с.74]. «Темні зони» невидимі для більшості користувачів; при цьому їх кількість становить близько 5% від загальної їх чисельності. У таких зонах розташовані переважно сайти військових відомств США, що використовують створену в роки холодної війни адресну систему Milnet. «Сутінкові зони» Інтернету вважаються покинутими і використовуються хакерськими групами для організації DOS - атак. Архітектура Інтернету створювалася в умовах, коли всередині мережі існувала довіра до дій окремих учасників. В результаті Інтернет що розрісся несе на собі відбиток «дитинства» і майже не містить вбудовані механізми безпеки. Якщо учасник мережі (роутер) заявляє, що він володіє блоком адресного простору, інша частина Інтернету вірить йому на слово і адресує до нього весь відповідний трафік. Значить, можна створити будь-який мережний блок і запустити його в Інтернет, надавши анонімність будь-якій атаці. «Сутінкові зони», поряд з технологіями підміни

авторства («спуфінга») кардинально змінюють способи ведення війни в інтернет-просторі.

Системи пошукових механізмів (англ. search engines) і механізмів вилучення контенту (data mining). За оцінками аналітиків, сьогодні найбільші пошукові системи (Google, Fast, Northern Light, Yahoo) сукупно індексують не більше 45% від загальної кількості сторінок, розміщених в Інтернеті. Найбільш популярна і релевантна пошукова система (з механізмом ранжирування індексованих сторінок на основі уподобань користувачів) - Google. Технологія Google заснована на обліку думки самих користувачів про веб-ресурсах. Існує думка, що Google є прообразом «держави майбутнього», що не потребує традиційних засобів примусу. Дійсно, з пошуковими системами безпосередньо пов'язане питання про механізми і суть влади в інтернеті. Якщо представництва тієї чи іншої організації тут не «обраховані» Спайдер-пошуковою системою, то для абсолютної більшості користувачів Інтернету ця організація не існує. Така ситуація створює в мережі механізми придушення і контролю окремих акторів, отже, допускає можливість появи «онлайнного» варіанту держави. В інтернеті діють зовсім інші актори, ніж у звичайному світі, і сукупна міць окремої нації-держави, переломлена в кіберпросторі, значно поступається можливостям компанії Google або громадського «онлайнного» співтовариства, наприклад, пов'язаного з антиглобалістським рухом. Виняток, що підтверджує правило, - США, яким доступний інституціональний контроль над Інтернетом, і сама уразлива частина мережі - інфраструктура. Втім існує безліч дрібних, в порівнянні з гігантами типу Google, пошукових механізмів і засобів індексації, які представляють, в тому числі, закриті корпоративні інформаційні системи та альтернативні пірінгові спільноти, типу Гнутелли (Gnutella), Морфеус (Morpheus) або Kazaa. Пошукові системи іноді використовуються для доступу до інформації, яка блокується національними урядами. Відома практика закриття доступу до певних сайтів урядом Китаю, який так бореться з опозицією комуністичному режиму країни. Google кешує (зберігає копії) індексовані сторінки, що дозволяє китайським опозиціонерам отримувати доступ до сайтів, які в КНР заборонені. Блокувати підходи до самого Google значно складніше, бо є безліч шляхів доступу, в тому числі з використанням пірінгових технологій, що розробляються хакерськими групами (Pick-A-Booty).

Висновки. До числа головних викликів які змушують шукати новий, кращий підхід до вироблення політики в сфері Інтернету належать:

1. Проблеми регулятивності Інтернету.
2. Мультиплікація людських груп транснаціонального або навіть глобального масштабу.
3. Різноманітність партнерських груп.
4. Конфлікти юрисдикцій.
5. «Фракталізація» суверенітету.
6. Цифрові території.
7. Конкуренція з міжнародними інституціями.

Набір функцій і повноважень, який дозволяє говорити про регулювання Інтернету включає: а) глобальне технічне управління ключовими ресурсами Інтернету: доменними іменами, IP-адресами, Інтернет-протоколом і системою корневих серверів; б) доступ до контенту і його обмеження. Для України доступним є виключно другий варіант регулювання.

Поняття «електронного суверенітету» включає в себе: власну операційна система, пошукові й інформаційні системи, антивірусну систему, систему шифрування, корневий домен, свій процесор, власна система геопозиціонування. На даний момент єдиною країною яка володіє повноцінним «електронним чи цифровим суверенітетом» є США. Для України найбільш актуальним можна вважати розвиток власної пошукової системи.

Бібліографічні посилання:

1. Alexander J. C. Core Solidarity, Ethnic Out-Groups, and So-cial Differentiation / In: Differentiation Theory and Social Change. Comparative and Historical Perspective. Ed. by Jeffrey C. Alexander and Paul Colomy. – New York: Columbia University Press, 1990. – P. 268 -272.
2. Натсак О. «Технополитика» Интернета / Органа Натсак // Международные процессы. - 2008. - Том 6. – № 1. - С. 71-75.